

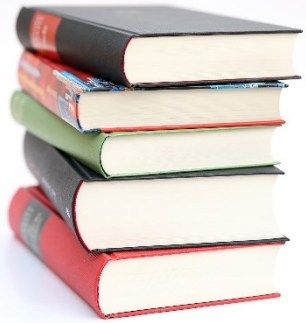


UNIVERSITY OF ŽILINA  
Faculty of Management Science  
and Informatics

# Privátne adresy a NAT pre IPv4 (Network Address Translation)

## Počítačové siete 1

Katedra informačných sietí  
Fakulta riadenia a informatiky, ŽU



# Čo nás dnes čaká

- **Využitie NAT a jeho charakteristiky**
- **Výhody a nevýhody NAT**
- **Koncept a konfigurácia:**
  - statické NAT
  - dynamické NAT
  - PAT
  - Port forwarding
- **NAT64**
- **Diagnostika problémov s NAT**

# Problém ...

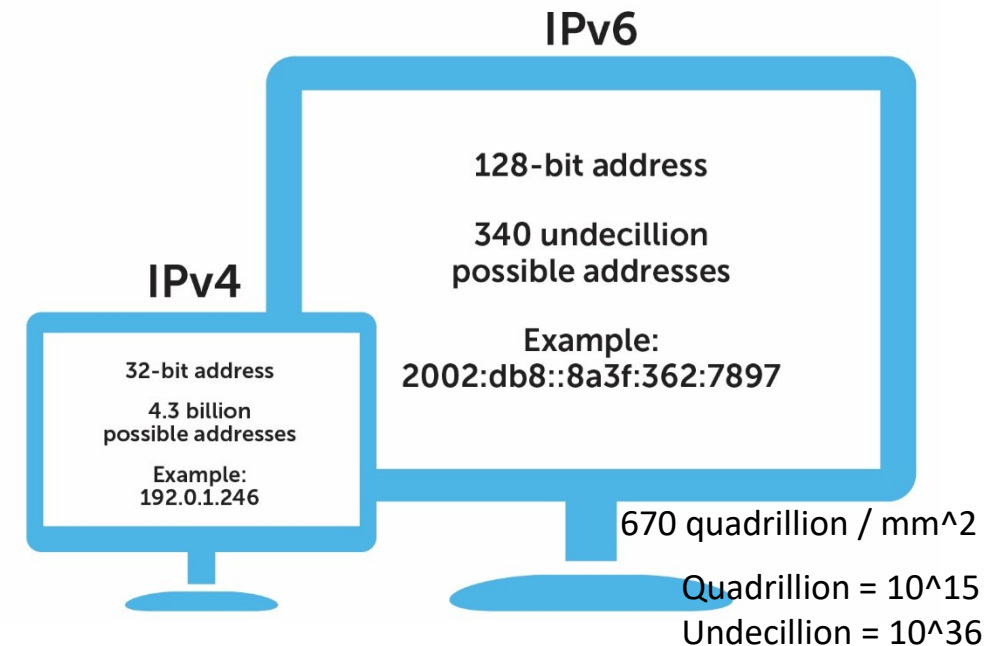
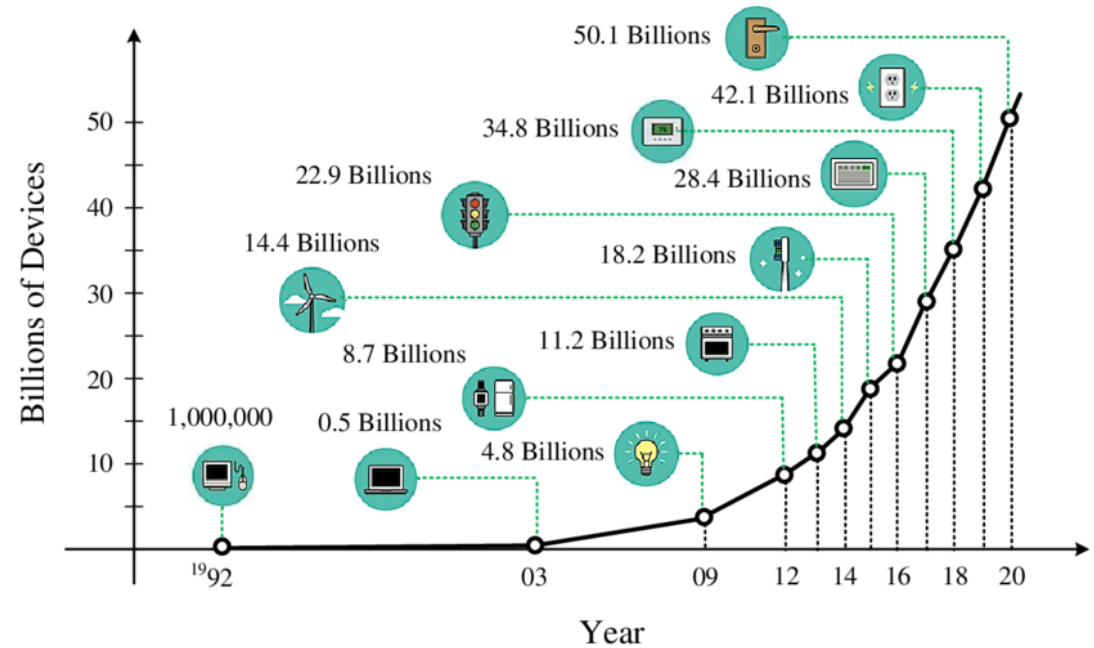
- Vďaka flexibilitnosti IP technológie nárast používania → každé IP zariadenie musí mať IP adresu
- Verejný adresný priestor
  - Problém → riadený a pridelovaný
    - V Európe prideluje RIPE (Réseaux IP Européens)
    - Zákazník prenajíma od ISP



Public Internet addresses are regulated by Registries (RIRs):

- ARIN
- RIPE NCC
- APNIC
- LACNIC
- AfriNIC

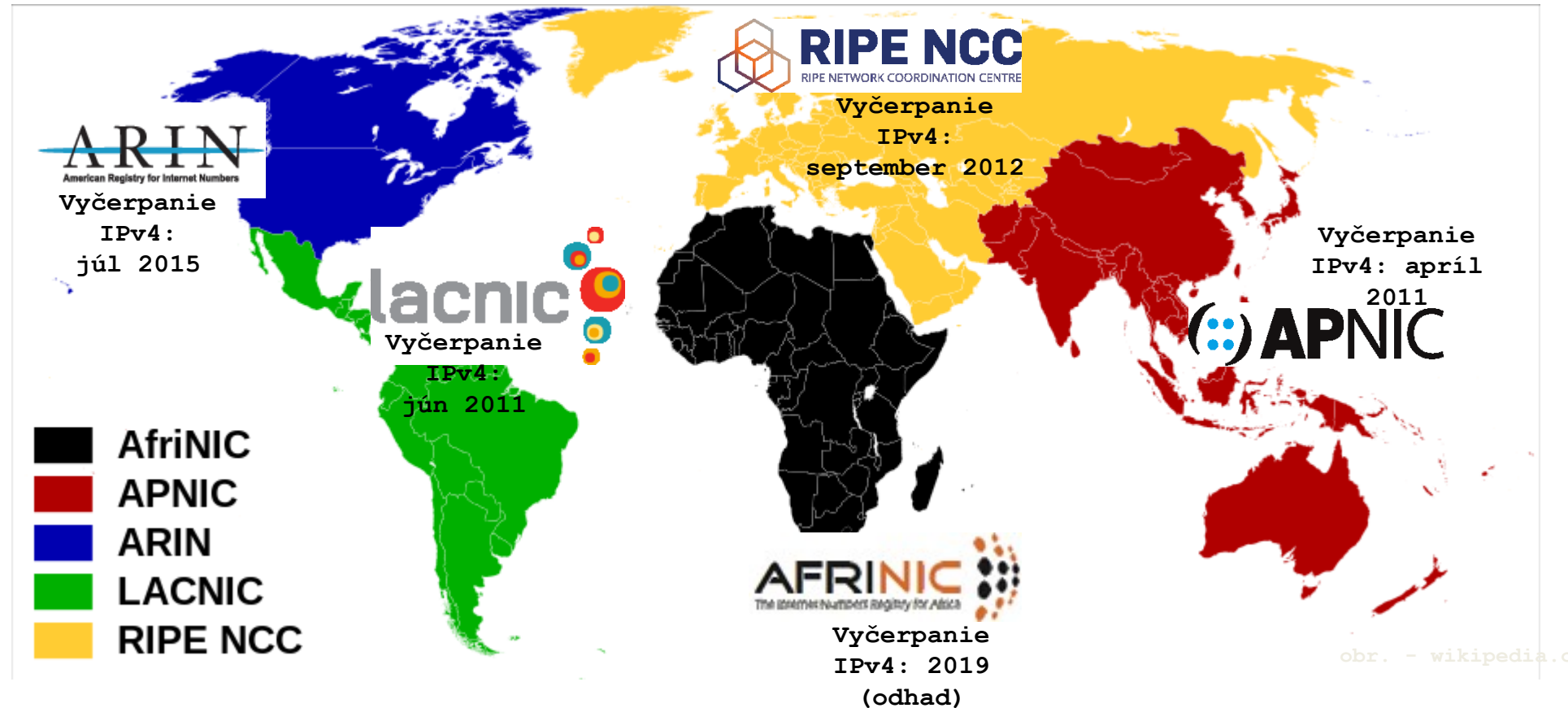
- Problém → Nedostatok prideliteľných verejných IP adries



# Aktuálny stav IPv4 adries vo svete

Kto to celé manažuje?

