Implementacija složenih mrežnih okruženja

DHCP

NAT

ACL

DHCP i NAT

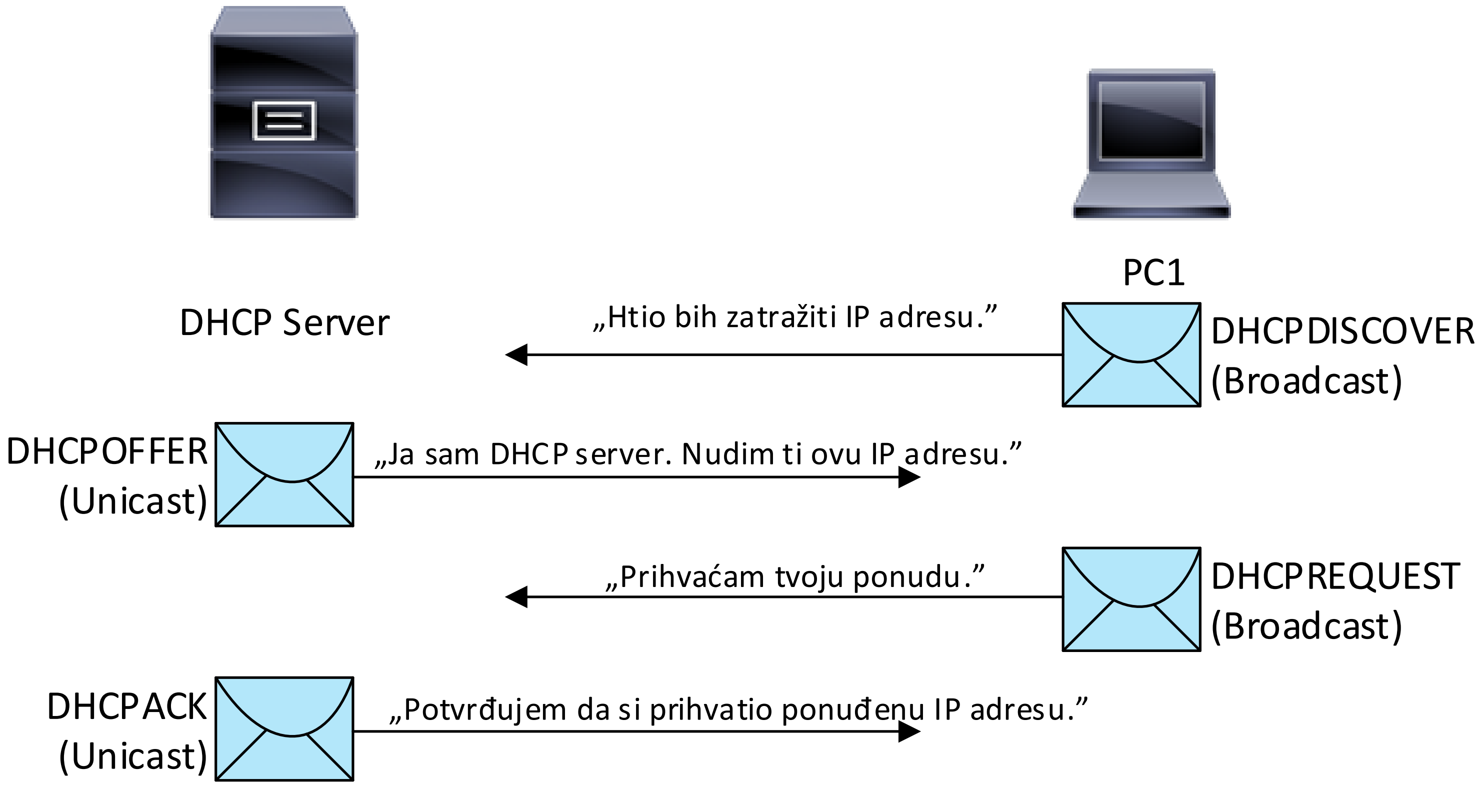
Privatni adresni prostor (RFC 1918):

Klasa	RFC 1918 raspon adresa	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**

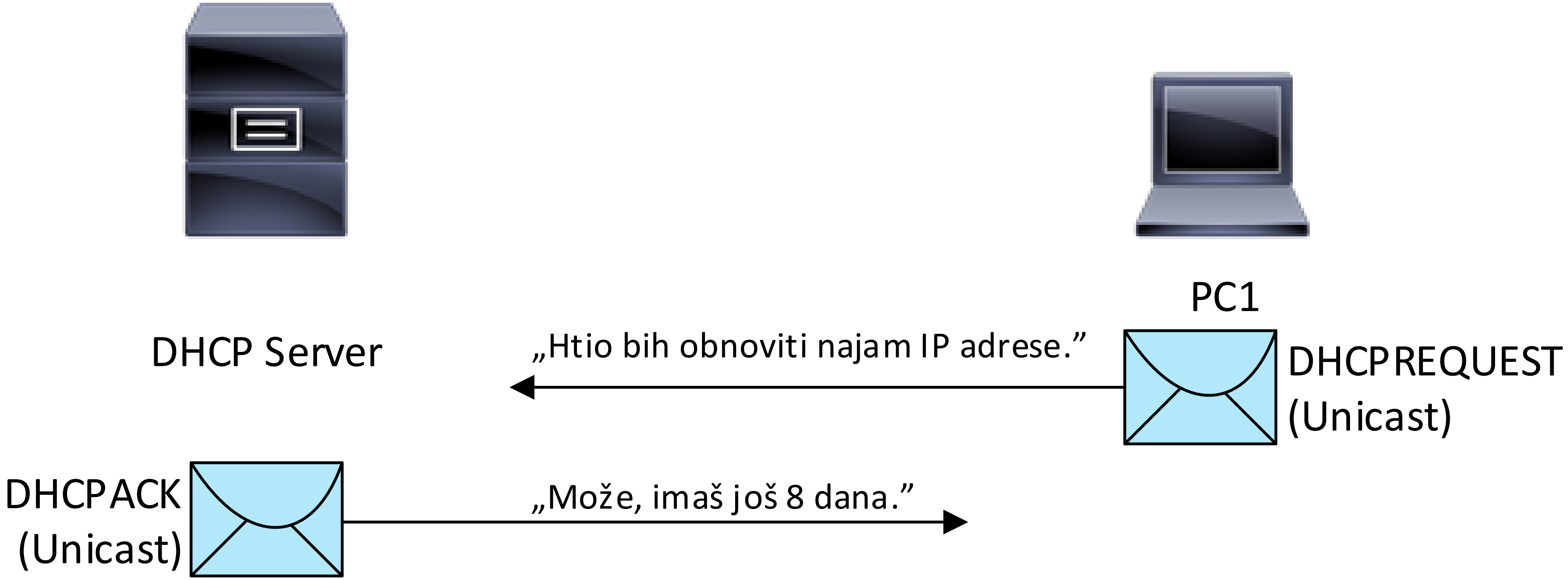
DHCP je servis za automatsku konfiguraciju IP parametara na računalima:

