Privátne adresy a NAT (Network Address Translation) pre IPv4

M5, CCNA4, v5
Pavel Segeč
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Problém ...

- Vďaka flexibilnosti IP technológie nárast používania → každé IP zariadenie musí mať IP adresu
- Verejný adresný priestor
  - Problém → riadený a prideľovaný
    - V Európe prideľuje RIPE (Réseaux IP Européens)
    - Zákazník prenajíma od ISP

Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE NCC
- APNIC
- LACNIC
- AfriNIC

  - Problém → Nedostatok prideliteľných verejných IP adries

Problém a riešenie

- Potreba nových metód riadenia adresných rozsahov v snahe riešenia adresnej krízy

= **Network Address Translation** (NAT)

- Princíp:
  - Vo vnútri siete použitie neriadeného privátneho adresného priestoru na adresáciu IP zariadení
  - Pri prechode paketu cez okraj do verejného Internetu → preklad zdrojovej privátnej IP do verejného adresného IP priestoru
    - NAT musí byť stavový, kde si vedie zoznam prebiehajúcich komunikácií a použitých mapovaní
  - Avšak stále je potrebný verejný IP adresný priestor
    - minimálne jedna adresa

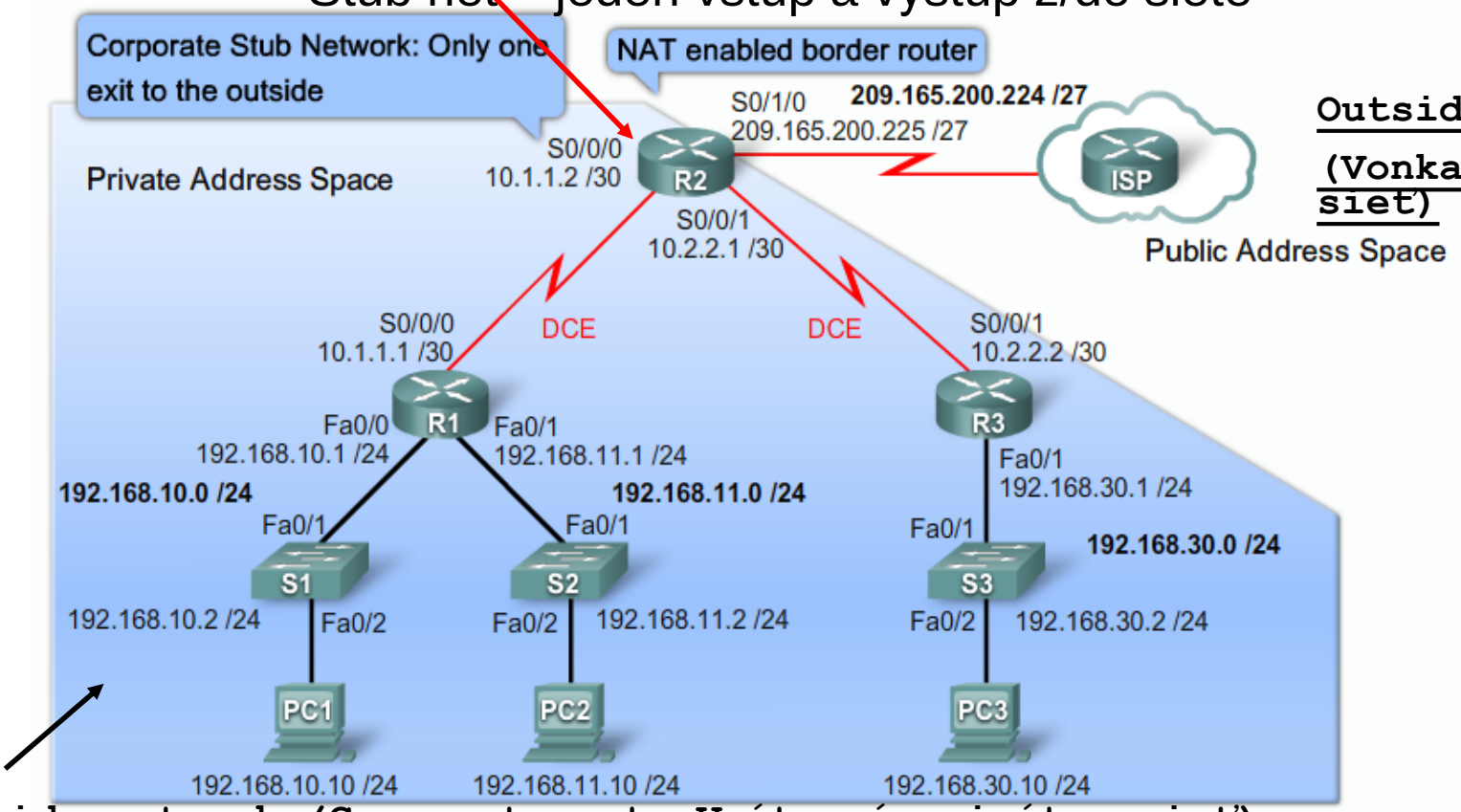
Vyčlenené privátne adresy pre NAT

- **Privátne IP adresy**
  - Vyčlenené podľa RFC 1918
  - Môže použiť hocikto
    - Neriadený priestor
  - Routre nesmú smerovať vo verejnej IP sieti privátne adresy z dôvodu nedodržania jedinečnosti identifikácie (adresovania) IP uzla
    - ACL, Route policy a pod.

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0 / 8
B	172.16.0.0 - 172.31.255.255	172.16.0.0 /12
C	192.168.0.0 - 192.168.255.255	192.168.0.0 /16

NAT zariadenie

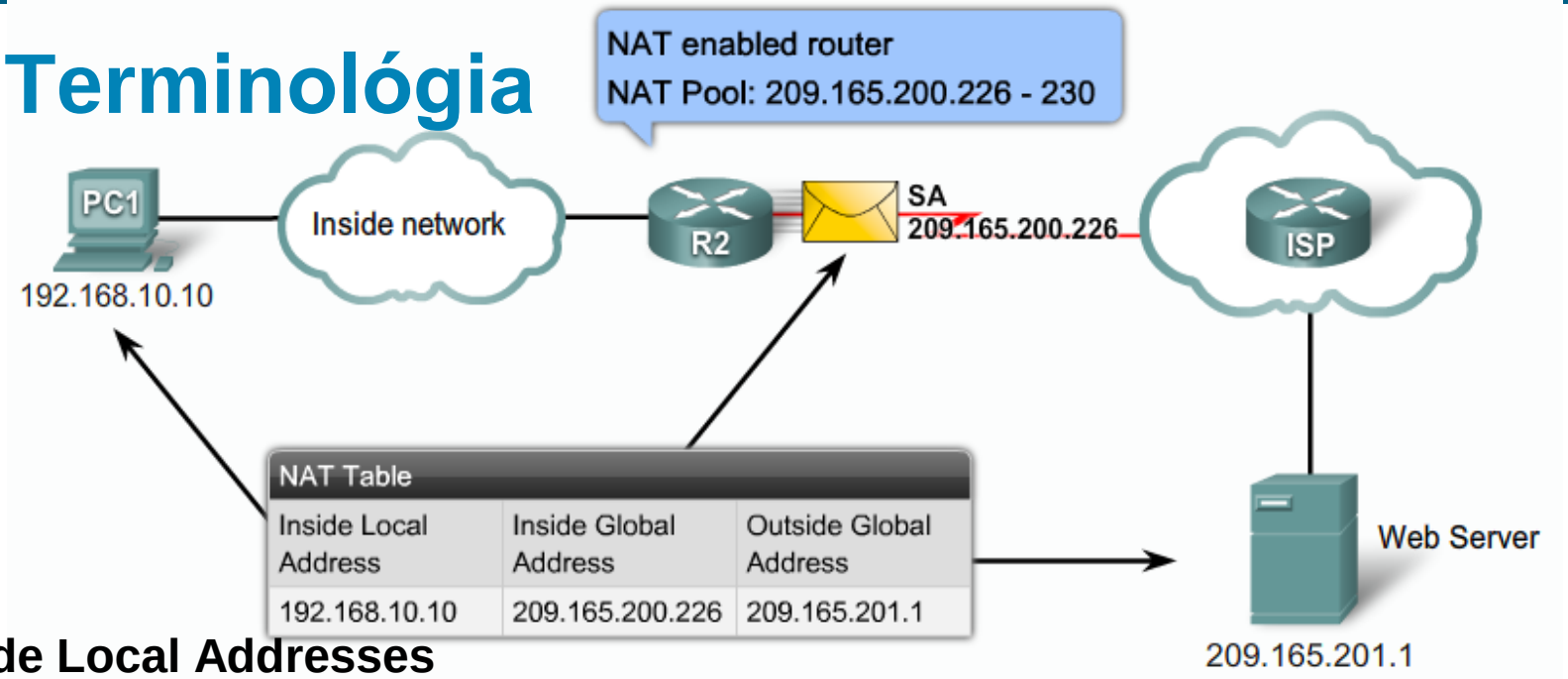
- Border gateway router
- Pracuje typicky na hranici tzv. stub siete
  - Stub net = jeden vstup a výstup z/do siete



