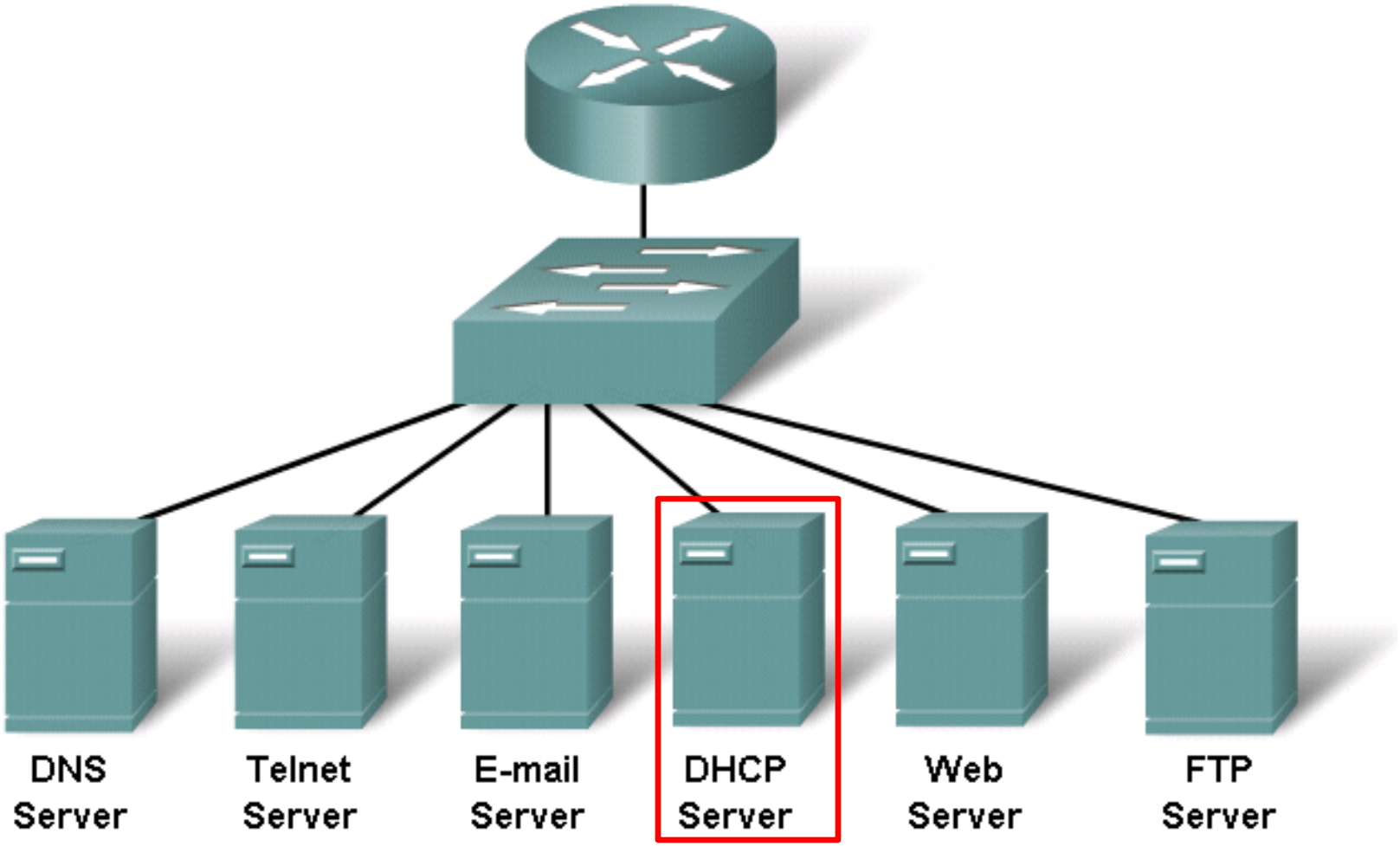
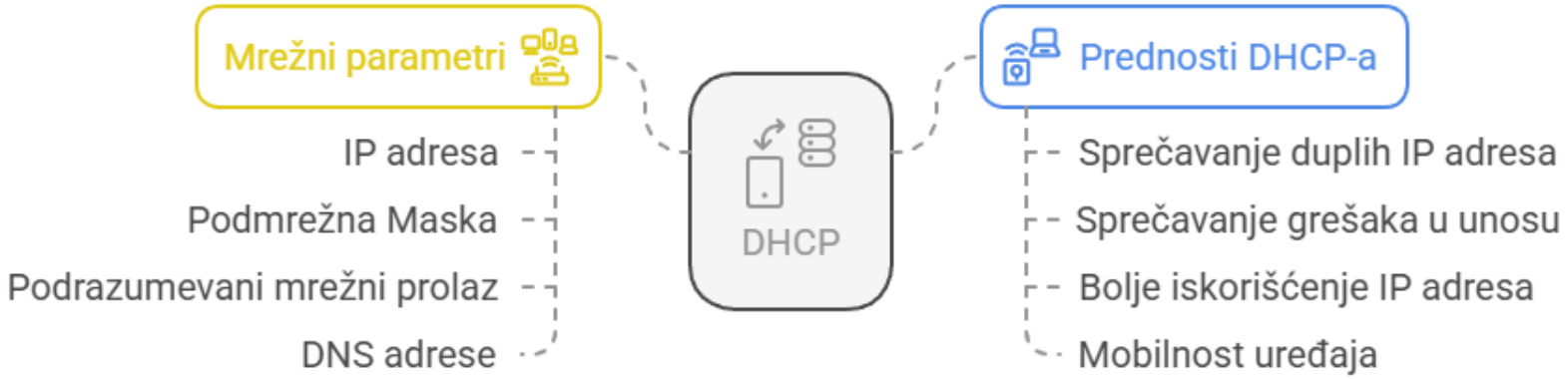
DHCP SERVIS

Predmet: Mrežni servisi

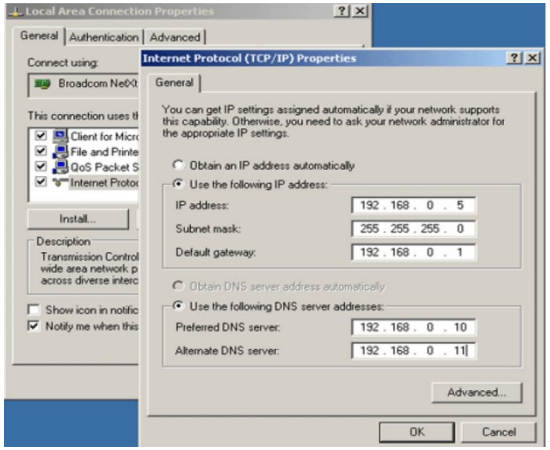
Predavač: dr Dušan Stefanović


DNS Server
Telnet Server
E-mail Server
DHCP Server
Web Server
FTP Server

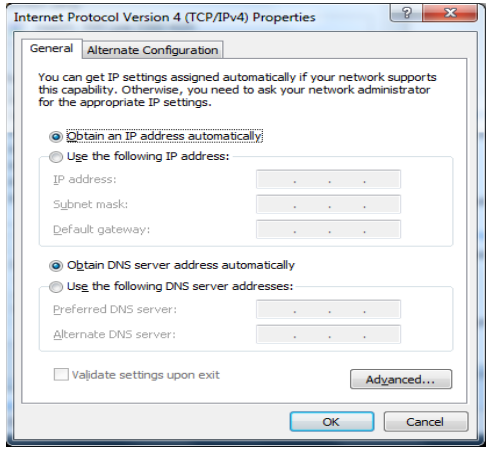
OSOBINE DHCP SERVISA



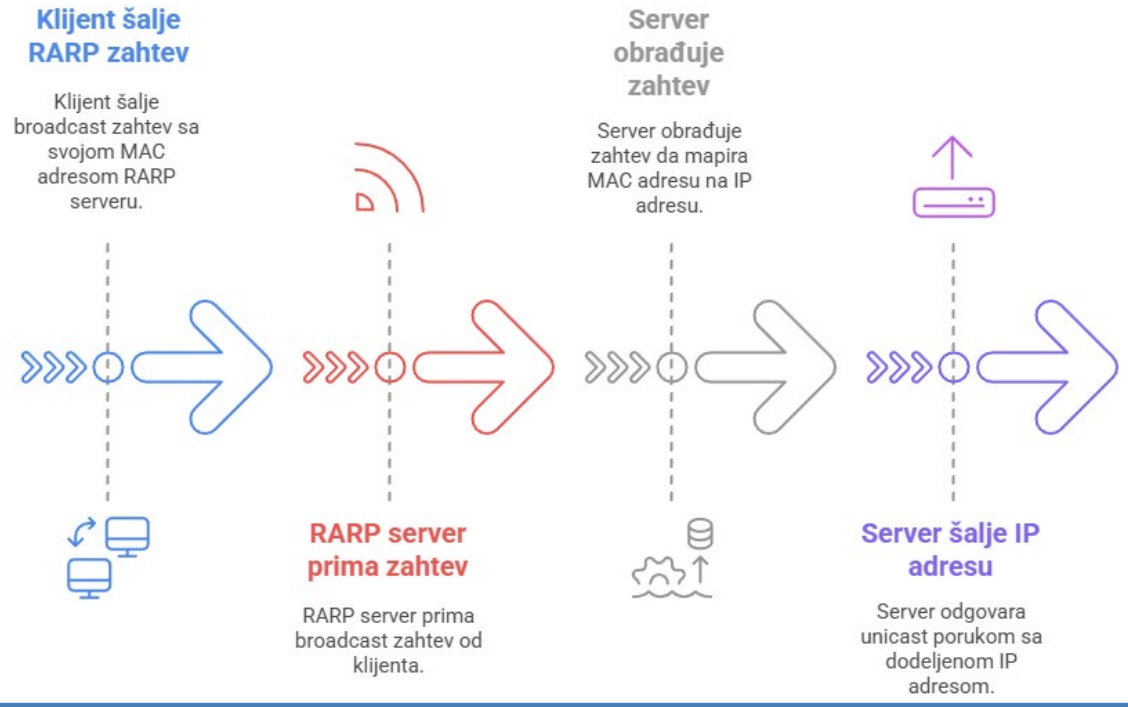
RUČNA KONFIGURACIJA MREŽNIH PARAMETARA

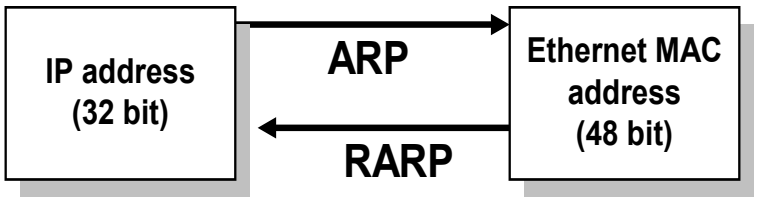


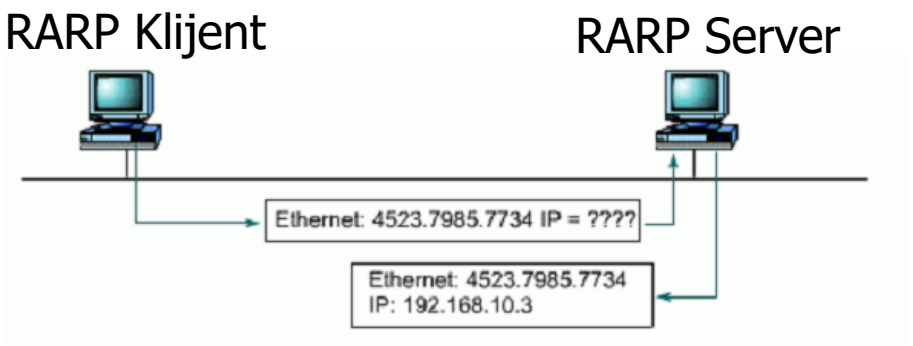
DINAMIČKA KONFIGURACIJA



PRVOBITNO REŠENJE ZA DINAMIČKU DODELU IP ADRESA(RARP)







OSOBINE BOOTP PROTOKOLA

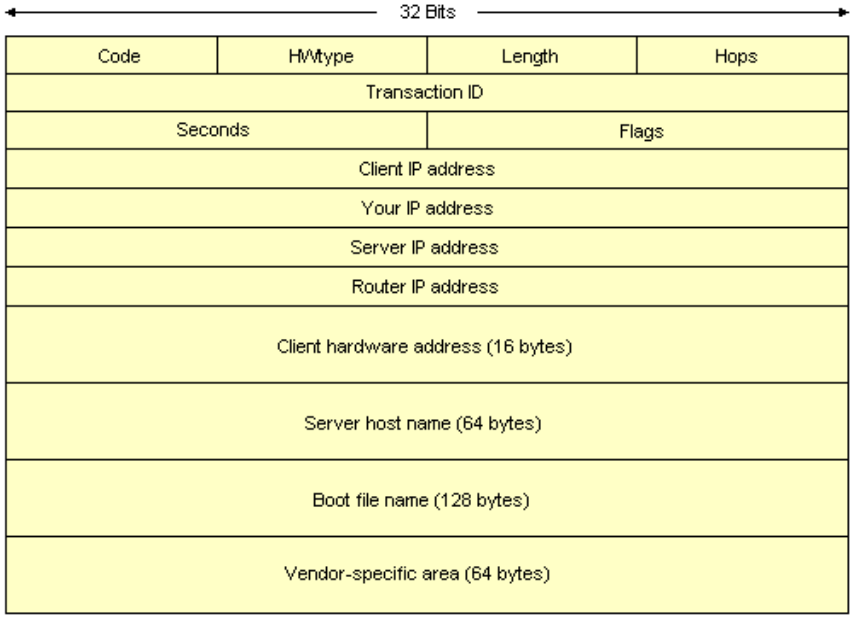
BOOTPstrap protokol(1985) je prva varijanta DHCP protokola i predstavlja alternativu RARP (Reverse ARP) protokolu koji je mogao da dodeli samo IP adresu računaru na osnovu njegove MAC adrese

