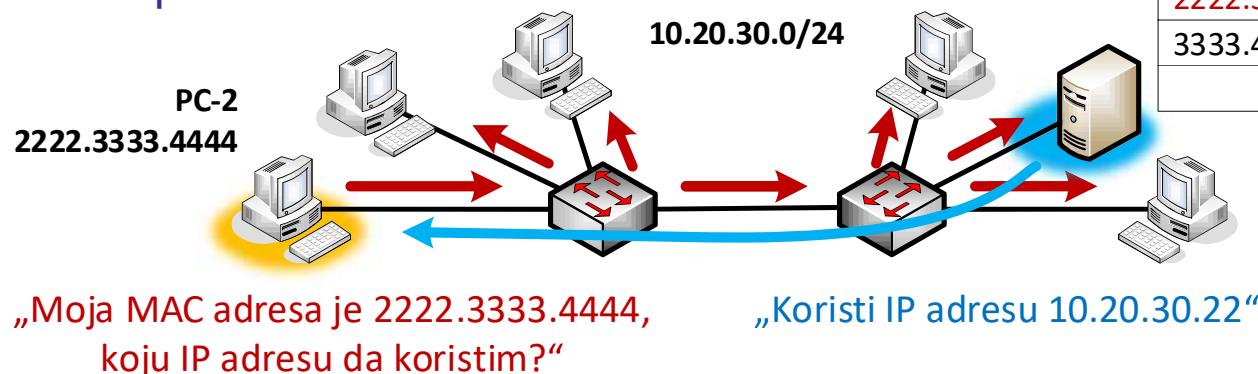


Dodela IP adresa

- IP adresa, maska i *default gateway* se dodeljuje svakom uređaju u IP mreži
- **Statičko dodeljivanje IP adresa**
 - Manuelno dodeljivanje fiksnih IP adresa
 - Konfiguracija sa svakom uređaju
 - Mogućnost grešaka – preklapanje adresa, pogrešna maska
 - Nefleksibilno – promena maske ili *default gateway*-a – mora na svim uređajima
 - Ne mogu se podržati privremeni (*ad-hoc*) korisnici – WiFi, VPN itd.
- **Dinamičko dodeljivanje IP adresa**
 - Automatsko dodeljivanje IP adrese, maske i *default gateway*
 - Konfiguracija na jednom mestu – serveru (određeni opseg IP adresa)
 - Smanjena mogućnost greške
 - Fleksibilno rešenje
 - Korisnik ne mora da bude poznat unapred – WiFi, VPN itd.
- Protokoli automatske dodele adresa
 - RARP – *Revers Address Resolution Protocol*
 - BOOTP – *BOOTstrap Protocol*
 - DHCP – *Dynamic Host Configuration Protocol*

RARP - Reverse ARP

- Prvobitni protokol dodele IP adresa, RFC 903, 1984.
- Obrnuta (reversna) uloga u odnosu na ARP protokol:
 - ARP – nalazi se MAC adresu na osnovu IP adrese
 - RARP – nalazi se IP adresu na osnovu MAC adrese
- Inicijalno je bio namenjen za specifične uređaje i radne stanice bez diska (*diskless*)
 - Operativni sistem i parametri (IP adresa) su se preuzimali sa servera
- RARP server
 - Manuelno se definiše mapiranje MAC adresa u određene IP adrese
 - Radne stanice po uključivanju pronađuju RARP server
 - RARP server na osnovu MAC adrese uređaja pronađuje uparenu IP adresu



ARP/RARP format zaglavlja

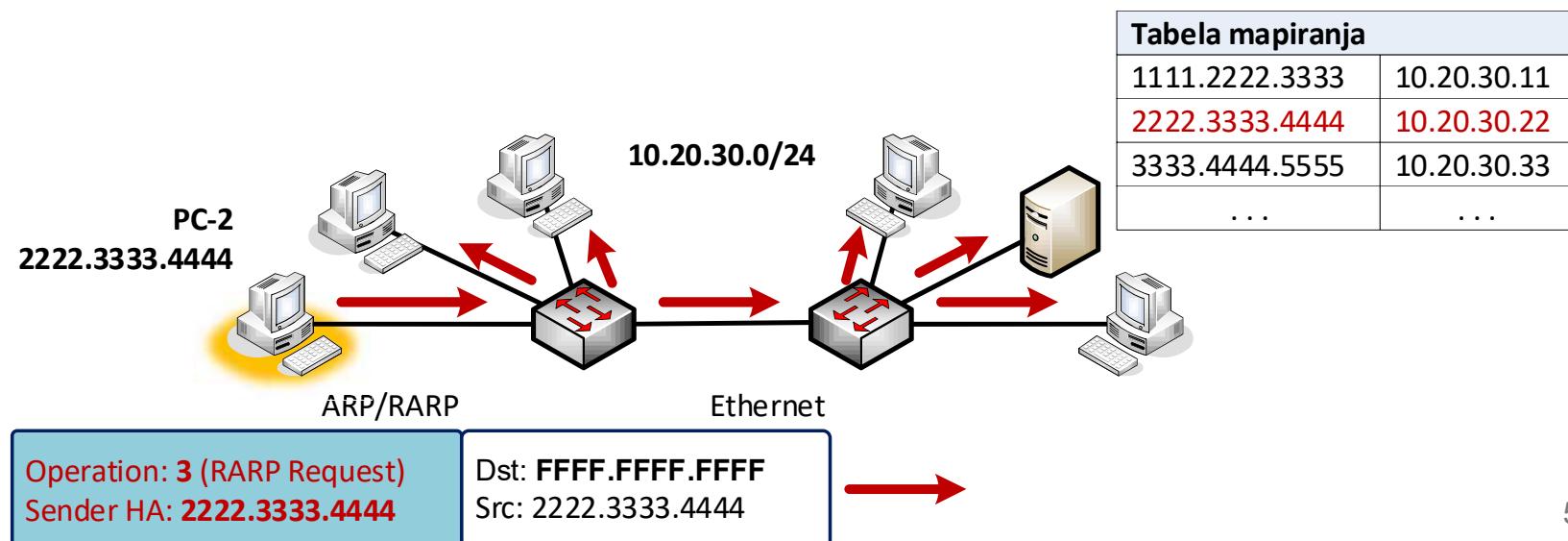
- Protokol L3 nivoa
 - Poruke se enkapsuliraju u Ethernet okvire
- Format zaglavlja – isti kao kod ARP-a
- Polje *Operation* – određuje ARP ili RARP funkcije
 - „1“ – ARP Request
 - „2“ – ARP Reply
 - „3“ – RARP Request
 - „4“ – RARP Reply

1. bajt	2. bajt	3. bajt	4. bajt
Hardware Type		Protocol Type (0x0800)	
HLEN	PLEN	Operation	
Sender HA (1..4)			
Sender HA (5..6)		Sender IP (1..2)	
Sender IP (3..4)		Target HA (0..1)	
Target HA (3..6)			
Target IP (1..4)			

RARP – princip rada

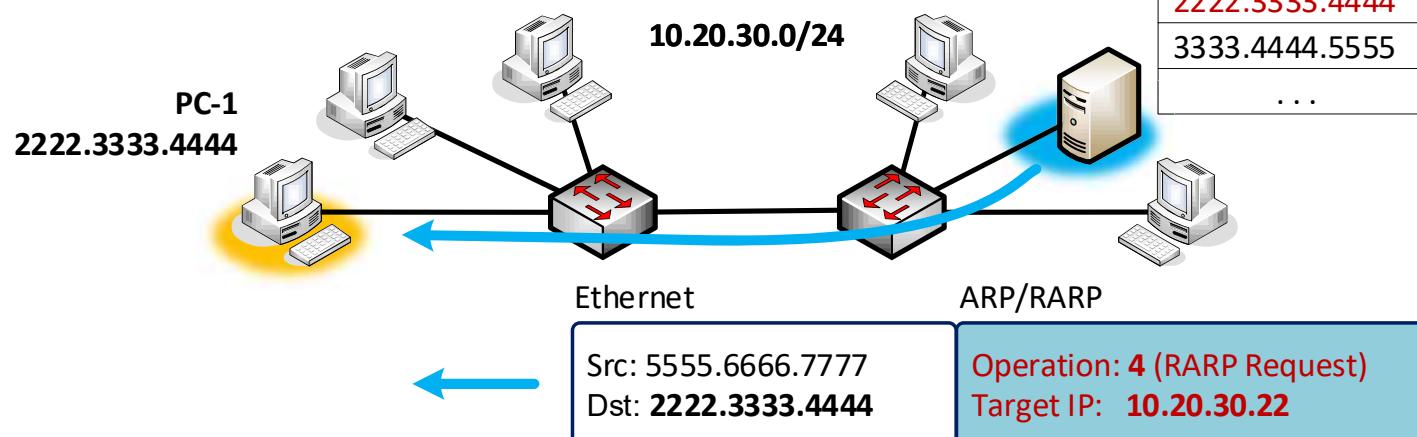
- **1. korak – RARP Request**

- Uređaj po uključivanju generiše RARP Request paket
 - paket se šalje na MAC brodcast adresu (FFFF.FFFF.FFFF)
- Svi uređaji primaju RARP Request paket
 - Samo ga RARP server prepoznaće, ostali ga odbacuju
- RARP server
 - Na osnovu MAC adrese u tabeli definicija mapiranja nalazi IP adresu



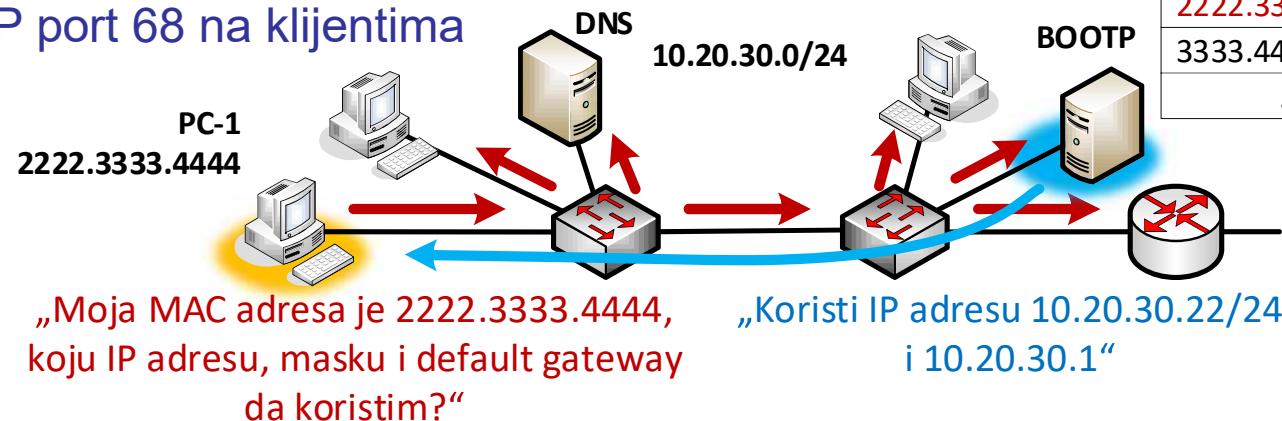
RARP – princip rada

- **2. korak – RARP Reply**
 - RARP server generiše odgovor – RARP *Reply* paket
 - Paket sadrži dodeljenu IP adresu
 - Paket se šalje na unikast MAC adresu uređaja koji je inicirao zahtev
 - Uređaj koji je inicirao zahtev prihvata paket, uzima IP adresu i počinje da je koristi
- Osnovni nedostaci
 - Ne dodeljuje se maska i *Default Gateway*
 - Komunikaciju samo na nivou L2 segmentu, ne i sa drugim mrežama