Inside network (Corporate net; Vnútorná privátna sieť):

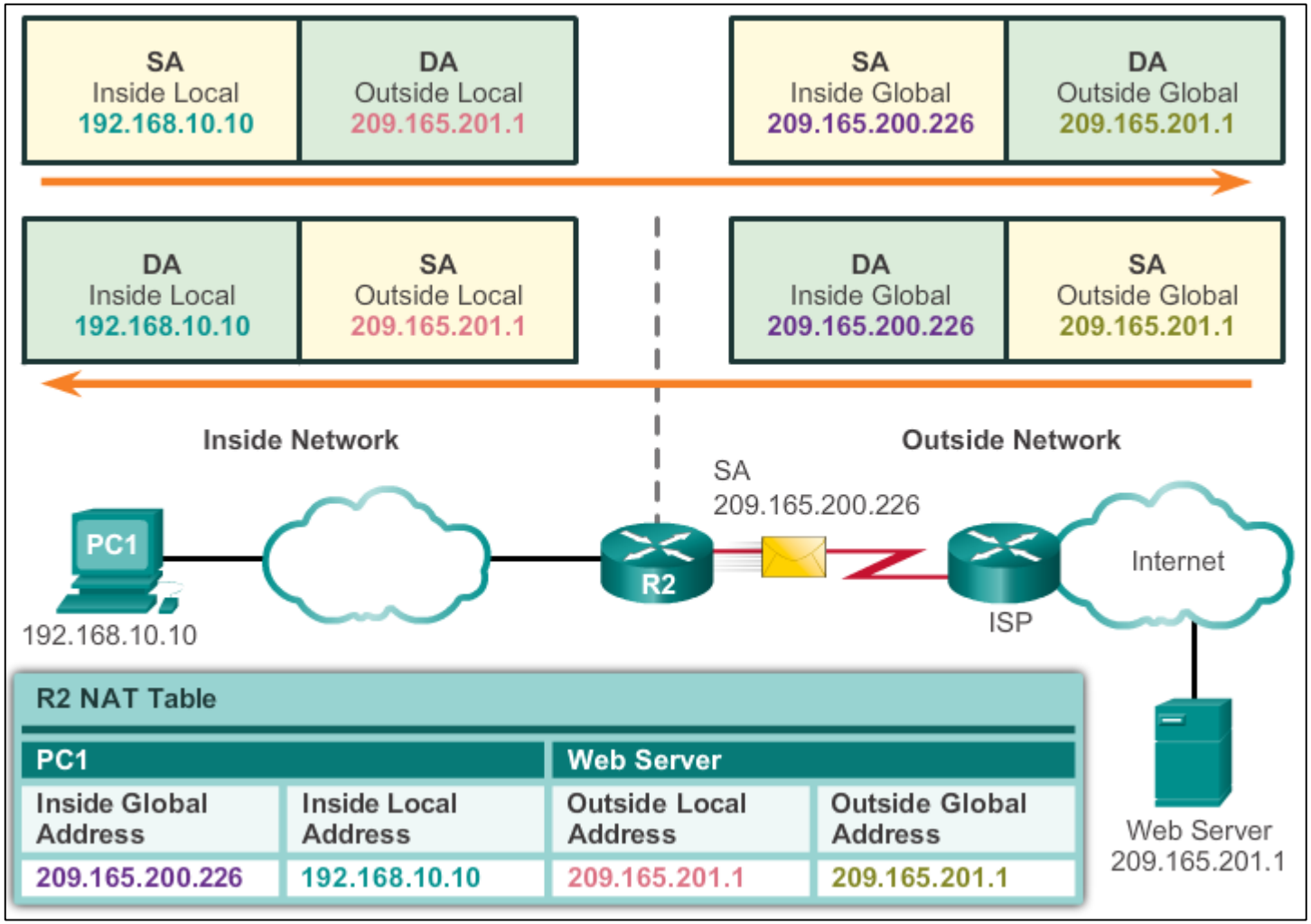
- **Používa privátne adresovanie**
- **Pri komunikácii mimo cez BG je objektom prekladu (NAT-ovania)**
- **Pri vnútornej komunikácii sa IP adresy neprekladajú**

NAT Terminológia



- **Inside Local Addresses**
  - IP adresa pridelená IP zariadeniu vo vnútri siete. Adresa je typicky privátna podľa RFC 1918.
- **Inside Global Address**
  - Platná verejná IP adresa, pridelená ISP.
  - Na túto adresu bude prekladaná privátna zdrojová adresa v odchodzom pakete ak ten opúšťa vnútornú sieť cez NAT.
- **Outside Global Address**
  - Platná verejná IP adresa, pridelená koncovému IP zariadeniu tak ako to vidí odosielateľ z vnútornej siete.
- **Outside Local Address**
  - Lokálna IP adresa pridelená zariadeniu vo vonkajšej sieti. Typicky ak táto sieť nepoužíva tiež NAT je zhodná z Outside Global Address.