BOOTP nije dinamički konfiguracioni protokol jer je IP adresa unapred predefinisana za klijenta na osnovu MAC adrese

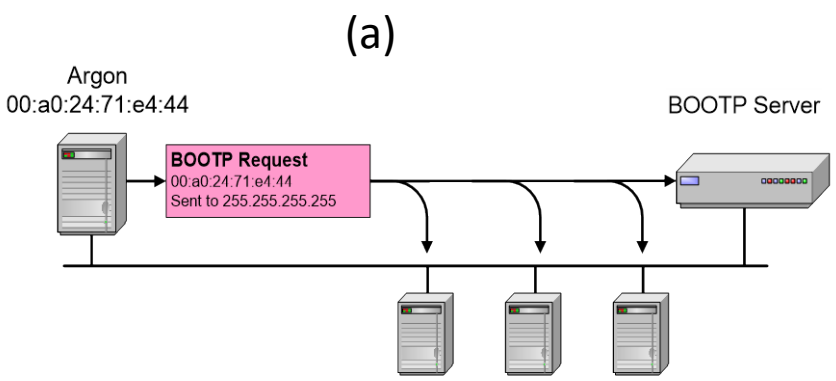
Obezbeđuje dodelu i ostalih konfiguracionih parametara

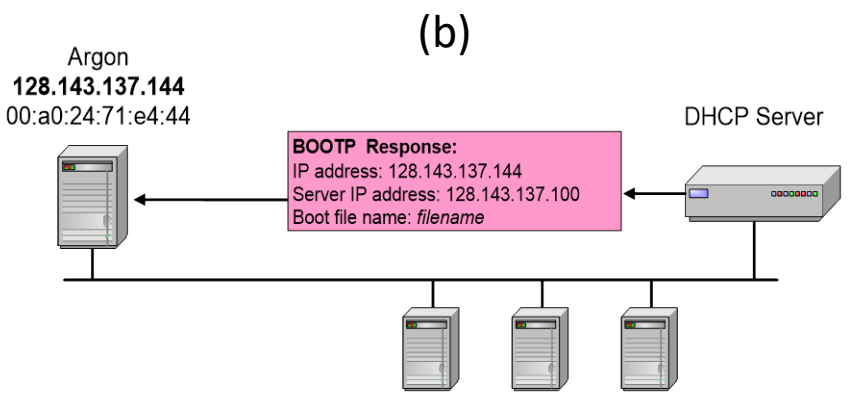
BOOTP koristi UDP poruke za konfigurisanje klijenata radi dobijanja IP adresa i drugih konfiguracionih parametara

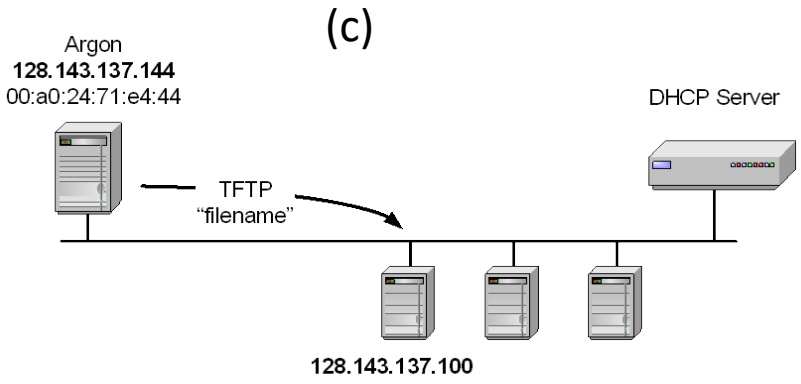
FORMAT BOOTP PROTOKOLA



OSOBINE BOOTP PROTOKOLA



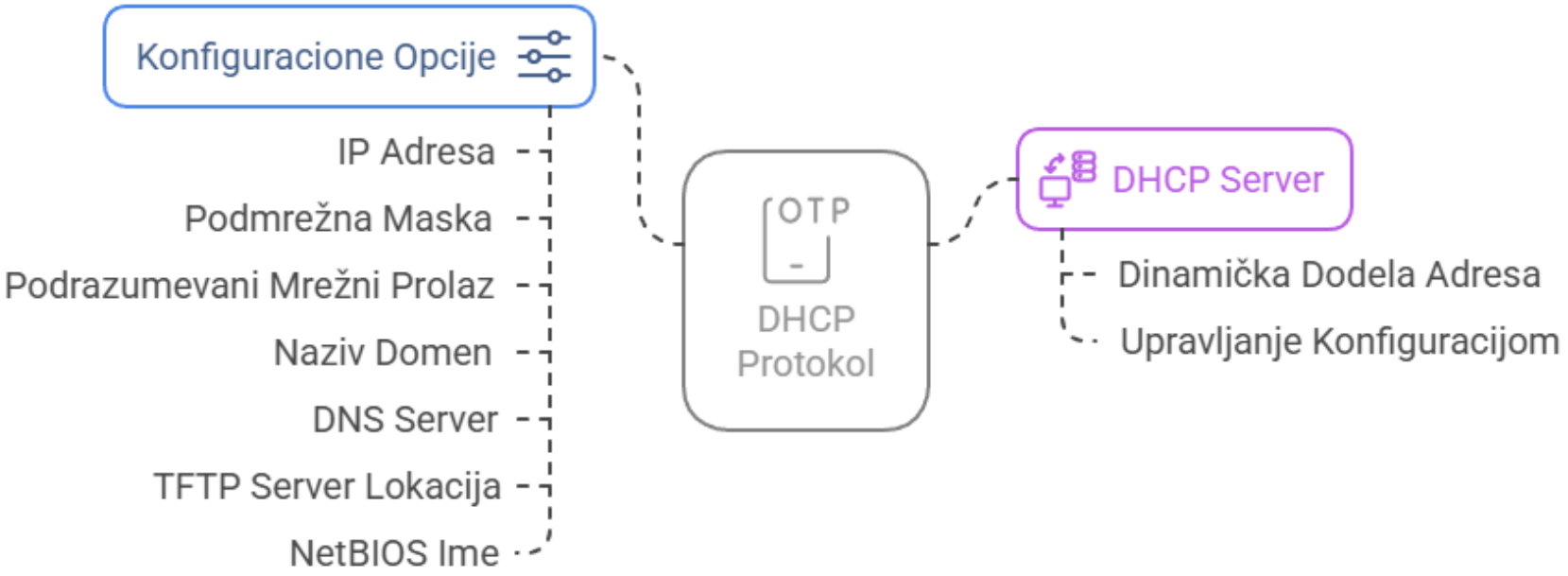




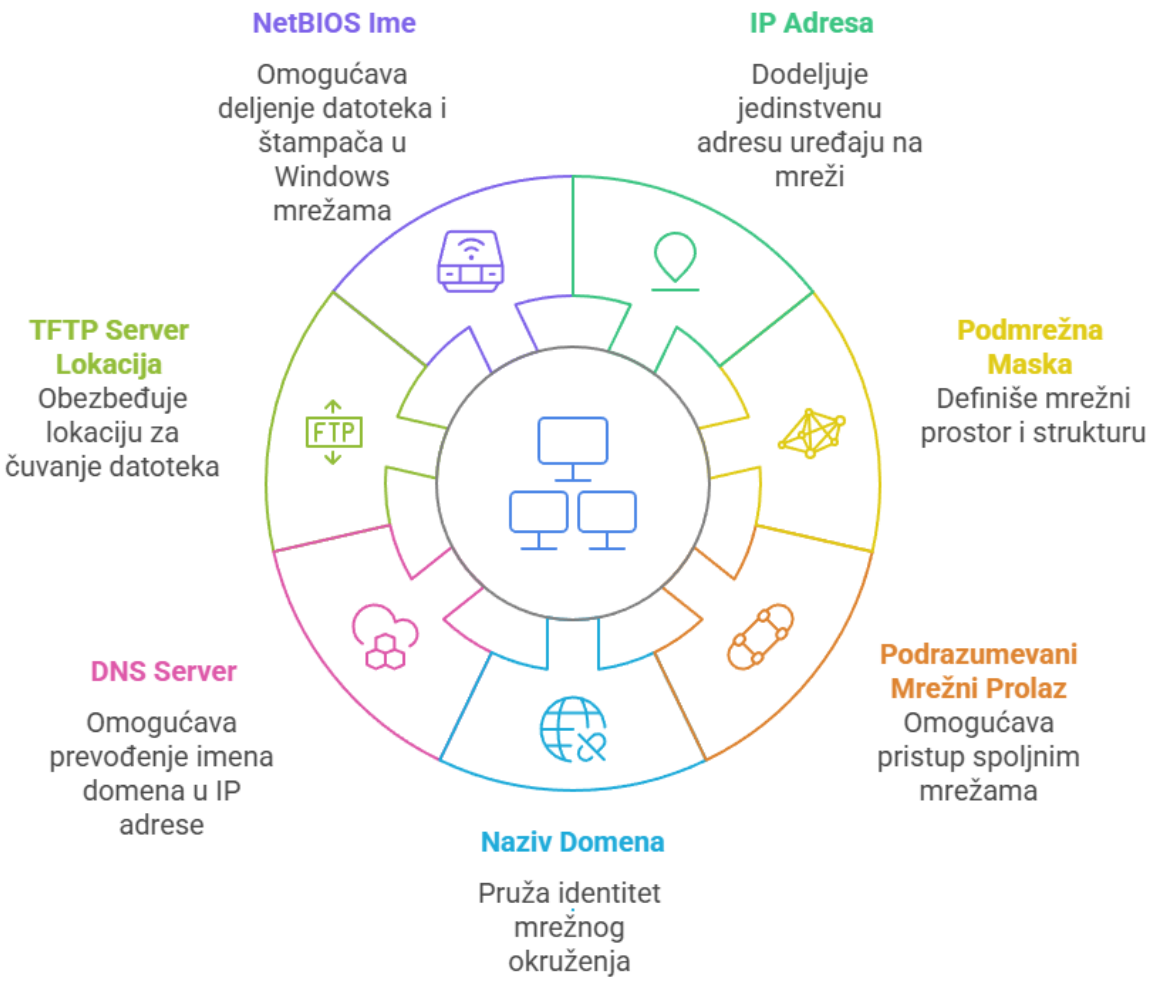
BOOTP protokol se koristi za downloading slike OS-a za radne stanice bez diska

Dodela IP adresa host-u je statička ne postoji lease time parametar

DHCP PROTOKOL



OSNOVNI PARAMETRI DODELE DHCP SERVERA



RAZLIKE IZMEĐU DHCP i BOOTP PROTOKOLA

BOOTP	DHCP
Statičko mapiranje	Dinamičko mapiranje
Trajna dodela adrese	Adresa se iznajmljuje na određeni period
Podržava samo 4 konfiguraciona parametra	Podržava preko 50 konfiguracionih parametra

DHCP KOMUNIKACIJA

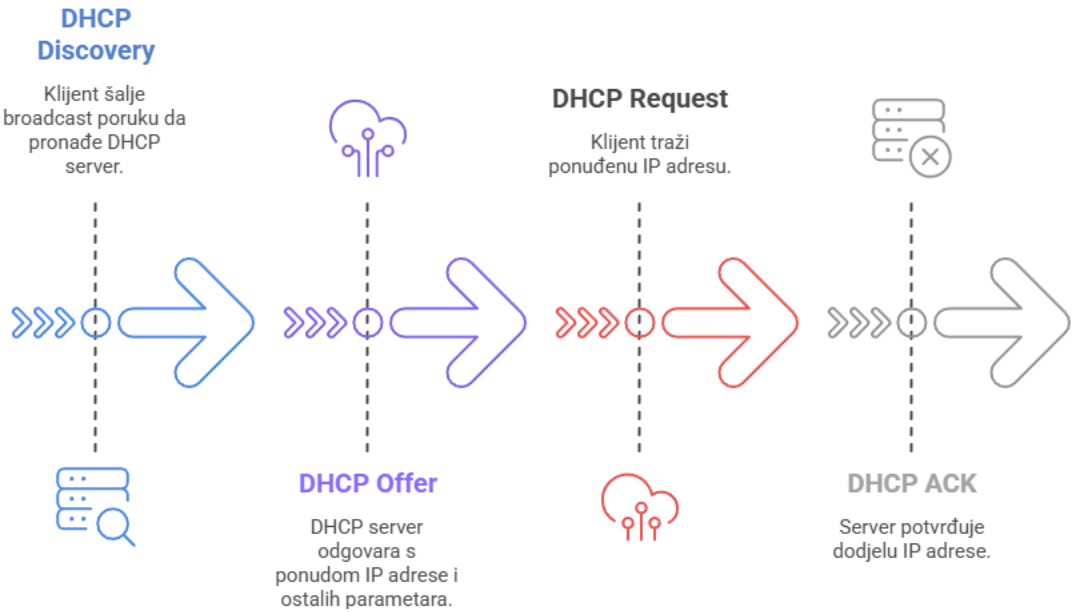
DHCP komunikacija odvija se u četri faze:

DHCP Discovery (prepoznavanje)

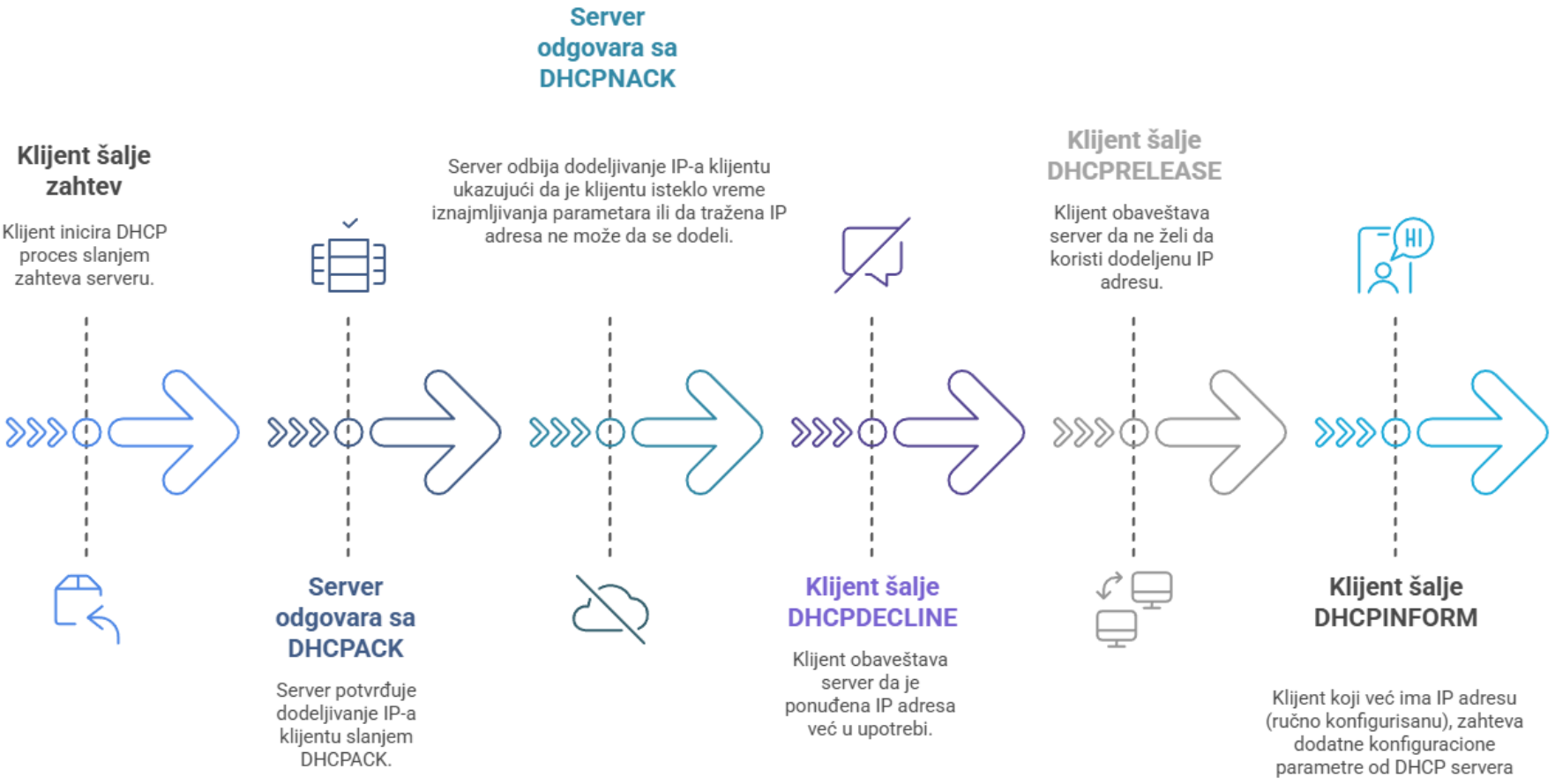
DHCP Offer (ponuda)

DHCP Request (zahtev)

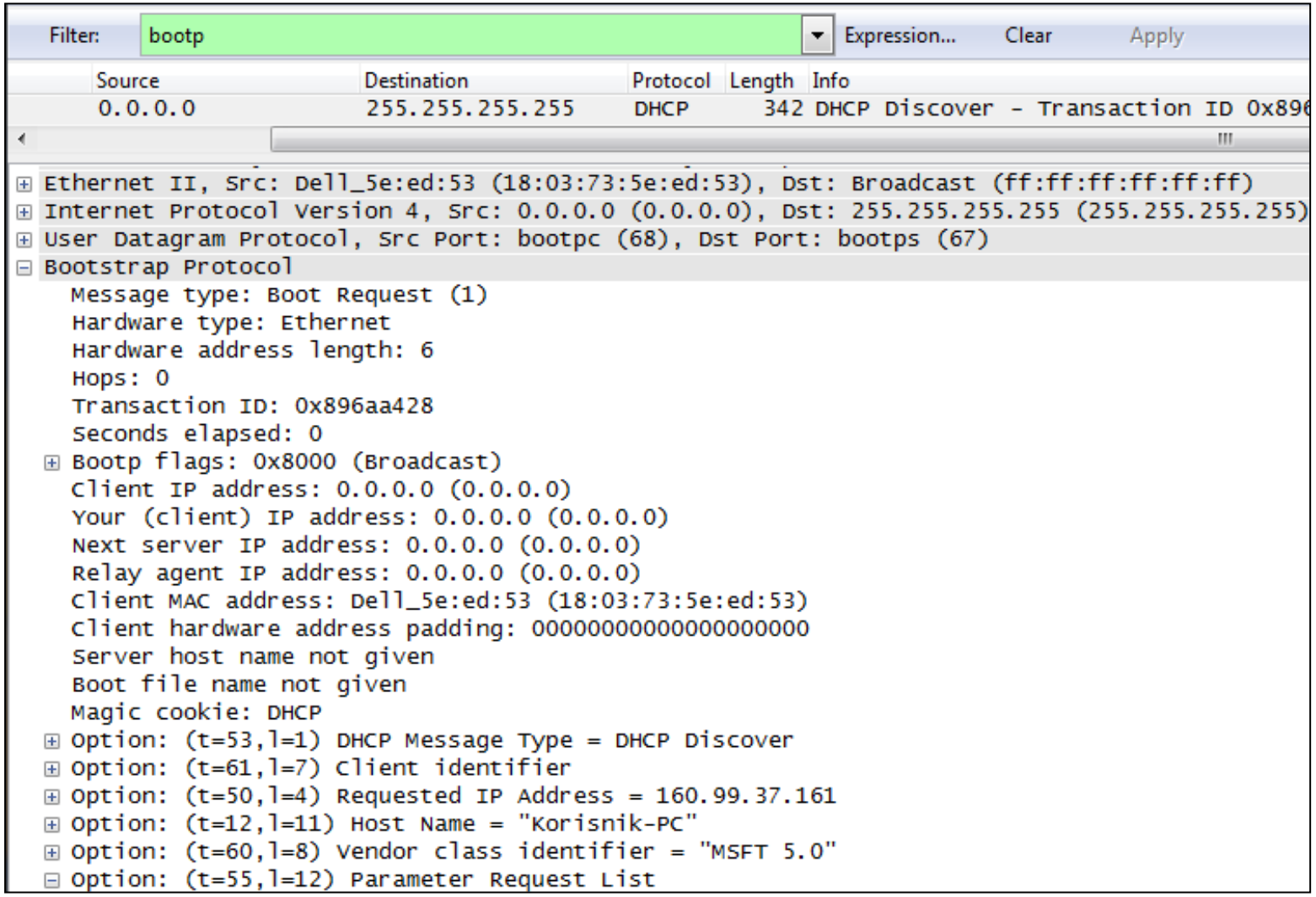
DHCP ACK (potvrda)



