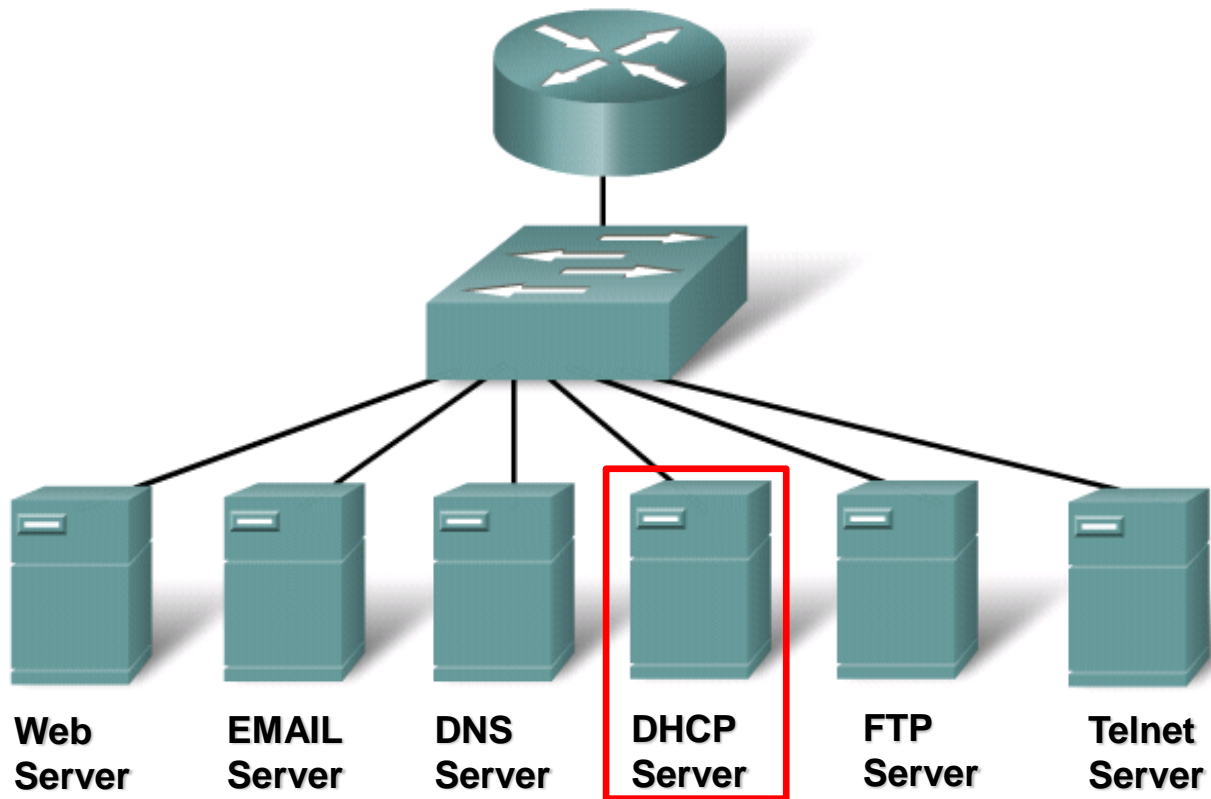


MREŽNI SERVISI



VTS NIŠ
OSNOVNE STRUKOVNE STUDIJE
SAVREMENE RAČUNARSKE TEHNOLOGIJE

DHCP SERVIS



DHCP SERVIS

OSOBI NE DHCP SERVIS A

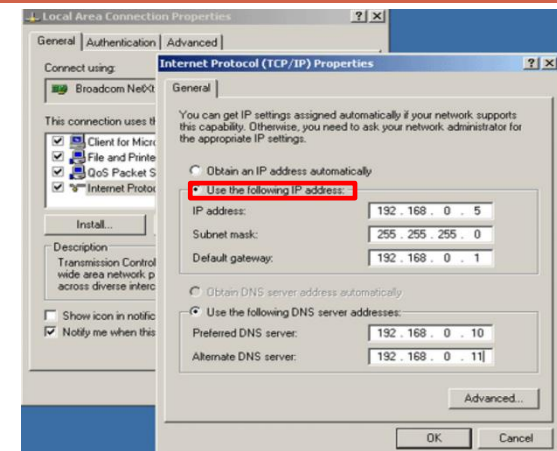
DHCP (Dynamic Host Configuration Protocol) je protokol za dinamičku konfiguraciju mrežnih parametara na mrežnim uređajima

Mrežni parametri koji uključuju **IP adresu**, **Podmrežnu Masku (Subnet Mask)**, **Podrazumevani mrežni prolaz (Default Gateway)** i **DNS IP adrese** mrežnom uređaju se mogu zadati **statički** (ručno) ili **dinamički** (preko DHCP-a)