- U nás RIPE
- Inde ďalšie regionálne internetové registračné úrady
- Manažujú pridelovanie a registráciu IP adries pre daný región (IPv4 aj IPv6)



- African Network Information Center (AFRINIC) pre Afriku
- **Asia-Pacific Network Information Centre (APNIC) pre Áziu, Austráliu, Nový Zéland a susedné krajiny.**
- **American Registry for Internet Numbers (ARIN) pre USA, Kanadu, niektoré časti Karibiku a Antarktídu.**
- **Latin America and Caribbean Network Information Centre (LACNIC) pre Latinskú Ameriku a časť Karibiku.**
- **Réseaux IP Européens Network Coordination Centre (RIPE NCC) pre Európu, Rusko, Stredný východ a centrálnu časť Ázie**

# Problém a riešenie

- Potreba nových metód riadenia adresných rozsahov pre riešenie 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
  - Smerovače nesmú smerovať vo verejnej IP sieti privátne adresy z dôvodu nedodržania jedinečnosti identifikácie (adresovania) IP uzla
    - **Ako (akým nástrojom) to vieme zabezpečiť?**

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 terminológia

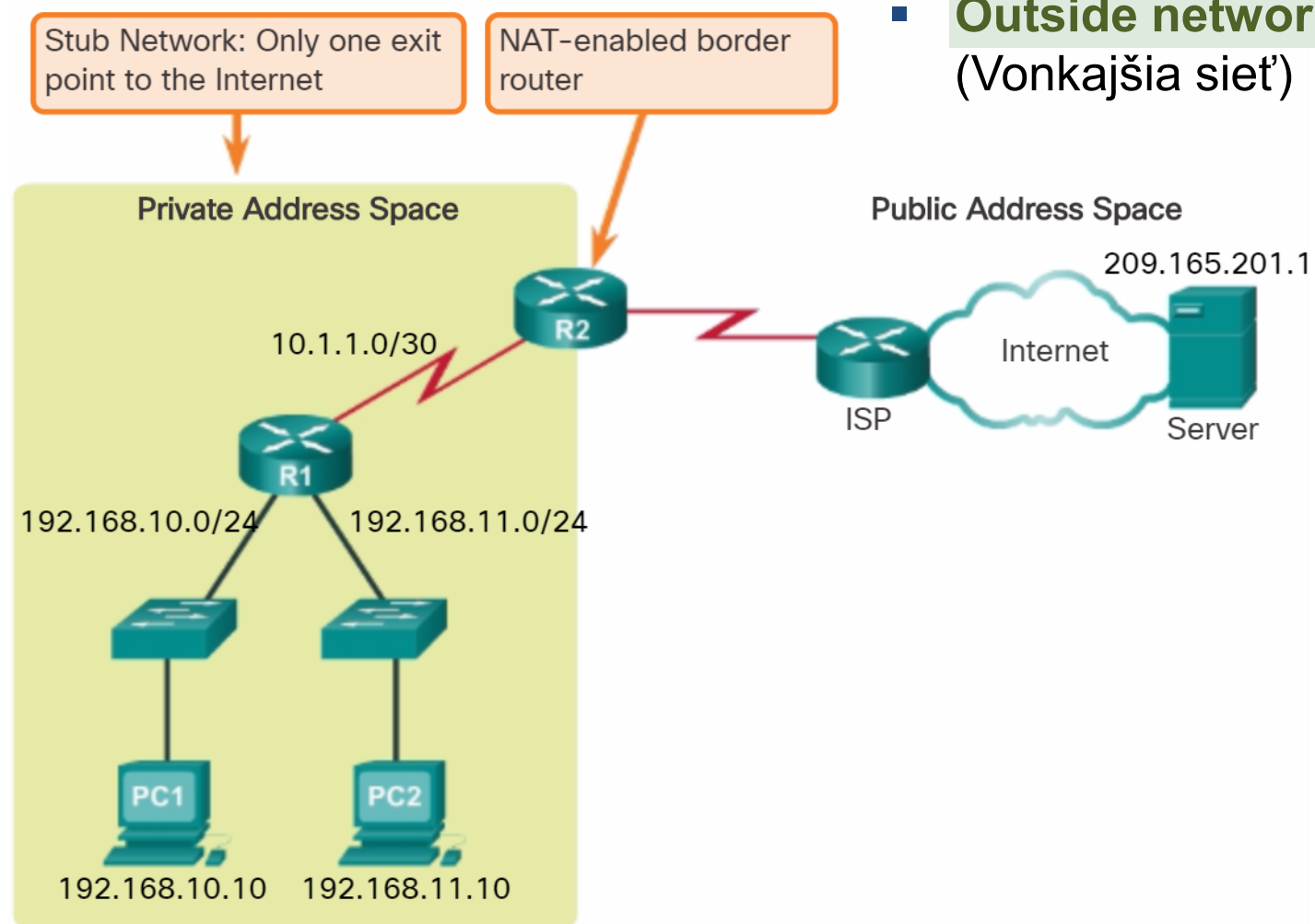
- **Border gateway router**

- NAT zariadenie
- Pracuje typicky na hranici tzv. stub siete
  - Stub net = jeden vstup a výstup z/do siete

- **Inside network**

(Vnútrotná privátna sieť)

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



- **Outside network**  
(Vonkajšia sieť)

# 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, ktorú prideli ISP.

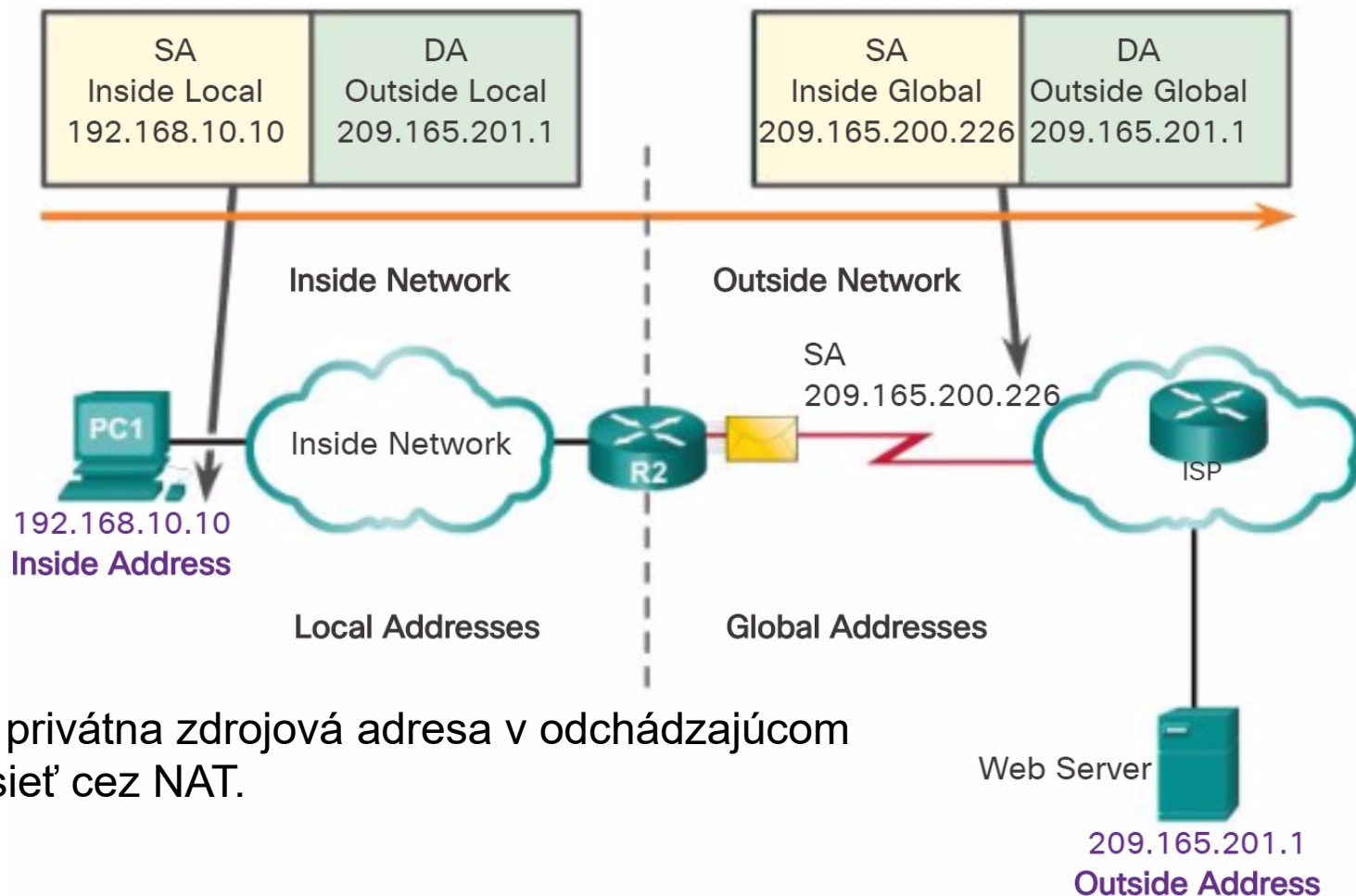
- Na túto adresu bude prekladaná privátna zdrojová adresa v odchádzajúcom pakete, ak ten opúšťa vnútornú sieť cez NAT.