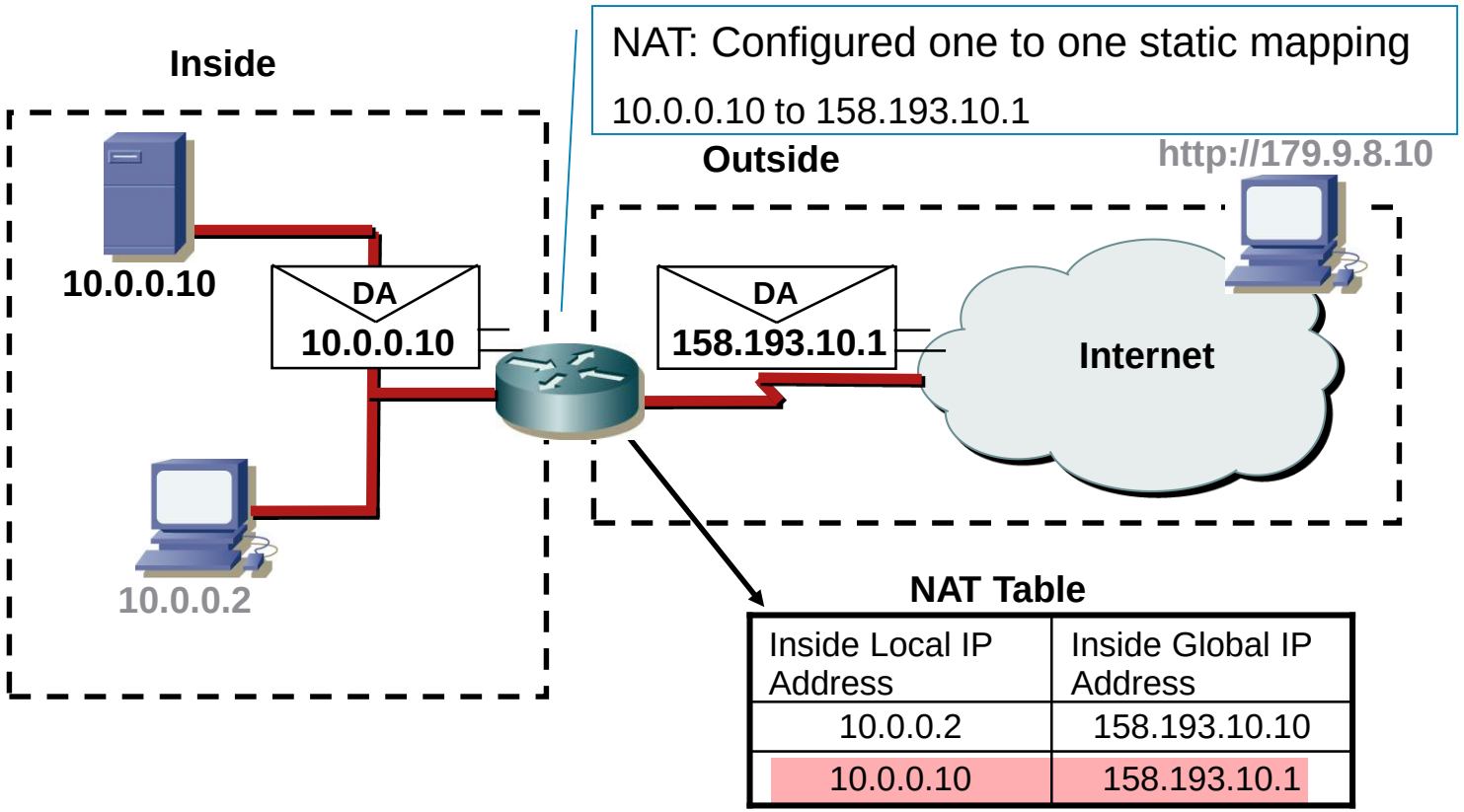
NAT proces


SA
Inside Local
192.168.10.10
DA
Outside Local
209.165.201.1
SA
Inside Global
209.165.200.226
DA
Outside Global
209.165.201.1
DA
Inside Local
192.168.10.10
SA
Outside Local
209.165.201.1
DA
Inside Global
209.165.200.226
SA
Outside Global
209.165.201.1
Inside Network
Outside Network
SA
209.165.200.226
PC1
192.168.10.10
R2
ISP
Internet
Web Server
209.165.201.1
R2 NAT Table
PC1
Web Server
Inside Global Address
Inside Local Address
Outside Local Address
Outside Global Address
209.165.200.226
192.168.10.10
209.165.201.1
209.165.201.1

NAT mapovanie

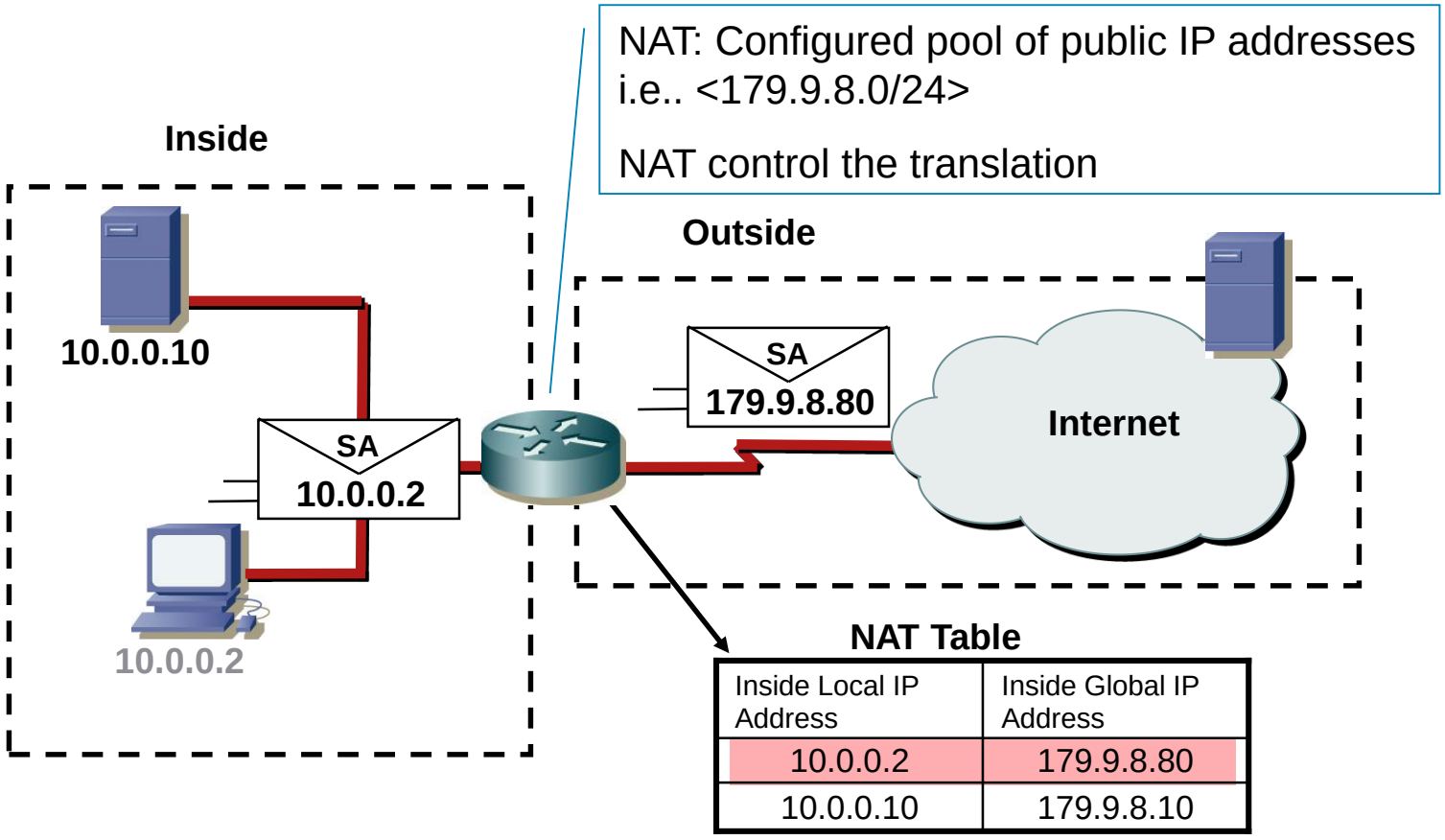
- **Statické mapovanie**
  - Tzv. „one-to-one mapping“
  - Spárovanie prekladu jednej privátnej adresy (inside local) na jednu verejnú adresu (inside global)
  - Výhodné, priam potrebné ak potrebujem zabezpečiť prístup na stanicu (napr. HTTP server) za NAT z Internetu
- **Dynamické mapovanie**
  - NAT má dostupný rozsah verejných adries
    - Tzv. IP address pool
  - NAT riadi preklad prideľovaním neobsadených verejných IP adries z rozsahu podľa príchodzích požiadaviek z vnútra siete