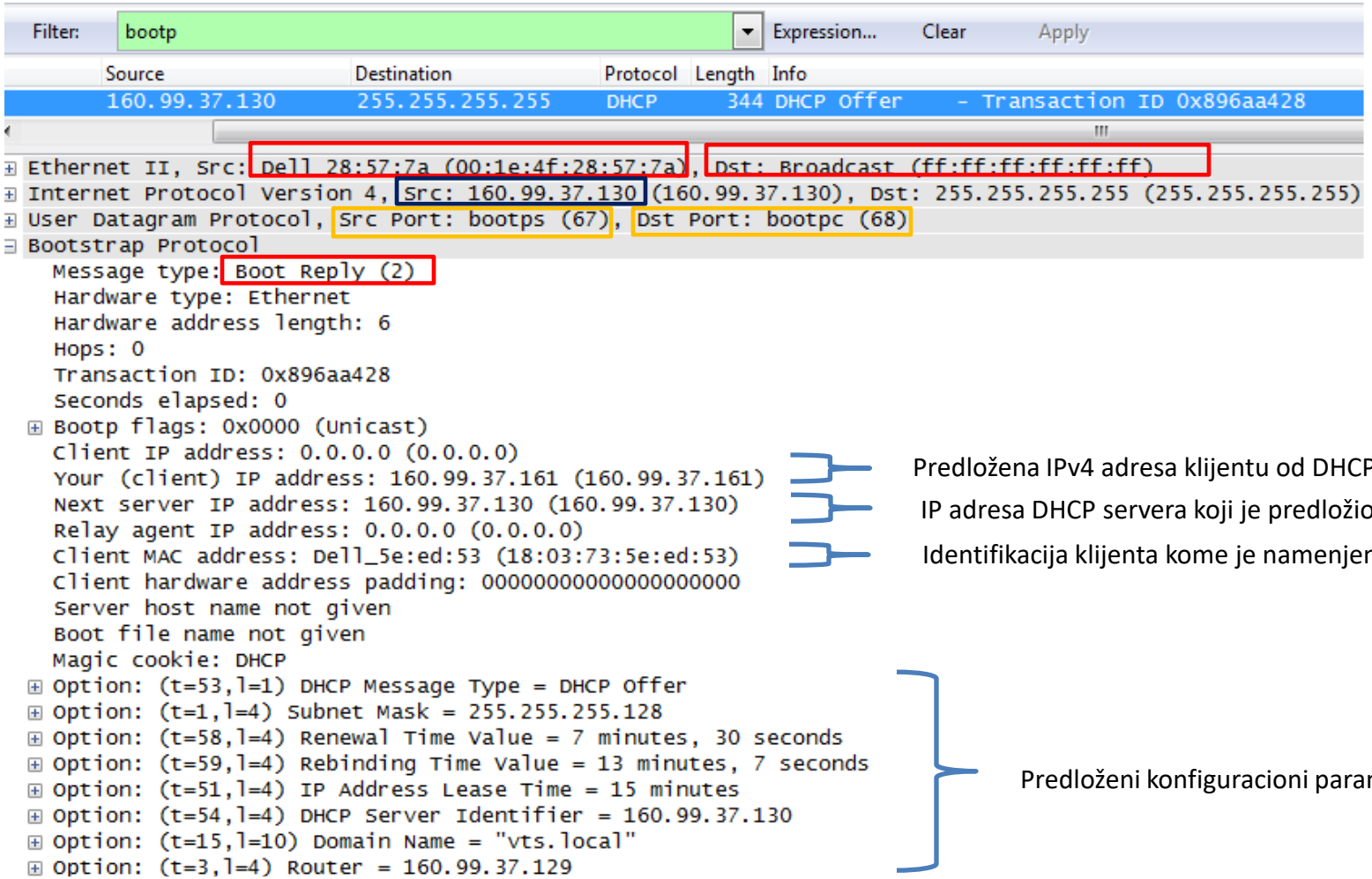
VRSTE PORUKA U DHCP KOMUNIKACIJI



DHCP DISCOVERY PORUKA



DHCP OFFER PORUKA



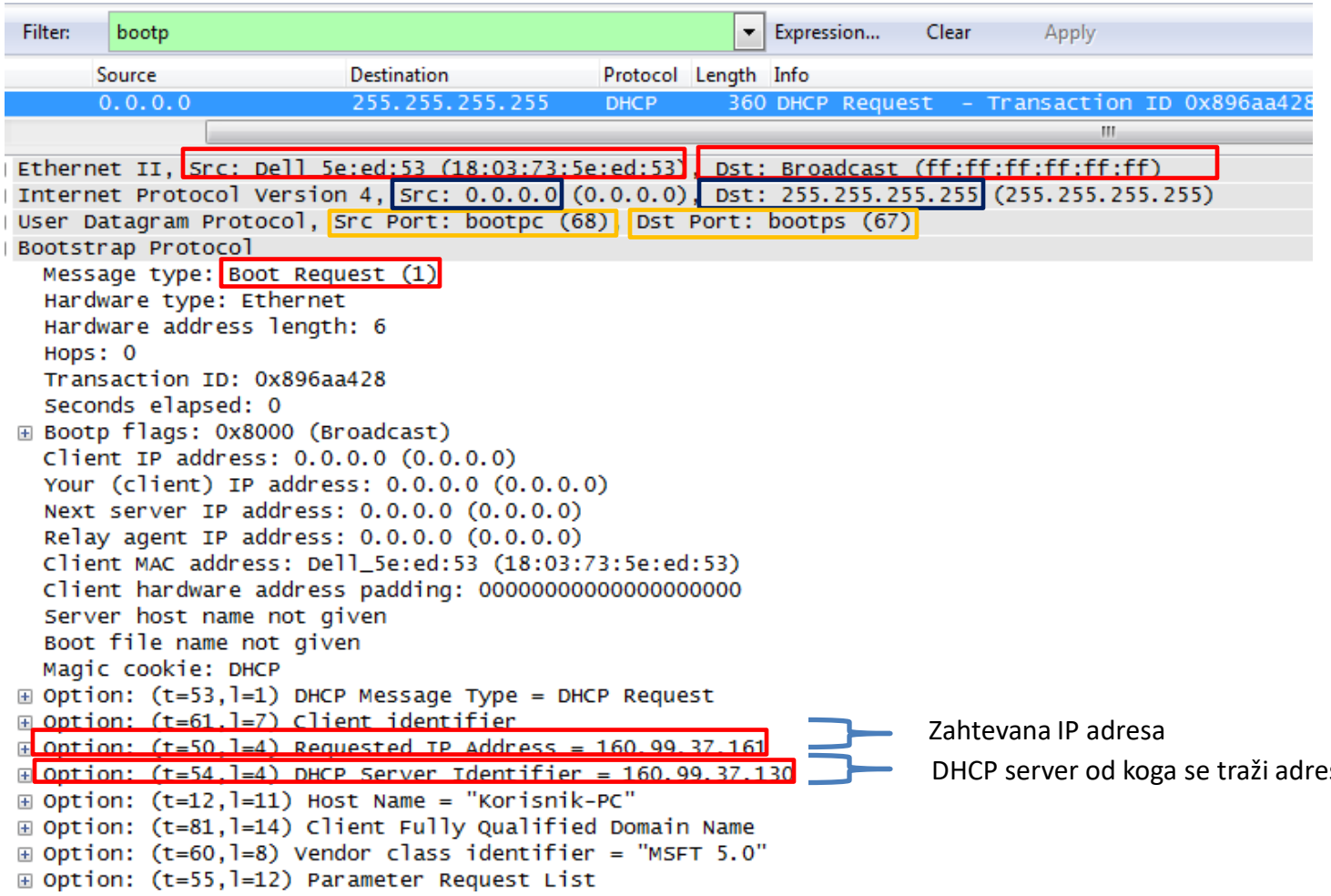
Predložena IPv4 adresa klijentu od DHCP servera

IP adresa DHCP servera koji je predložio adresu

Identifikacija klijenta kome je namenjena ponuda

Predloženi konfiguracioni parametri

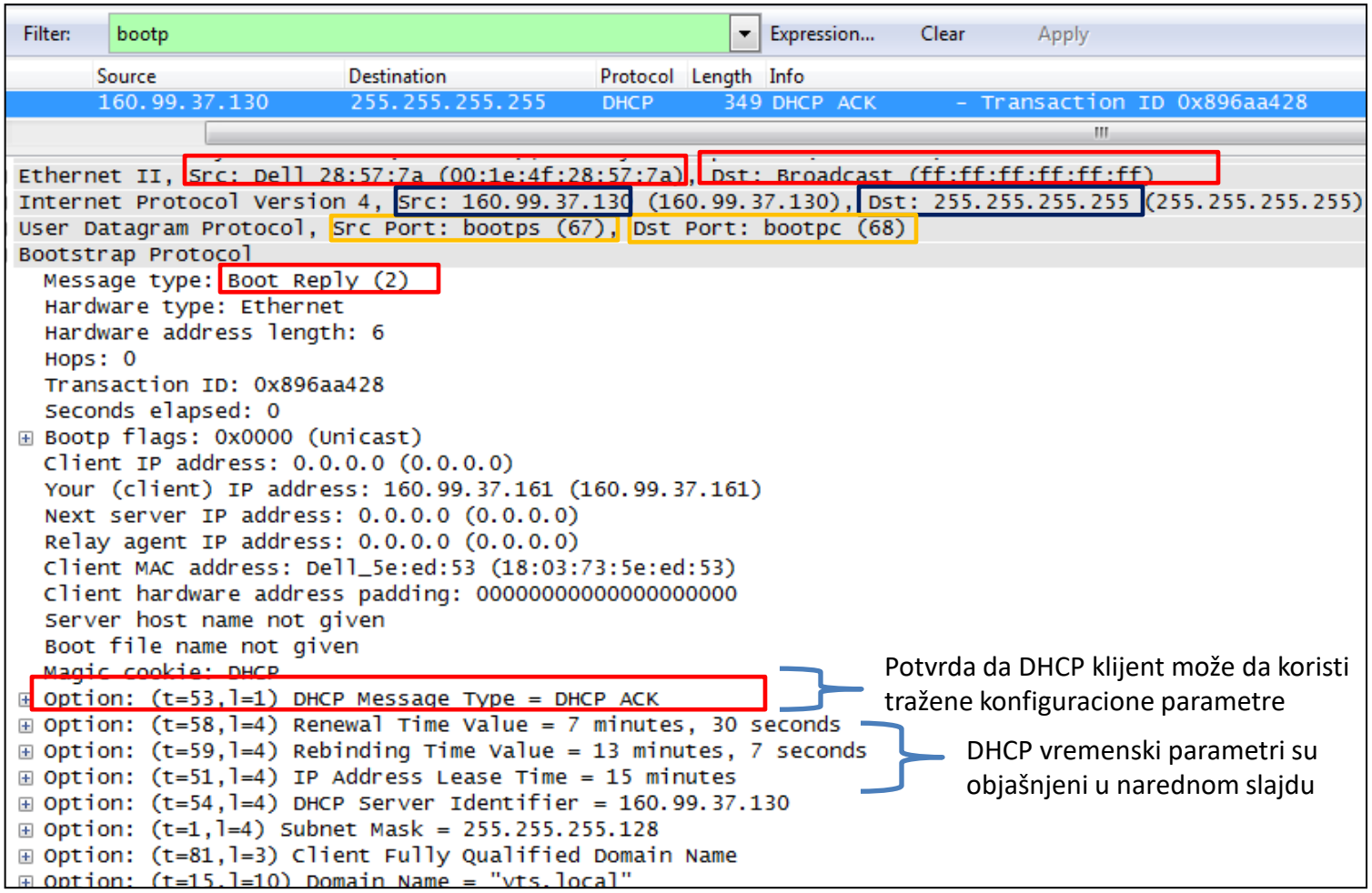
DHCP REQUEST PORUKA



Zahtevana IP adresa

DHCP server od koga se traži adresa

DHCP ACK



Potvrda da DHCP klijent može da koristi tražene konfiguracione parametre

DHCP vremenski parametri su objašnjeni u narednom slajdu

DHCP VREME IZNAJMLJIVANJA KONFIGURACIONIH PARAMETARA

DHCP server je podešen da IP adresu klijentu iznajmljuje samo za određeno vreme (lease time)

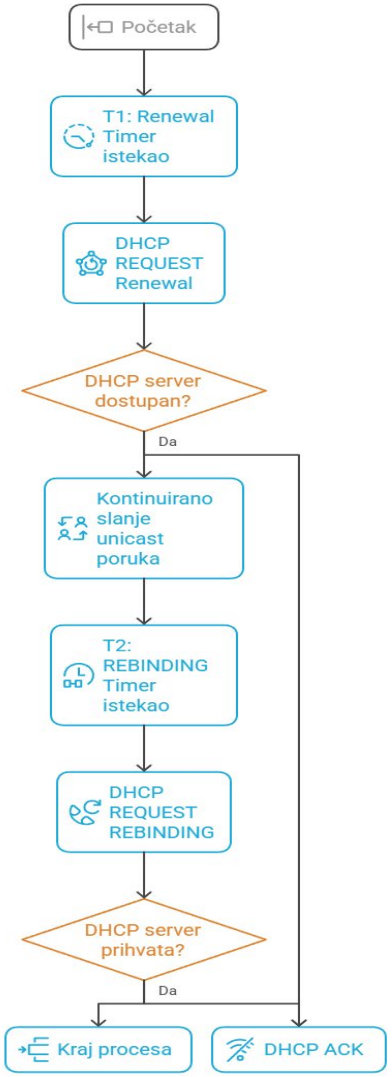
DHCP klijent može da zatraži produženje korišćenja IP adrese (renewal proces)

Renewal Timer (*T1*)

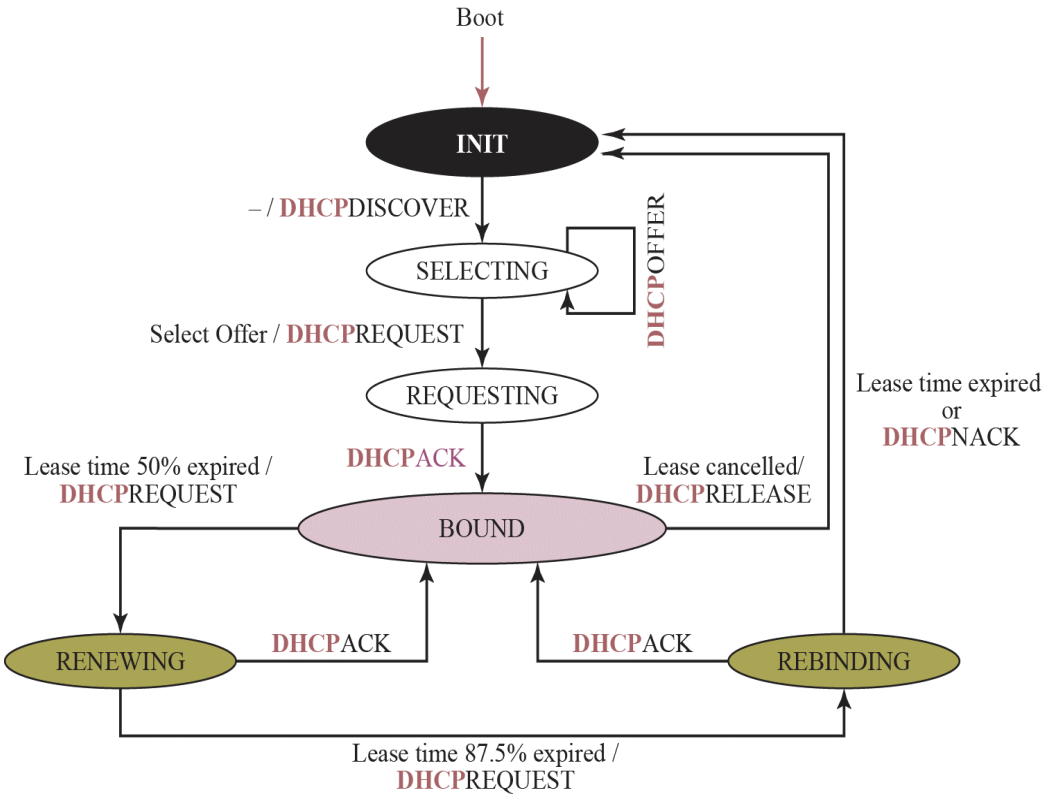
Nakon isteka ovog vremena koje obično iznosi 50% lease time, klijent započine renewing proces slanjem **unicast** poruke ***DHCP REQUEST*** **Renewal**, tražeći produženje korišćenja mrežnih parametara

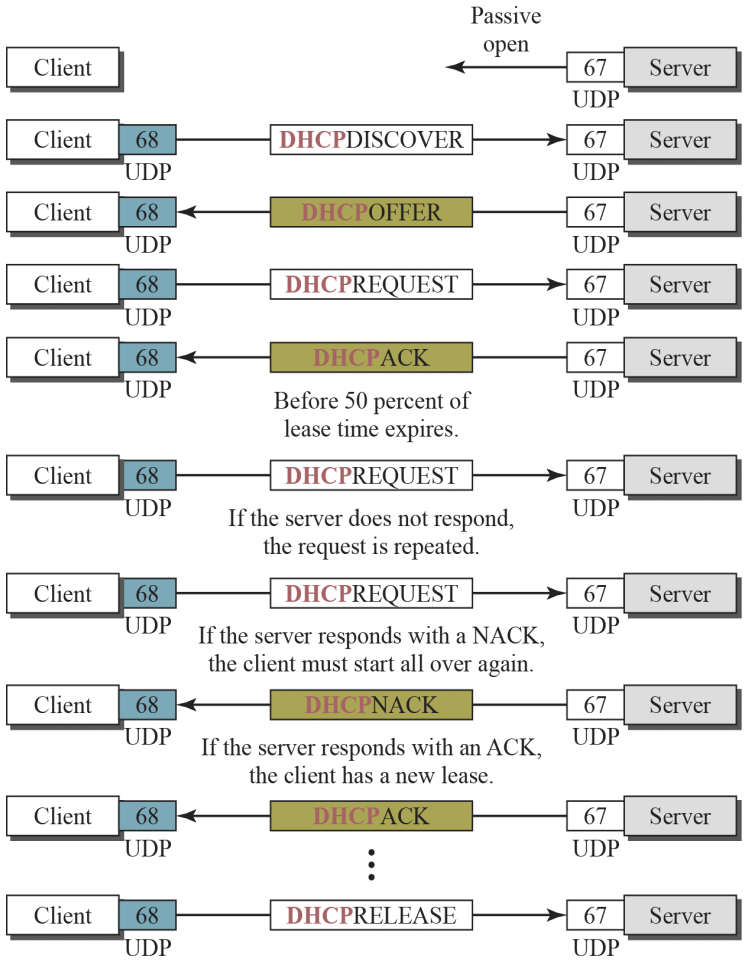
Ukoliko je DHCP server nedostupan, on će u kontinuitetu slati unicast DHCP Request poruku sve dok ne pređe u *REBINDING* stanje pokretanjem REBINDING Timer(T2) koji obično iznosi 85% lease time.