BOOTP - *Bootstrap Protocol*

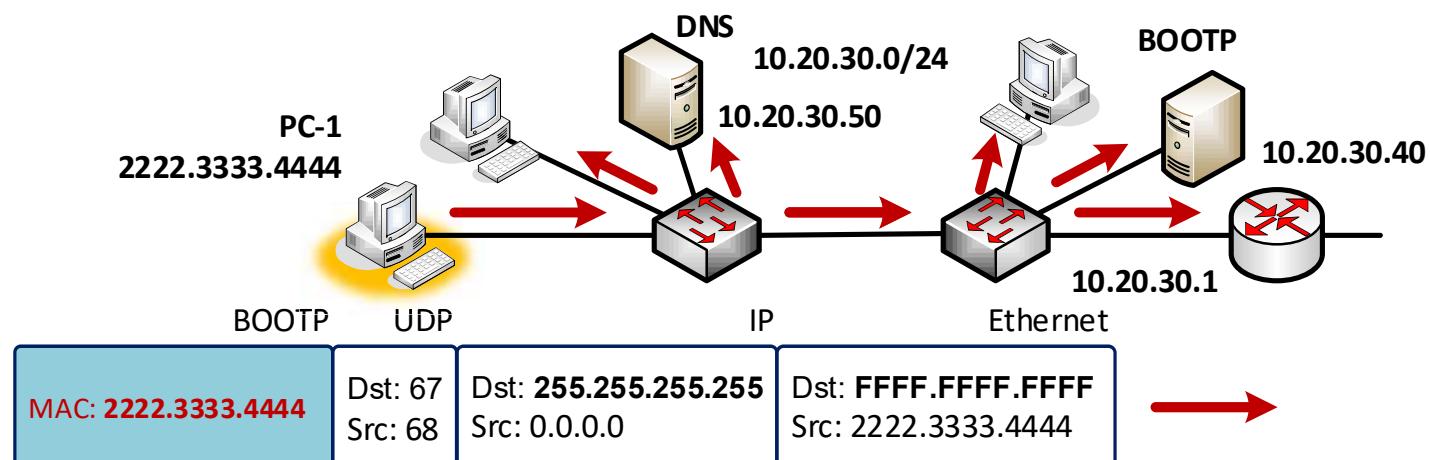
- BOOTP - *Bootstrap Protocol*, RFC 951, 1985
- Dodeljivanje IP adrese na osnovu MAC adrese (namena kao i RARP)
- BOOTP server
 - Manuelno se definiše mapiranje MAC adresa u određene IP adrese
- Dodatno, BOOTP može da pošalje i:
 - *Default Gateway*
 - Masku
 - DNS server itd.
- Protokol aplikativnog nivao, koristi UDP
 - UDP port 67 na serveru
 - UDP port 68 na klijentima



BOOTP – princip rada

• Korak 1 - BOOT-REQUEST poruka

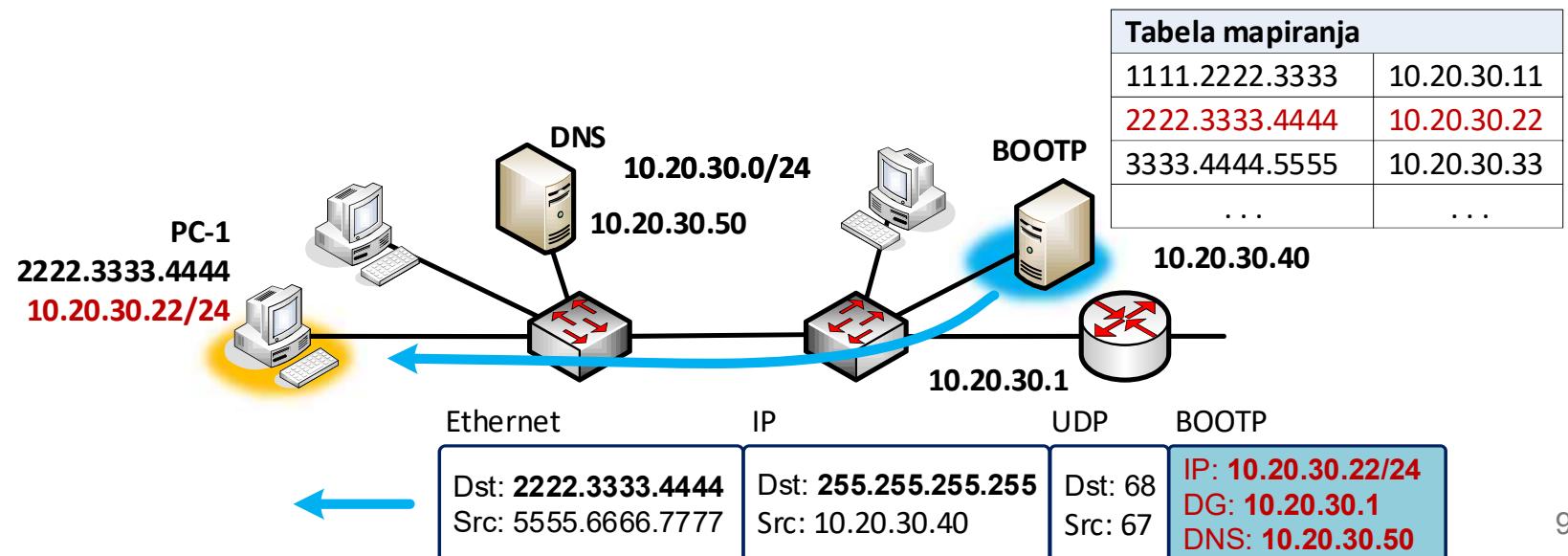
- Uređaj po uključivanju generiše BOOT-REQUEST poruku
 - Sadrži MAC adresu pošiljaoca
 - Enkapsulira se u UDP poruku, odredišni port 67
 - UDP se enkapsulira u IP poruku, brodcast odredišna IP adresa
 - IP se enkapsulira u Ethernet okvir, brodcast odredišna MAC adresa
- Svi uređaji primaju BOOT-REQUEST paket na L2 i L3 nivou, prosleđuju ga na L4 nivo
- BOOTP server preuzima poruku na UDP portu 67, ostali je odbacuju



BOOTP – princip rada

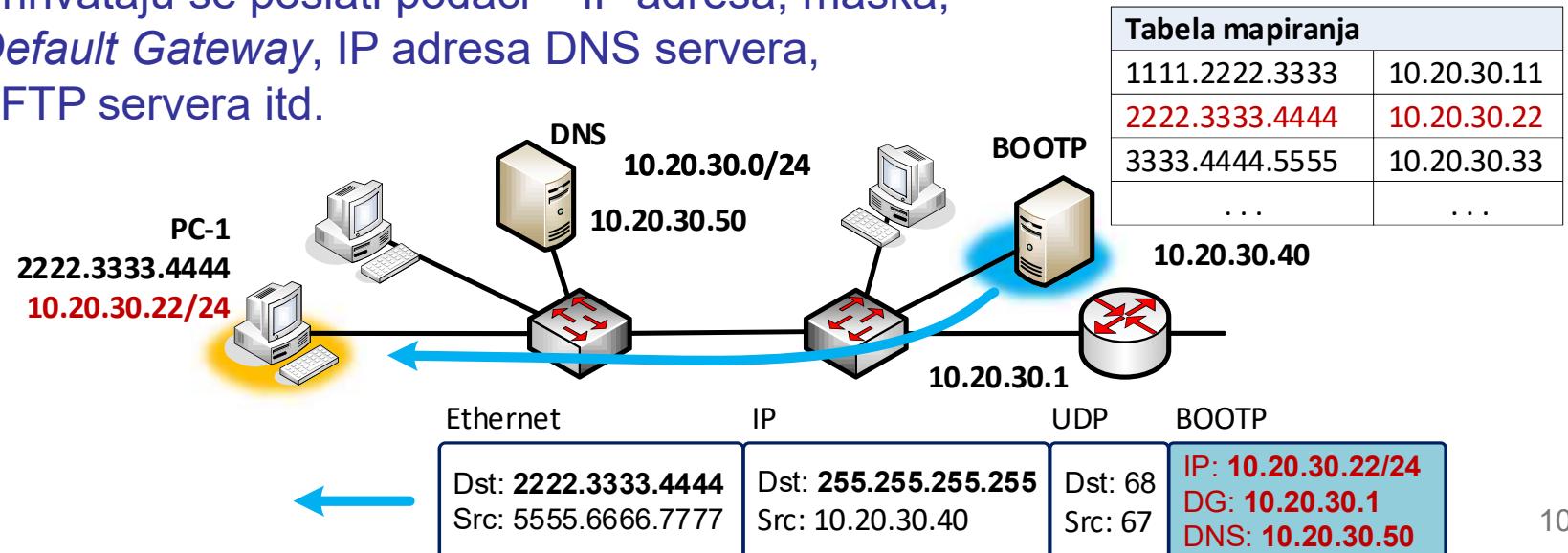
• Korak 2 - BOOT-REPLY poruka

- BOOTP server za MAC adresu se iz tabele mapiranja nalazi IP adresu
- Kreira se BOOT-REPLY poruka, koja sadrži:
 - Dodeljenu IP adresu i masku uređaja
 - *Default Gateway*
 - IP adresu DNS servera
 - IP adresu TFTP servera (*Trivial File Transfer Protocol*) itd.



BOOTP – princip rada

- **Korak 2 (nastavak)**
 - BOOT-REPLY poruka
 - Enkapsulira se u UDP poruku, odredišni port 68
 - UDP se enkapsulira u IP poruku, brodcast odredišna IP adresa
 - IP se enkapsulira u Ethernet okvir, unikast odredišna MAC adresa uređaja
 - Svi primaju poruke na L2 i L3 nivou
 - Samo odredišni uređaj „sluša“ na UDP portu 68
 - Ne može da se koristi slučajno izabrani klijentski port, jer bi on mogao da se javi i na drugim uređajima, pa bi poruke mogle da završe i na njima
 - Prihvataju se poslati podaci – IP adresa, maska, *Default Gateway*, IP adresa DNS servera, TFTP servera itd.



BOOTP

- Osnovni nedostatak
 - Statičko dodeljivanje IP adresa na osnovu MAC adresa
- Posledice:
 - Potrebno je unapred poznavati MAC adrese korisnika
 - Manuelna konfiguracija za sve korisnike
 - Mapiranje “1-na-1”
 - Permanentna dodatak adresa
 - Ne mogu se podržati privremeni (*ad-hoc*) korisnici
 - Wireless, VPN...

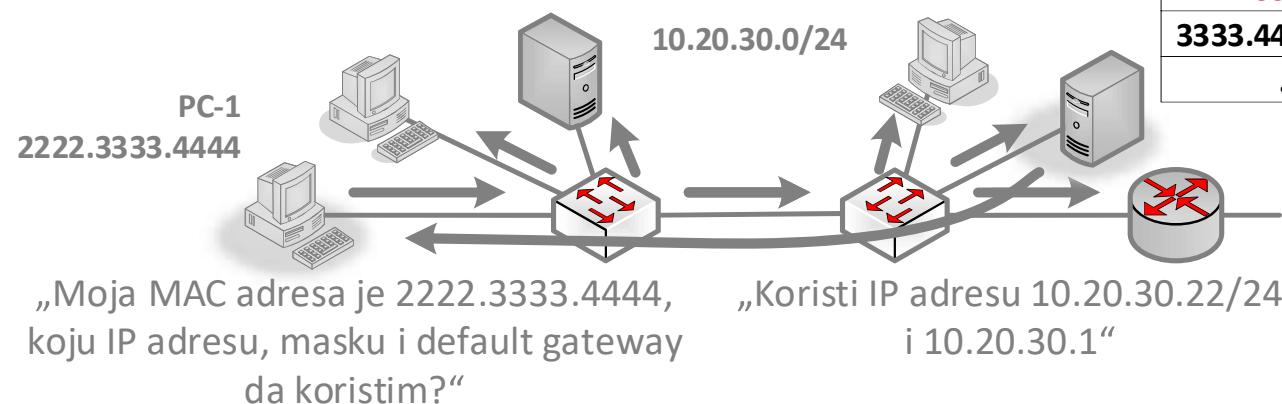
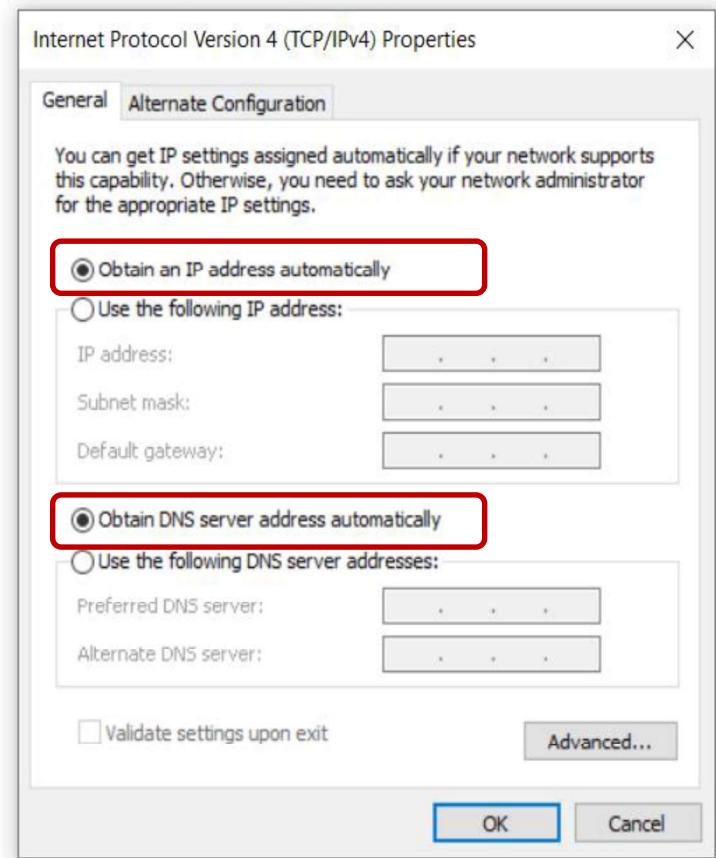


Tabela mapiranja	
1111.2222.3333	10.20.30.11
2222.3333.4444	10.20.30.22
3333.4444.5555	10.20.30.33
...	...