- **IP adresa**
- **subnet maska**
- **Gateway**
- **DNS**
- **TFTP…**

DHCP


PC1
DHCP Server
„Htio bih zatražiti IP adresu.”
DHCPDISCOVER
(Broadcast)
DHCPOFFER
(Unicast)
„Ja sam DHCP server. Nudim ti ovu IP adresu.”
„Prihvaćam tvoju ponudu.”
DHCPREQUEST
(Broadcast)
DHCPACK
(Unicast)
„Potvrđujem da si prihvatio ponuđenu IP adresu.”

DHCP-obnova IP adrese



PC1

DHCP Server

„Htio bih obnoviti najam IP adrese.”

DHCPREQUEST (Unicast)

DHCPACK (Unicast)

„Može, imaš još 8 dana.”

DHCP – format poruke

8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware addres Length (1)	Hops (1)
Transaction Identifier			
Seconds -2 bytes		Flags -2 bytes	
Client IP Address (CIADDR) -4 bytes			
Your IP Address (YIADDR) -4 bytes			
Server IP Address (SIADDR) -4 bytes			
Gateway IP Address (GIADDR) -4 bytes			
Client Hardware Address (CHADDR) -16 bytes			
Server Name (SNAME) -64 bytes			
Boot Filename -128 bytes			
DHCP Options -variable			

Option Code	Option Name
1	Subnet mask
3	Router
6	DNS servers
15	DNS domain name
51	Lease time
33	Static route
150	TFTP SERVER

DHCP – format poruke

Operation (OP) code: Određuje koji je tip poruke (npr. 1 je request, a 2 je odgovor)

Hardware Type: Pokazuje o kojem tipu hardwarea se radi (npr. 1 je ethernet, 15 je Frame Relay i slično..isti kodovi se koriste i kod ARP poruka)

Hardwarea Address Length: veličina adrese

Hops: Kontrola prosljeđivanja poruka. Klijent postavlja ovu vrijednost na 0

Transaction Identifier: Koriste klijenti kako bi znali povezati odgovore od servera sa svojim zahtjevima

Seconds: Vrijeme u sekundama koje je prošlo od kad je klijent počeo tražiti ili obnavljati IP adresu. Koriste serveri kako bi prioretizirali zahtjeve.

Flags (zastavice): Koristi se samo jedan od 16 bitova i to broadcast zastavica. Klijent postavlja ovu zastavicu kada ne zna svoju IP adresu i to je znak serveru ili DHCP relay agentu da pošalju odgovor kao broadcast

Client IP address: Koristi je klijent samo za vrijeme obnove najma IP adrese kada ima valjanu IP adresu i to je njegova IP adresa koju koristi. Inače ovo polje ima vrijednost 0.

Your IP Address: Koristi server kada dodjeljuje IP adresu klijentu

Server IP Address: Koristi server kada želi uputiti klijenta na server koji će klijent koristiti u nastavku procesa. To može biti isti ili neki drugi server. IP adresa servera koji šalje poruku nalazi se u opcionom polju „Server Identifier“

Gateway IP Address: Ovo polje se koristi kada DHCP server i klijent nisu na istom L2 segmentu. U tom slučaju se koristi DHCP Relay agent

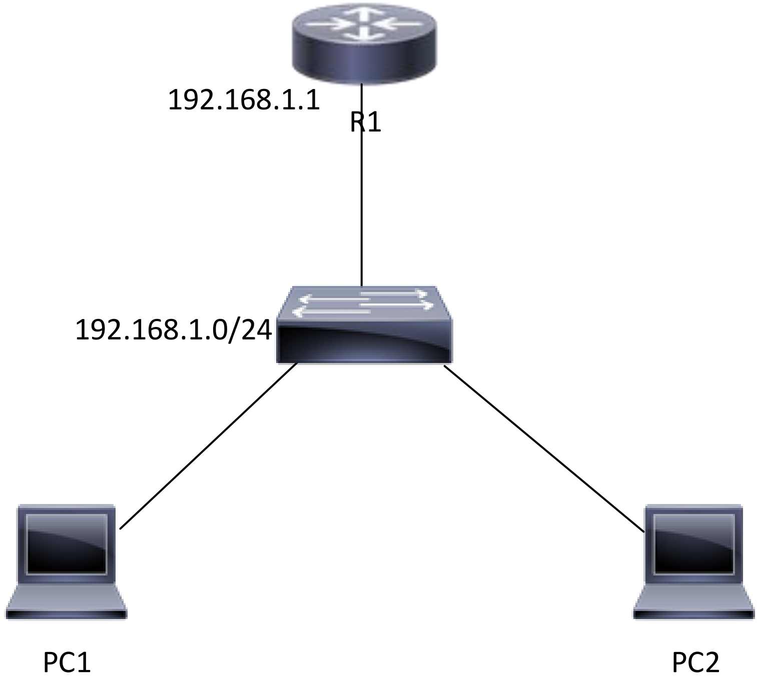
Client Hardwarea Address: Fizička adresa uređaja

Server name: Koriste DHCP serveri kada komuniciraju s klijentima. Može biti domensko ime servera

Boot Filename: Mogu koristiti klijenti ako im treba nekakva datoteka za podizanje sustava. Koristi se za IP telefone

DHCP Options: Ovo polje mogu koristiti i klijenti i serveri za različite opcionalne parametre