- **Outside Global Address**

- Adresa cieľa ako je viditeľná z vonkajšej siete. Platná verejná IP adresa (globálne smerovateľná), pridelená koncovému IP zariadeniu.

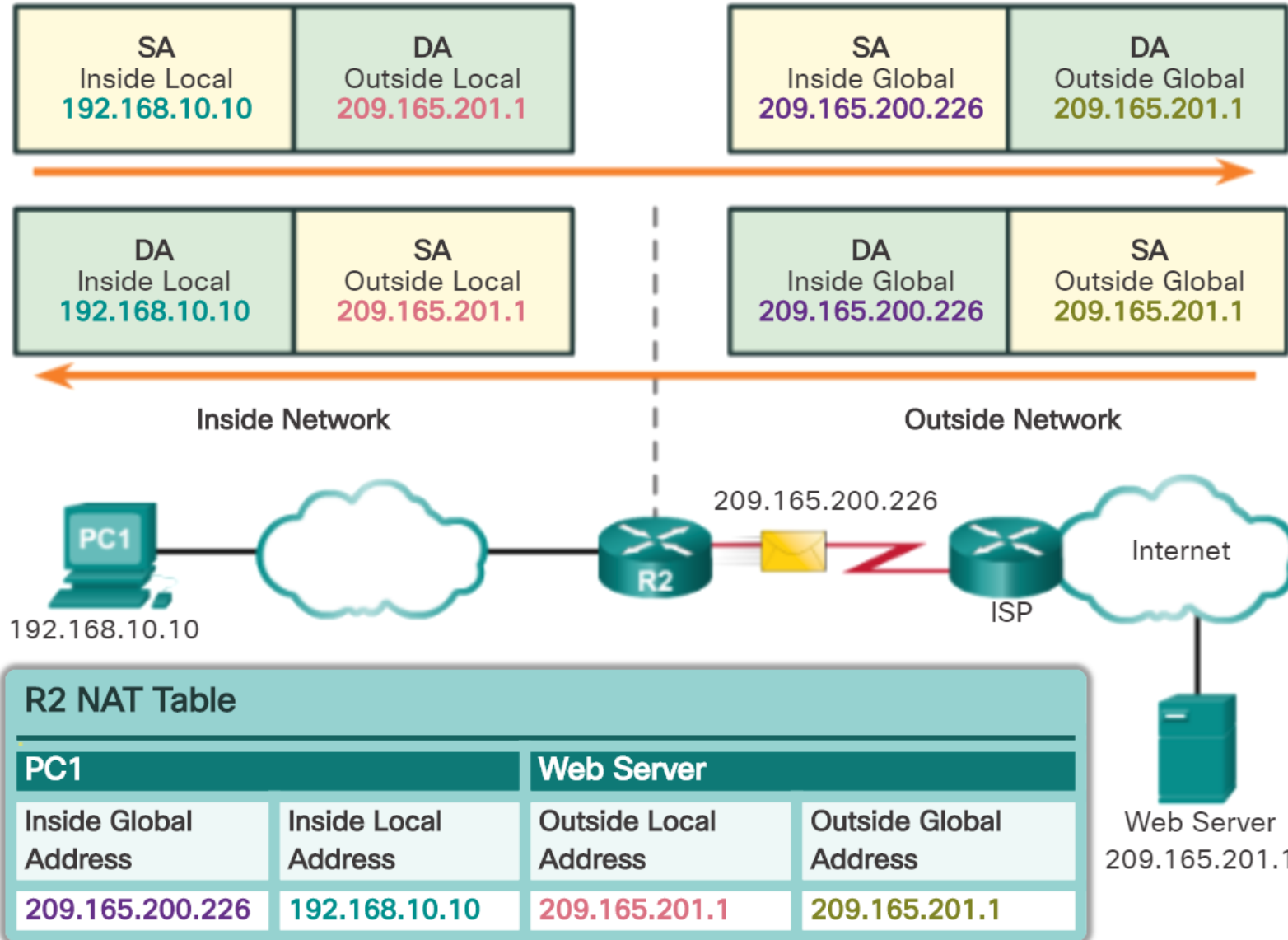
- **Outside Local Address**

- Adresa cieľa, ale taká ako ju vidí odosielateľ z vnútornej siete – zväčša je rovnaká ako Outside Global Add, ale výnimočne môže byť iná (lokálna, privátna).





# NAT proces



# Spôsoby NAT mapovania

## ▪ 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

**1 : 1**

## ▪ Dynamické mapovanie

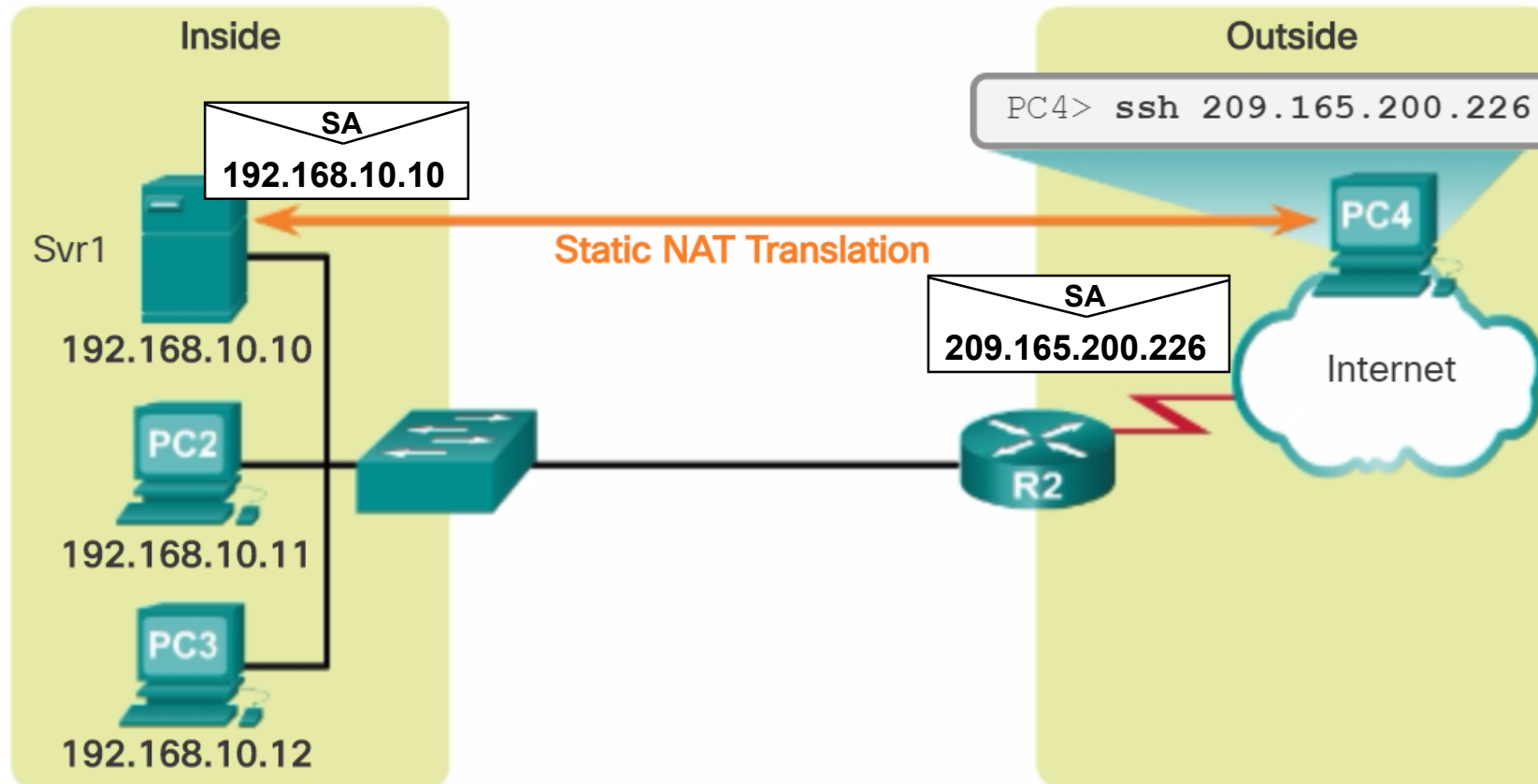
- NAT má dostupný rozsah verejných adries
  - Tzv. **IP address pool**
- NAT riadi preklad pridelovaním neobsadených verejných IP adries z rozsahu podľa príchodších požiadaviek z vnútra siete