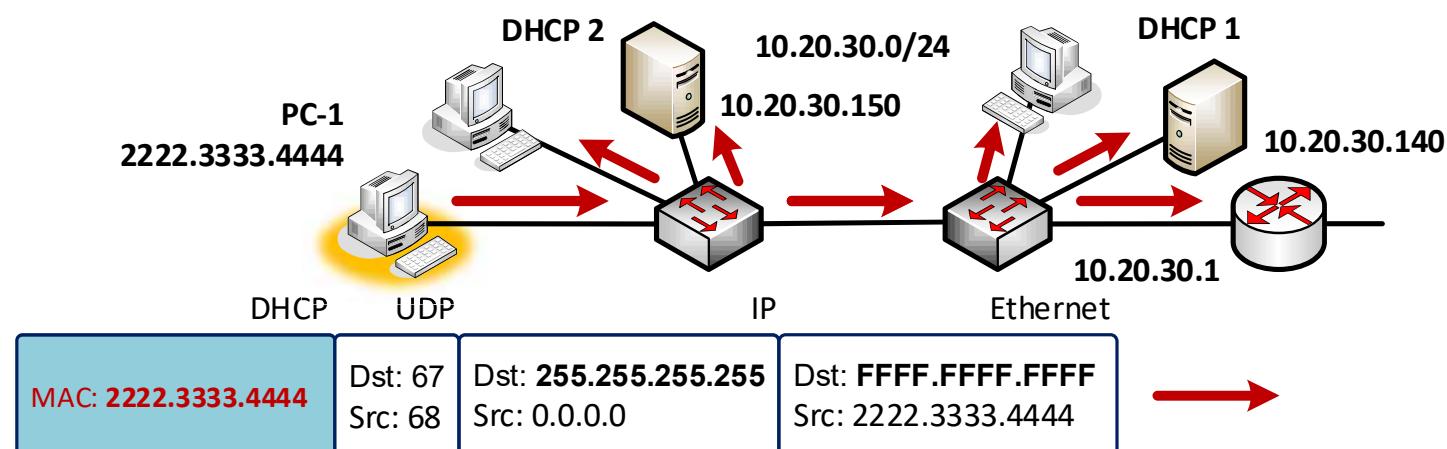
DHCP

- DHCP - *Dynamic Host Configuration Protocol*
 - Unapređena varijanta BOOTP protokola
 - Sličnosti sa BOOTP
 - UDP portovi 67 i 68
 - Sličan format poruka
 - Slanje dodatnih parametara
 - Razlike u odnosu na BOOTP
 - **Dinamičko dodeljivanje IP adresa iz predefinisanog opsega**
 - Ograničen vremenski period važenja
 - Osim adrese i maske, može se dodeliti preko 20 različitih parametara
 - *Default Gateway*
 - DNS server
 - WINS naziv (*Windows Internet Name Service*)
 - itd.
 - Može da postoji više DHCP servera na jednoj mreži
 - DHCP proces u 4 koraka



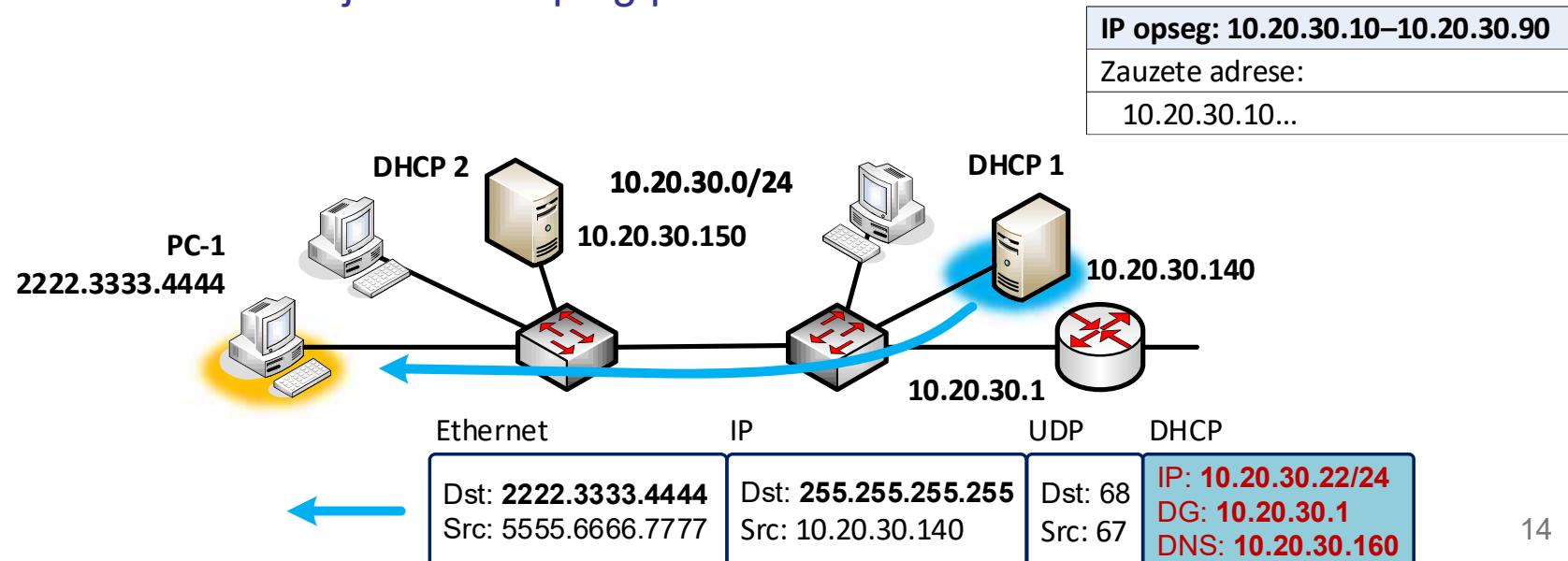
DHCP – princip rada

- 1. korak – **DHCP-DISCOVER** poruka
 - Uredaj po uključivanju generiše **DHCP-DISCOVER** poruku
 - Sadrži MAC adresu pošiljaoca
 - Enkapsulira se u UDP poruku, odredišni port 67
 - UDP se enkapsulira u IP poruku, brodcast odredišna IP adresa
 - IP se enkapsulira u Ethernet okvir, brodcast odredišna MAC adresa
 - Svi uređaji primaju DHCP-DISCOVER paket na L2 i L3 nivou, prosleđuju ga na L4 nivo
 - Svi DHCP serveri preuzimaju poruku na UDP portu 67, ostali je odbacuju



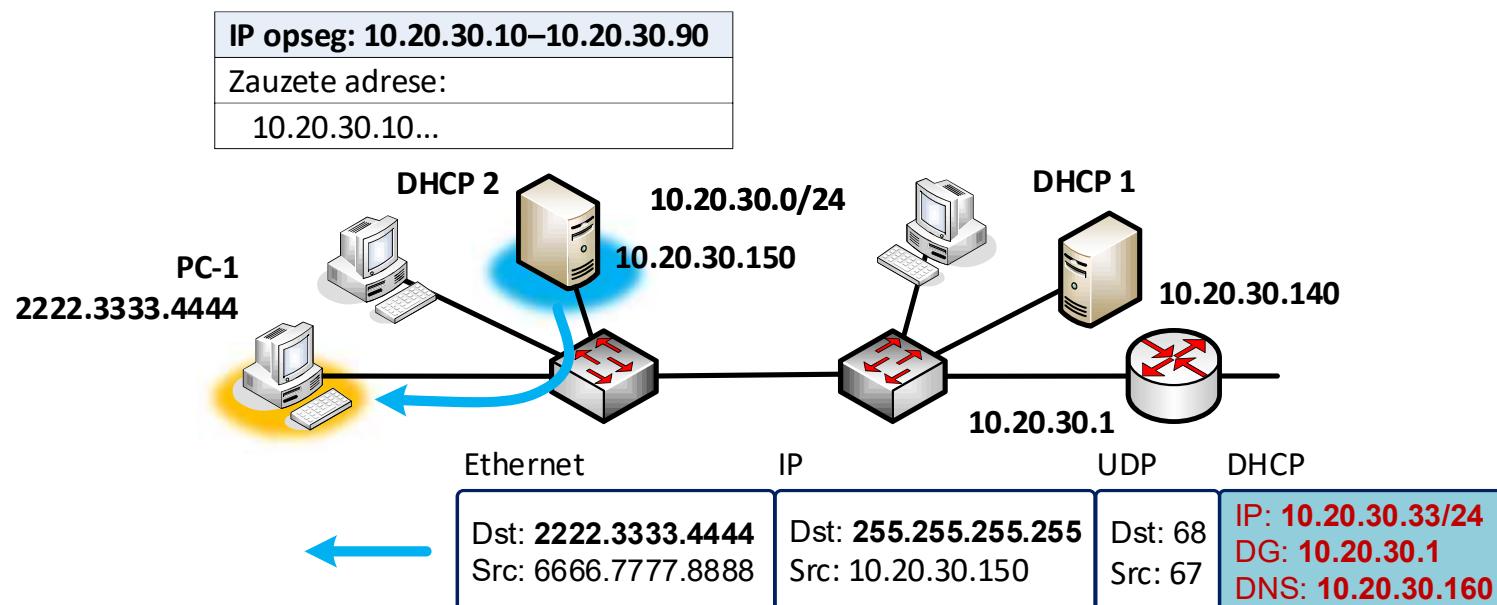
DHCP – princip rada

- 2. korak – **DHCP-OFFER** poruka
 - DHCP server sprovodi sledeće:
 - Dodeljuje slobodnu IP adresu iz opsega rezervisanih IP adresa
 - Generiše se **DHCP-OFFER** poruku:
 - Izabrana IP adresa, maska, *default gateway*, DNS
 - Drugi opcioni parametri - TFTP server, WINS...
 - Poruka se enkapsulira u UDP paket, IP brodkast paket i MAC okvir (brodkast ili unikast, u zavisnosti od implementacije, fleg polja i drugih uslova)
 - DHCP server može da proveri da li je neka adresa zauzeta slanjem ICMP ping paketa