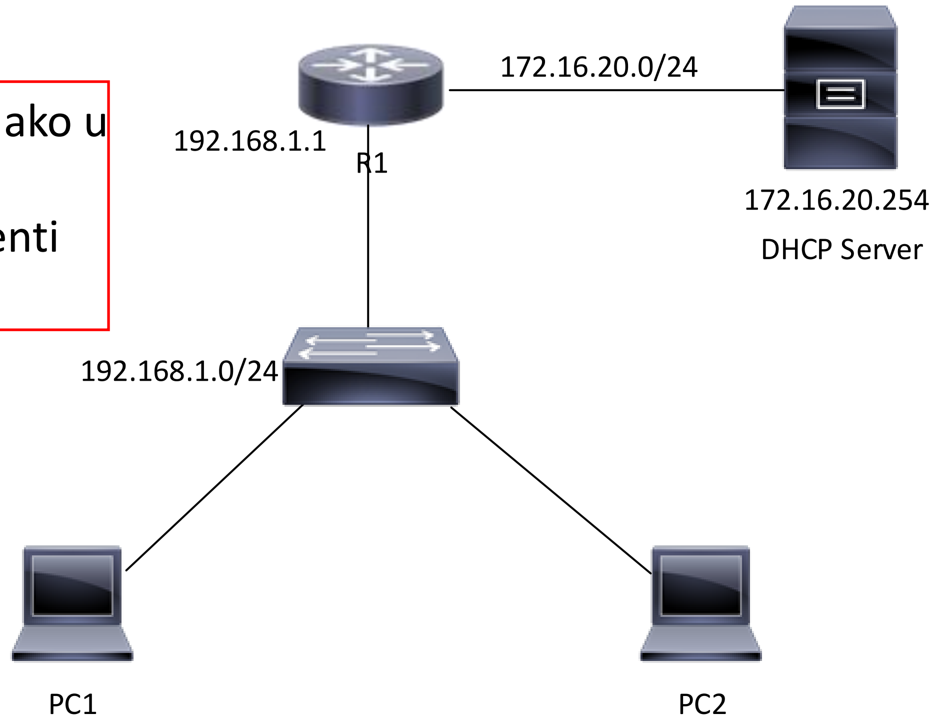
DHCP – konfiguracija



```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.10.100 192.168.10.254
R1(config)#ip dhcp pool LAN-POOL-1
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#option 150 ip 192.168.10.1
R1(dhcp-config)#end
```

DHCP – konfiguracija

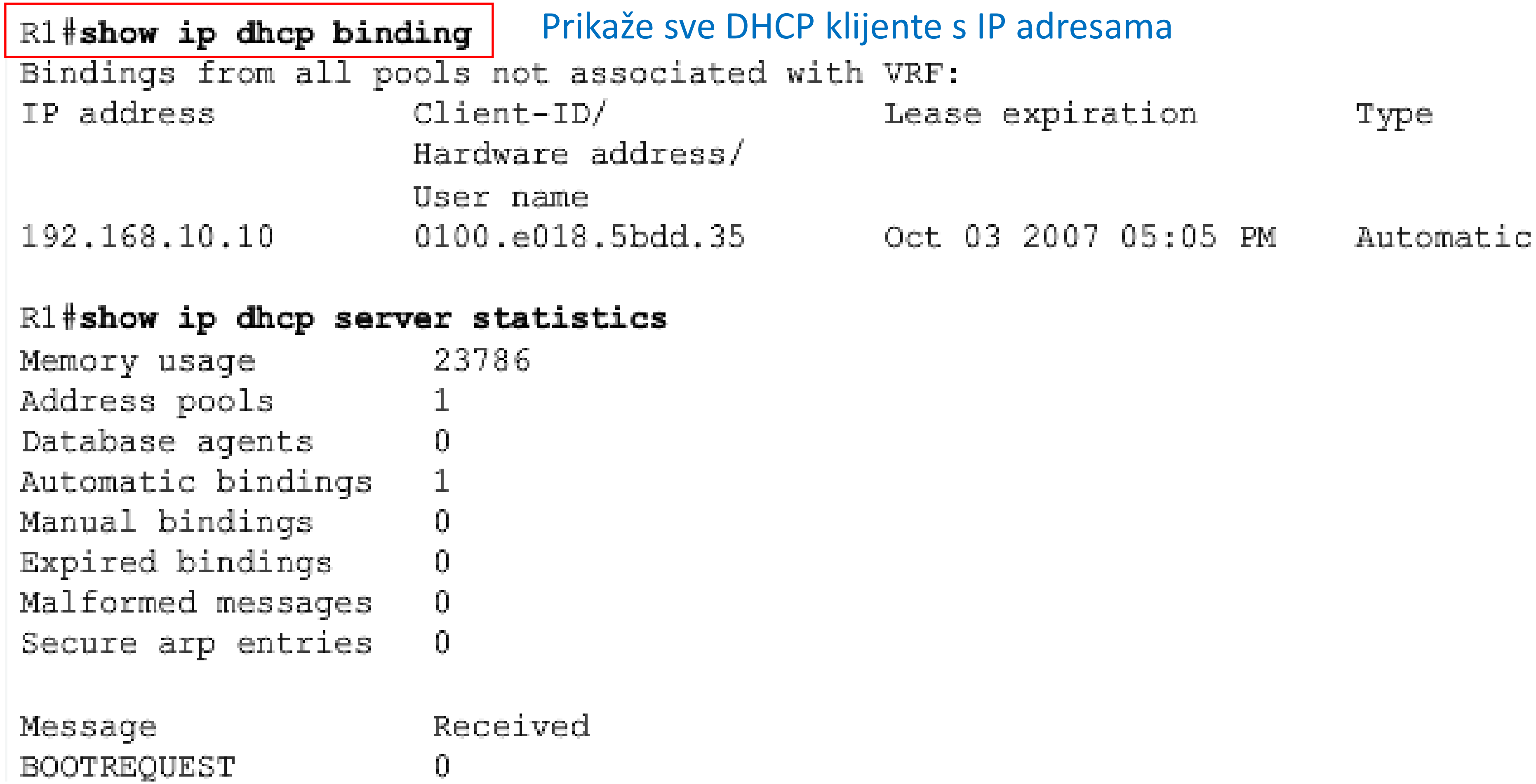
DHCP je broadcast promet, ako u L2 segmentu mreže
Ne postoji DHCP server klijenti neće dobiti IP adrese



```
R1(config)#interface fa 0/0
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#ip helper-address 172.16.20.254
R1(config-if)#exi
```