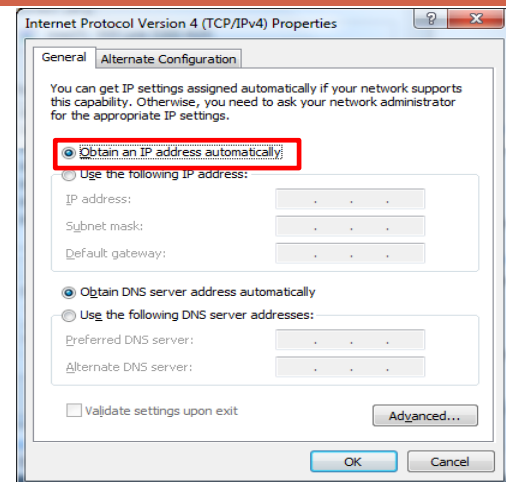
Dinamičko zadavanje mrežnih parametara :

1. Sprečava dupliciranje IP adresa
2. Sprečava greške u unosu mrežnih parametara
3. Obezbeđuje bolje iskorišćenje IP adresa
4. Obezbeđuje mobilnost (Laptop, Smartphone)

RUČNA KONFIGURACIJA MREŽNIH PARAMETARA



DINAMIČKA KONFIGURACIJA



DHCP SERVIS

PRVOBITNO REŠENJE ZA DINAMIČKU DODELU IP ADRESA(RARP)

Reverse Address Resolution Protocol (RARP)

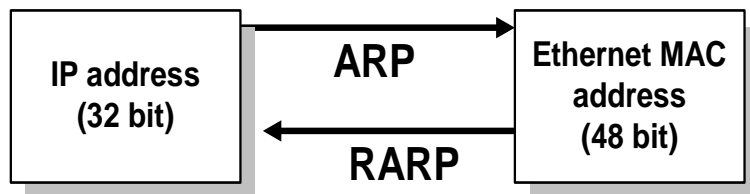
Princip sličan ARP-u

Broadcast zahtev sa MAC adresom klijenta šalje se RARP serveru

RARP server odgovara unicast porukom, IP adresom koja je unapred definisana na osnovu MAC adrese

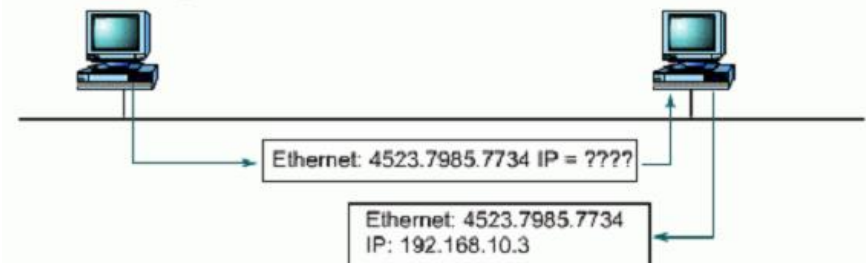
Šalje samo IP adresu (ne prosleđuje Default gateway i Subnet Mask)

Protokol su koristili terminali koji nisu imali storage sistem, već su na osnovu MAC adrese trežili IP adresu



RARP Klijent

RARP Server



DHCP SERVIS



OSOBI NE BOOTP PROTOKOLA

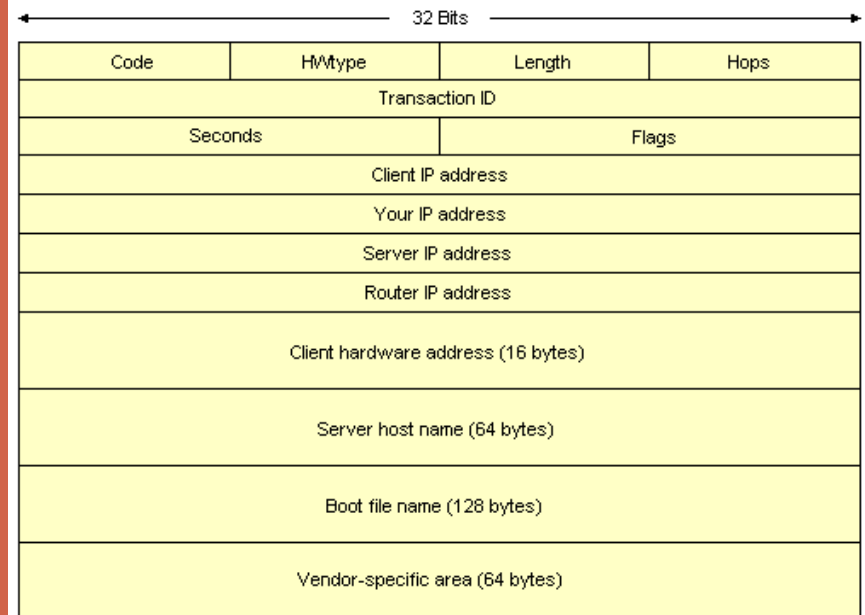
BOOTP strap protokol (1985) je prva varijanta DHCP protokola i predstavlja alternativu RARP (Reverse ARP) protokolu koji je mogao da dodeli samo IP adresu računaru na osnovu njegove MAC adrese