Statické NAT – princíp činnosti



Mapovanie platí pre oba smery prenosu
in => out
out => in

Dynamické NAT – princíp činnosti

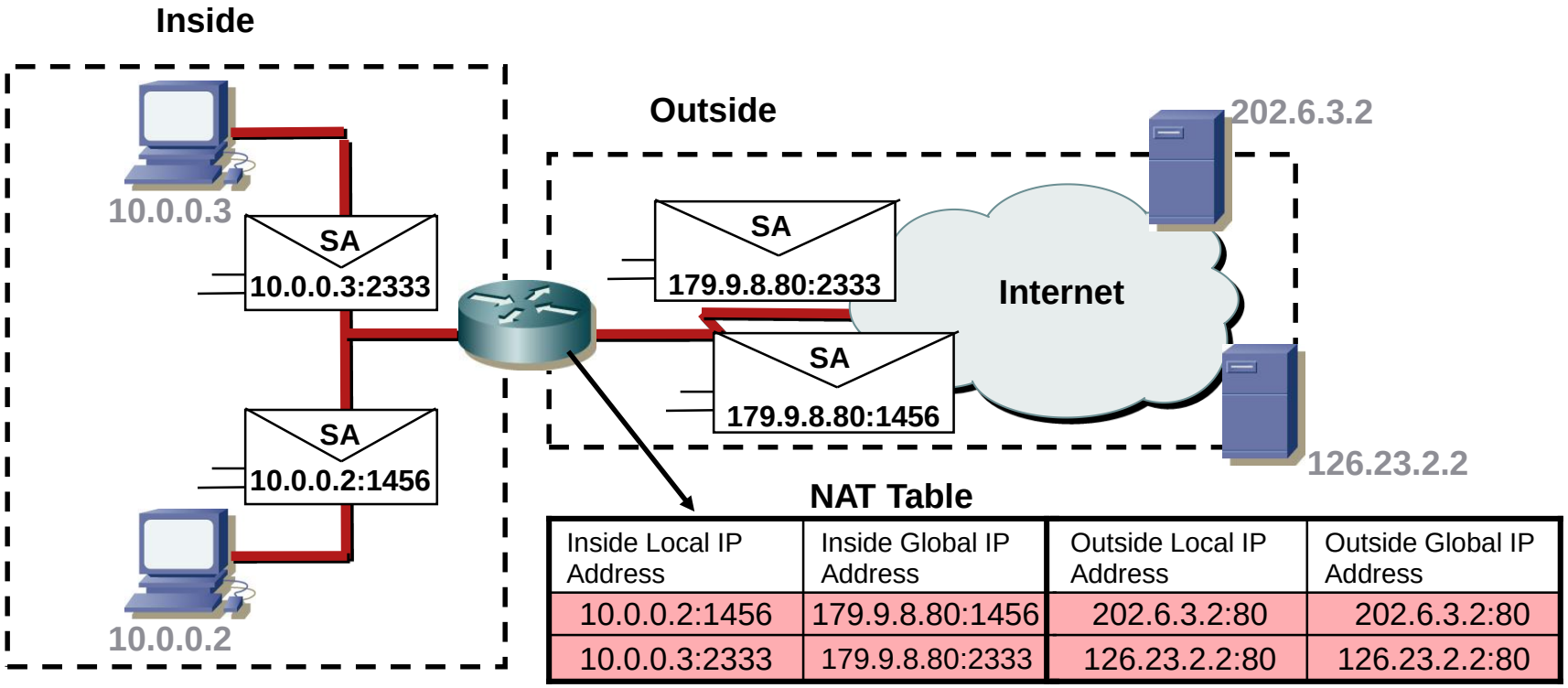


PAT (Protocol Address Translation)

- **Tzv. NAT overloading**
- Použitý ak:
  - Mám pridelenú len jednu verejnú adresu na WAN rozhraní routra (typické pri malých zákazníkoch)
    - PAT mapuje viaceré IP adresy na jednu verejnú IP adresu, kde sa prebiehajúce komunikácie rozlišujú číslom portu (16 bit)
- Alebo
  - Mám pridelený verejný adresný rozsah, kde počet verejných adries je menší ako počet IP zariadení, ktoré používam za NAT
    - Mapujem viaceré privátne IP adresy na viaceré verejné, ale musím rozlišovať komunikácie portom
- PAT sa typicky snaží zachovať pôvodný zdrojový port
  - Ak je port použitý, PAT použije prvý voľný port

PAT vlastnosti

- PAT používa jedinečné zdrojové čísla portov spolu s inside global adresou za účelom rozlíšenia NAT prekladu



NAT Table

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
10.0.0.2:1456	179.9.8.80:1456	202.6.3.2:80	202.6.3.2:80
10.0.0.3:2333	179.9.8.80:2333	126.23.2.2:80	126.23.2.2:80

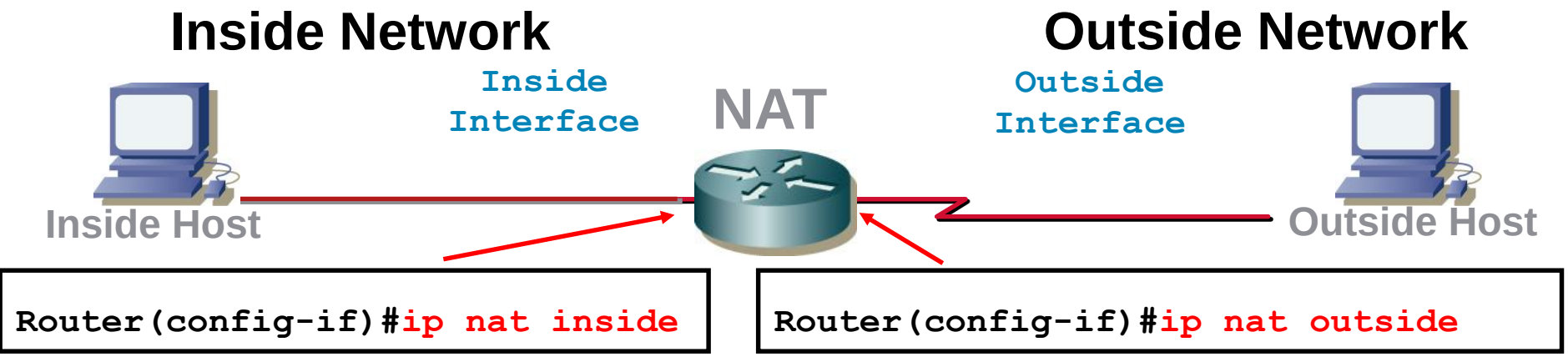
Výhody NAT/PAT

- Nasadenie na Stub Net – zvyšovanie flexibilty
  - Eliminuje potrebu preadresovania IP zariadení ak sa zmení provider a tým aj adresný priestor
    - Šetrenie času a peňazí
- Šetrí adresný priestor, potrebujem menej verejných IP adries
  - PAT overloading
- Zvyšuje bezpečnosť siete
  - Ak NAT nie je otvorené, nepustí komunikáciu z von dnu

Konfigurácia

Konfigurácia NAT/PAT

Zadefinovanie Inside/Outside rozhraní



- Pri NAT sa definujú vždy!!!!
- Rozhranie border routra pri NAT môže byť
  - Inside (vnútorné s privátnou adresáciou)
  - alebo Outside (s verejnou adresáciou)
- NAT preklad nastáva:
  - Len pri prechode paketu z inside na outside a naopak
  - Nikdy medzi rozhraniami toho istého typu, alebo nezadefinovanými

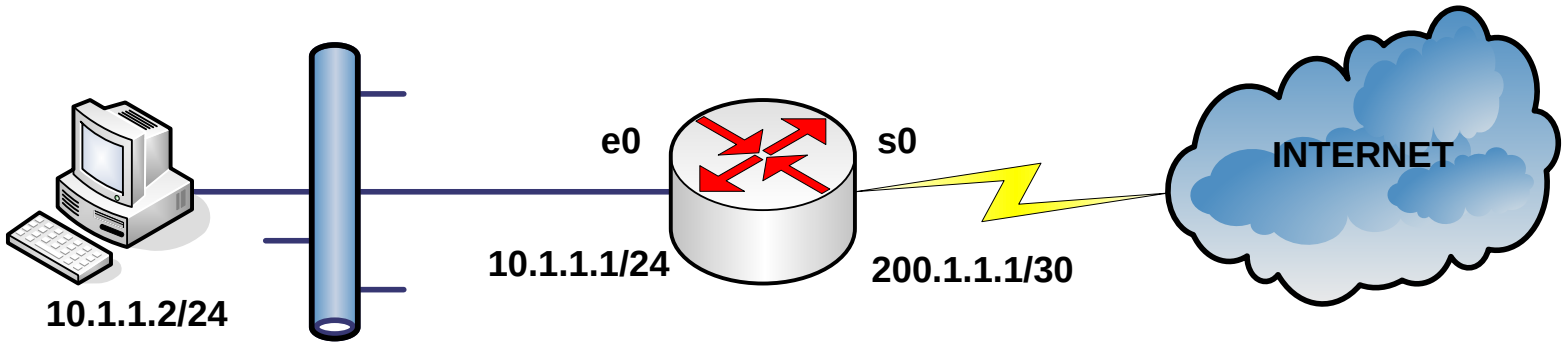
Konfigurácia statického NAT prekladu

- Príkazom zadám priamo do konfiguráku mapovanie, ktoré ostáva permanentne uložené v mapovacej prekladovej tabuľke NAT-u
  - Aj po reštarte, za predpokladu copy run start

```
Router(config)# ip nat inside source static INSIDE_LOCAL INSIDE_GLOBAL
```