**n : n ,**

**FCFS**

# Statické NAT

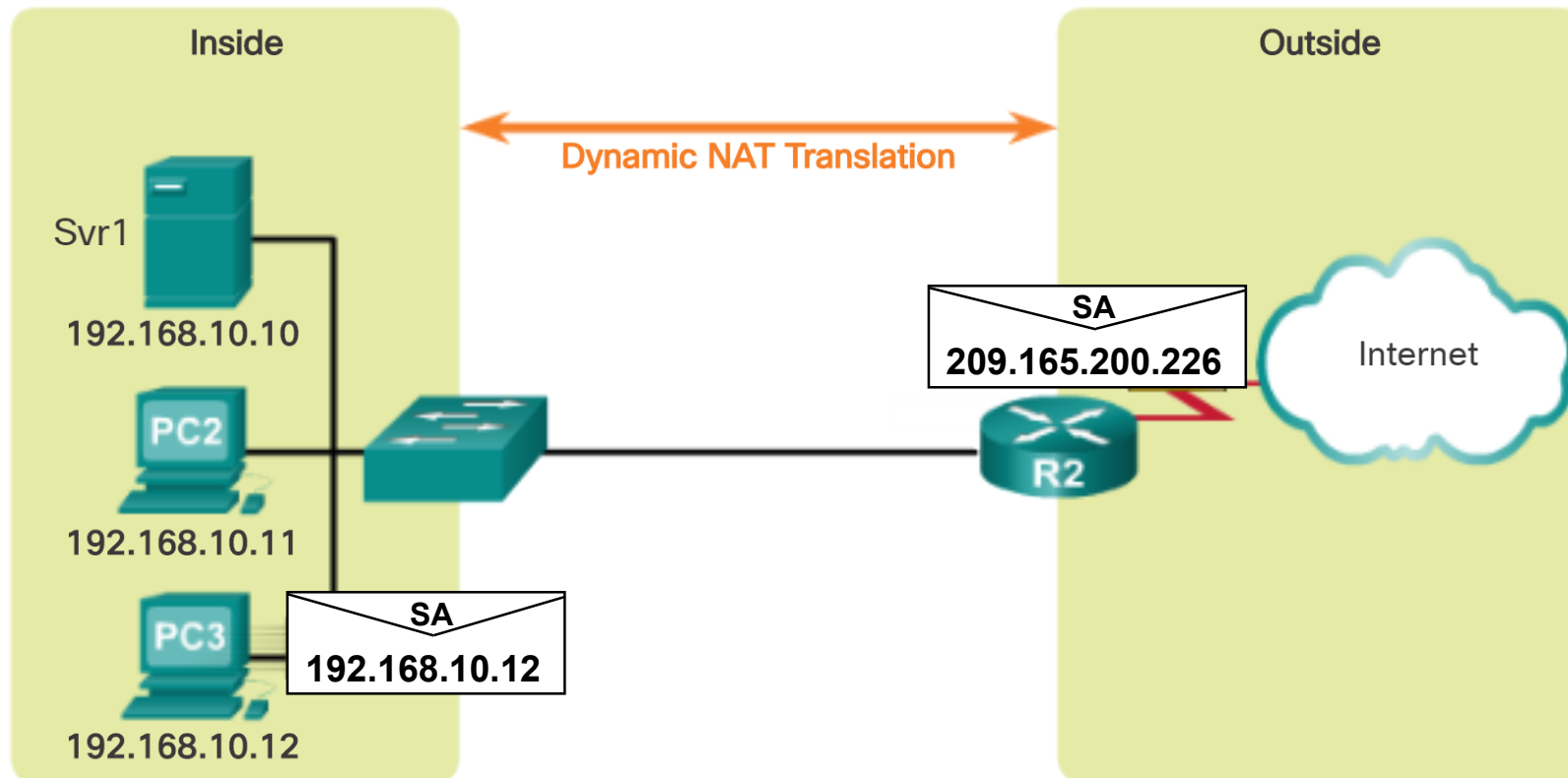
Static NAT Table	
Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



1 : 1

# Dynamické NAT

IPv4 NAT Pool	
Inside Local Address	Inside Global Address Pool - Addresses reachable via R2
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230



**n : n ,**  
**FCFS**

# PAT (Protocol Address Translation)

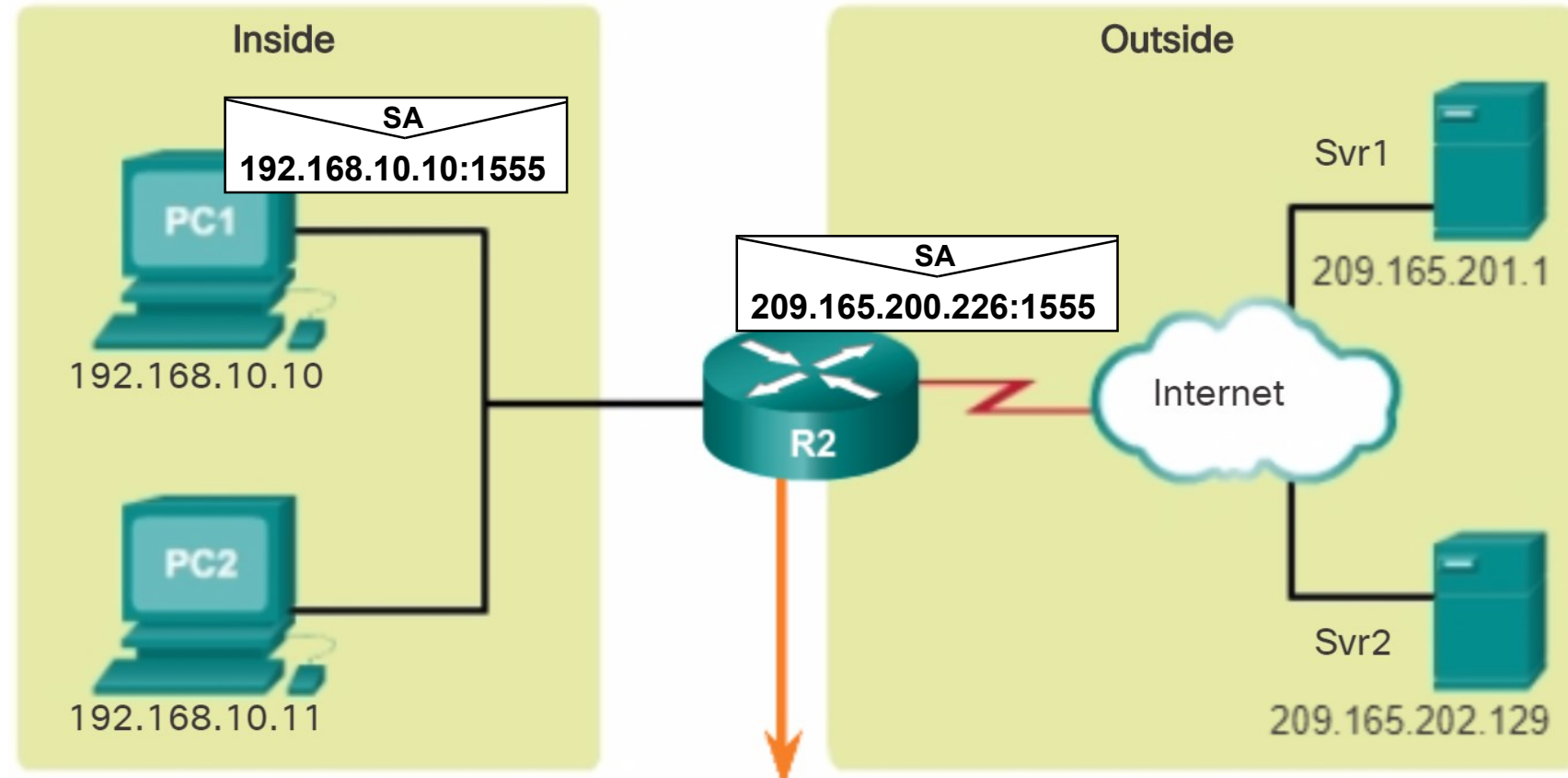
- Tzv. **NAT overloading**
- Použitý ak:
  - Mám pridelenú **len jednu verejnú adresu** na WAN rozhraní smerovača (typické pri malých zákazníkoch)
    - PAT mapuje viaceré IP adresy na jednu verejnú IP adresu, kde sa prebiehajúce komunikácie rozlišujú číslom portu (16 bit)
  - Alebo
    - Mám pridelený **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

$$n : m ,$$

kde  $1 \leq m < n$

# PAT vlastnosti

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



NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.10:1331	209.165.202.129:80	209.165.202.129:80