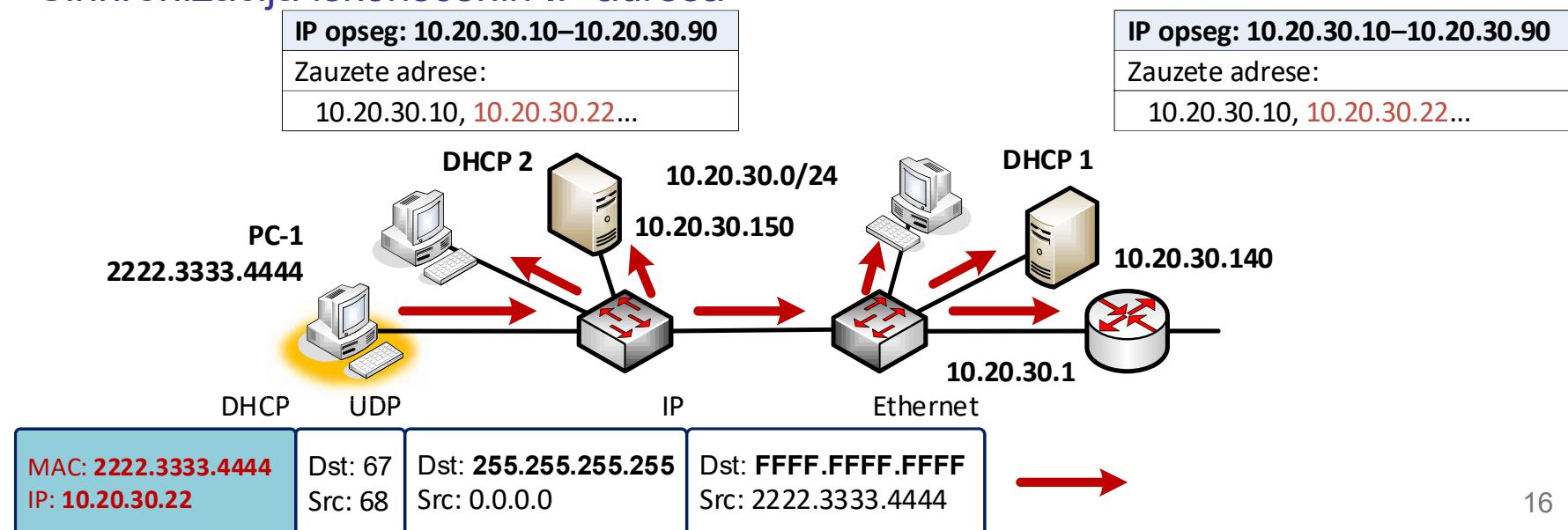
DHCP – princip rada

- 2. korak – **DHCP-OFFER** poruka
 - Drugi DHCP server (ako postoji)
 - Na isti način šalje svoju **DHCP-OFFER** poruku
 - Nezavisno bira slobodnu IP adresu, koja može da bude različita
 - Samo početni uređaj prima okvire i preuzima DHCP-OFFER poruku



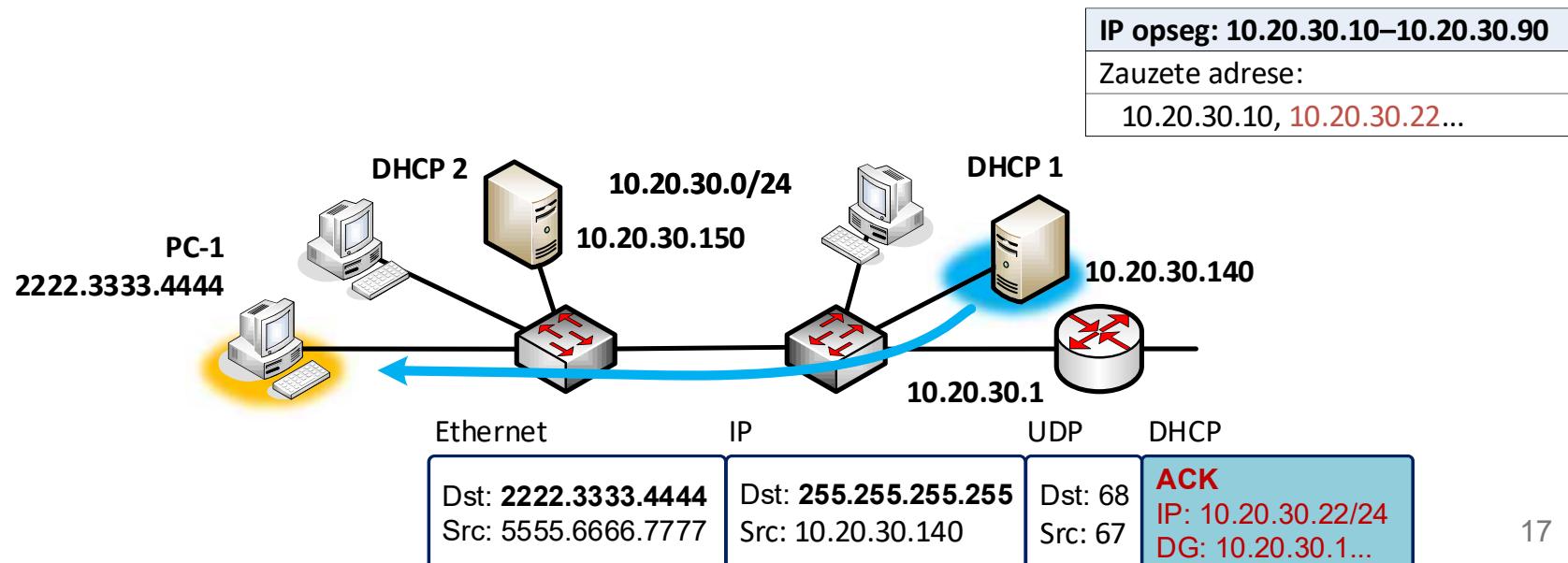
DHCP – princip rada

- 3. korak - **DHCP-REQUEST** poruka
 - Početni uređaj prihvata IP adresu iz prve DHCP-OFFER poruke
 - **DHCP-REQUEST** poruka:
 - Sadrži IP adresu koja se zahteva za korišćenje, kao i ostale parametre
 - Enkapsulira se u UDP poruku, odredišni port 67
 - UDP se enkapsulira u IP poruku, brodcast odredišna IP adresa
 - IP se enkapsulira u Ethernet okvir, brodcast odredišna MAC adresa
- Oba DHCP servera prihvataju DHCP-REQUEST poruku
 - Sinhronizacija iskorišćenih IP adresa



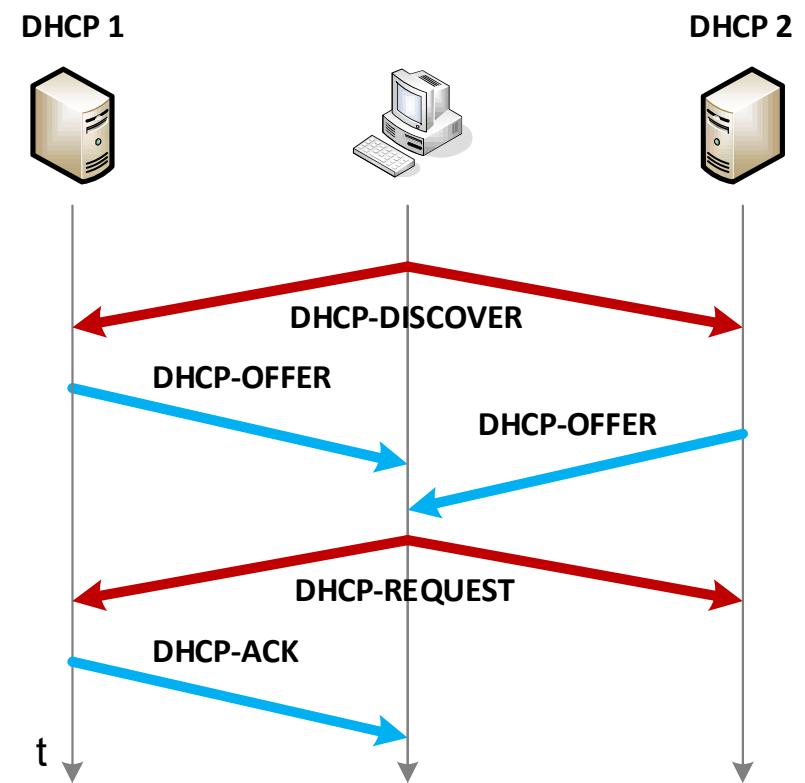
DHCP – princip rada

- 4. korak – **DHCP-ACK** poruka
 - Svi DHCP serveri prihvataju DHCP-REQUEST poruku
 - Samo DHCP server koji je ponudio zahtevanu IP adresu generiše potvrdu – **DHCP-ACK** poruka
 - Poruka se šalje na brodcast IP adresu, unikast ili brodcast na L2 nivou, (u zavisnosti od implementacije, pojedinih opcija iz fleg polja i drugih uslova)
 - IP adresa se označava kao iskorišćena (na određeno vreme)
 - Početni uređaj prihvata DHCP-ACK poruku
 - Počinje da koristi dobijene parametre



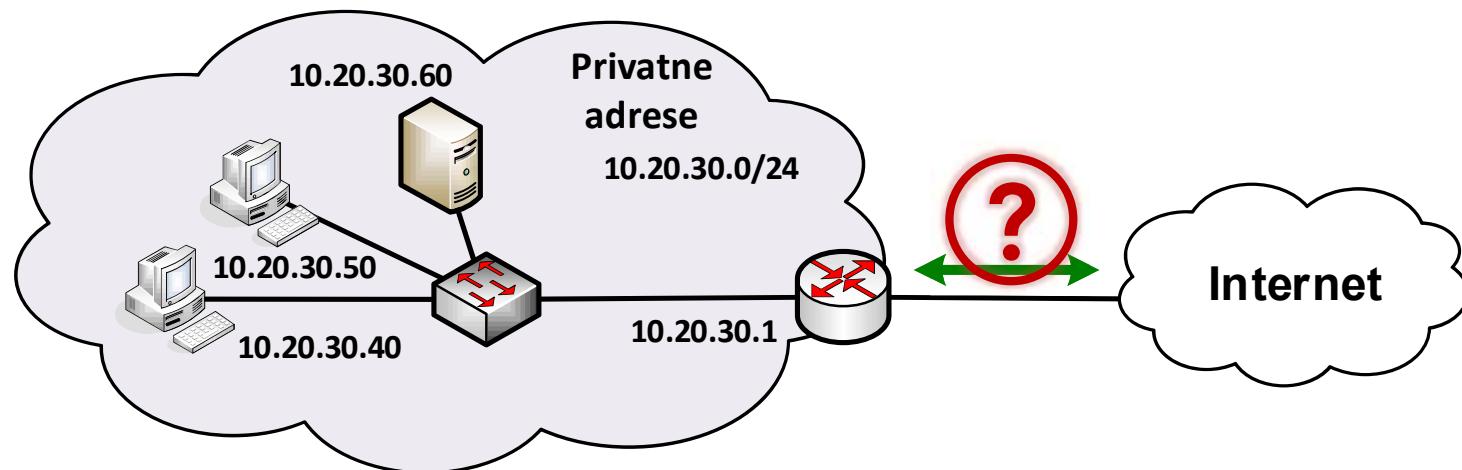
DHCP – princip rada

- 4. koraka
 1. DHCP-DISCOVER (brodcast)
 2. DHCP-OFFER (unicast)
 3. DHCP-REQUEST (brodcast)
 4. DHCP-ACK (unicast ili brodcast)
- Implementacija
 - DHCP serveri
 - Na istoj LAN mreži (brodcast domen)
 - DHCP na ruteru
 - Za sve pripadajuće LAN mreže



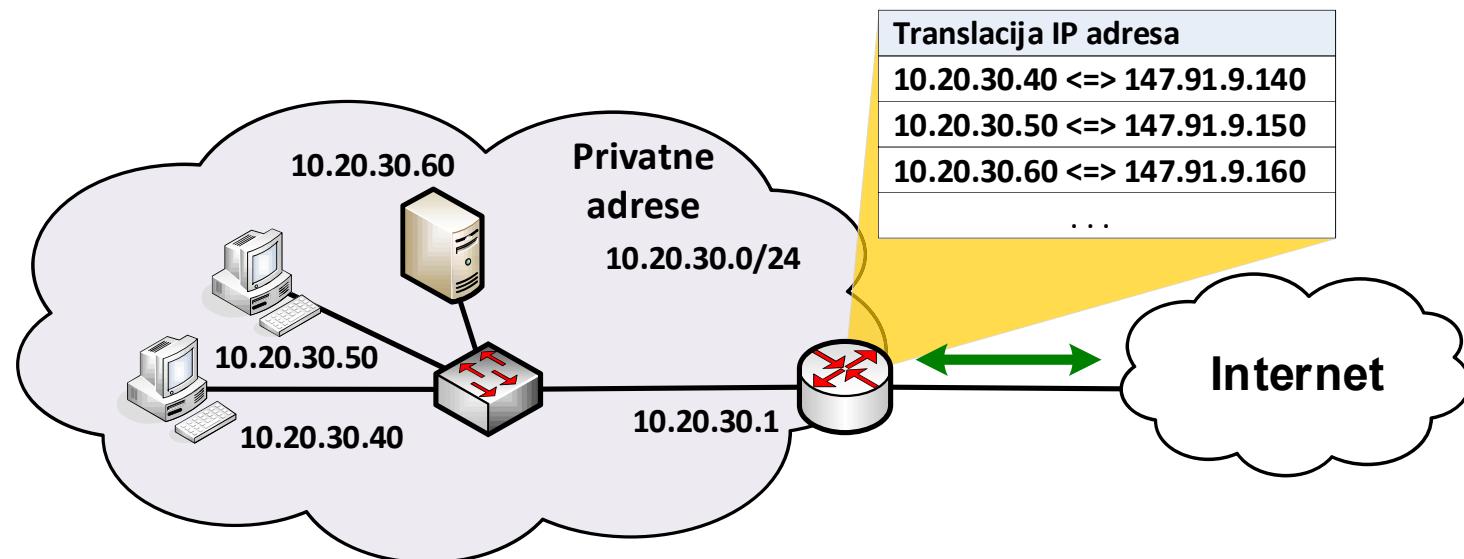
NAT – Network Address Translation

- Privatne IP adrese
 - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Štede potrošnju javnih IP adresa
- Ne smeju da se oglase ne Internetu
- Kako omogućiti komunikaciju sa Internetom?