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

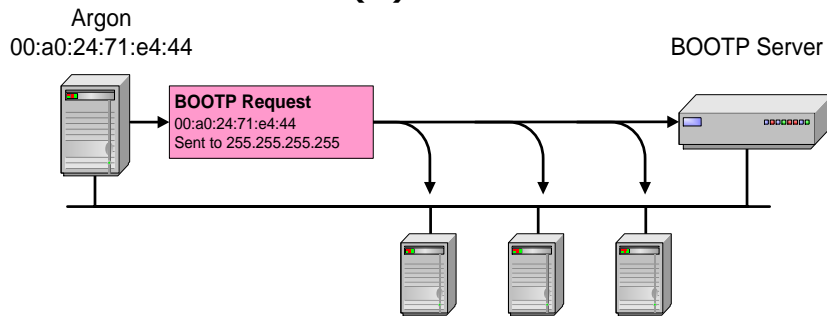


DHCP SERVIS

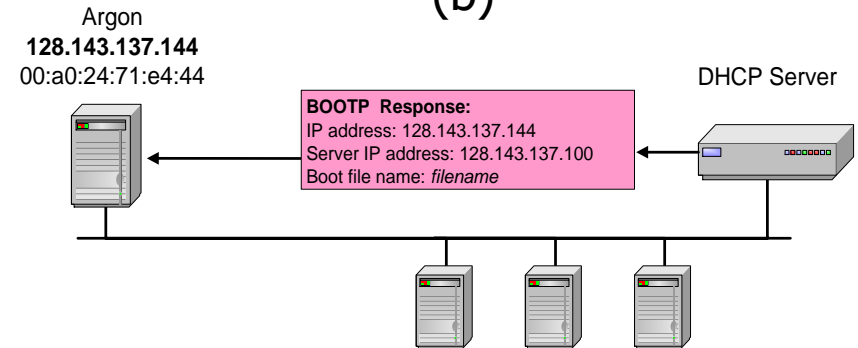


OSOBI NE BOOTP PROTOKOLA

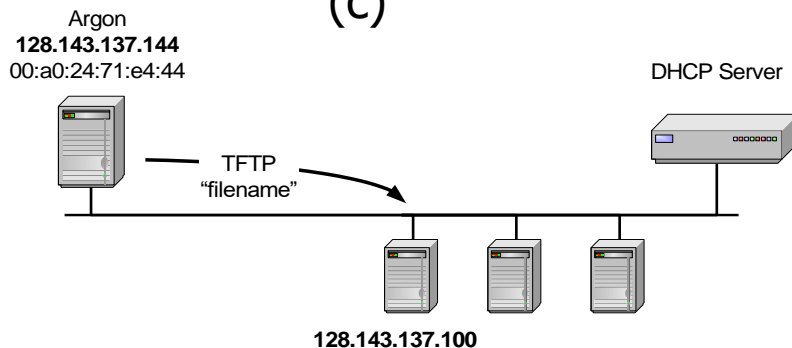
(a)



(b)



(c)



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 SERVIS



DHCP PROTOKOL

DHCP protokol (1993) je modernija verzija BOOTP protokola

DHCP dozvoljava dodatne konfiguracione opcije i omogućuje dinamičku dodelu adresa

DHCP server obezbeđuje sledeće konfiguracione parametre host-u:

IP Address (IP adresu)

Subnet Mask (Podmrežna maska)

Default Gateway (Podrazumevani mrežni prolaz)

Domain Name (Naziv domena)

DNS Server

TFTP Server Location (IP adresa TFTP servera)

NetBIOS Name

...

najčešće korišćeni
konfiguracioni parametri

DHCP SERVIS



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 SERVIS



DHCP PORUKE

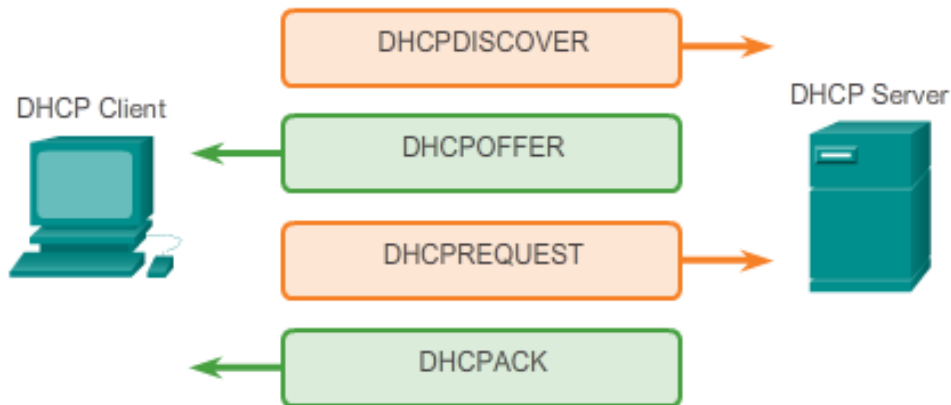
DHCP komunikacija odvija se u četiri faze:

DHCP Discovery (prepoznavanje)

DHCP Offer (ponuda)

DHCP Request (zahtev)

DHCP ACK (potvrda)