Klijent šalje **broadcast DHCP REQUEST REBINDING** poruku sa svojom IP adresom u nadi da će se javiti bilo koji dostupan DHCP server. DHCP server može prihvatiti (DHCP ACK) ili ne prihvatiti zahtev(DHCP NACK)



DHCP ALGORITAM RADA



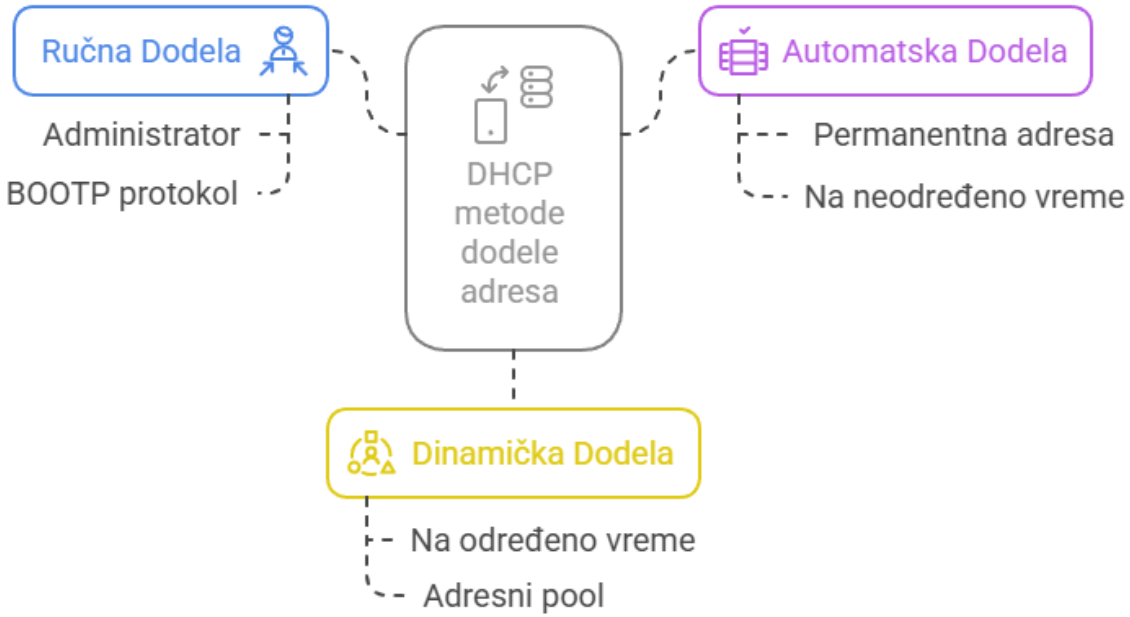


METODE DODELE ADRESA

DHCP standard uključuje tri različita metoda dodele adresa:

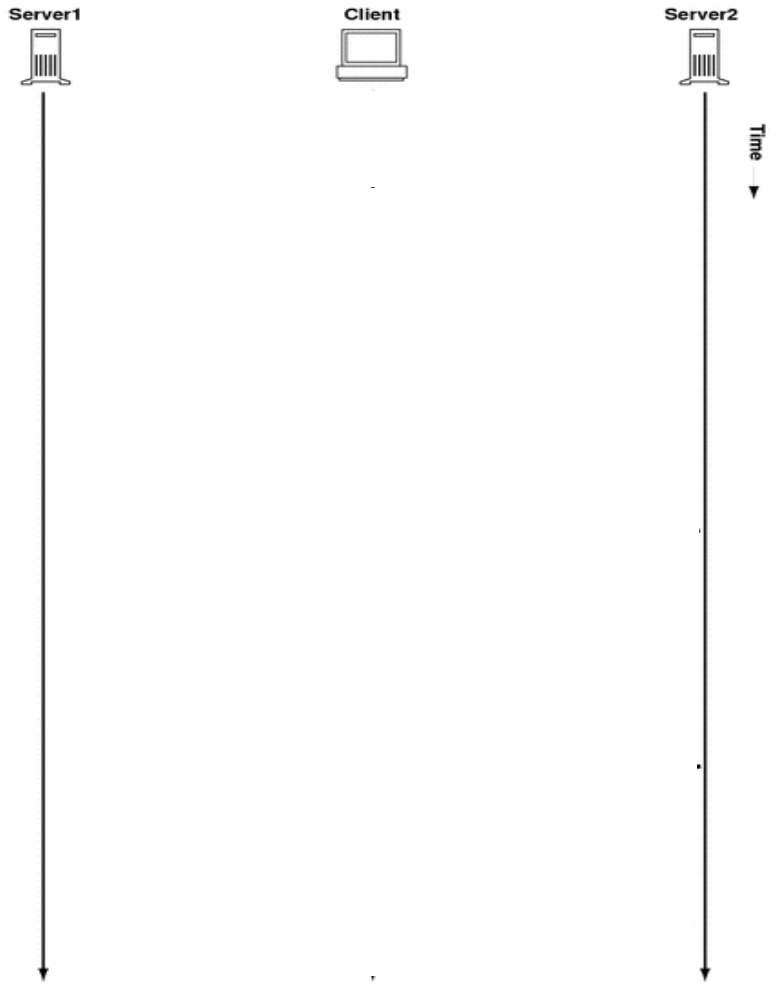
Ručna Dodela: Određena IP adresa je dodeljena uređaju od strane administratora. DHCP je servis koji je izvršio dodelu. Princip rada BOOTP protokola
Automatska Dodela: DHCP automatski zadaje permanetnu IP addresu uređaju iz svog pool-a slobodnih IP adresa **na neodređeno vreme.**
Dinamička Dodela: DHCP zadaje IP adresu iz svog pool-a **za određen vremenski period**

Administrator ne bira koju će metodu koristiti već ih kombinuje.



POSTUPAK DODELE MREŽNIH PARAMETARA

1. Klijent šalje DHCP discovery poruku u potrazi za DHCP serverima
2. DHCP serveri koji su primili poruku šalju predlog IP adrese i konfiguracione parametre
3. Klijent prima ponude i obično bira prvu pristiglu, tako što njemu šalje zahtev a koji stiže do svih DHCP servera
4. Server odgovara potvrdno i odobrava klijentu korišćenje mrežnih parametara
5. Pre isteka perioda iznajmljivanja, klijent započinje proces produženja (request renewal) korišćenja mrežnih parametara
6. Potvrda za produženje korišćenja mrežnih parametara
7. Vraćanje adrese DHCP serveru



STATIČKE / DINAMIČKE IP ADRESE

Desktop računar	**Server**	**Ruter**	**Svič**
Laptop	**IP telefon**	**Štampač**	**RADIUS server**
AP	**PDA**	**iTouch**	**Frižider**

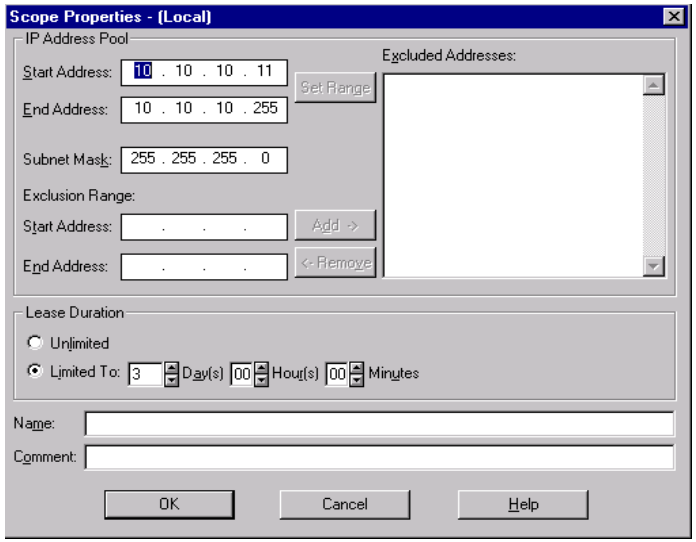
DHCP SERVER

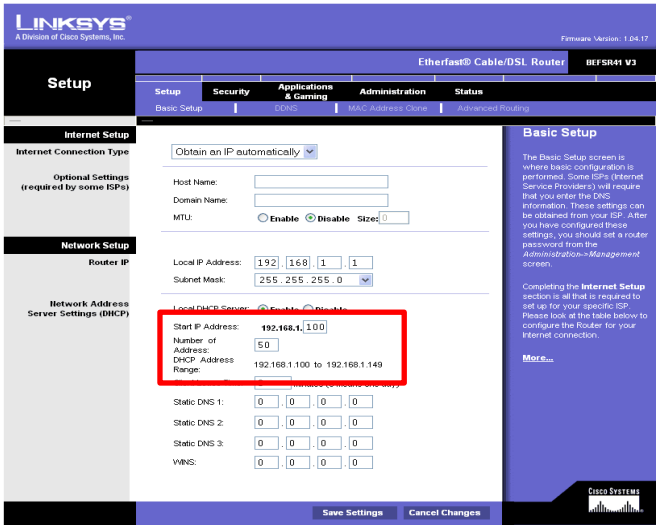
Skup adresa koje su na raspolaganju DHCP serveru su smeštene u adresnom pool-u.

Prvi problem koji je povezan sa upravljanjem adresa je obezbedjivanje adresnog opsega koji je dovoljno veliki da opslužи sve klijente.

Ukoliko imamo dovoljno adresa na raspolaganju može se koristiti duži *lease time*, u suprotnom preporučuje se kraći *lease time* kako bi poboljšali iskorišćenost adresnog opsega

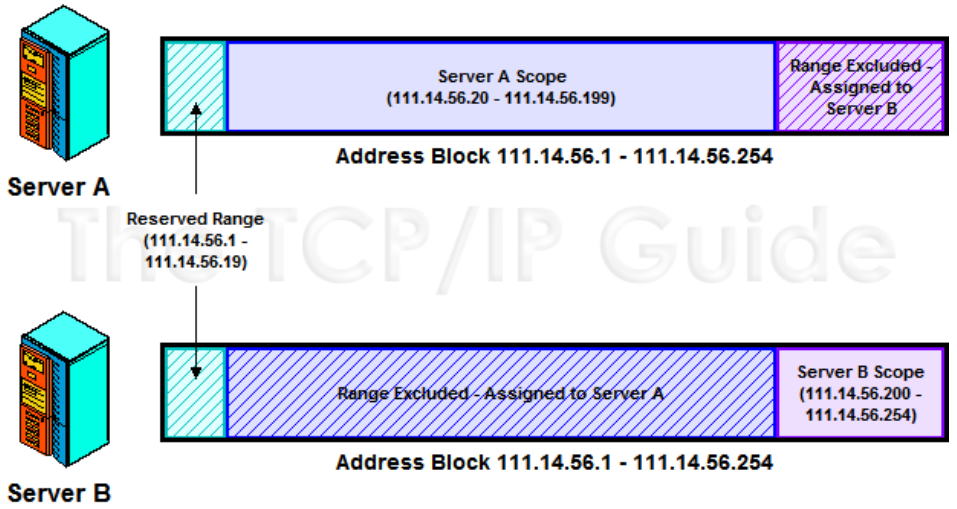
OSOBINE ADRESNOG POOL-A





UPRAVLJANE ADRESAMA PRIMENOM NEPREKLAPAJUĆIH OPSEGA

Dva DHCP servera obezbeđuju otpornost na otkaz (fault-tolerance) DHCP servisa



Dva DHCP servera sa nepreklapajućim opsezima (DHCP Multi-Server Non-Overlapping Scopes)

PREDNOST

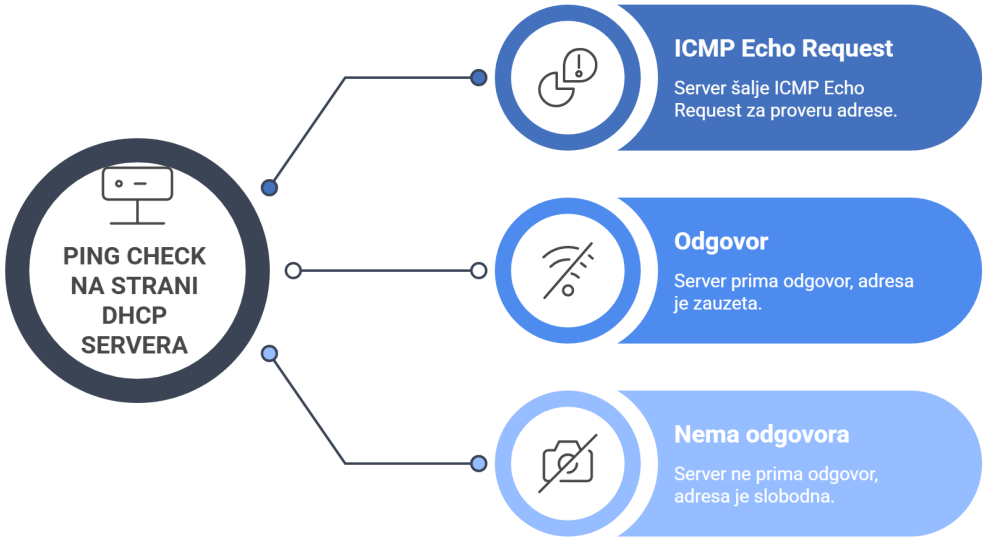
Ne javlja se problem dodele iste adrese različitim klijentima