Konfigurácia NAT/PAT

Konfigurácia statického NAT




```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#ip nat inside source static 10.1.1.2 200.1.1.1
```

Konfigurácia dynamického NAT prekladu

- Pozostáva z:
  - Definovanie Inside/outside rohraní
  - Definovanie rozsahu verejných adries (tzv. NAT pool), z ktorých bude pri preklade vyberané

```
Router(config)#ip nat pool MENO_POOLU START-IP END-IP netmask MASKA
```

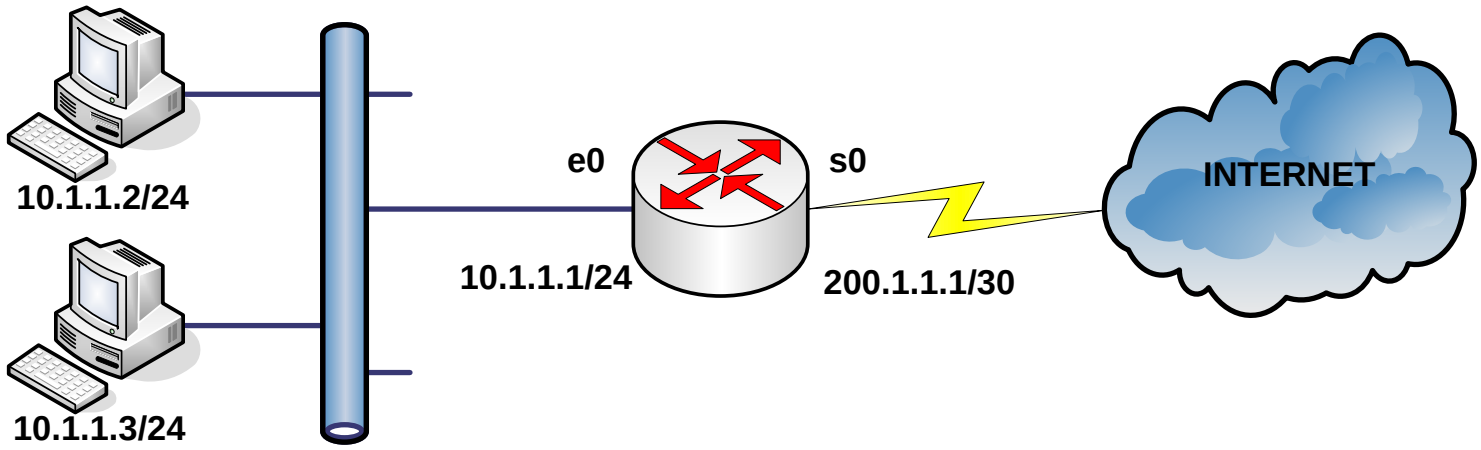
  - Zadefinovania IP adries cez ACL, pre ktoré NAT bude vykonávať preklad

```
Router(config)#access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

  - Spojenie ACL a daného pool-u do funkčného dynamického NAT

```
Router(config)#ip nat inside source list CISLO-ACL-LISTU pool MENO-POOLU
```

Konfigurácia dynamického NAT




```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#ip nat pool MOJ_ROZSAH 211.2.2.8 211.2.2.10 netmask 255.255.255.252
Gw(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Gw(config)#ip nat inside source list 1 pool MOJ_ROZSAH
```

Overenie konfigurácie NAT

```
Gw# sh run | include nat
 ...
!
interface Ethernet0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
...
!
interface Serial0
 ip address 200.1.1.1 255.255.255.252
 ip nat outside
...
!
ip nat pool MOJ_ROZSAH 211.2.2.8 211.2.2.10 netmask 255.255.255.252
ip nat inside source list 1 pool MOJ_ROZSAH
!
access-list 1 permit 10.1.1.0 0.0.0.255
!
...
```

Overenie funkčnosti a konfigurácie NAT

- Zobrazenie aktívnej prekladovej tabuľky
- Static / dynamic NAT

```
! Static NAT
Gw# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 211.2.2.9          10.1.1.2           ---                ---


! Aktivna relacia / static aj dynamic
Gw# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 211.2.2.9          10.1.1.2           158.193.152.108    158.193.152.108
```

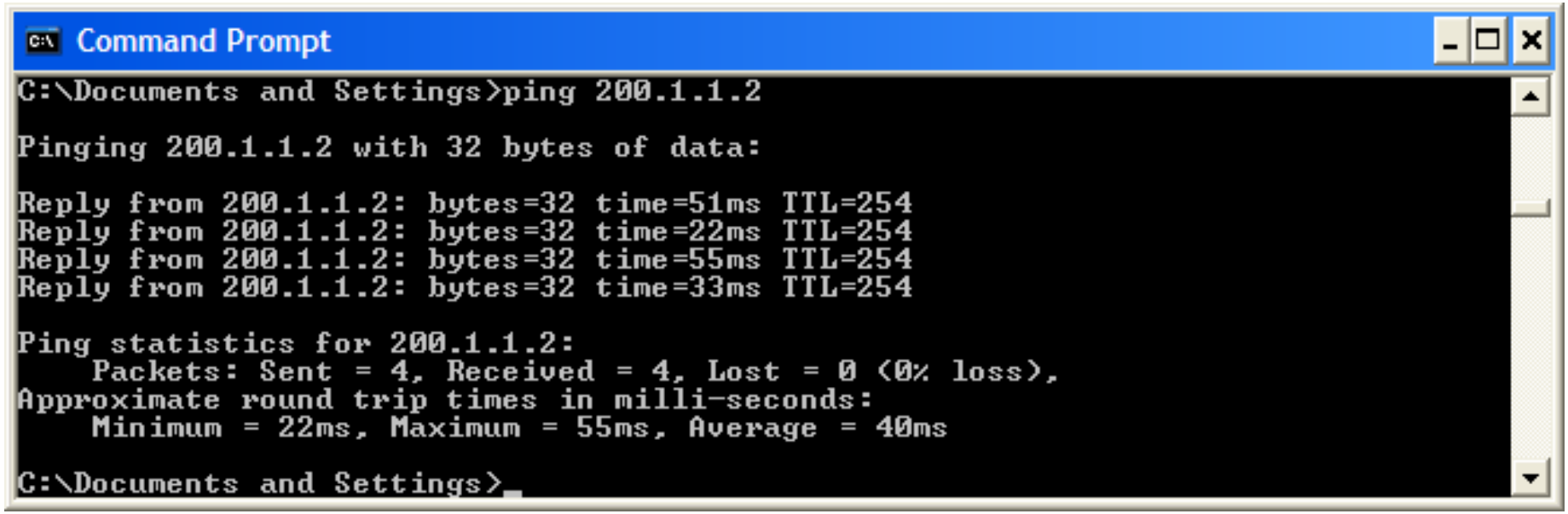
Overenie funkčnosti a konfigurácie NAT

- Zobrazenie štatistík

```
Gw#sh ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0
Inside interfaces:
  Ethernet0
Hits: 41  Misses: 3
CEF Translated packets: 36, CEF Punted packets: 16
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool MOJ_ROZSAH refcount 1
 pool MOJ_ROZSAH: netmask 255.255.255.252
        start 211.2.2.8 end 211.2.2.10
        type generic, total addresses 3, allocated 1 (33%), misses 0
Queued Packets: 0
Gw#
```

Overenie funkčnosti a konfigurácie NAT