DHCP SERVIS



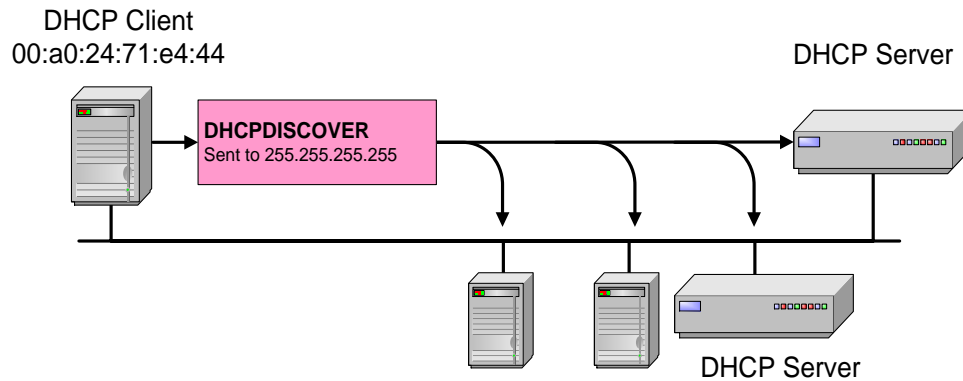
DHCP PORUKE

- DHCPACK:** Potvrda od DHCP servera da se slaže da klijent koristi konfiguracione parametre
- DHCPNACK:** Negativni odgovor od servera klijentu, ukazujući da je klijentu isteklo vreme iznajmljivanja parametara ili da tražena IP adresa ne može da se dodeli. Klijent startuje konfiguracioni proces od početka
- DHCPDECLINE:** Poruka od klijenta serveru koja ukazuje da se ponuđena adresa već koristi, klijent startuje konfiguracioni proces od početka
- DHCPRELEASE:** Poruka od klijenta serveru da više ne želi da koristi dodeljenu IP adresu.
- DHCPINFORM:** Poruka od klijenta koji već ima IP adresu (ručno konfigurisanu), zahtevajući dodatne konfiguracione parametre od DHCP servera

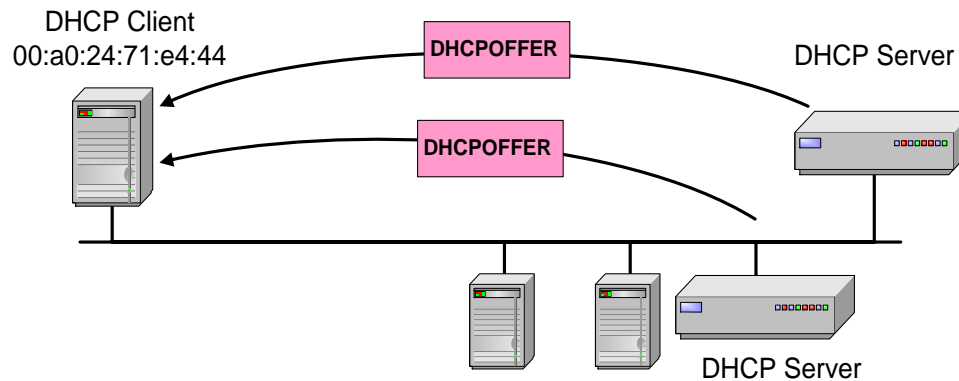
DHCP SERVIS



DCHP DISCOVERY



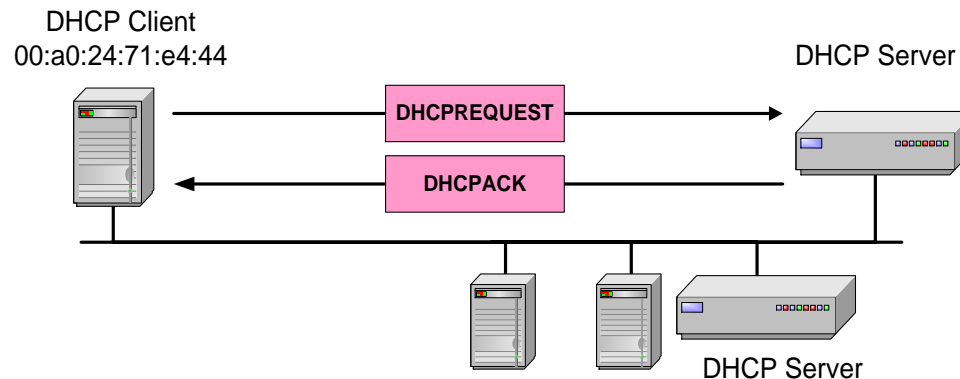
DCHP OFFER



DHCP SERVIS



DHCP REQUEST / DHCP ACK



Od ovog trenutka DHCP klijent počinje da koristi dodeljenu IP adresu i konfiguracione parametre

DHCP server je za klijenta kreirao unos na osnovu dodeljene IP adrese i njegove MAC adrese u vidu jedinstvenog identifikatora za koji su vezani njegovi parametri

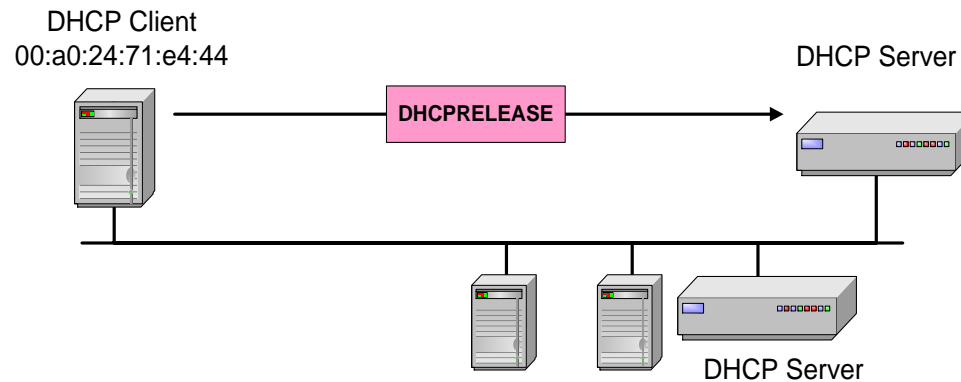
Nakon 50% isteklog vremena klijent ponovo šalje zahtev za produženjem korišćenja konfiguracionih parametara.