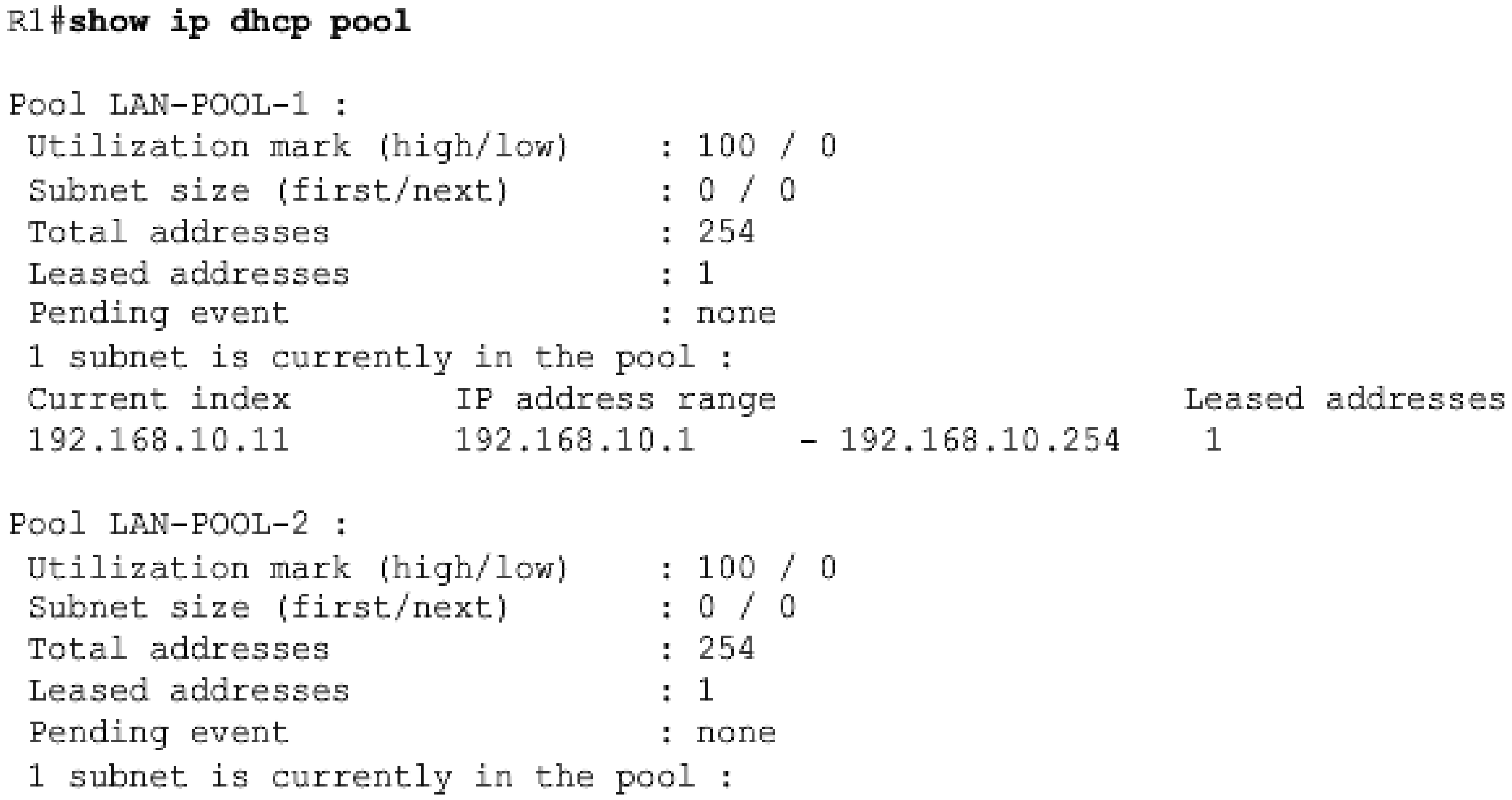
DHCP – verifikacija

Prikaže sve DHCP klijente s IP adresama



```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.10       0100.e018.5bdd.35       Oct 03 2007 05:05 PM    Automatic

R1#show ip dhcp server statistics
Memory usage         23786
Address pools        1
Database agents      0
Automatic bindings   1
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
```

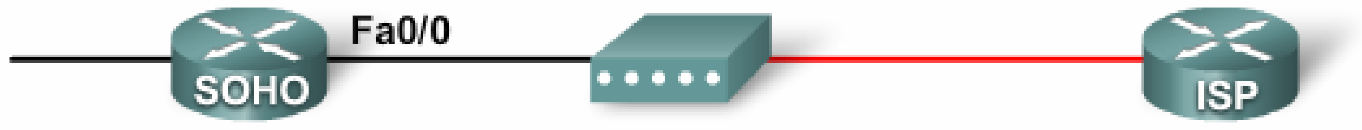
DHCP – verifikacija

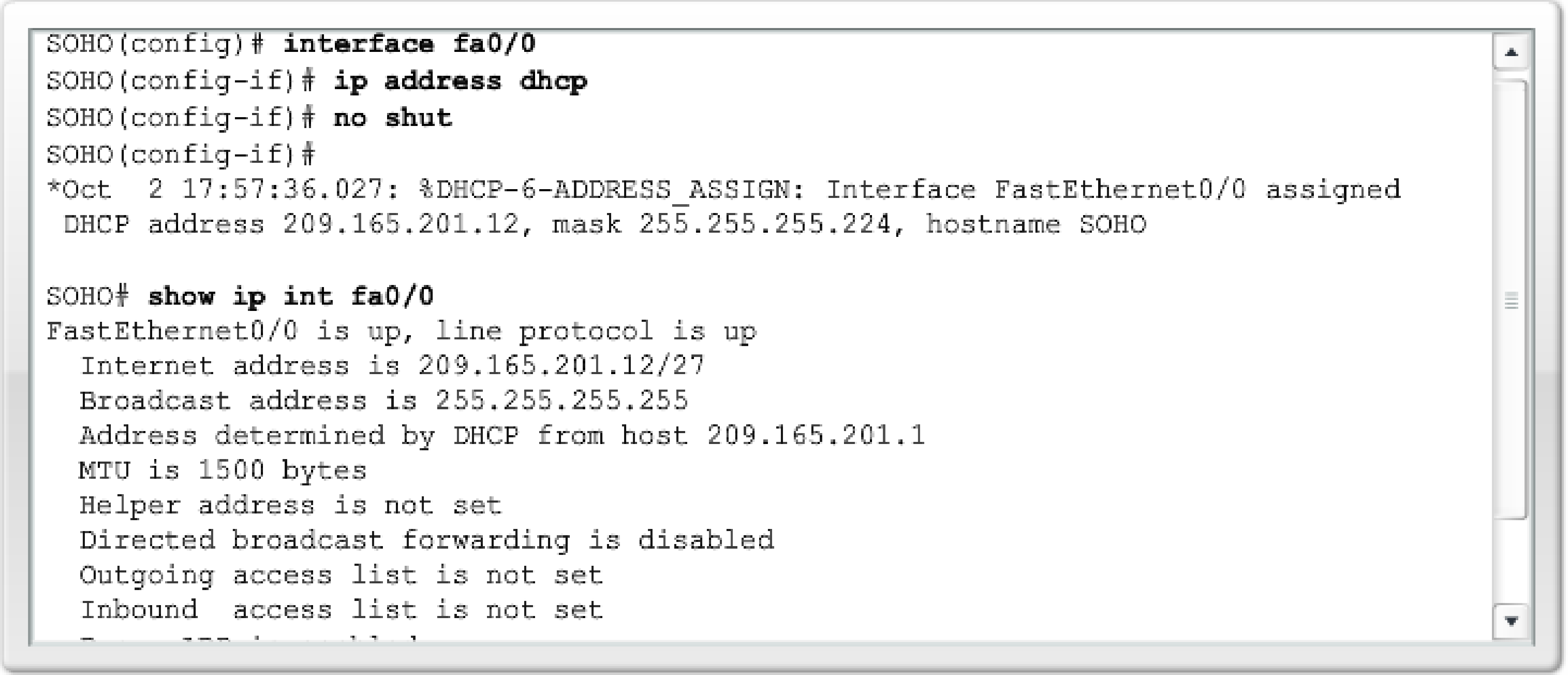


```
R1#show ip dhcp pool

Pool LAN-POOL-1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.10.11        192.168.10.1     - 192.168.10.254    1

Pool LAN-POOL-2 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
```