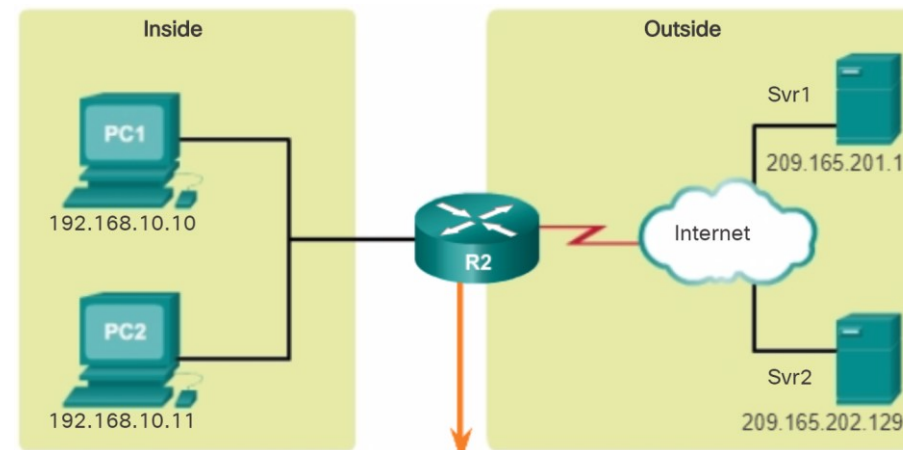
# Zhodnotenie NAT/PAT

## Výhody

- Nasadenie na Stub Net – zvyšovanie flexibility
  - Eliminuje potrebu preadresovania IP zariadení ak sa zmení ISP 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

## Nevýhody

- Procesná záťaž
  - Zníženie výkonu smerovača
- Nefunguje natívna end-to-end IP konektivita
- Problematické tunelovanie

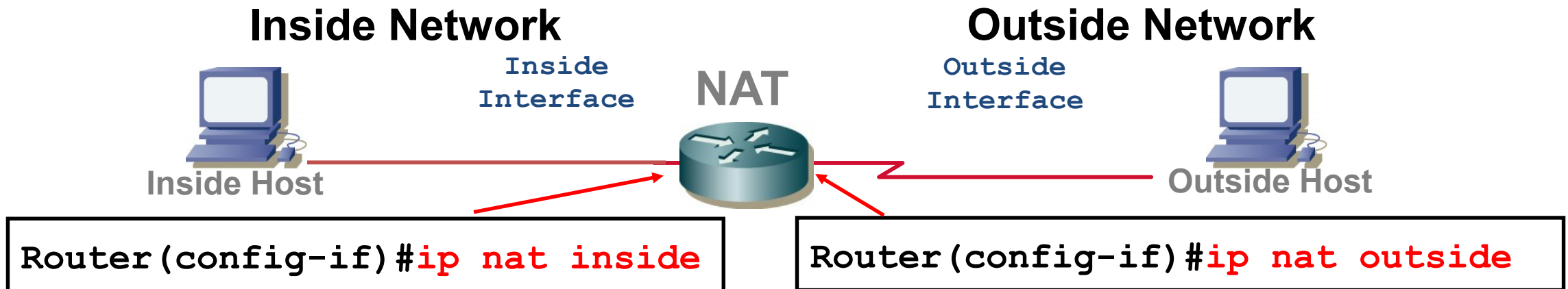




# Konfigurácia NAT



# Zadefinovanie Inside/Outside rozhraní



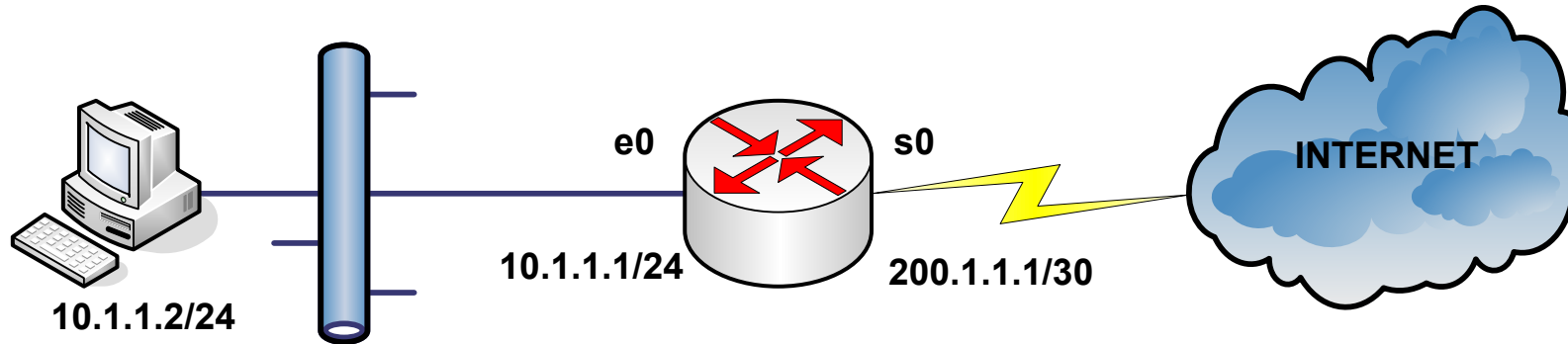
- Pri NAT sa definujú vždy!!!!
- Rozhranie border routra pri NAT môže byť
  - **Inside** (vnútorné s privátnou adresáciou)
  - alebo **Outside** (s verejnou adresáciou)
- NAT preklad nastáva:
  - Len pri prechode paketu z inside na outside a naopak
  - Nikdy medzi rozhraniami toho istého typu, alebo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

# Konfigurácia statického NAT prekladu

- Príkazom zadám mapovanie priamo do konfiguráku
- 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 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
```

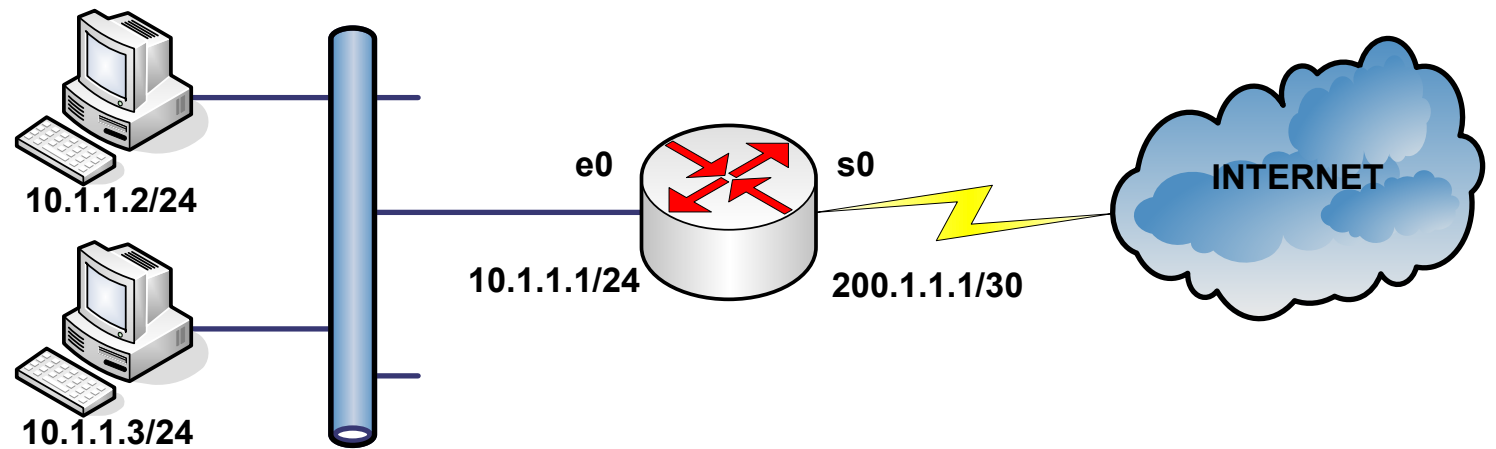
- Zdefinovania IP adries cez ACL, pre ktoré NAT bude vykonávať preklad