```
Gw#debug ip nat
*Mar  1 00:16:16.663: NAT*: s=10.1.1.2->211.2.2.9, d=200.1.1.2 [49659]
*Mar  1 00:16:16.743: NAT*: s=200.1.1.2, d=211.2.2.9->10.1.1.2 [49659]
*Mar  1 00:16:17.655: NAT*: s=10.1.1.2->211.2.2.9, d=200.1.1.2 [49734]
*Mar  1 00:16:17.687: NAT*: s=200.1.1.2, d=211.2.2.9->10.1.1.2 [49734]
*Mar  1 00:16:18.675: NAT*: s=10.1.1.2->211.2.2.9, d=200.1.1.2 [49822]
*Mar  1 00:16:18.695: NAT*: s=200.1.1.2, d=211.2.2.9->10.1.1.2 [49822]
*Mar  1 00:16:19.655: NAT*: s=10.1.1.2->211.2.2.9, d=200.1.1.2 [49906]
*Mar  1 00:16:19.679: NAT*: s=200.1.1.2, d=211.2.2.9->10.1.1.2 [49906]
```



Problém s NAT

- Ak prekladám na IP z iného rozsahu ako outside rozhranie
- Zabezpečiť smerovanie pre túto sieť
- Riešenie
  - Null interface
    - `ip route NAT_POOL null 0`
  - Loopback rozhranie s IP z NAT pool-u a príkaz network v routing procese

Vymazanie NAT prekladovej tabuľky

```
Router#clear ip nat translation *
```

```
Gw#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 211.2.2.9          10.1.1.2           ---                ---
Gw#clear ip nat translation *
Gw#sh ip nat translations
Gw#


Gw#
```

- Rušenie NAT/PAT sa vykonáva tak, ako sa konfiguruje ale pred tým uviesť
  - **no**
- Problém ak je NAT aktívne (t.j. je aktívny aspoň jeden záznam v prekladovej tabuľke)
  - Treba zmazať

Konfigurácia PAT (PNAT)

Prečo PNAT?

- NAT rieši len mapovanie 1:1
  - Za jednu privátnu adresu je treba jedna verejná
  - Limitovaný počet spojení z vnútra von daný počtom verejných adries
  - SOHO často len jedna verejná IP adresa
- Port Address Translation
  - Preťažovanie verejného rozhrania
    - SOHO
  - Preťažovanie rozsahu IP adries
    - Enterprise

Konfigurácia PAT

Preťažovanie rozhrania

- Pozostáva z:
  - Definovanie Inside / outside
  - Zadefinovania IP adries cez ACL, pre ktoré NAT bude vykonávať preklad

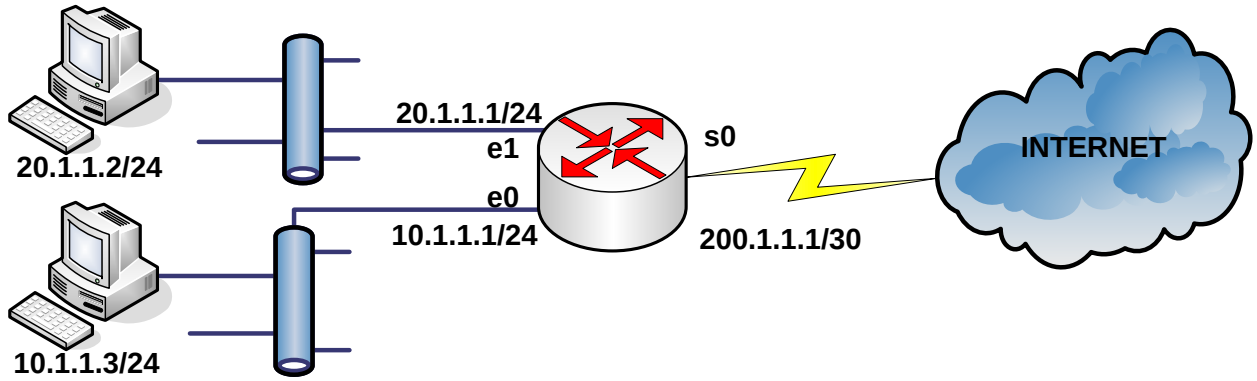
```
Router(config)#access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

  - Určenie rozhrania, ktoré sa „preťaží“

```
Router(config)#ip nat inside source list CISLO-ACL-LISTU interface INT overload
```

Konfigurácia PAT

Preťaženie rozhrania – príklad




```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config)#int ethernet 1
Gw(config-if)#ip address 20.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Gw(config)#access-list 1 permit 20.1.1.0 0.0.0.255
Gw(config)#ip nat inside source list 1 interface serial 1/0 overload
```

Konfigurácia PAT

Preťaženie adresného rozsahu

- Pozostáva:
  - Zadefinovanie IP adries cez ACL, pre ktoré PAT bude vykonávať preklad

```
Router(config)#access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

  - Zadefinovanie rozsahu verejných adries (tzv. NAT pool), z ktorých bude pri preklade vyberané

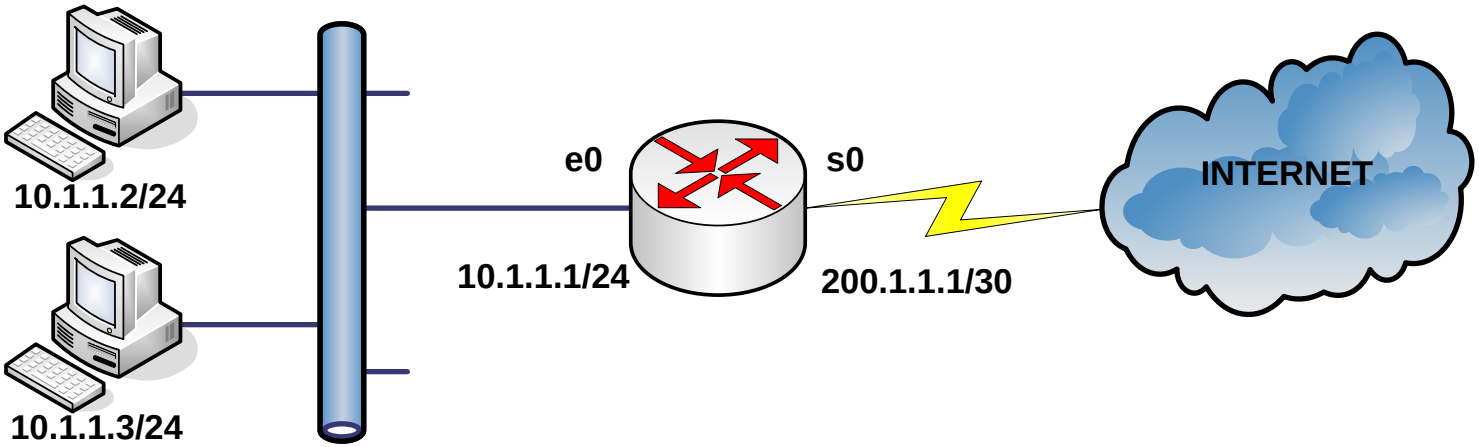
```
Router(config)#ip nat pool MENO_POOLU START-IP END-IP netmask MASKA
```

  - Spojenie ACL a daného pool-u do funkčného dynamického PAT