Ako DHCP server pošalje DHCPNACK, klijent oslobađa adresu.

DHCP SERVIS



DHCP RELEASE



Od ovog trenutka DHCP klijent je ostao bez IP adrese i konfiguracionih parametara

DHCP SERVIS



DHCP DISCOVERY PORUKA

Filter: **bootp** Expression... Clear Apply

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x896

⊕ Ethernet II, Src: Dell_5e:ed:53 (18:03:73:5e:ed:53), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

⊕ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)

⊕ 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: 0x896aa428
Seconds elapsed: 0

⊕ Bootp flags: 0x8000 (Broadcast)
Client IP address: 0.0.0.0 (0.0.0.0)
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 Discover
⊕ Option: (t=61,l=7) Client identifier
⊕ Option: (t=50,l=4) Requested IP Address = 160.99.37.161
⊕ Option: (t=12,l=11) Host Name = "Korisnik-PC"
⊕ Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
[-] Option: (t=55,l=12) Parameter Request List

} identifikacija klijenta na osnovu MAC adrese

DHCP SERVIS



DHCP OFFER PORUKA

Filter: bootp Expression... Clear Apply

Source	Destination	Protocol	Length	Info
160.99.37.130	255.255.255.255	DHCP	344	DHCP offer - Transaction ID 0x896aa428

Ethernet II, Src: Dell_28:57:7a (00:1e:4f:28:57:7a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 160.99.37.130 (160.99.37.130), Dst: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

Bootstrap Protocol

Message type: Boot Reply (2)

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x896aa428

Seconds elapsed: 0

Bootp flags: 0x0000 (unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 160.99.37.161 (160.99.37.161)

Next server IP address: 160.99.37.130 (160.99.37.130)

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 offer

Option: (t=1,l=4) Subnet Mask = 255.255.255.128

Option: (t=58,l=4) Renewal Time Value = 7 minutes, 30 seconds

Option: (t=59,l=4) Rebinding Time Value = 13 minutes, 7 seconds

Option: (t=51,l=4) IP Address Lease Time = 15 minutes

Option: (t=54,l=4) DHCP Server Identifier = 160.99.37.130

Option: (t=15,l=10) Domain Name = "vts.local"

Option: (t=3,l=4) Router = 160.99.37.129



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 SERVIS



DHCP REQUEST PORUKA

Filter: bootp Expression... Clear Apply

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x896aa428

Ethernet II, Src: Dell_5e:ed:53 (18:03:73:5e:ed:53), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
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: 0x896aa428
Seconds elapsed: 0

- ⊕ Bootp flags: 0x8000 (Broadcast)
Client IP address: 0.0.0.0 (0.0.0.0)
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 Request
- ⊕ Option: (t=61,l=7) Client identifier
- ⊕ Option: (t=50,l=4) Requested IP Address = 160.99.37.161
- ⊕ Option: (t=54,l=4) DHCP Server Identifier = 160.99.37.130
- ⊕ Option: (t=12,l=11) Host Name = "Korisnik-PC"
- ⊕ Option: (t=81,l=14) client Fully Qualified Domain Name
- ⊕ Option: (t=60,l=8) vendor class identifier = "MSFT 5.0"
- ⊕ Option: (t=55,l=12) Parameter Request List



Zahtevana IP adresa



DHCP server od koga se traži adresa

DHCP SERVIS



DHCP ACK

Filter: bootp Expression... Clear Apply

Source	Destination	Protocol	Length	Info
160.99.37.130	255.255.255.255	DHCP	349	DHCP ACK - Transaction ID 0x896aa428

Ethernet II, Src: Dell 28:57:7a (00:1e:4f:28:57:7a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 160.99.37.130 (160.99.37.130), Dst: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)

Bootstrap Protocol

Message type: Boot Reply (2)

Hardware type: Ethernet

Hardware address length: 6

Hops: 0

Transaction ID: 0x896aa428

Seconds elapsed: 0

Bootp flags: 0x0000 (unicast)

Client IP address: 0.0.0.0 (0.0.0.0)

Your (client) IP address: 160.99.37.161 (160.99.37.161)

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 ACK

Option: (t=58,l=4) Renewal Time Value = 7 minutes, 30 seconds

Option: (t=59,l=4) Rebinding Time Value = 13 minutes, 7 seconds

Option: (t=51,l=4) IP Address Lease Time = 15 minutes

Option: (t=54,l=4) DHCP server Identifier = 160.99.37.130

Option: (t=1,l=4) Subnet Mask = 255.255.255.128

Option: (t=81,l=3) Client Fully Qualified Domain Name

Option: (t=15,l=10) Domain Name = "vts.local"