DHCP – usmjernik kao DHCP klijent

Configuring a DHCP Client





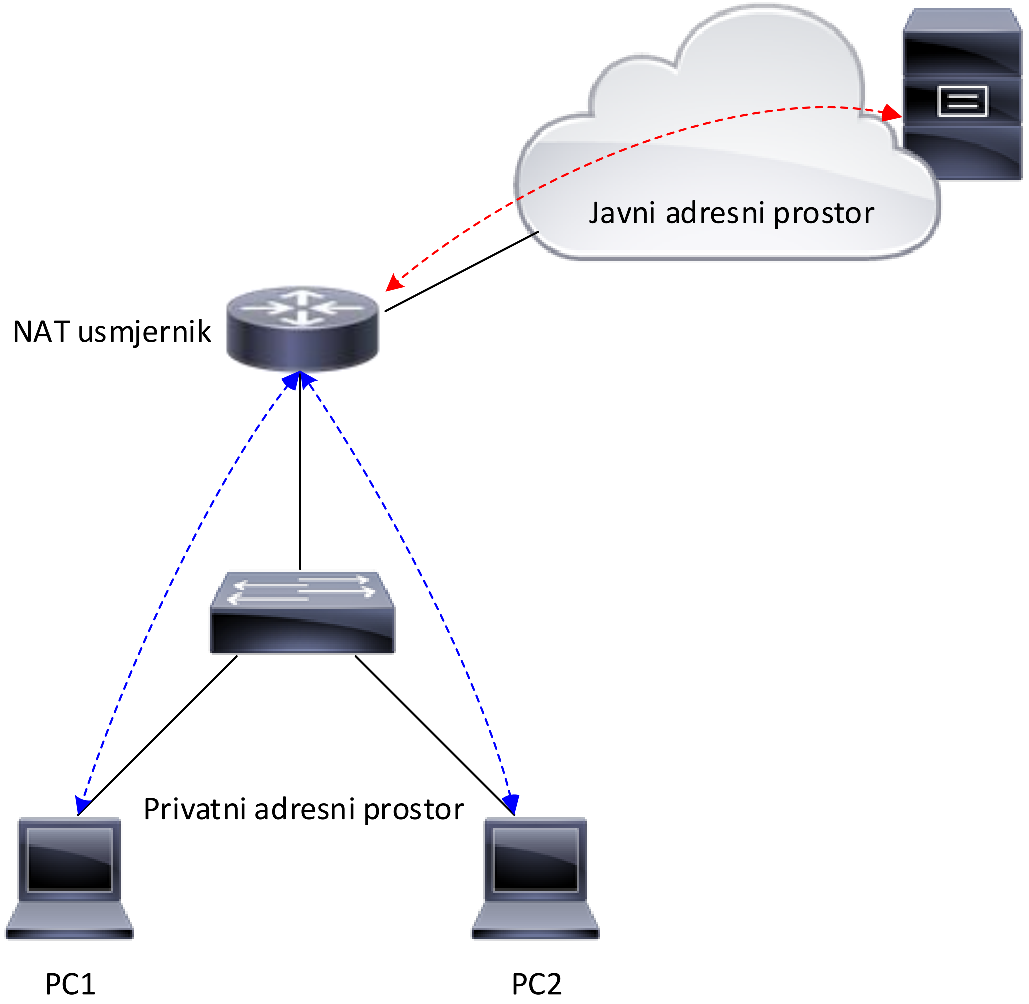
```
SOHO(config)# interface fa0/0
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shut
SOHO(config-if)#
*Oct  2 17:57:36.027: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
 DHCP address 209.165.201.12, mask 255.255.255.224, hostname SOHO

SOHO# show ip int fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP from host 209.165.201.1
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
```