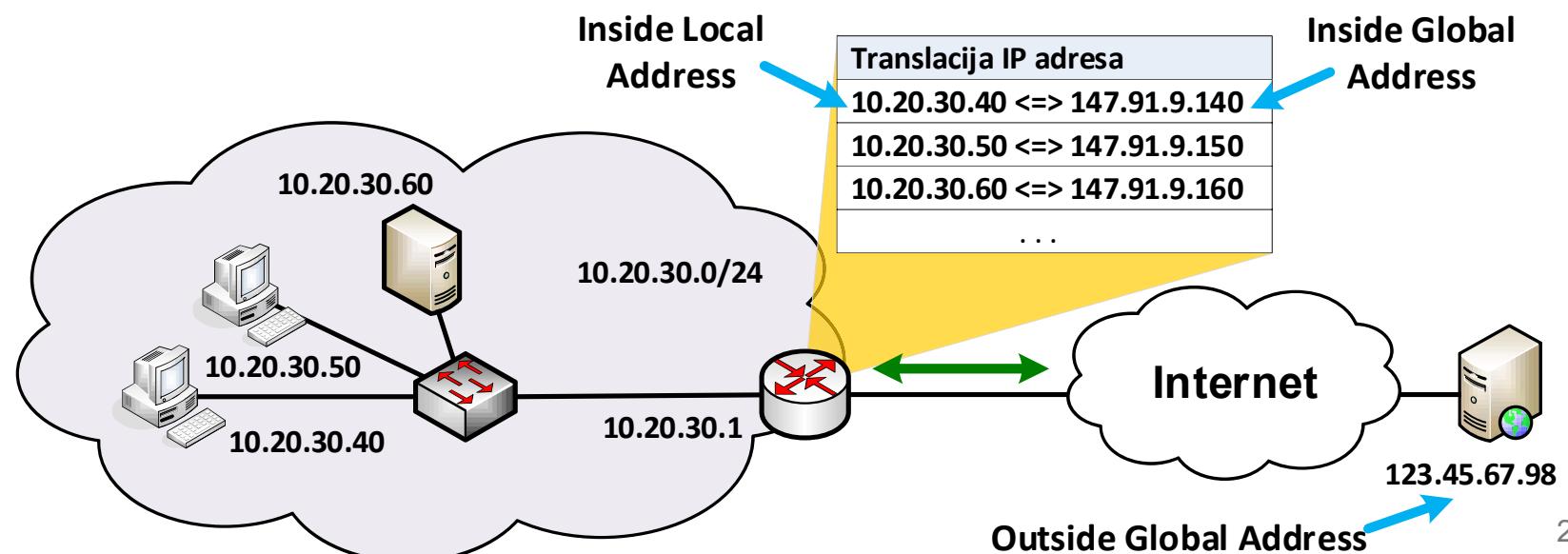
NAT – Network Address Translation

- NAT – Network Address Translation
 - Translacija adresa
 - Pretvaranje IP adresa iz jednog skup adresa u drugi
 - Najčešća primena
 - Translacija privatnih adresa u javne (i obrnuto)
 - NAT se sprovodi na graničnom ruteru
 - Jedinstvena tačka povezivanja sa ostatom mreži



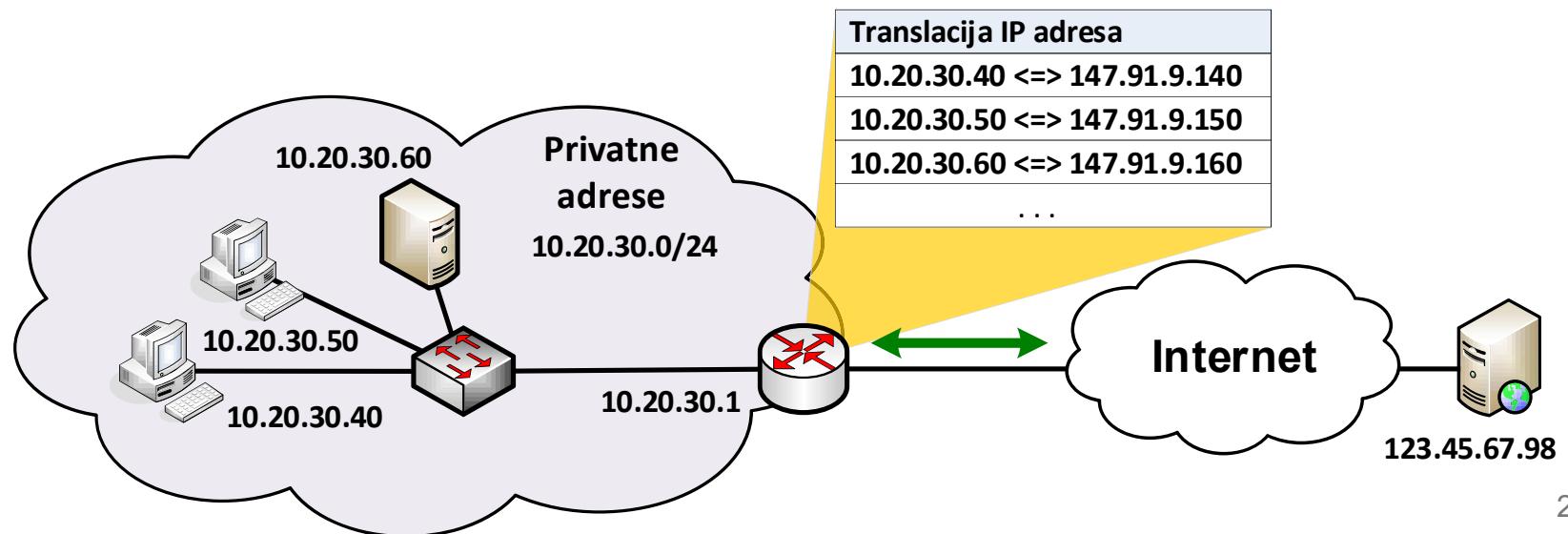
NAT Terminologija

- **Inside Local Address**
 - Adresa dodeljena hostu na unutrašnjoj mreži čije se adrese transliraju
- **Inside Global Address**
 - Legitimna (Internet) IP adresa dodeljena od strane provajdera
 - Adresa u koju se pretvara *Inside Local* adresa
- **Outside Global Address**
 - IP adresa uređaja na spoljašnjoj mreži



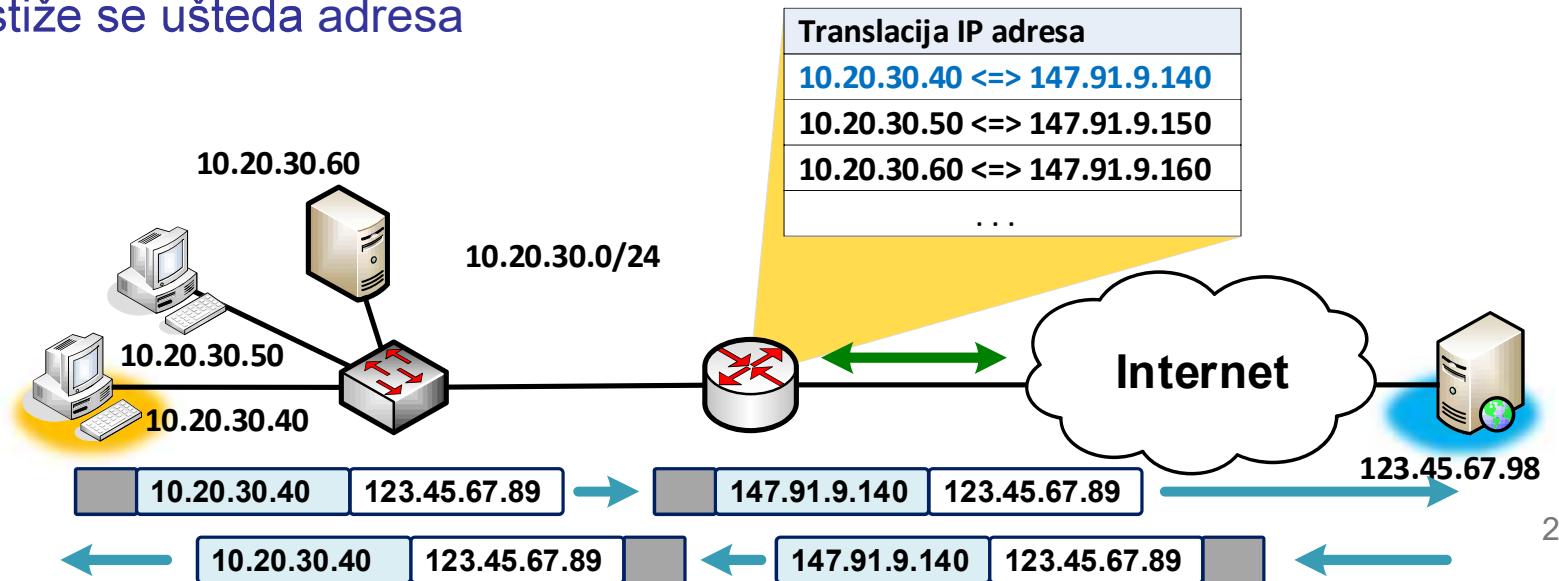
Statički NAT

- Fiksno mapiranje „jedan-na-jedan“
 - Jedna lokalna adresa uvek se mapira u istu globalnu adresu
- NAT tabela
 - Unapred definisana pravila mapiranja – par lokalne i globalne adrese
- Inicijalizacija komunikacije iz unutrašnje mreže ka spolja
 - Uobičajeno ponašanje – klijenti u unutrašnjoj mreži, serveri u spoljašnjoj