Potvrda da DHCP klijent može da koristi tražene konfiguracione parametre

DHCP vremenski parametri su objašnjeni u narednom slajdu

DHCP SERVIS

DHCP VREME IZNAJMLJIVANJA KONFIGURACIONIH PARAMETARA

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

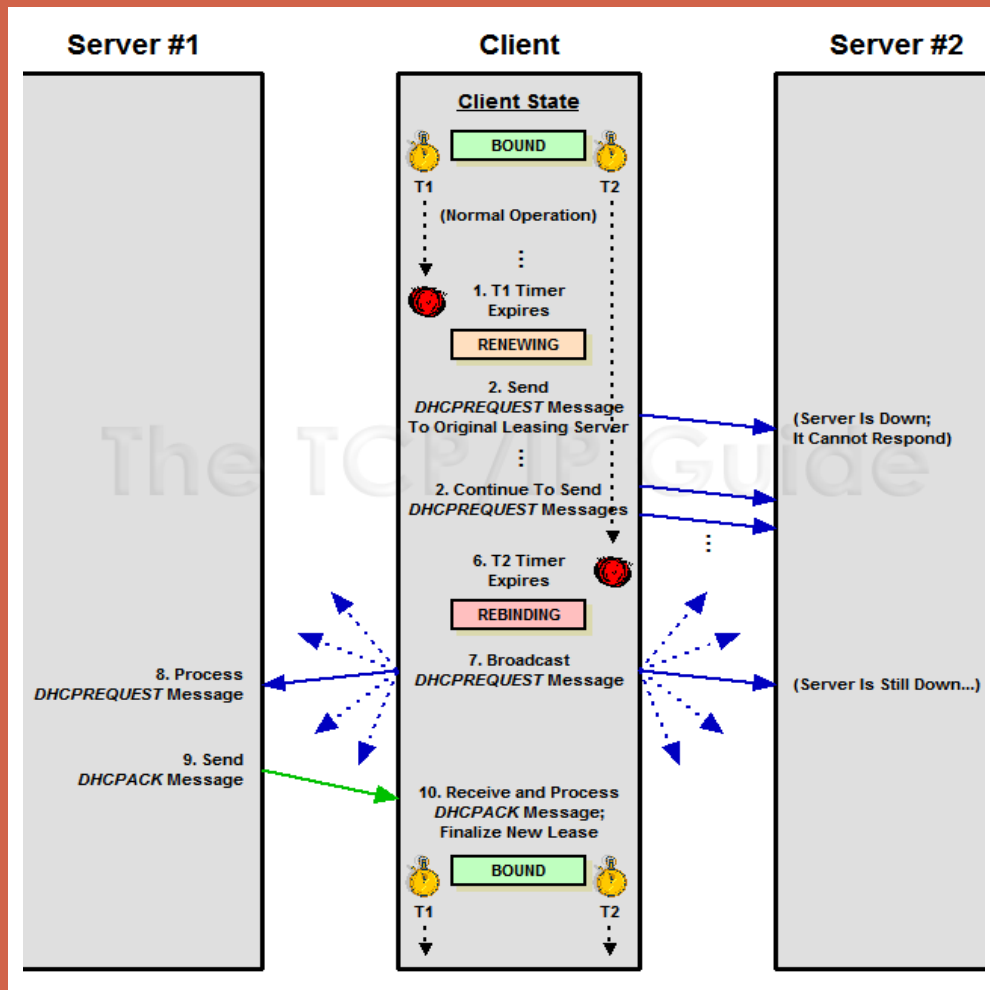
DHCP klijent može da zatraži produženje korišćenja IP adrese (renewal proces)

Renewal Timer ($T1$)

Nakon isteka ovog vremena koje obično iznosi 50% lease time, klijent započne 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.