```
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

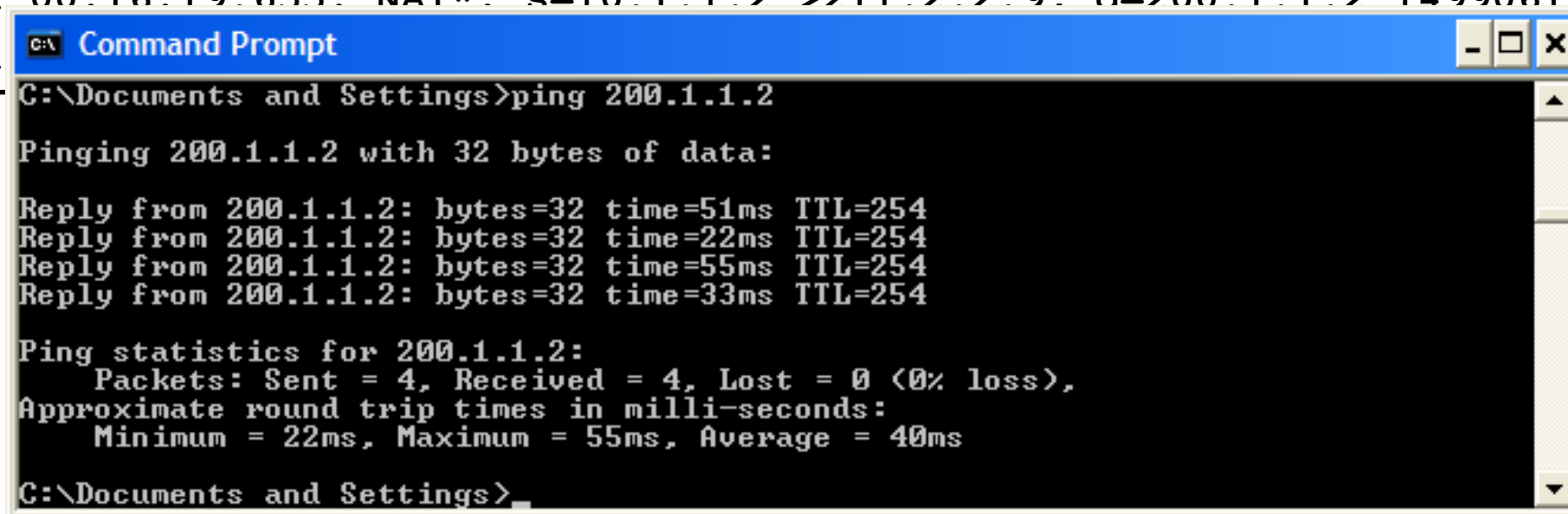
```
Gw#sh ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0
Inside interfaces:
  Ethernet0
Hits: 41 Misses: 3
CEF Translated packets: 36, CEF Punted packets: 16
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 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
```



# 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
```



```
C:\Documents and Settings>ping 200.1.1.2

Pinging 200.1.1.2 with 32 bytes of data:

Reply from 200.1.1.2: bytes=32 time=51ms TTL=254
Reply from 200.1.1.2: bytes=32 time=22ms TTL=254
Reply from 200.1.1.2: bytes=32 time=55ms TTL=254
Reply from 200.1.1.2: bytes=32 time=33ms TTL=254

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 55ms, Average = 40ms

C:\Documents and Settings>
```

# Problém s NAT

- Ak prekladám na IP z iného rozsahu ako outside rozhranie
- Ako 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 *
```

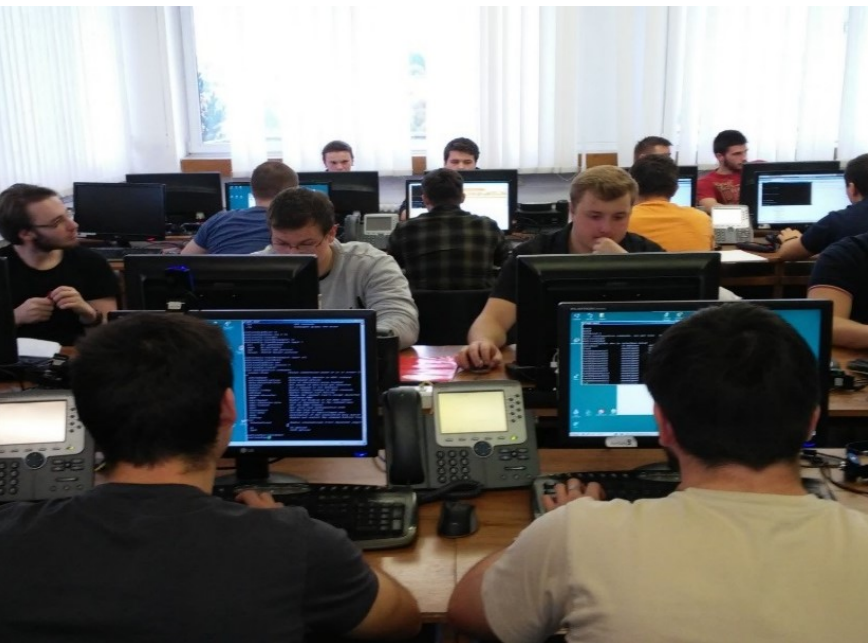
```
Gw#sh ip nat translations
```

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
```

- 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

# Pret'azovanie rozhrania

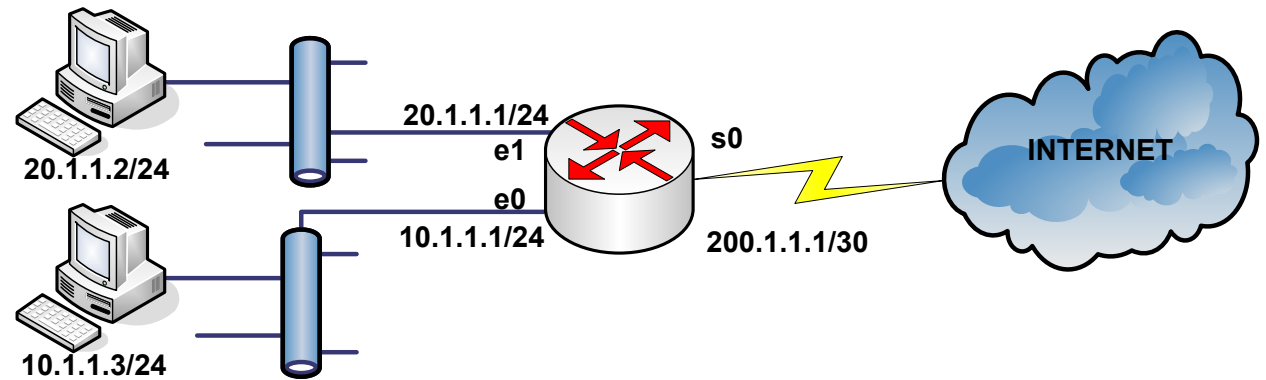
- Pozostáva z:
  - Definovanie Inside / outside
  - Zadefinovania IP adries cez ACL, pre ktoré NAT bude vykonávať preklad

```
R1 (config) #access-list CISLO-ACL-LISTU permit SOURCE WILDCARD-MASK
```

- Určenie rozhrania, ktoré sa „preťaží“

```
R1 (config) #ip nat inside source list CISLO-ACL-LISTU interface INT overload
```

## 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
```

# Pret'azenie adresného rozsahu

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

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

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

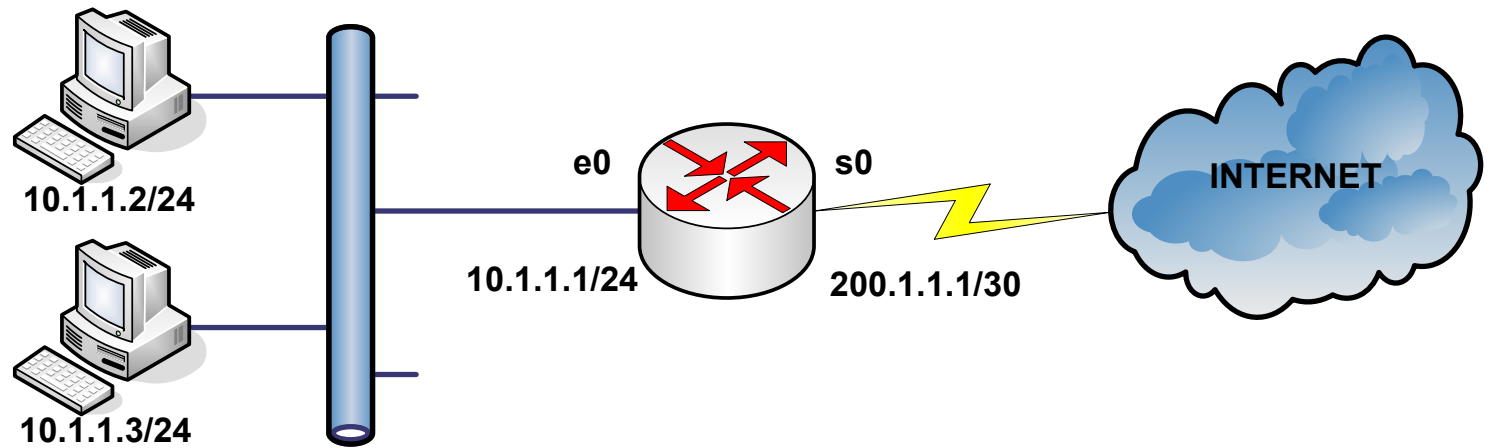
```
Router(config)#ip nat pool MENO_POOLU START-IP END-IP netmask MASKA
```