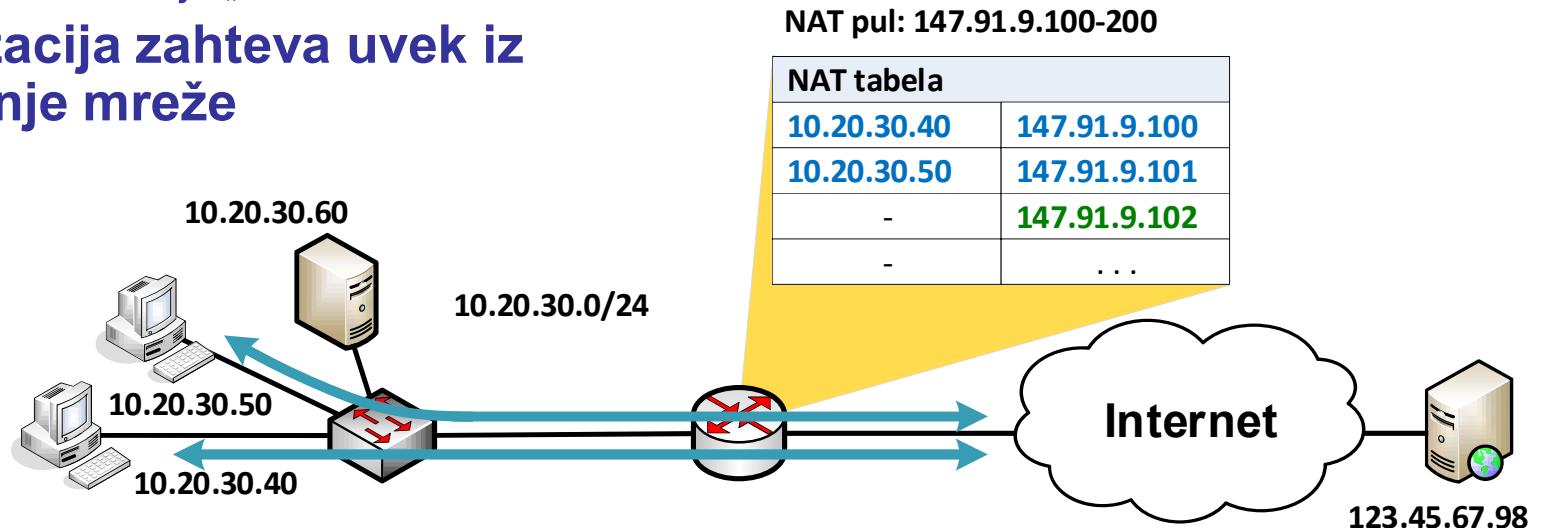
Statički NAT

- Proces na ruteru
 - Iz unutrašnje ka spoljašnjoj:
 - Izvorišne lokalne adrese iz zaglavlja IP paketa se pretvaraju u globalne
 - Iz spoljašnje ka unutrašnjoj:
 - Odredišne globalne adrese iz zaglavlja IP paketa se pretvaraju u lokalne
- Prednost
 - Inicijalizacija komunikacije iz spoljne mreže ka unutrašnjoj
 - Serverima u unutrašnjoj mreži mogu da pristupaju klijenti iz spoljašnje mreže
- Nedostatak
 - Ne postiže se ušteda adresa



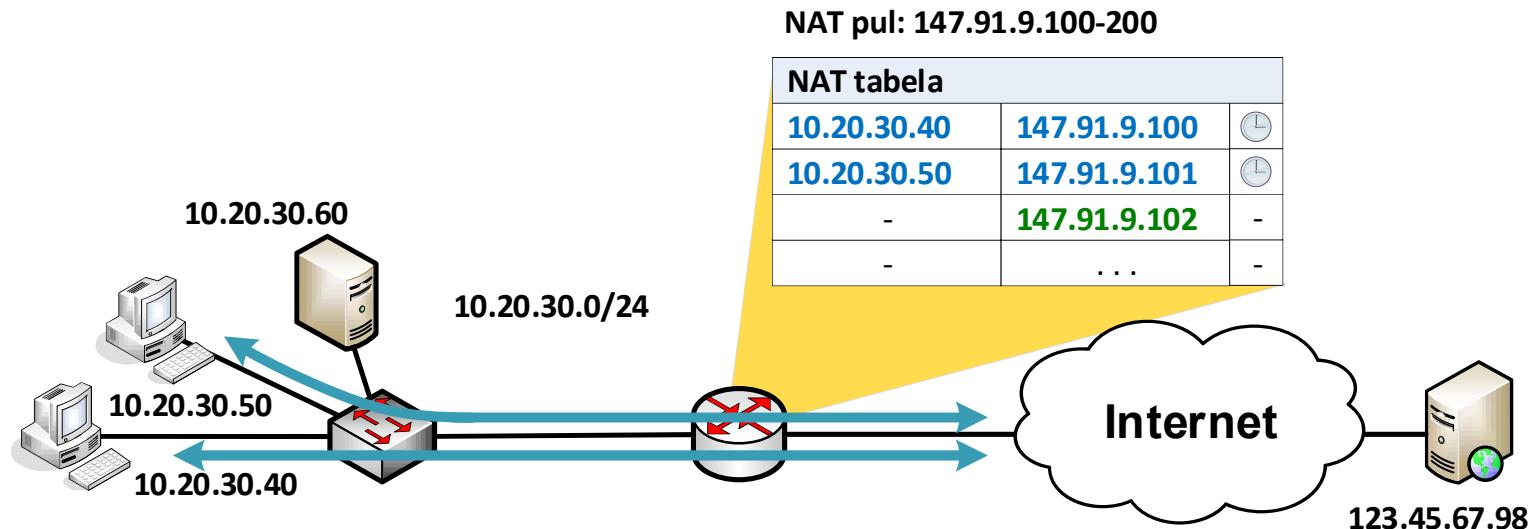
Dinamički NAT

- Definiše se skup globalnih IP adresa, tzv. pul (*pool*)
- Pri komunikaciji iz unutrašnje mreže uzima se slobodna adresa
- NAT tabela se dinamički popunjava sa parom lokalne i globalne adrese
- U jednom trenutku jednu globalnu adresu može koristiti samo jedna lokalna
 - Maksimalni broj konekcija – broj adresa u NAT pulu
- Tokom vremena
 - Po završetku komunikacije briše se korišćeno mapiranje – oslobađa se adresa
 - Efekat - više unutrašnjih adresa se može mapirati u manji broj globalnih adresa
 - Ušteda adresa je „statistička“
- **Inicijalizacija zahteva uvek iz unutrašnje mreže**



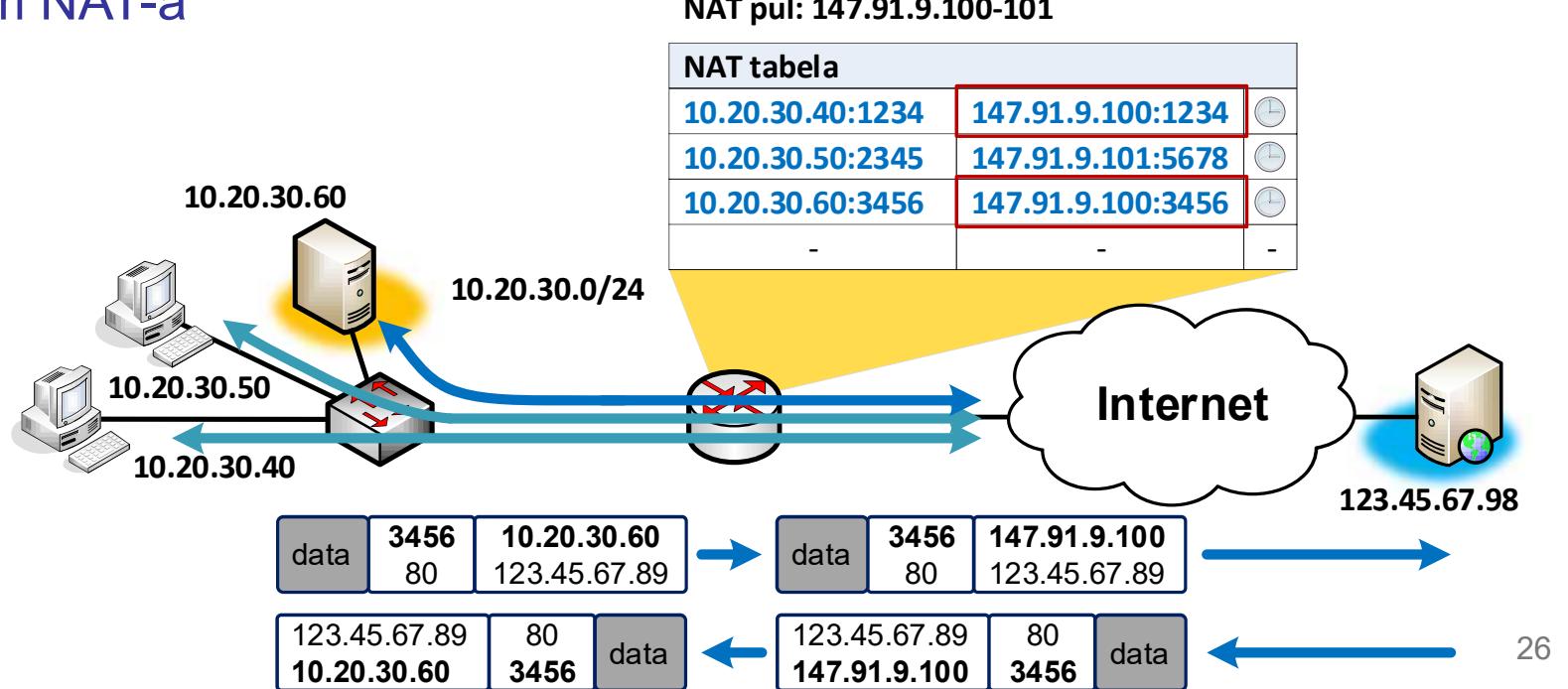
Dinamički NAT

- Oslobođanje globalne adrese kada se komunikacija završi
 - TCP – može se prepoznati kada se sesije regularno zatvaraju, ali šta ako se sesija nasilno prekine (npr. jedan uređaj se ugasi)?
 - UDP – ne zna se koliko će da traje i da li ima još paketa, čak iako se ne koristi
 - ICMP – kratkotrajne sesije (npr. ping)
- Uvodi se tajmer za svaki red u NAT tabeli
 - Red se briše nakon isteka tajmera (*timeout*)



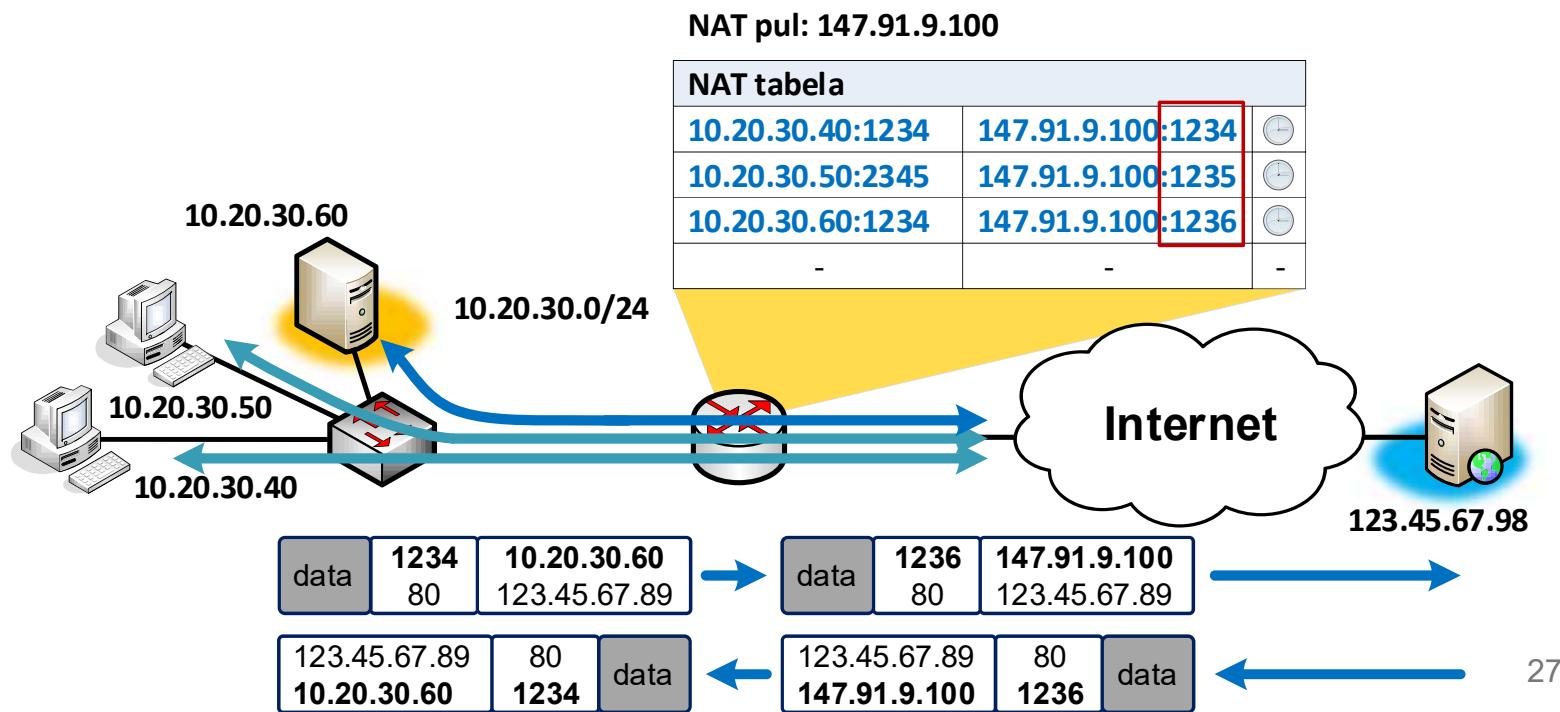
Overload NAT

- Kako više lokalnih adresa **istovremeno** da koristi manji broj globalnih adresa?
 - Potrebne dodatne informacije za obezbeđivanje jednoznačnosti
 - Koristi se TCP i UDP port – **PAT (Port Address Translation)**
- Klijent mora da bude u unutrašnjoj mreži
 - Klijentski port se slučajno bira na strani klijenta, pa može i da se promeni prilikom NAT-a