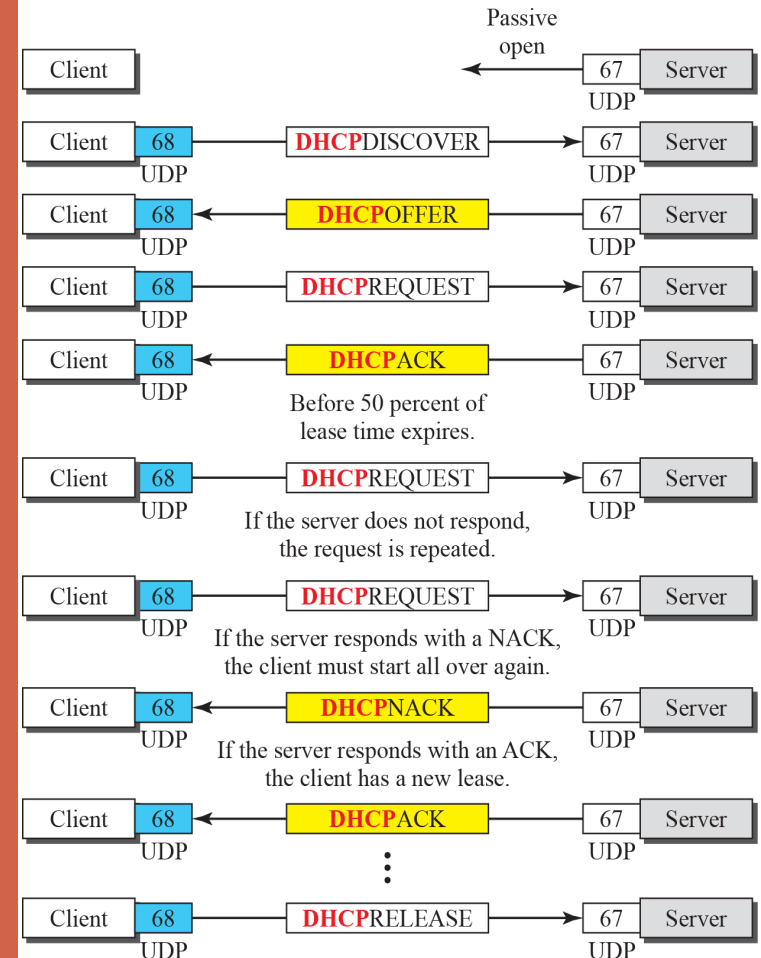
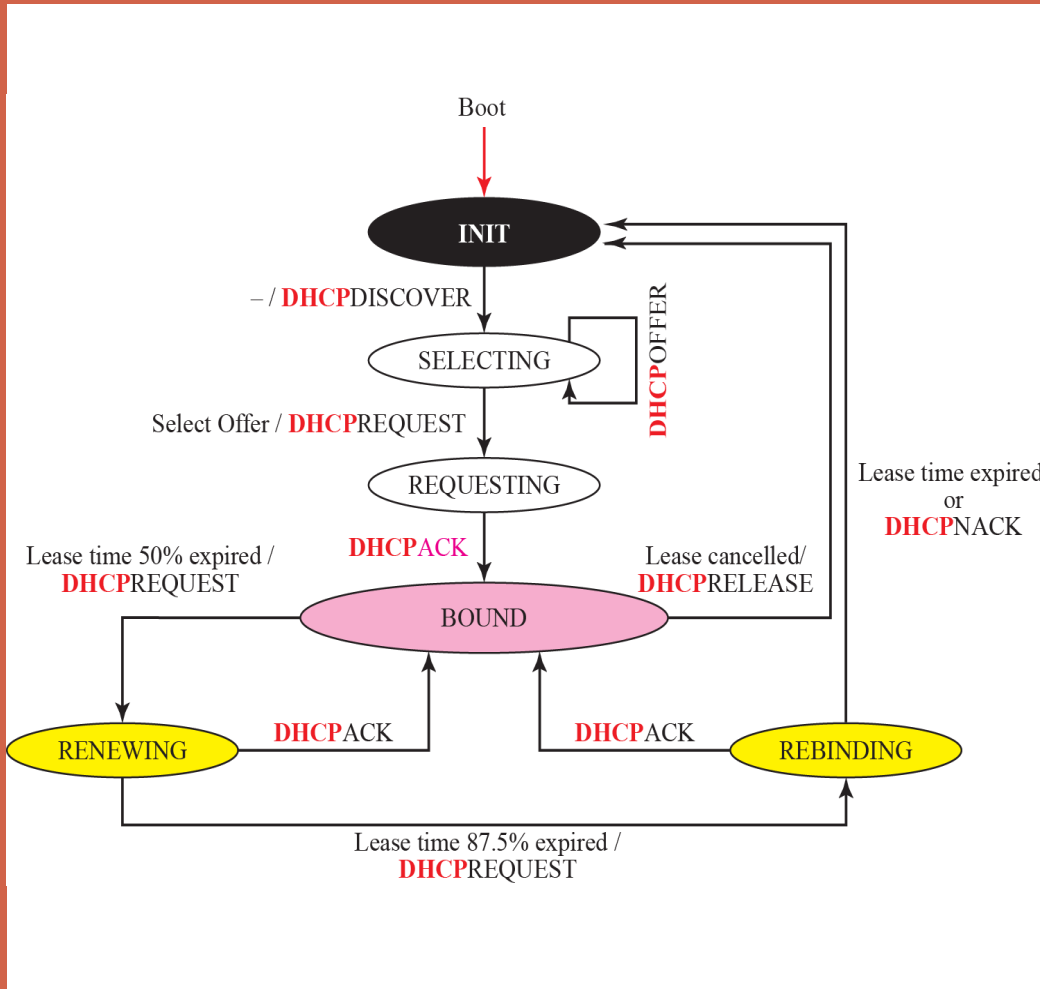
Klijent šalje **broadcast DHCP REQUEST REBINDING** poruku sa svojom IP adresom u nadi da će se javiti bilo koji dostupan DHCP server. DHCP server može prihvatiti (DHCP ACK) ili ne prihvatiti zahtev(DHCP NACK)



DHCP SERVIS



DHCP ALGORITAM RADA



DHCP SERVIS



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 adresu 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