DHCP – tshoot

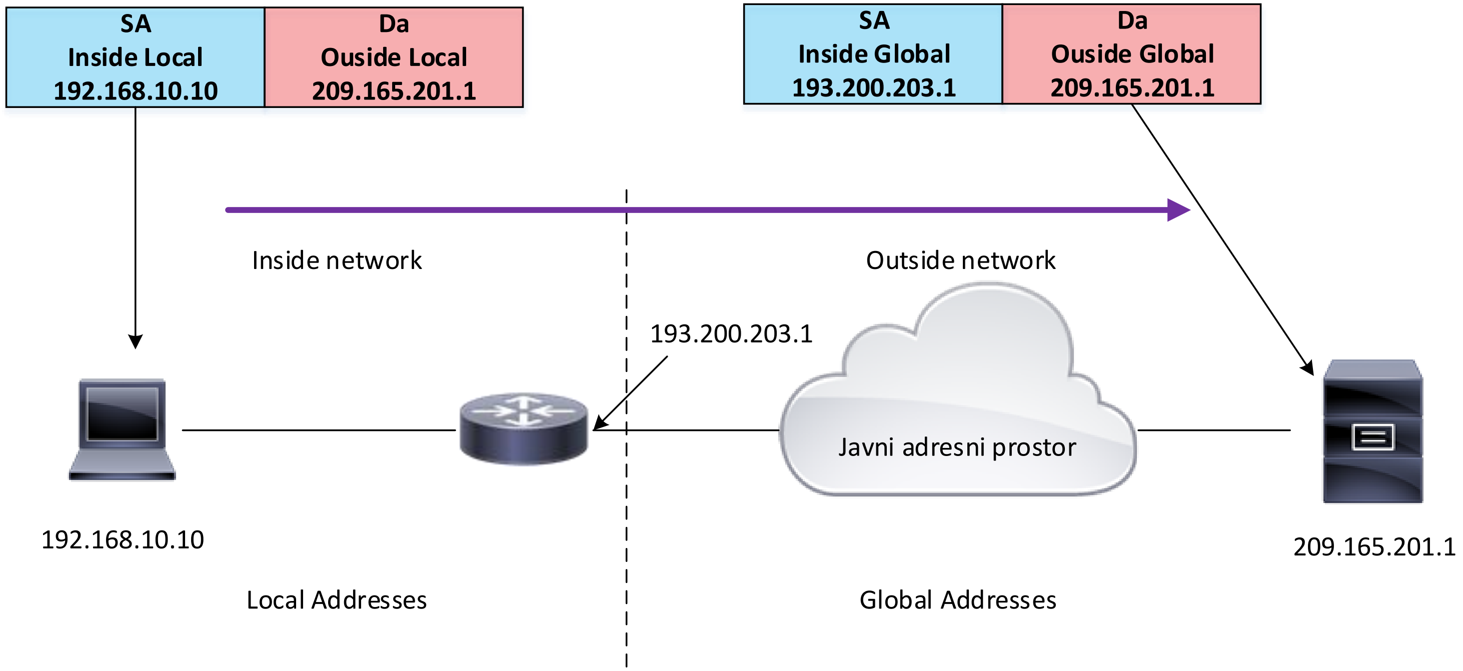
1. Rješavanje IP konflikata (iste IP adrese u mreži)
2. Provjera fizičke povezivosti (provjeriti ispravnost kabliranja, tip kabela i konektore)
3. Provjeriti funkcioniranje mreže konfiguriranjem statičke IP adrese
4. Provjeriti konfiguraciju sučelja na preklopnicima (STP portfast, sučelje je u pravom VLAN-u)

?

NAT – Network Address Translation

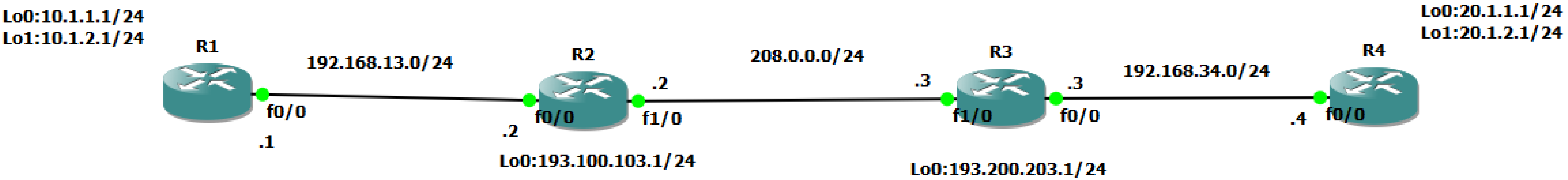


NAT – Network Address Translation



NAT prevodi bilo koje IP adrese u bilo koje druge (privatne ili javne svejedno)
Inside local= IP adresa unutar naše mreže koja će se prevoditi u neku javnu
Inside global= Naša javna IP adresa u koju se prevode naše privatne IP adrese
Outside global= Javna ip adresa hosta na Internetu
Outside Local= Adresa hosta na internetu kako je vide računala u našoj mreži (uglavnom je ista kao i Outside global, ali može biti i drugačija).

NAT – Outside Local



NAT – Outside Local

Na R2 konfiguriram NAT

```
ip nat inside source static 10.1.1.1 193.100.103.1
ip nat outside source static 193.200.203.1 192.168.12.2
```

zatim pingam s R1 koristeći source lo0

```
R1#ping 208.0.0.3 so lo 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 208.0.0.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/19/28 ms
```

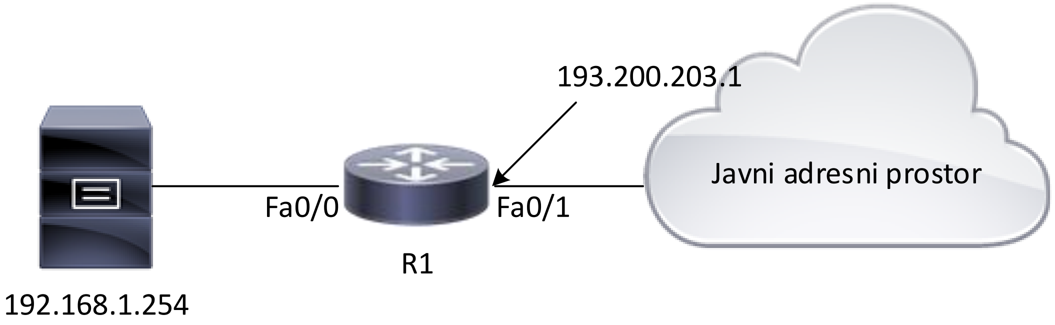
provjerim translacije na R2

```
R2#sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
--- ---                    ---           192.168.12.2       193.200.203.1
-193.100.103.1          10.1.1.1                   ---             ---
```

ovo je moguće samo ako radimo prevođenje neke javne IP adrese u neku našu privatnu koja je dostupna unutar naše mreže...dakle prevođenje u oba smjera.

"**Outside local address**—The IP address of an **outside host** **as it appears to the inside network.** Not necessarily a legitimate address, it is allocated **from an address space routable on the inside**."