PAT sa jednom globalnom adresom

- Može da se koristi i samo jedna globalna adresa

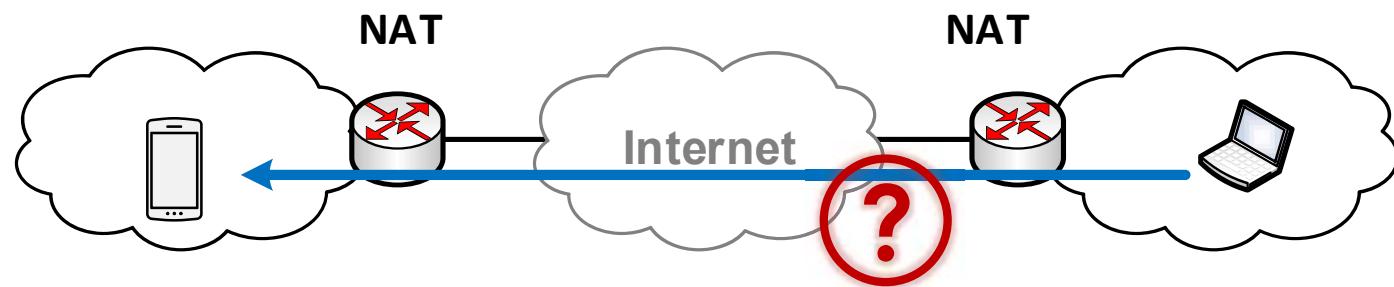


Port forwarding

- Kako za server u unutrašnjoj mreži omogućiti pristup iz spoljašnje?
- Potrebno je statičko mapiranje
- **Port forwarding** – statičko mapiranje za određene adrese
 - Spoljni zahtev na globalnu IP adresu i serverski port će se mapirati u lokalnu IP adresu servera, a serverski port će ostati nepromenjen
 - Omogućava da se serveru priđe iz spoljašnje mreže
- Nedostatak:
 - Može samo jedna lokalna IP adresa da se bude uparena sa serverskim portom, odnosno samo jedan server za svaki servis (port)
 - Npr. ne može da postoji više veb servera dostupnih sa spoljne mreže na predefinisani port 80

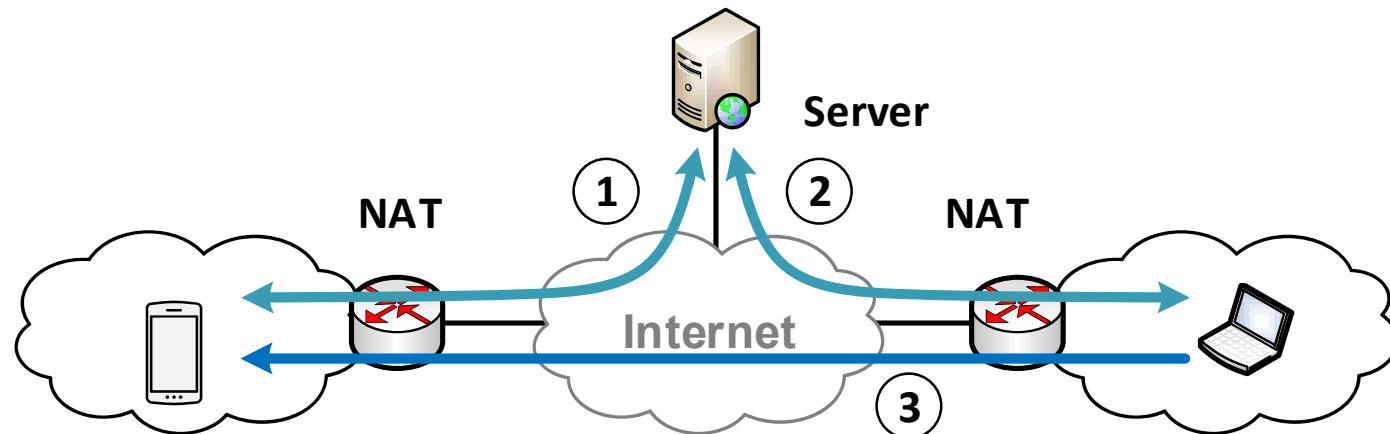
Direktna komunikacija preko NAT-a

- Dinamički NAT/PAT
 - Inicijalizacija komunikacije - iz unutrašnje mreže
- Kako se sprovodi direktna komunikacija dva uređaja u različitim unutrašnjim mrežama (iza NAT-a)?
 - Real-time aplikacije – Skype, Viber, WhatsApp...



Direktna komunikacija preko NAT-a

- Rešenje:
 - Uređaji se najpre registruju na javno dostupnom serveru (koraci 1 i 2)
 - Server uređajima prosledi „NAT-ovane“ adrese i portove za pristup
 - Uređaji nastavljaju direktno da komuniciraju



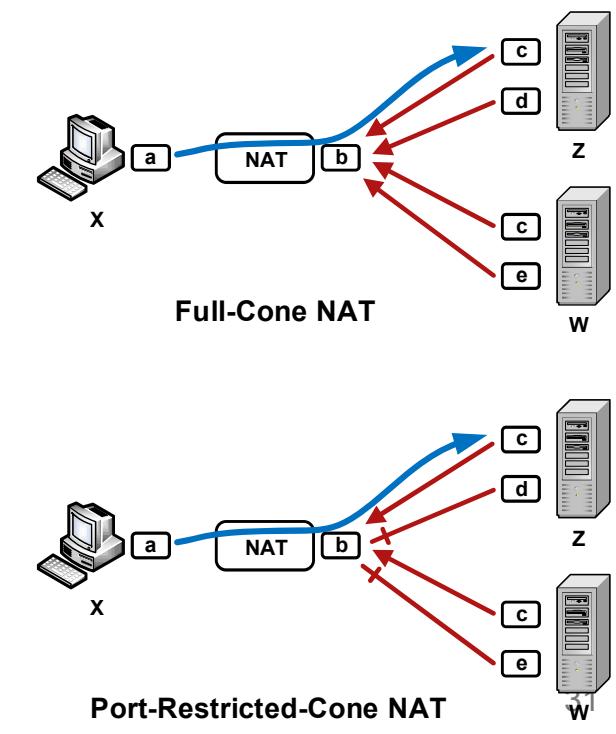
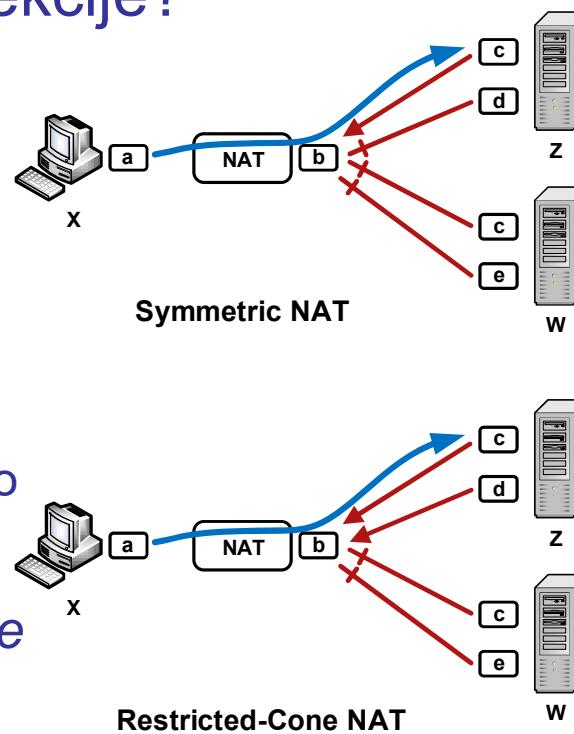
- Problem:
 - TCP – kako se uspostavlja direktna TCP veza?
 - Kako NAT dozvoljava trećem uređaju da koristi prethodno mapiranu adresu?

NAT i UDP

- TCP – komunicira se samo sa uređajem sa kojim je prethodno uspostavljena konekcija (*Connection Oriented*)
- UDP protokol – nema otvaranja konekcije, pa na adresu i port može svako da pristupi (čak i na klijentski port, ako ga poznaj)
- Kome se dozvoljava da koristi globalnu adresu i port za otvorene NAT konekcije?

- 4 slučaja:

- *Symmetric*
 - najrestriktivnije
- *Full-Cone*
 - Najmanje restriktivno
- *Restricted-Cone*
- *Port-Restricted-Cone*

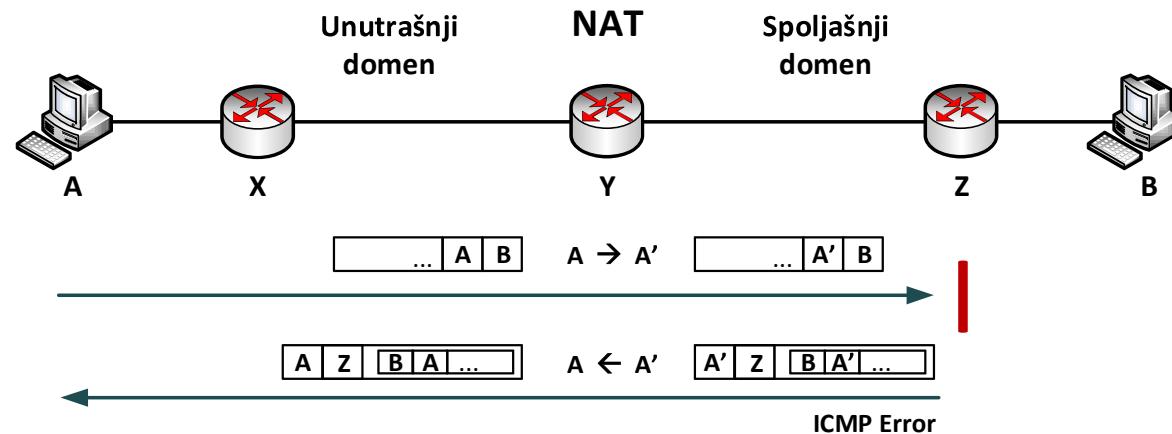


NAT i ICMP i ostale aplikacije

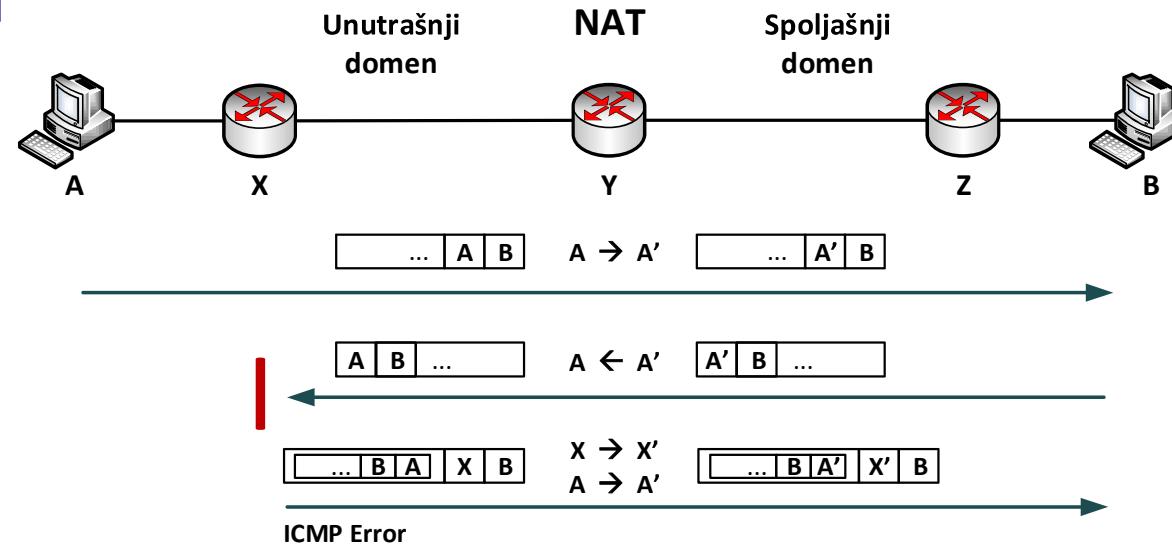
- Kako se primenjuje NAT za ICMP paketa, koji ne koriste UDP/TCP portove?
- Dve vrste ICMP poruka
 - Poruke upita (*ICMP query messages*)
 - Poseduju identifikaciono polje koje se koristi za NAT mapiranje (*Query Identifier, Query ID*)
 - Poruke o grešci (*ICMP error messages*)
 - Ne poseduje identifikaciono polje
 - Originalni IP paket se prenosi u telu ICMP error poruke (*payload*)
 - Potrebno je promeniti lokalne adrese i portove i u originalnom paketu
- Pojedine aplikacije prenose informacije o IP adresama u svojim podacima
 - *Application Level Gateway (ALG)*
 - NAT uređaj mora da gleda i menja i aplikativne podatka, kako bi NAT bio transparentan