```
Router(config)#ip nat inside source list CISLO-ACL-LISTU pool MENU_POOLU overload
```

Konfigurácia PAT

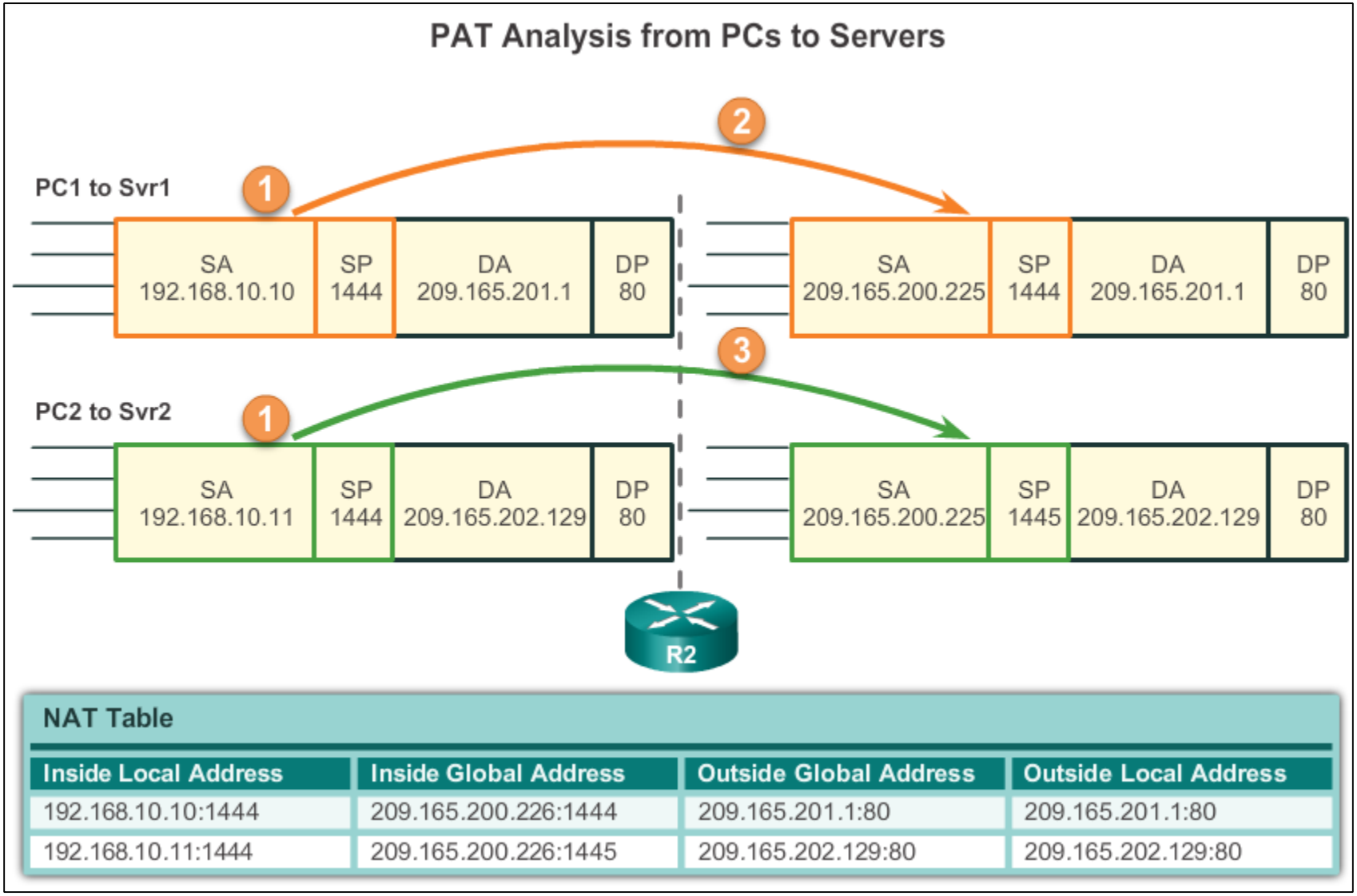
Preťaženie rozsahu adries - príklad




```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#ip nat pool MOJ_ROZSAH 211.2.2.8 211.2.2.10 netmask 255.255.255.252
Gw(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Gw(config)#ip nat inside source list 1 pool MOJ_ROZSAH overload
```

Konfigurácia PAT

Analýza PAT

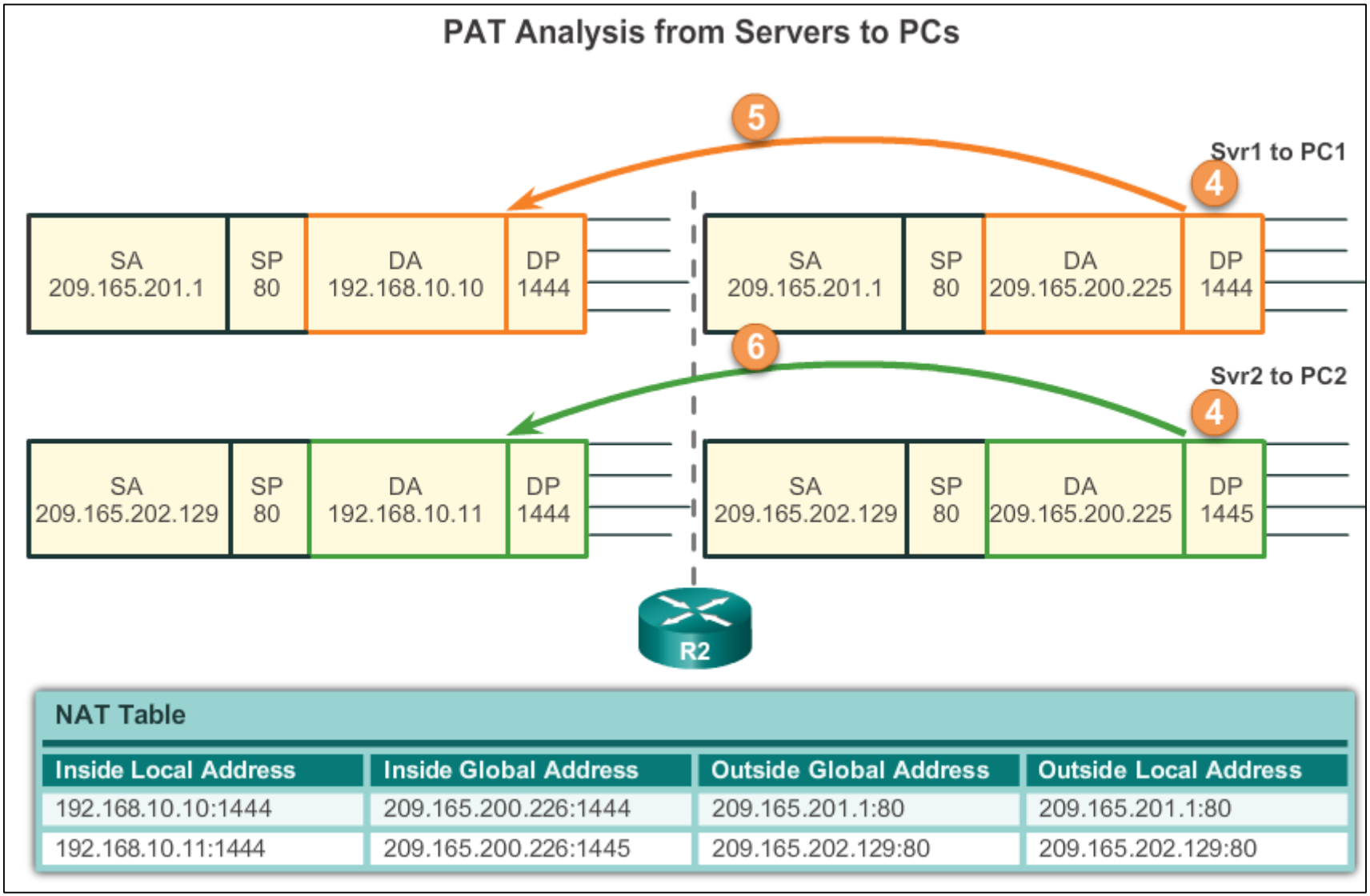


NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Konfigurácia PAT

Analýza PAT



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.226:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.226:1445	209.165.202.129:80	209.165.202.129:80

Overenie funkčnosti a konfigurácie PAT

- Zobrazenie aktívnej prekladovej tabuľky