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

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

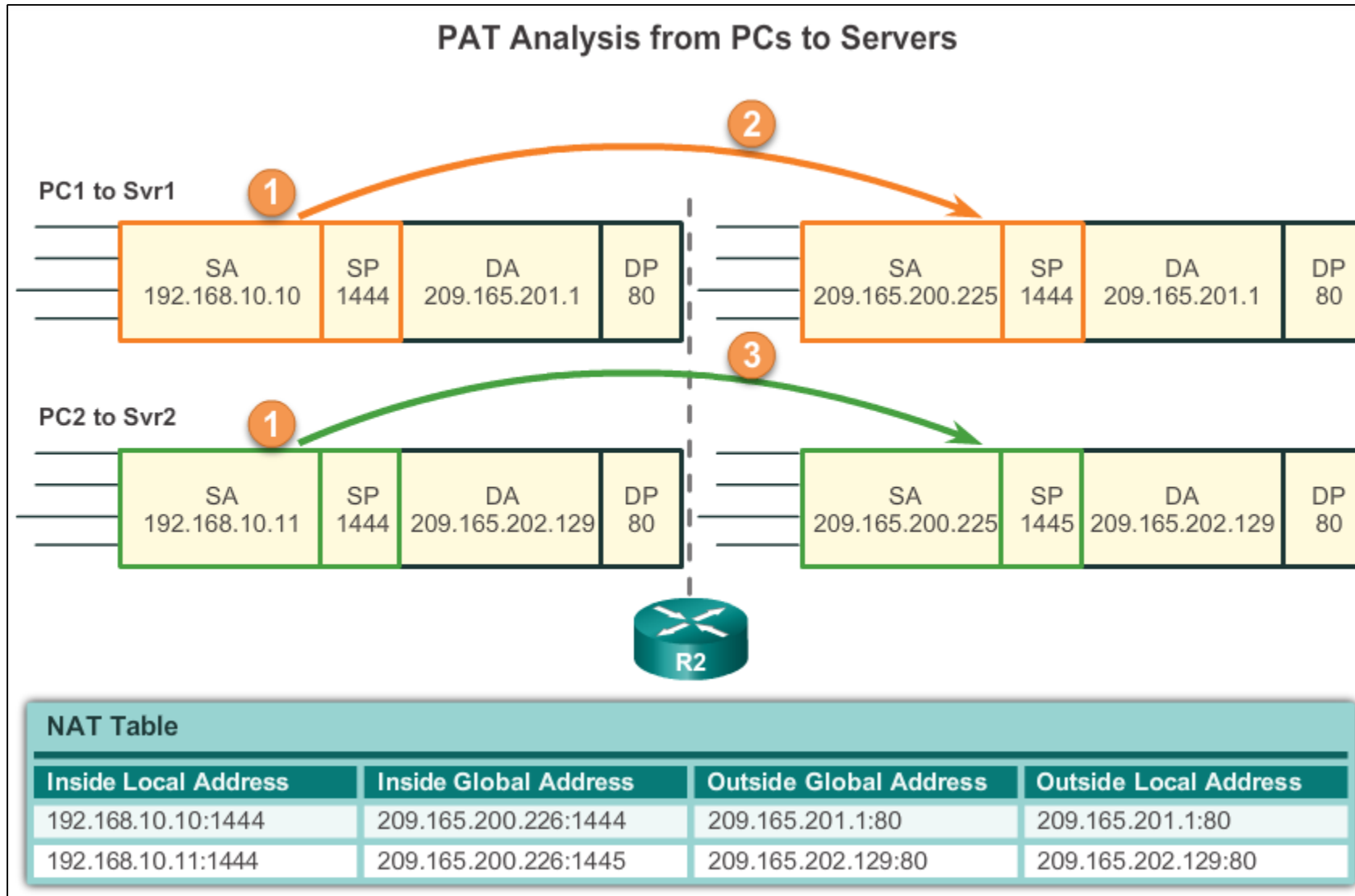


# Pret'aženie rozsahu adries - príklad

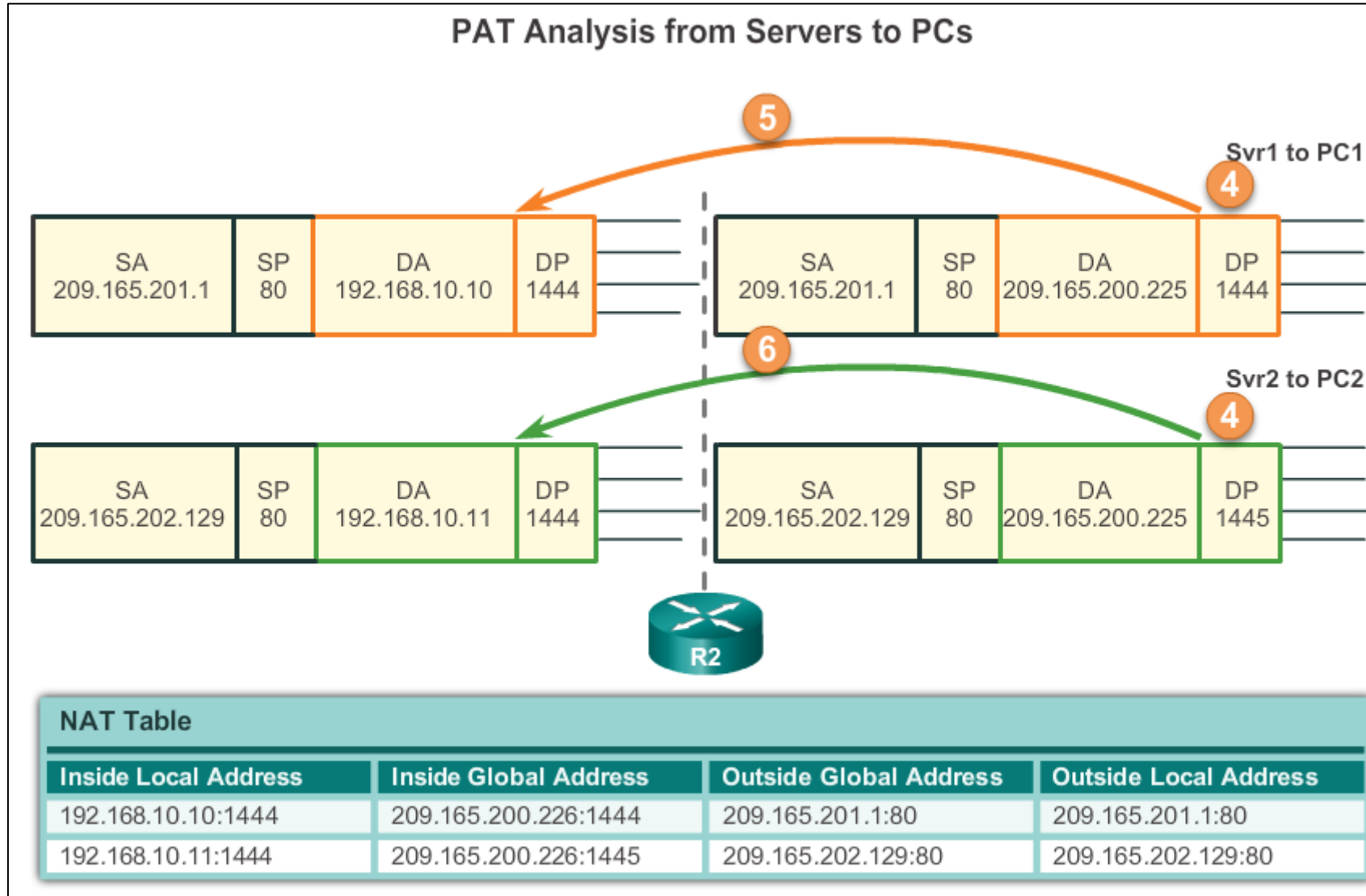


```
Gw(config)#int ethernet 0
Gw(config-if)#ip address 10.1.1.1 255.255.255.0
Gw(config-if)#ip nat inside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#int serial 0
Gw(config-if)#ip address 200.1.1.1 255.255.255.252
Gw(config-if)#ip nat outside
Gw(config-if)#no shut
Gw(config-if)#exit
Gw(config)#ip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

# Analýza PAT



# Analýza PAT



# 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

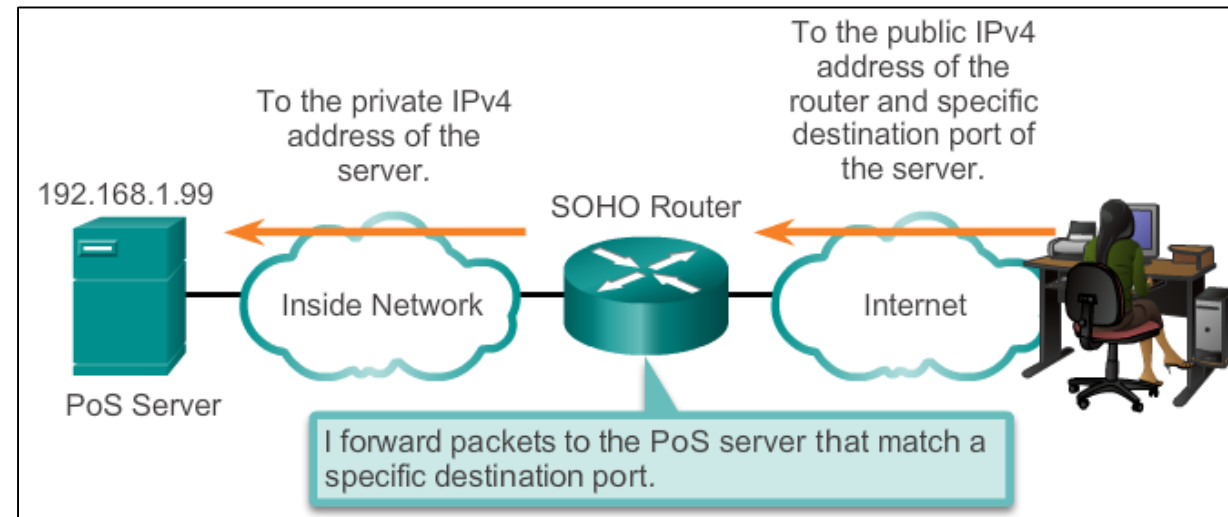
```
Gw#sh ip nat statistics
Total active translations: 4 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial1/0
Inside interfaces:
  FastEthernet0/0
...
```