NAT – statički NAT



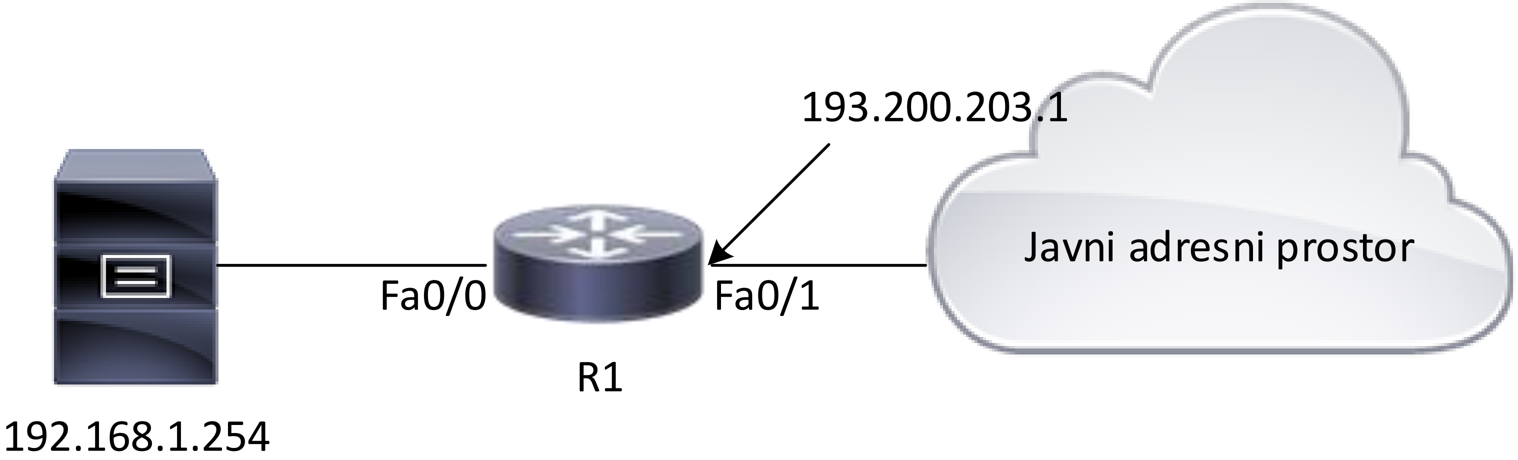
```
R1(config)#interface fa 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface fa 0/1
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat inside source static 192.168.1.254 89.100.200.254
```

Provjeru funkcionalnosti (telnet sa servera prema 8.8.8.8) radimo naredbom:

```
R1#show ip nat translations
Pro   Inside global             Inside local            Outside local      Outside global
tcp   89.100.200.254:1025       192.168.1.254:1025       8.8.8.8:23         8.8.8.8:23
```

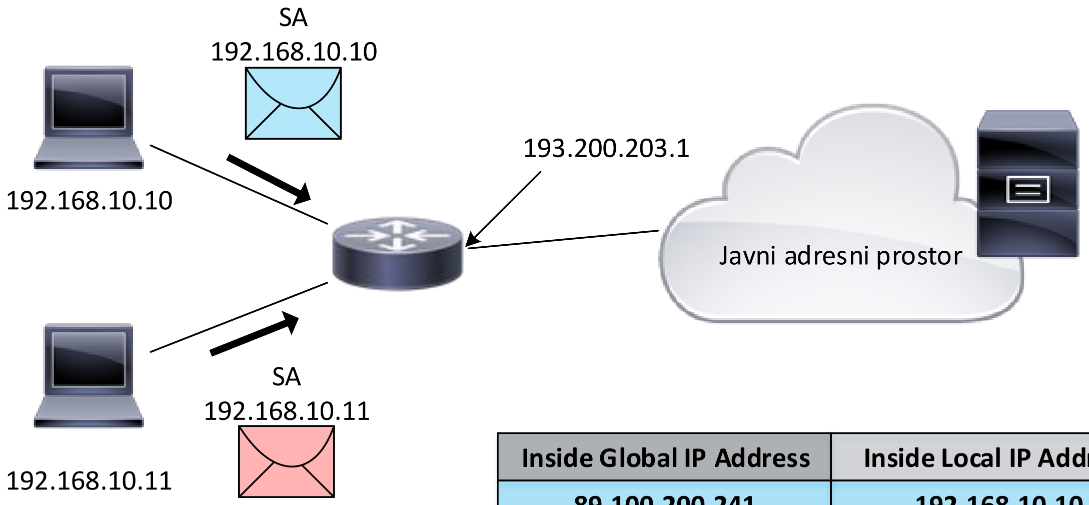
NAT – portforwarding

```
R1(config)#ip nat inside source static tcp 192.168.1.254 80 89.100.200.254 80
```



89.100.200.254 je javna IP adresa iz našeg adresnog prostora koji smo zakupili ili dobili na raspolaganje

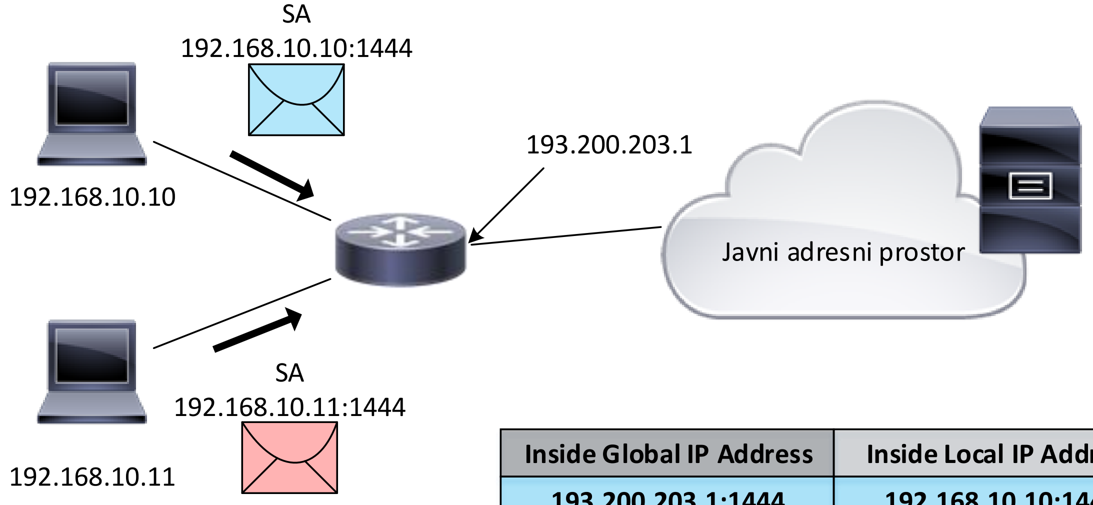
NAT – dinamički NAT



Inside Global IP Address	Inside Local IP Address
89.100.200.241	192.168.10.10
89.100.200.242	192.168.10.11

```
R1(config)#ip nat pool TEST_POOL 89.100.200.241 89.100.200.250 netmask 255.255.255.240
R1(config)#interface fa 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface fa 0/1
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 2 permit 192.168.10.0 0.0.0.255
R1(config)#ip nat inside source list 2 pool TEST_POOL
```