```
Gw# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 200.1.1.1:1792    10.1.1.2:1792      200.1.1.2:1792     200.1.1.2:1792
tcp 200.1.1.1:6110     10.1.1.2:6110      200.1.1.2:80       200.1.1.2:80
tcp 200.1.1.1:6112     10.1.1.2:6112      200.1.1.2:80       200.1.1.2:80
tcp 200.1.1.1:6114     10.1.1.2:6114      200.1.1.2:80       200.1.1.2:80
```

- Zobrazenie štatistík

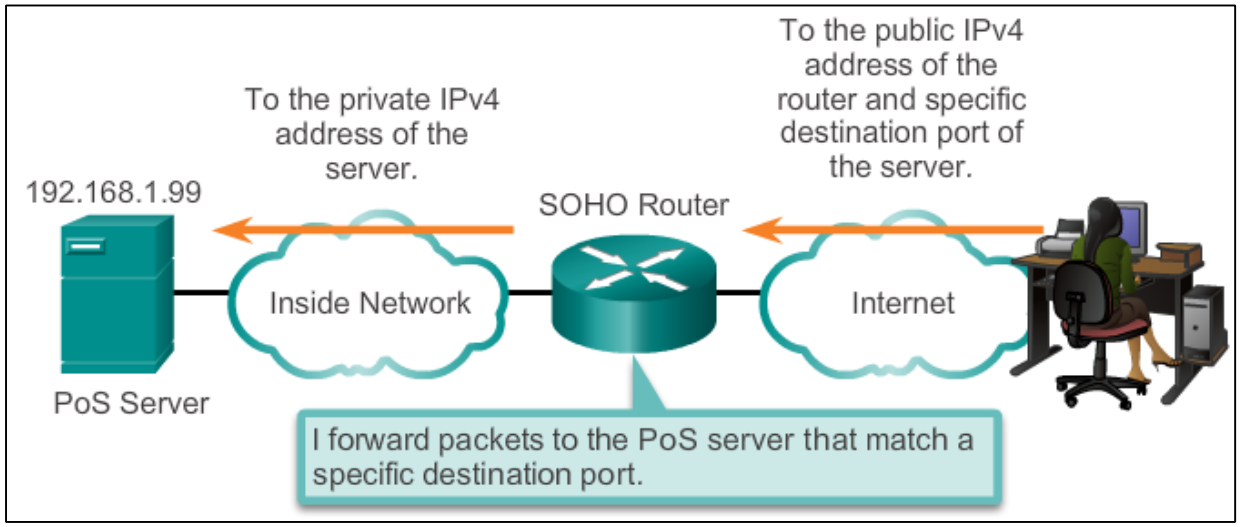
```
Gw#sh ip nat statistics
Total active translations: 4 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial1/0
Inside interfaces:
  FastEthernet0/0
…
```

```
Gw#debug ip nat
```

```
Gw#sh run
```

Port Forwarding

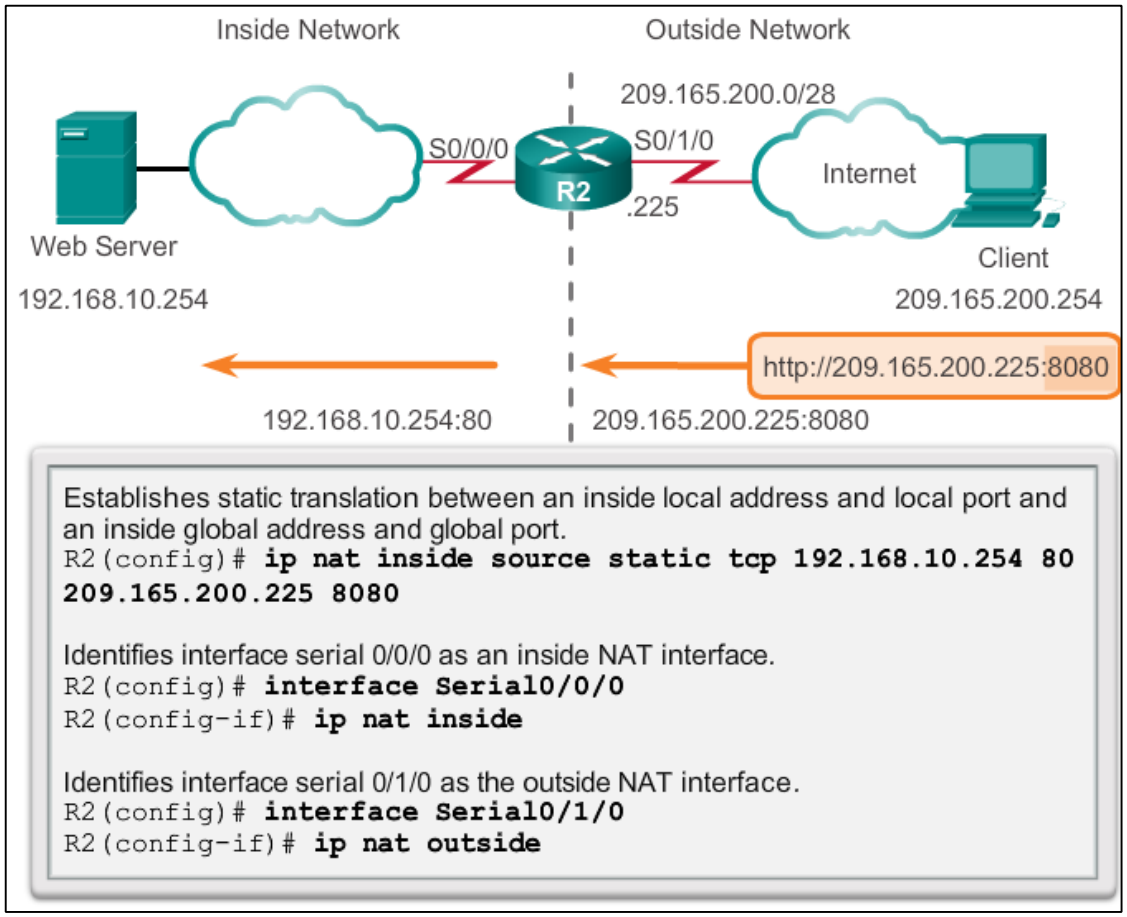
- Port forwarding je technika použitá na prechod špecifickej prevádzky na danom porte medzi sieťami.
  - Paket zaslaný na danú verejnú IP adresu a port je presmerovaný na špecifikovanú privátnu adresu a port.
- Port forwarding je užitočná pri zabezpečení prístupu na služby sieťových serverov, ktoré nemajú verejnú IP adresu



Port Forwarding

Konfigurácia Port Forwarding

Je to vlastne statický NAT prekladá, ktorý zároveň špecifikuje TCP alebo UDP portové číslo



Problematické okruhy okolo NAT

NAT has several advantages, including the following:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets.
- NAT allows the existing scheme to remain, and it still supports the new assigned addressing scheme outside the private network.

Cisco IOS NAT does support the following traffic types although they carry IP addresses in the application data stream:

- ICMP
- File Transfer Protocol (FTP), including PORT and PASV commands
- NetBIOS over TCP/IP, datagram, name, and session services
- Progressive Networks' RealAudio
- White Pines' CuSeeMe
- DNS "A" and "PTR" queries
- H.323/NetMeeting, versions 12.0(1)/12.0(1)T and later
- VDOLive, version 11.3(4)11.3(4)T and later
- Vxtreme, versions 11.3(4)11.3(4)T and later
- IP multicast, version 12.0(1)T, the source address translation only

Cisco IOS NAT does not support the following traffic types:

- Routing table updates
- DNS zone transfers
- BOOTP
- talk, ntalk
- Simple Network Management Protocol (SNMP)

- **Nevýhody**:
  - Stúpa zaťaženia NAT routra, klesá výkonnosť, stúpa oneskorenie tvorené spracovaním
    - Processing Delay
  - Zvýšené požiadavky na HW
  - Problem so službami pracujúcimi s IP adresami na viac vrstvách
  - Skomplikované tunelovanie

NAT for IPv6

- IPv6 tiež používa NAT, ale v úplne inom kontexte
  - IPv6 nepoužíva privátne adresy.
- V IPv6 sa NAT používa na transparentný prechod medzi IPv4 a IPv6.
  - Jedna z IPv4 => IPv6 prechodových techník
- NAT64 nie je považované za trvalo nasaditeľnú techniku
  - Určený iba na nasadenie pre dobu prechodu na plnú IPv6.


KATEDRA INFORMAČNÝCH SIETÍ
FAKULTA RIADENIA A INFORMATIKY ŽU

ĎAKUJEM