```
Gw#debug ip nat
```

```
Gw#sh run
```

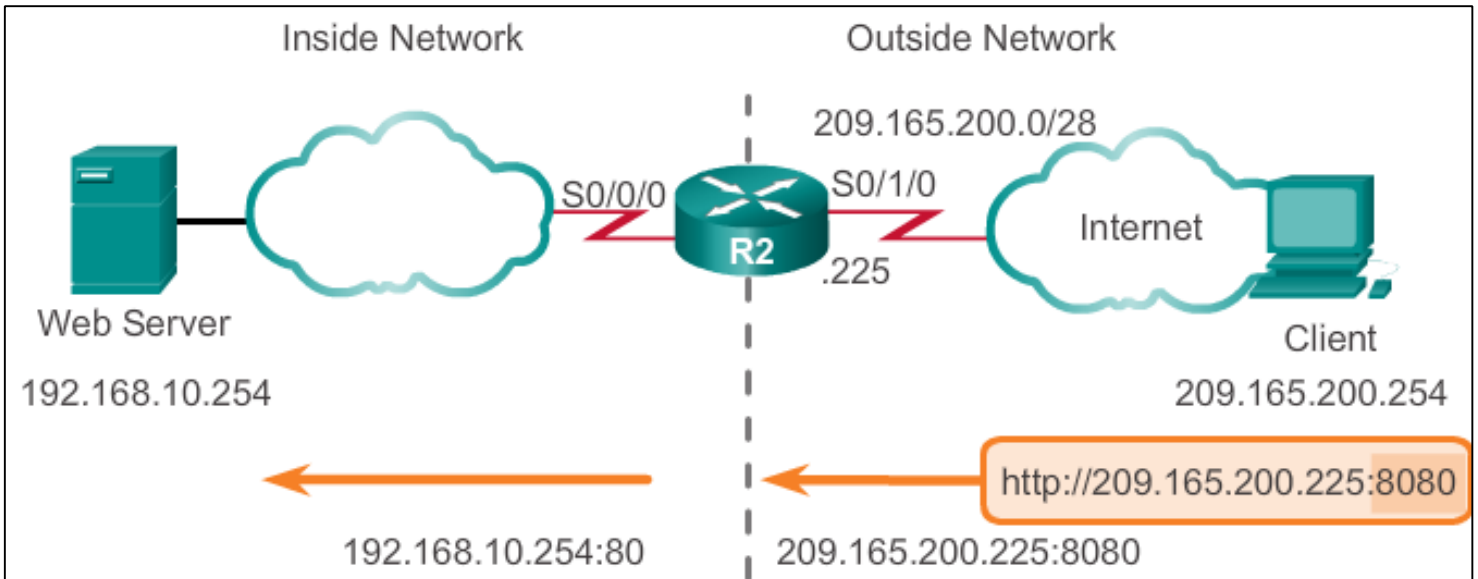
# Port Forwarding

- 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



# Konfigurácia Port Forwarding

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



Establishes static translation between an inside local address and local port and an inside global address and global port.

```
R2 (config) # ip nat inside source static tcp 192.168.10.254 80  
209.165.200.225 8080
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2 (config) # interface Serial0/0/0  
R2 (config-if) # ip nat inside
```

Identifies interface serial 0/1/0 as the outside NAT interface.

```
R2 (config) # interface Serial0/1/0  
R2 (config-if) # ip nat outside
```

# 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)

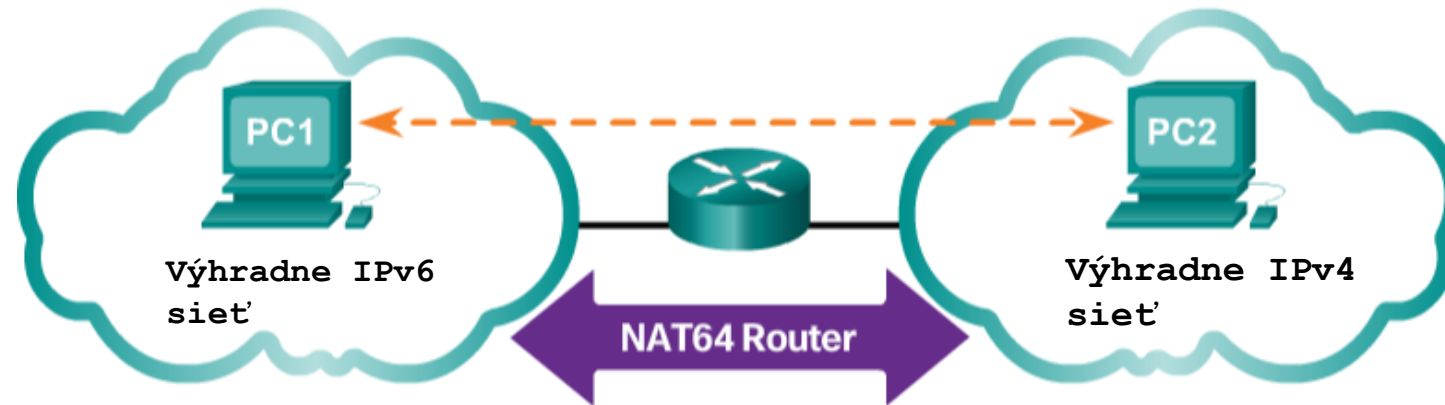
- Nevýhody:
  - Stúpa zaťaženia NAT routra, klesá výkonnosť, stúpa oneskorenie tvorené spracovaním
    - Processing Delay
  - Zvýšené požiadavky na HW
  - Problém so službami pracujúcimi s IP adresami na viac vrstvách
  - Skomplikované tunelovanie

# NAT pre IPv6

RFC 4193 Block	Prefix/L	Global ID (random)	Subnet ID	Number of addresses in subnet
	48 bits		16 bits	64 bits
fd00::/8	fd	xx:xxxx:xxxx	yyyy	18 446 744 073 709 551 616

IPv6 ULA

- IPv6 tiež používa NAT, ale v úplne inom kontexte
  - IPv6 nepoužíva privátne adresy tak, ako ich poznáme z IPv4
- 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.







UNIVERSITY OF ŽILINA  
Faculty of Management Science  
and Informatics



MINISTERSTVO  
ŠKOLSTVA, VEDY,  
VÝSKUMU A ŠPORTU  
SLOVENSKEJ REPUBLIKY

# Ďakujem za pozornosť.

Obsahom bola **kapitola 9 (NAT)** z kurzu **CCNA 2 RSE**.  
Otestujte sa cvičným testom na Netacad z RSE\_09.  
Vyjadrite svoj názor na [prednášku](#) tohto týždňa (alebo cvičenie).