NEDOSTATAK

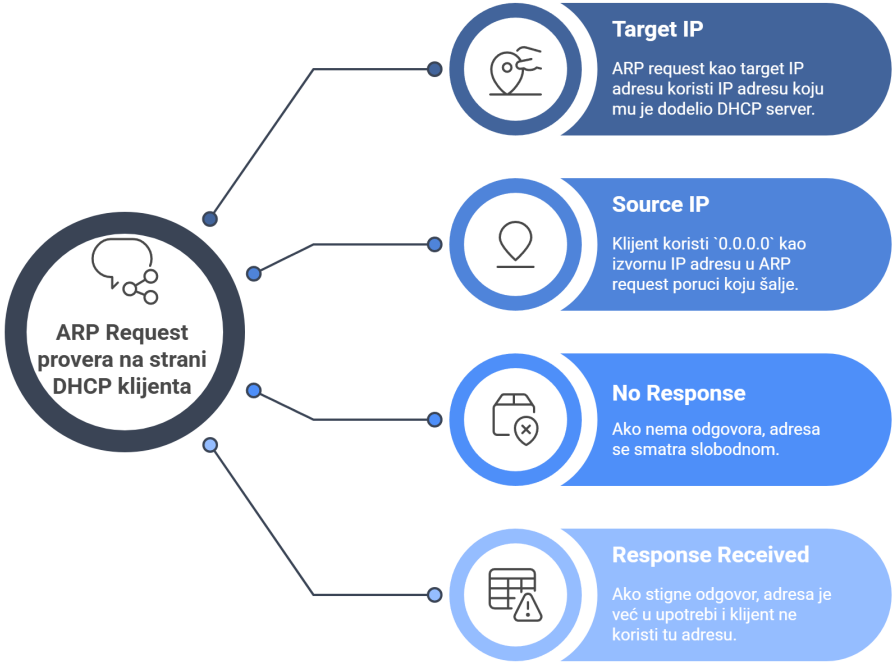
U slučaju otkaza jednog DHCP servera koristi se samo deo IP adresnog opsega iz pool-a

NAČINI DETEKCIJE KONFLIKTA – DUPLE IP ADRESE

ICMP ECHO REQUEST SE ŠALJE OD STRANE DHCP SERVERA (OPCIJONO PODEŠAVANJE)



GRATIOUS ARP SE ŠALJE OD STRANE DHCP KLIJENTA (UVEK SE ŠALJE)



DHCP SERVER - DETEKCIJA KONFLIKTA

DHCP server pod Windows-om pre nego što dodeli IP adresu pustiće ICMP Echo Request poruku da bi proverio da li se neki računar odaziva na tu adresu.

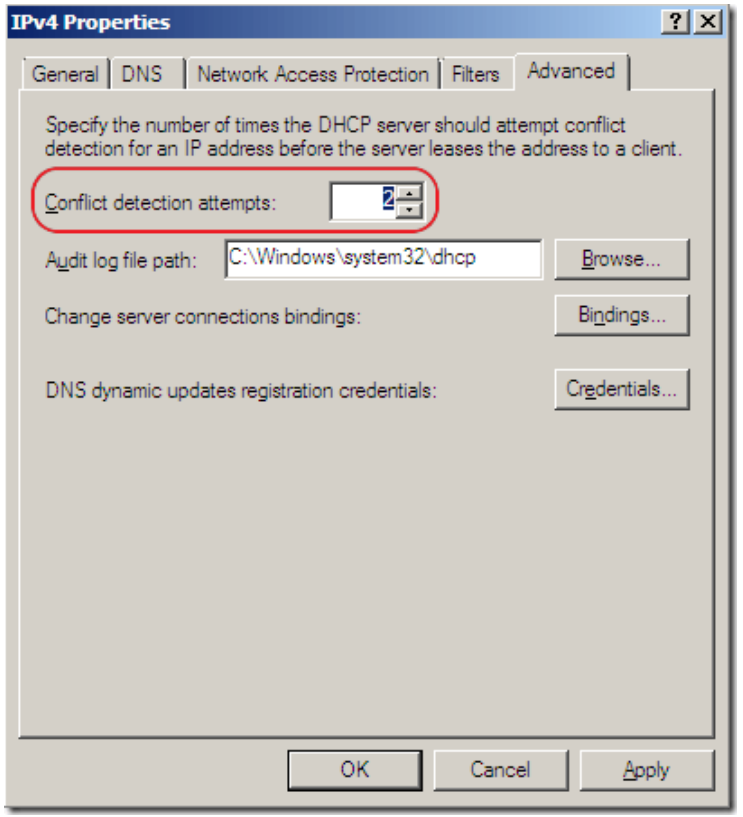
Podrazumevano, ova opcija je isključena jer unosi dodatno kašnjenje u radu DHCP servera

Problem može da predstavlja firewall na uređaju koji blokira ICMP Echo Request poruku

Ne preporučuju se više od 2 pokušaja, jer svaki pokušaj unosi kašnjenje od 1 sekunde

DHCP klijent pod Windows XP kada dobije IP adresu koristi **gratuitous ARP** zahtev da bi proverio eventualni konflikt pre nego što prihvati IP adresu.

Ukoliko DHCP klijent detektuje konflikt, on DHCP serveru šalje DHCP DECLINE poruku.



DHCP KLIJENT
PRIKAZ KONFIGURACIONIH PARAMETARA

IPCONFIG /ALL

```
Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : vts.local
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 18-03-73-5E-ED-53
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ac5d:98b4:f651:284f%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 160.99.37.201(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.128
   Lease Obtained. . . . . . . . . . : 3. septembar 2014 11:12:53
   Lease Expires . . . . . . . . . . : 3. septembar 2014 11:27:53
   Default Gateway . . . . . . . . . : 160.99.37.129
   DHCP Server . . . . . . . . . . . : 160.99.37.130
   DHCPv6 IAID . . . . . . . . . . . : 169345907
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-16-30-01-FD-18-03-73-5E-ED-53

   DNS Servers . . . . . . . . . . . : 160.99.37.130
                                       160.99.37.249
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

DHCP KLIJENT
ZAHTEV ZA VRAĆANJE PARAMETARA DHCP SERVERU

IPCONFIG /RELEASE <naziv LAN adaptera>

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :
```

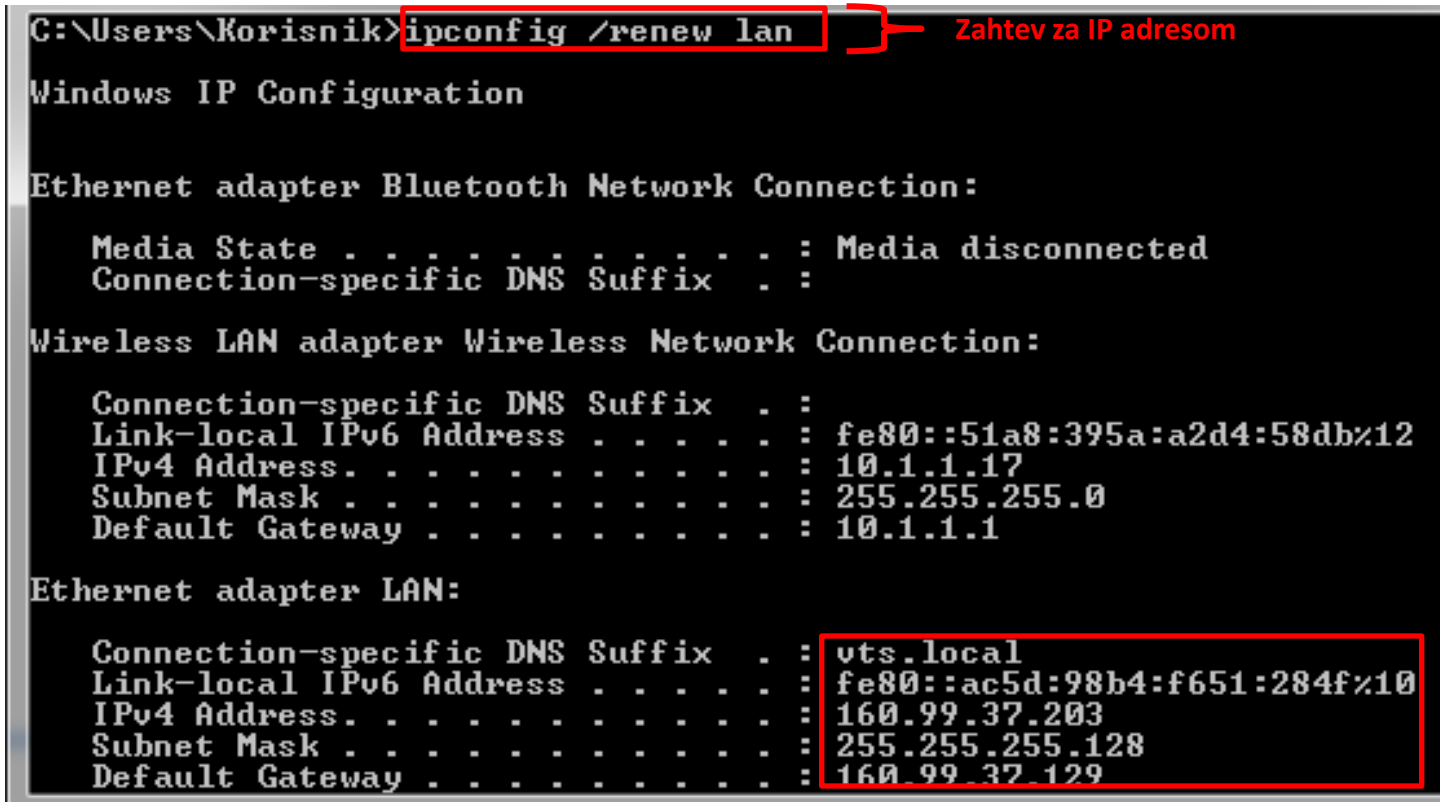
Filter: bootp — Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
422	0	160.99.37.201	160.99.37.130	DHCP	342	DHCP Release - Transaction ID 0x64a24548

```
Frame 422: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Dell_5e:ed:53 (18:03:73:5e:ed:53), Dst: Dell_28:57:7a (00:1e:4f:28:57:7a)
Internet Protocol Version 4, Src: 160.99.37.201 (160.99.37.201), Dst: 160.99.37.130 (160.99.37.130)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x64a24548
  + Seconds elapsed: 3
  + Bootp flags: 0x0000 (Unicast)
    Client IP address: 160.99.37.201 (160.99.37.201)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Dell_5e:ed:53 (18:03:73:5e:ed:53)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  + Option: (t=53,l=1) DHCP Message Type = DHCP Release
  + Option: (t=54,l=4) DHCP Server Identifier = 160.99.37.130
  + Option: (t=61,l=7) Client identifier
```