NAT i ICMP i ostale aplikacije

- Translacija ICMP Error poruka iz unutrašnjeg domena prema spoljašnjem



- Translacija ICMP Error poruka iz spoljašnjeg domena prema unutrašnjem

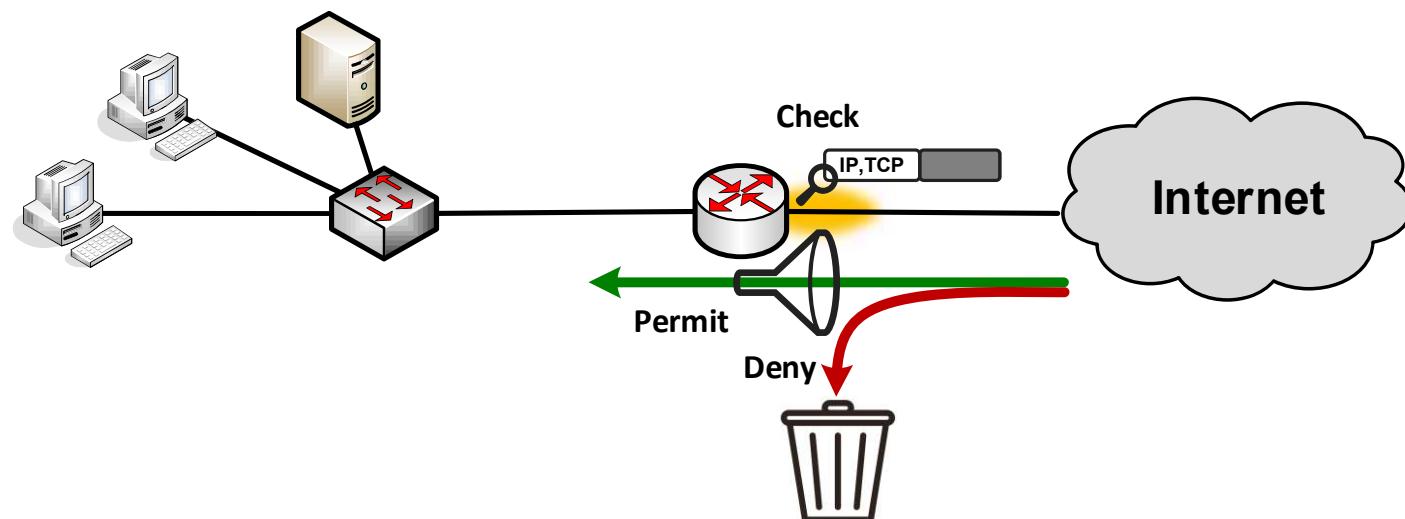


Korišćenje NAT-a

- Prednosti:
 - Uobičajeno je da se za privatne korporacijske mreže koriste privatne IP adrese
 - Veća sloboda u dodeljivanju i korišćenju privatnih IP adresa
 - Ne mora da se vrši promena adresa u privatnoj mreži prilikom promene provajdera
 - Povećana je sigurnost (dinamički NAT) – privatni deo mreže je izolovan
 - Manja je potrošnja javnih IP adresa
- Mane:
 - Složenija konfiguracija i administracija
 - Komplikovanije procesiranje na ruterima i povećava se kašnjenje saobraćaja
 - Otežano je praćenje događaja na osnovu pritužbi sa Interneta (hakeri, virusi, narušavanje autorskih prava, DoS...)
 - Može da predstavlja problem za pojedine aplikacije koje se na aplikativnom nivou oslanjaju na IP adrese

ACL – kontrola prosleđivanja paketa

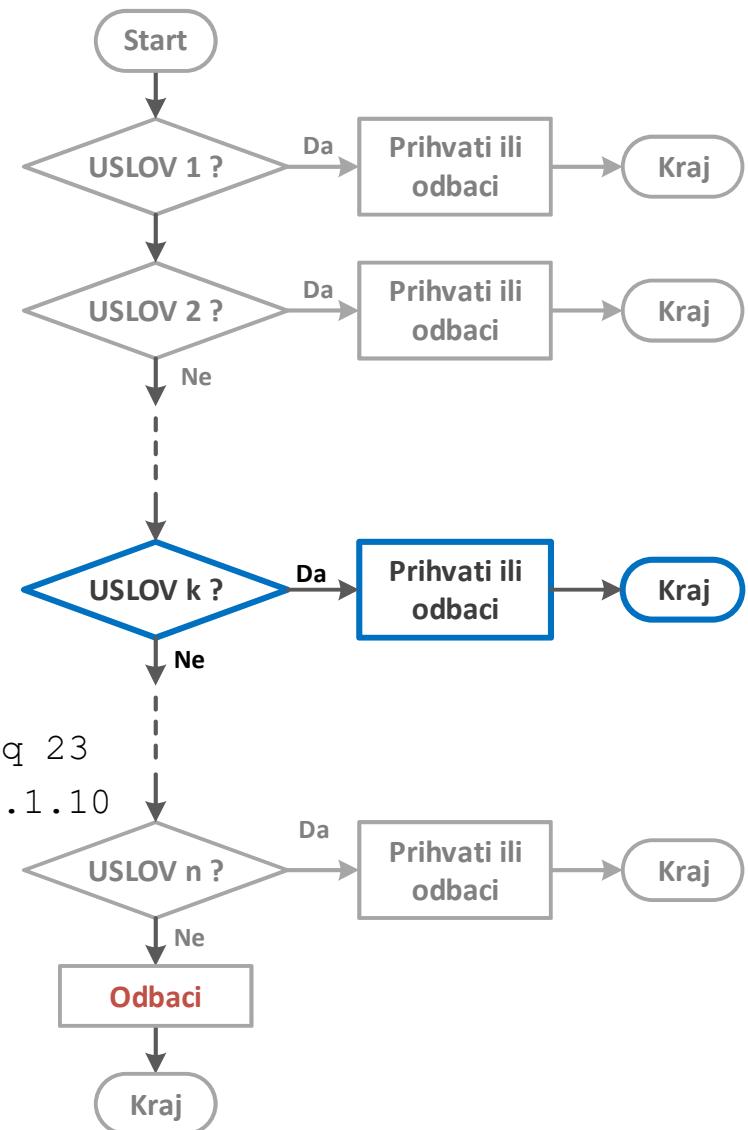
- **ACL – Access Control Lists, „Akses liste“**
 - Dozvola ili zabrana prolaska paketa kroz interfejse rutera
 - Inspekcija zaglavlja na L3 i L4 nivou
 - Uslov
 - Poređenje IP adresa, TCP/UDP portova, ICMP poruka
 - Akcija
 - Dozvola (*Permit*) – propuštanje paketa
 - Zabrana (*Deny*) – odbacivanje paketa (uništavanje) – slanje na *Null* interfejs
 - Filtriranje paketa – *Packet Filtering*



ACL – kontrola prosleđivanja paketa

- Za svaki paket
 - Prolazak kroz uređenu listu uslova i pravila
- Nailazak na prvi ispunjeni uslov
 - Izvršava se pridruženo pravilo
 - Završava se prolaz kroz listu
- Kraj liste - ni jedno pravilo nije ispunjeno
 - **Paket se odbacuje (*Implicit Deny*)**
- Primer

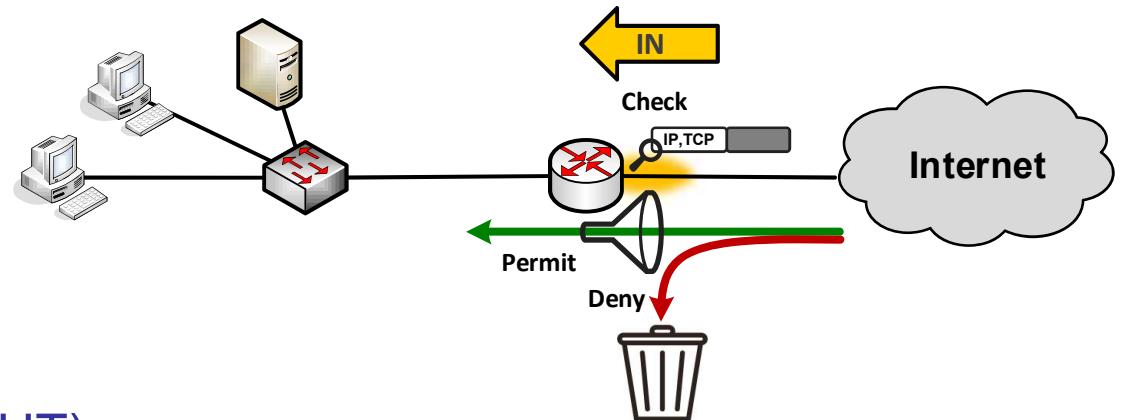
```
ip access-list extended EMAIL-SERVER
  permit tcp host 172.16.3.5 host 172.16.1.10 eq 23
  permit udp host 172.16.1.70 eq 53 host 172.16.1.10
  permit tcp any host 172.16.1.10 eq 25
  permit tcp any eq 25 host 172.16.1.10
  permit tcp any host 172.16.1.10 eq 110
  permit tcp any host 172.16.1.10 eq 80
  deny tcp 172.16.3.1 host 172.16.1.10 eq 23
  permit icmp any host 172.16.1.10 echo-reply
  deny ip any host 172.16.1.10
```



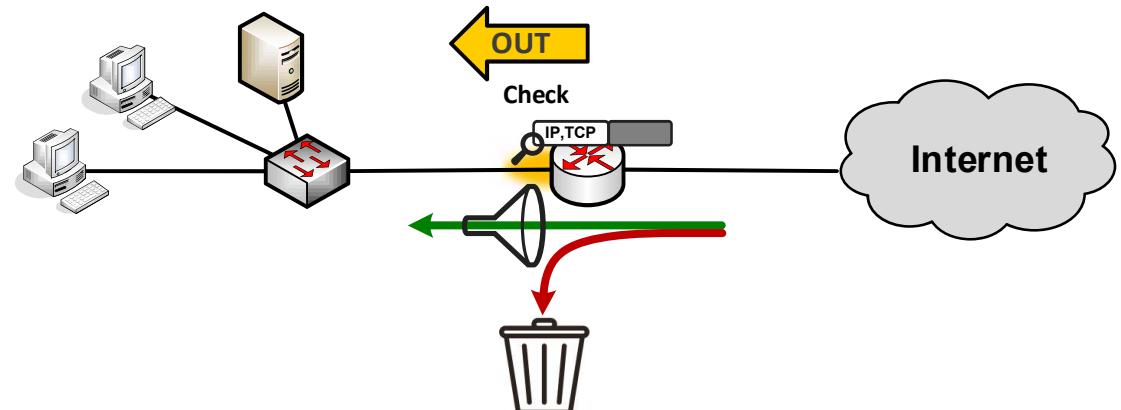
ACL – kontrola prosleđivanja paketa

- Primena na interfejsima ruteru

- Na ulasku u interfejs (IN)



- Na izlasku iz interfejsa (OUT)



Literatura

- Wendell Odom
„CCNA - Cisco official exam certification guide“
Cisco Press
- James Kurose, Keith Ross
„Computer Network - A Top-Down Approach“
- James Kurose, Keith Ross
„Umrežavanje računara: Od vrha ka dnu“
prevod 7. izdanja
CET