NAT – PAT (Port Address Translation)

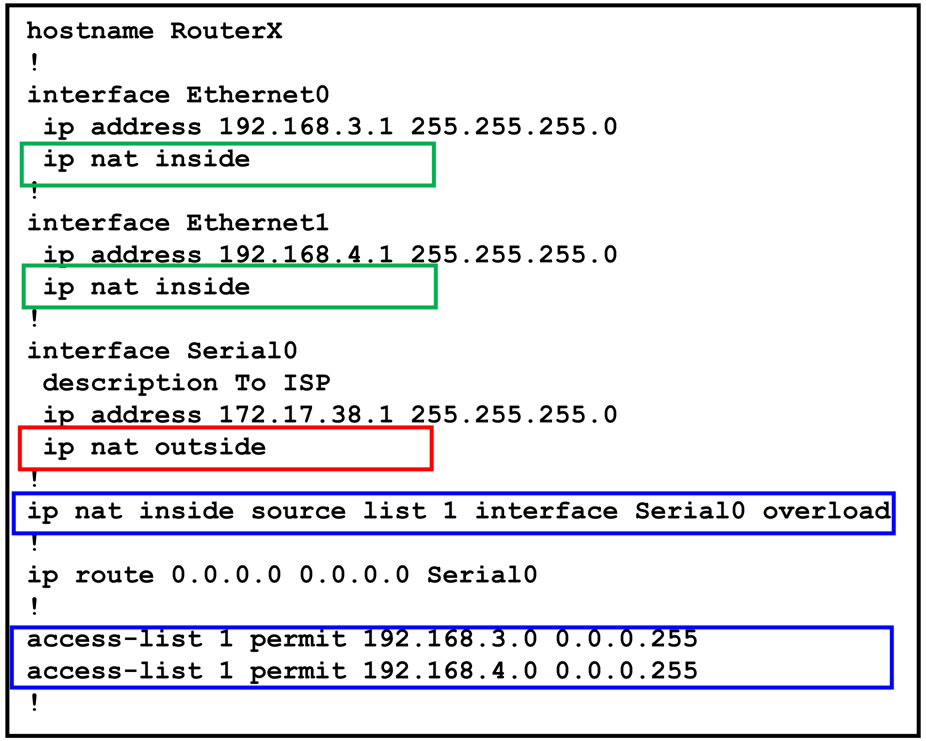


Inside Global IP Address	Inside Local IP Address
193.200.203.1:1444	192.168.10.10:1444
193.200.203.1:1445	192.168.10.11:1444

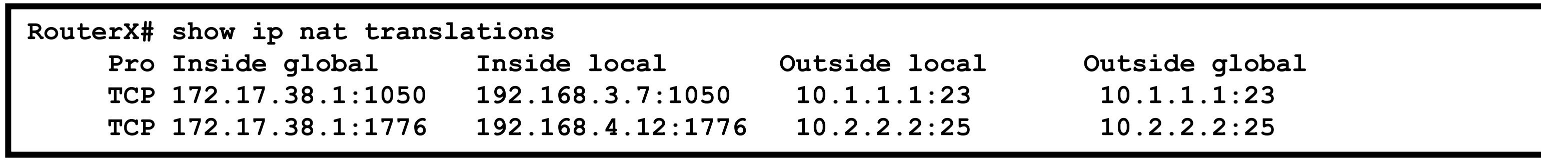
```
R1(config)#ip nat pool TEST_POOL 89.100.200.241 89.100.200.250 netmask 255.255.255.240
R1(config)#interface fa 0/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface fa 0/1
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 2 permit 192.168.10.0 0.0.0.255
R1(config)#ip nat inside source list 2 pool TEST_POOL overload
                ili
R1(config)#ip nat inside source list 2 interface serial 0/0/0 overload
```

PAT

NAT – running config



```
hostname RouterX
!
interface Ethernet0
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
!
interface Ethernet1
 ip address 192.168.4.1 255.255.255.0
 ip nat inside
!
interface Serial0
 description To ISP
 ip address 172.17.38.1 255.255.255.0
 ip nat outside
!
ip nat inside source list 1 interface Serial0 overload
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
!
```



```
RouterX# show ip nat translations
     Pro Inside global       Inside local         Outside local       Outside global
     TCP 172.17.38.1:1050   192.168.3.7:1050     10.1.1.1:23         10.1.1.1:23
     TCP 172.17.38.1:1776   192.168.4.12:1776    10.2.2.2:25         10.2.2.2:25
```

Univerzalna ACL za NAT

Ip access-list extended NAT_ACL

Deny ip any 10.0.0.0 0.255.255.255

Deny ip any 172.16.0.0 0.15.255.255

Deny ip any 192.168.0.0 0.0.255.255

Permit ip any any

Ove tvrdnje su potrebne da isključe iz NAT procesa sav promet koji bi trebao ići u VPN tunele

NAT – Brisanje translacija

```
RouterX# clear ip nat translation *
```

Brisanje svih dinamičkih translacija

```
RouterX# clear ip nat translation inside global-ip
local-ip [outside local-ip global-ip]
```

Brisanje pojedine translacije

```
RouterX# clear ip nat translation protocol inside global-ip
global-port local-ip local-port [outside local-ip
local-port global-ip global-port]
```

Brisanje pojedine PAT translacije

NAT – TSHOOT

Provjeriti:

- Da nema ACL na ulaznim interface-ima routera (ili da te ACL ne smetaju NAT-u)
- Da klasifikacijska ACL dozvoljava sve potrebne mreže (one koje trebaju ići u NAT)
- Da ima dovoljno adresa u NAT pool-u (ako je previše računala na jednu IP adresu moguće je da NAT ne radi kako očekujemo)
- Da su odgovarajući interface-i odabrani kao unutarnji (inside-mreže koje treba NAT-irati i te mreže se nalaze u ACL), odnosno vanjski (outside-npr..gdje se nalazi javna IP adresa u koju se prevode privatne)

NAT – Show i debug

```
RouterX# debug ip nat

NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23312]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
```

```
RouterX# show ip nat translations
```

```
RouterX# show ip nat statistics
      Total active translations: 1 (1 static, 0 dynamic; 0 extended)
      Outside interfaces:
      Ethernet0, Serial2
      Inside interfaces:
      Ethernet1
      Hits: 5  Misses: 0
      …
```

?

Hvala na pažnji!