IP adresa koju klijent vraća DHCP serveru

DHCP KLIJENT
ZAHTEV ZA DODELOM PARAMETARA OD DHCP SERVERA



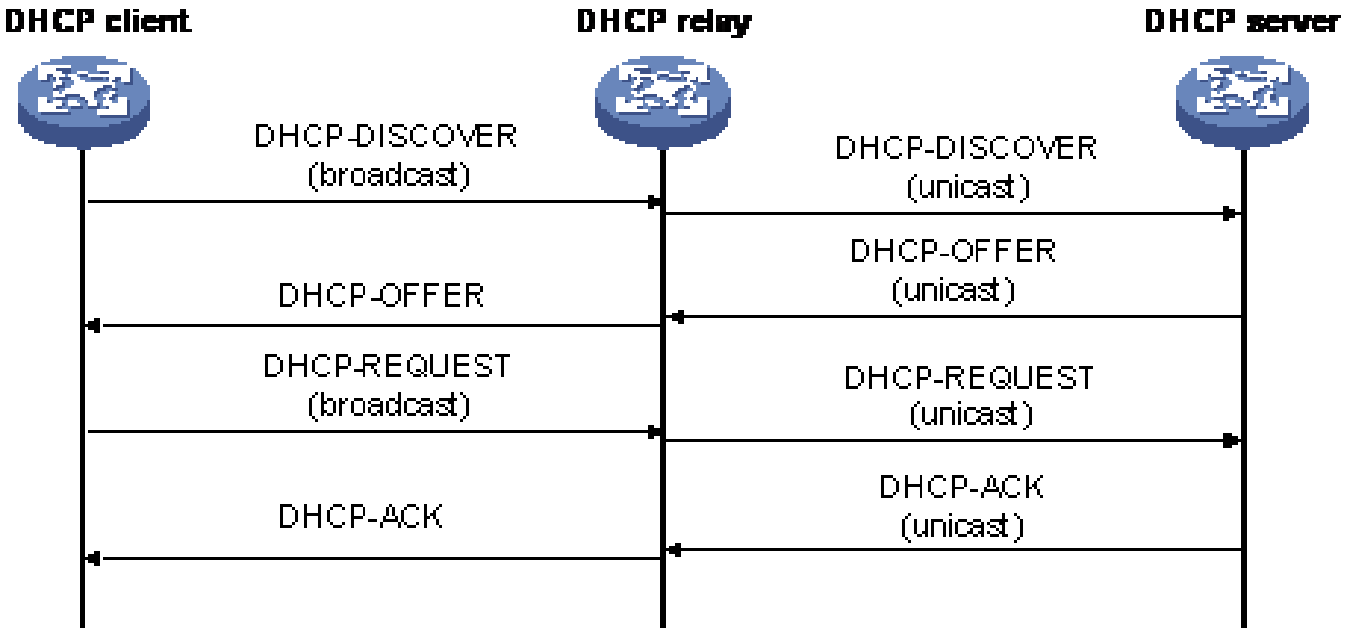
DHCP RELAY AGENT

DHCP klijenti koriste IP broadcast za pronalaženje DHCP servera u mreži

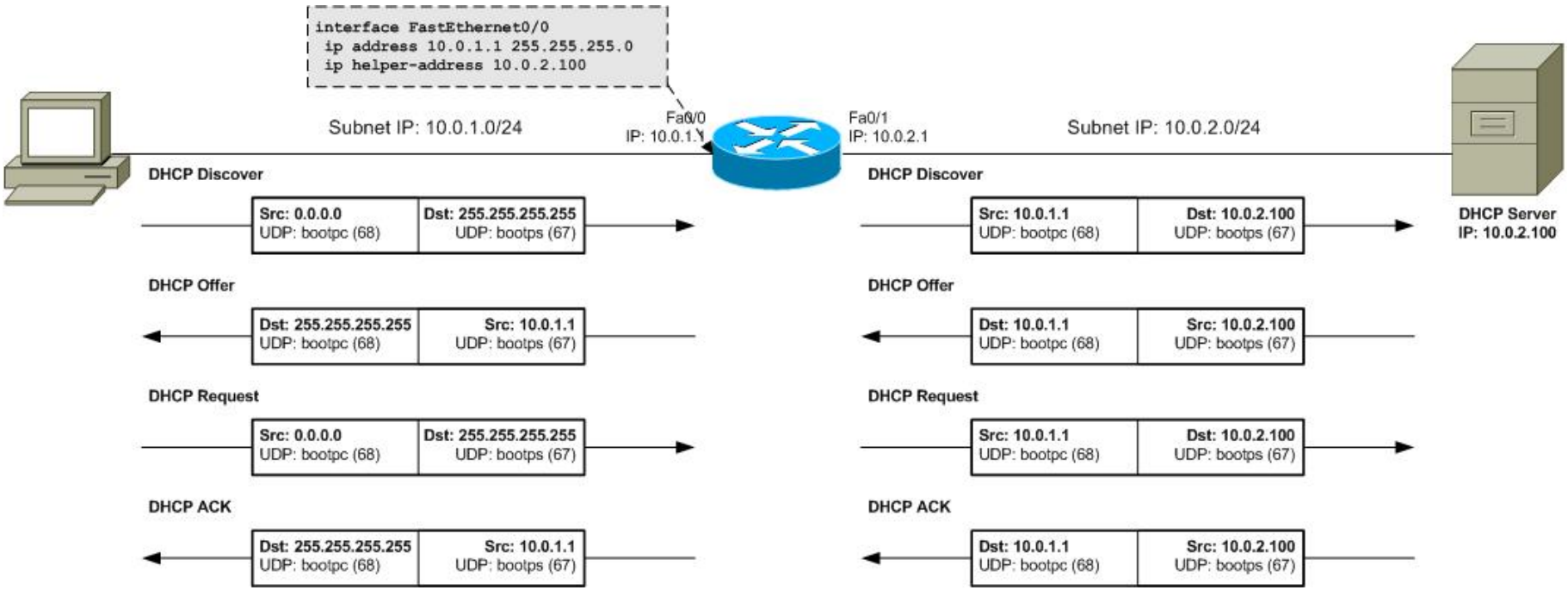
Šta se dešava ukoliko klijent i server nisu u istoj mreži tj. odvojeni su ruterom?

Ruteri ne prosleđuju broadcast poruke u drugim mrežama

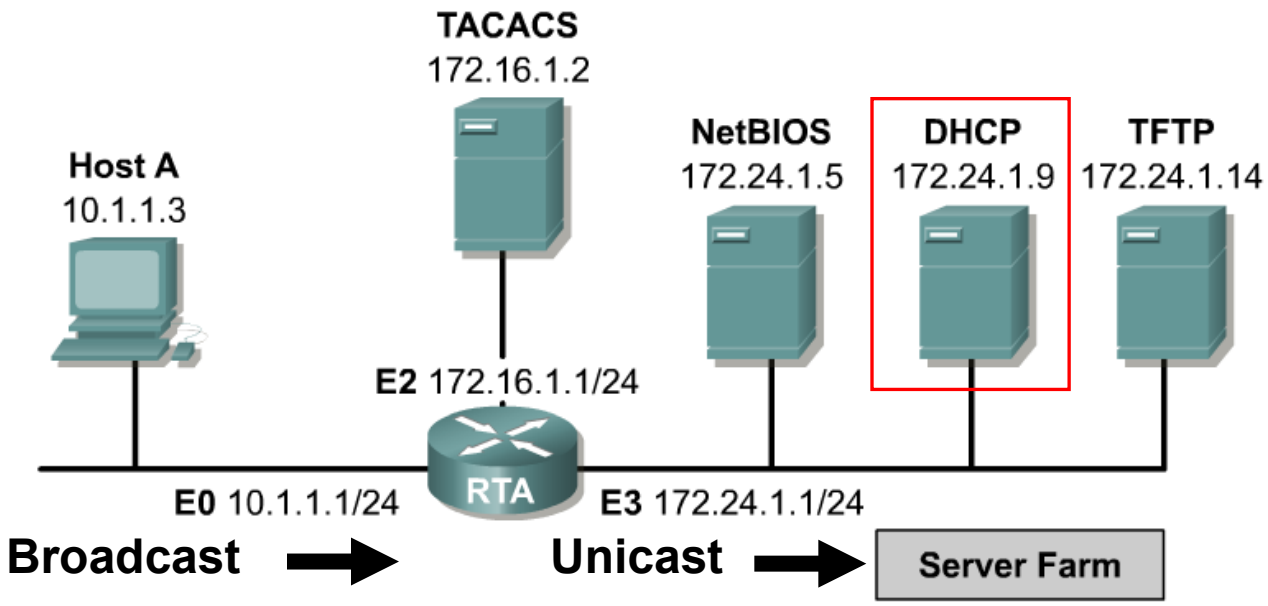
Administratori mogu da podese ruter da određene broadcast poruke na osnovu UDP porta prosleđuju na drugim segmentima



DHCP KOMUNIKACIJA PREKO RELAY AGENT-a



DHCP RELAY AGENT
KONFIGURACIJA NA RUTERU




```
RTA(config)#interface e0
RTA(config-if)#ip helper-address 172.24.1.255
RTA(config)#interface e3
RTA(config-if)#ip directed-broadcast
```

```
RTA(config)#interface e3
RTA(config-if)#ip directed-broadcast
```

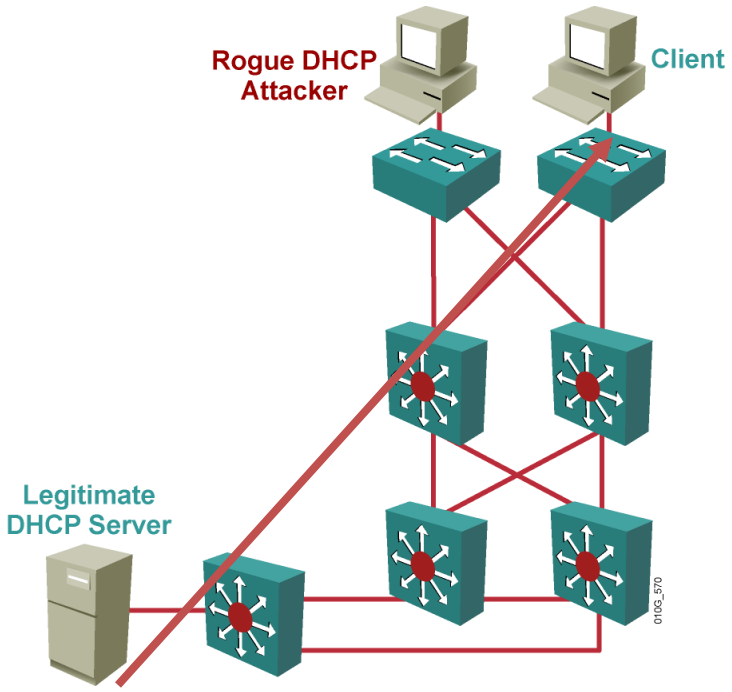
LAŽNI DHCP SERVER (DHCP SPOOF ATTACK)

- Lažni DHCP server odgovara klijentima sa DHCP requests porukom na isti način na koji to radi legitimni DHCP server.
- Lažni DHCP server DHCP klijentima može da ponudi:

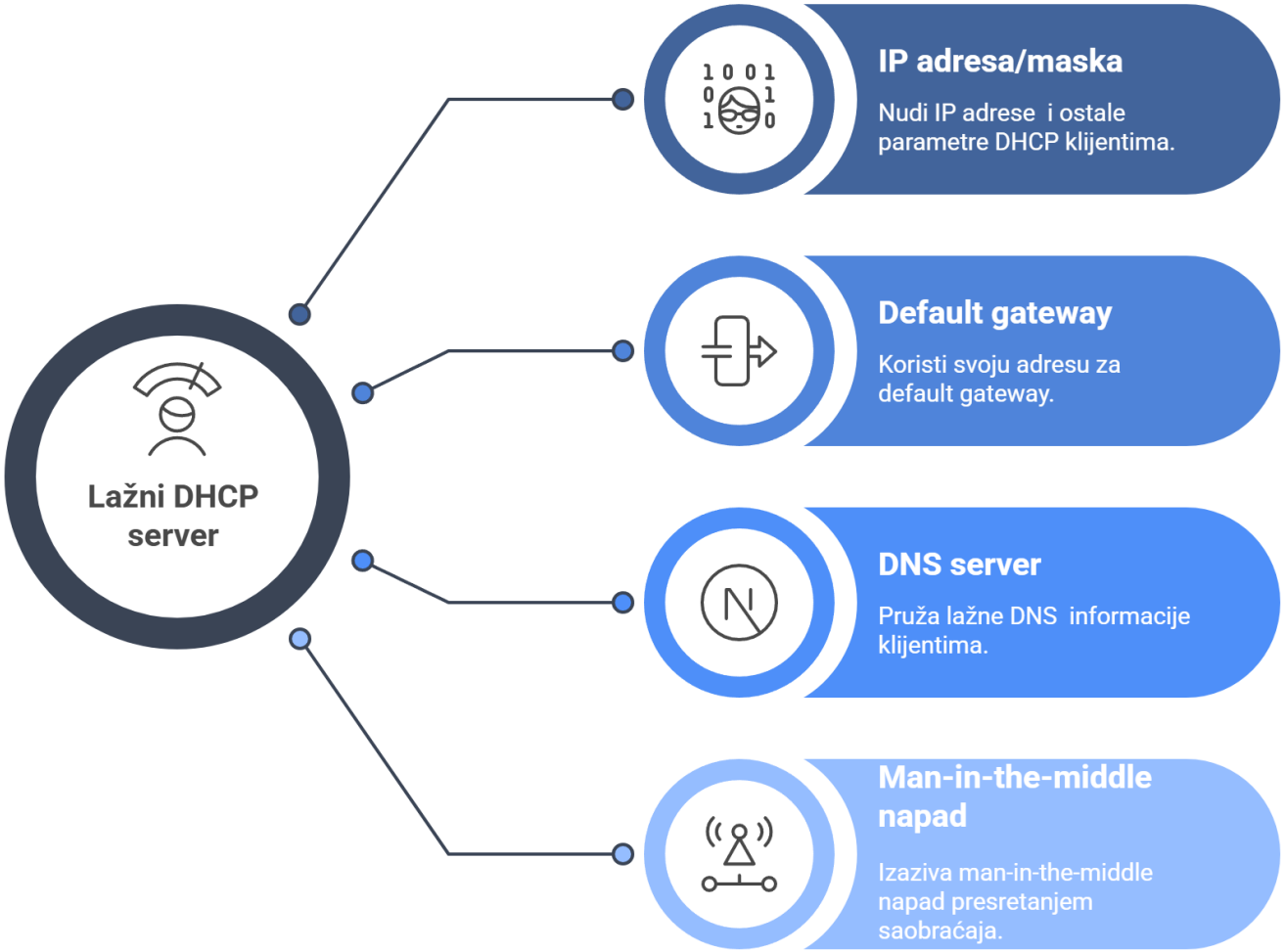
  IP address/Mask

  Default gateway

  Domain Name System (DNS) server
- Lažni DHCP server može svoju adresu da koristi kao default gateway, što izaziva da klijenti sav saobraćaj van svoje mreže šalju DHCP serveru, koji zatim pakete prosleđuje ka pravom odredištu.
- Napad je poznat kao **man-in-the-middle**

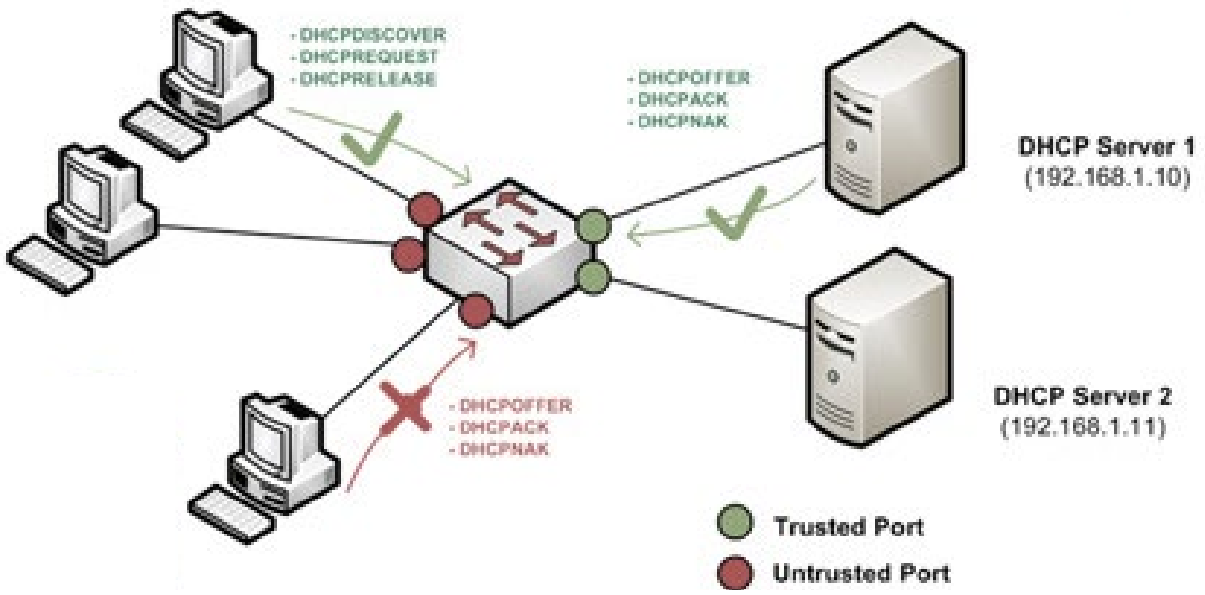


LAŽNI DHCP SERVER (DHCP SPOOF ATTACK)



DHCP SNOOPING OPCIJA

- Sam DHCP protokol nema ugrađeni mehanizam da se bori protiv lažnih DHCP servera
- Rešenje se ogleda u zaštiti portova na samom aktivnom mrežnom uređaju kao što je LAN svič
- Portovi na sviču se definišu kao trusted ili untrusted
- Portovi koji su trusted prosleđuju sve DHCP poruke, dok portovi koji su untrusted blokiraće DHCP poruke koje šalju DHCP serveri tzv. DHCP response poruke(DHCP OFFER, DHCP ACK ili DHCP NAK)



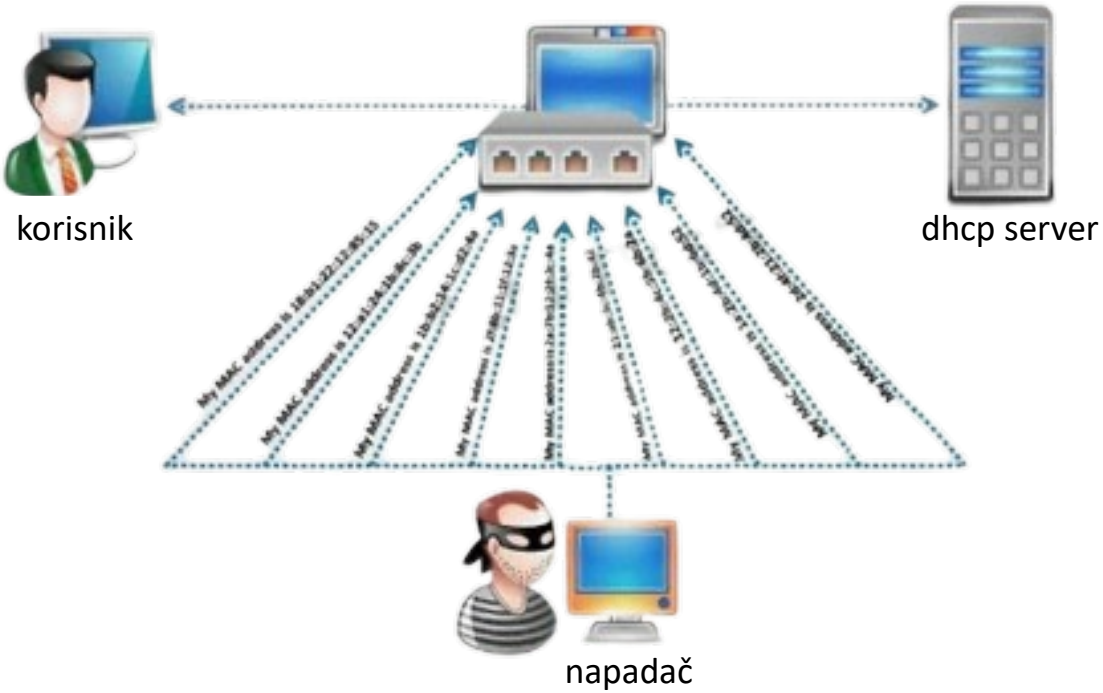
DHCP IZGLADNJIVANJE SERVERA (DHCP STARVATION)

Napadač pokreće DoS napad šaljući na 1000 DHCP zahteva (DHCP discovery).

DHCP server ne može da odredi da li je zahtev legitiman.

Napad može da za par minuta isprazni adresni pool na DHCP serveru

Rezultat je da legitimni korisnik ne može da dobije konfiguracione parametre (DOS napad) ili da napad predstavlja pripremu za DHCP SPOOF napad.

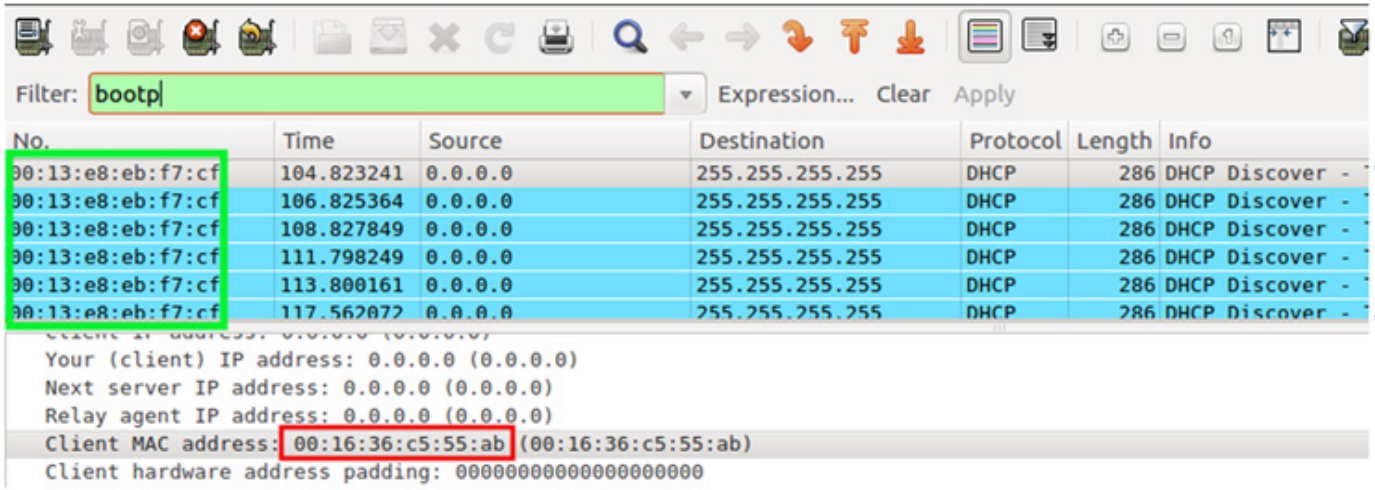


DHCP IZGLADNJIVANJE SERVERA (DHCP STARVATION)

DHCP Snooping upoređuje MAC adresu koja se nalazi u payload-u DHCP protokola i izvorišnu MAC adresu frejma primenom opcione komande ip dhcp snooping verify mac-address.

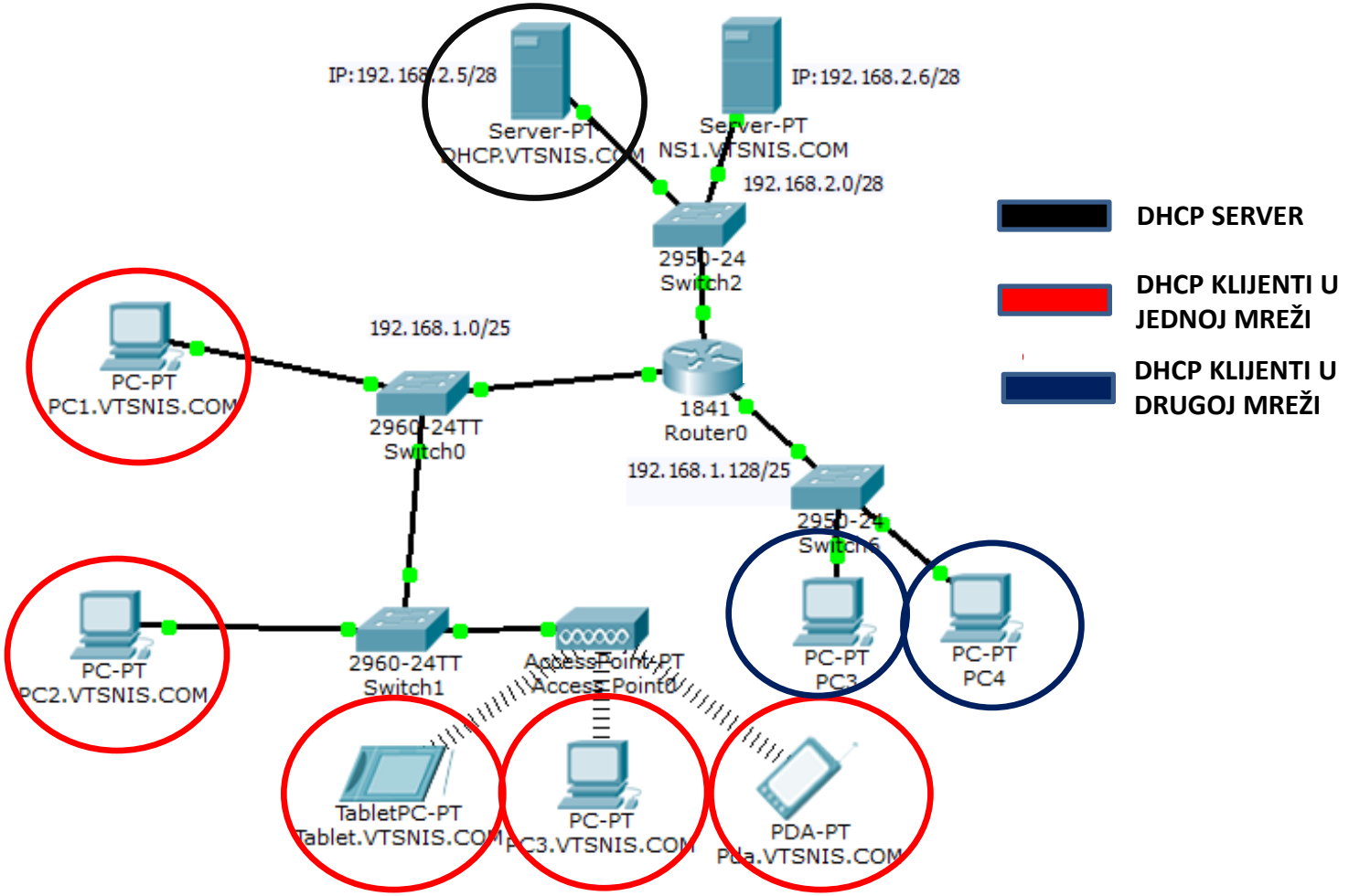
Moguće je podesiti "maximum threshold" ili broj paketa u sekundi koji mogu da prođu kroz port.

Ako je broj DHCP paketa dostigne prag, port će preći u shutdown stanje i generisaće poruku o DoS napadu.



Svi DHCP discovery zahtevi se šalju sa istom Mac adresom. Port security opcija iz tog razloga nema efekta.

DHCP KONFIGURACIJA
LAB VEŽBA



DHCP KONFIGURACIJA
PACKET TRACER

DHCP server opslužuje dve IP mreže.

Potrebno je obezbediti da ruter prosleđuje DHCP poruke do DHCP servera jer se DHCP server ne nalazi u mreži DHCP klijenata

Na DHCP serveru kreirati dva pool-a sa odgovarajućim mrežnim prolazima:

Pool1: 192.168.1.10-192.168.1.50

Pool2: 192.168.1.150 – 192.168.1.185