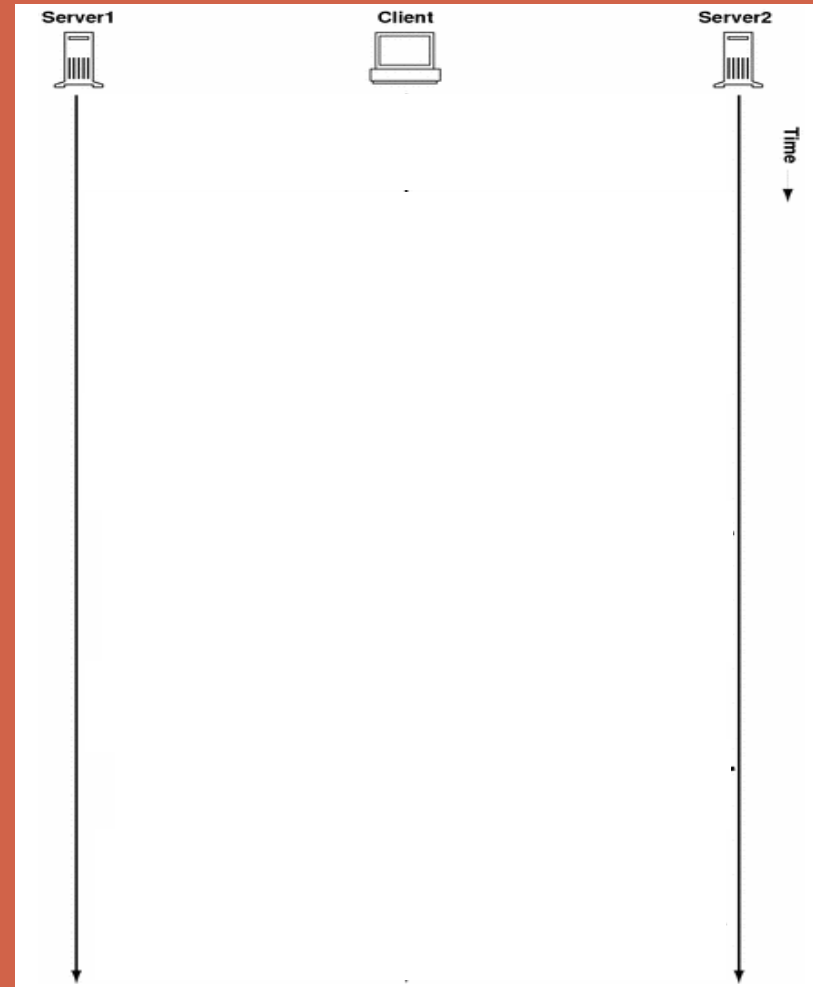
Administrator ne bira koju će metodu koristiti već ih kombinuje.

DHCP SERVIS



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



DHCP SERVIS



STATIČKE / DINAMIČKE IP ADRESE

Desktop računar

Laptop

AP

Server

IP telefon

PDA

Ruter

Štampač

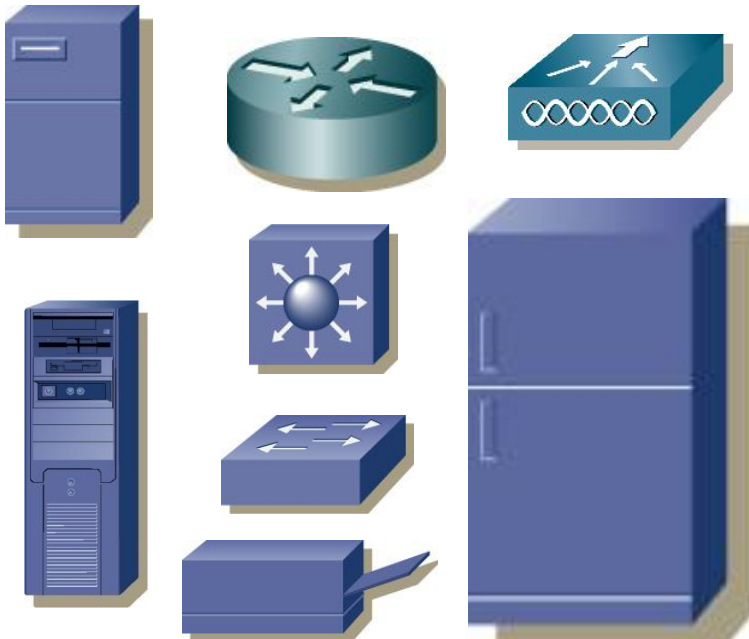
iTouch

Svič

RADIUS server

Frižider

Statičke IP Adrese



Dinamičke (DHCP) IP Adrese



DHCP SERVIS



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 opsluzi 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

Scope Properties - (Local)

IP Address Pool

Start Address: 10 . 10 . 10 . 11

End Address: 10 . 10 . 10 . 255

Subnet Mask: 255 . 255 . 255 . 0

Exclusion Range:

Start Address: . . .

End Address: . . .

Lease Duration

Unlimited

Limited To: 3 Day(s) 00 Hour(s) 00 Minutes

Name: _____

Comment: _____

OK Cancel Help

LINKSYS
A Division of Cisco Systems, Inc.

Firmware Version: 1.04.17

Setup

Etherfast® Cable/DSL Router BEFSR01 V3

Setup Security Applications & Gaming Administration Status

Basic Setup

Internet Setup

Internet Connection Type: Obtain an IP automatically

Host Name: _____

Domain Name: _____

MTU: Enable Disable Size: 0

Network Setup

Router IP

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Local DHCP Server (DHCPv1, DHCPv2)

Start IP Address: 192.168.1.100

Number of Addresses: 50

DHCP Address Range: 192.168.1.100 to 192.168.1.149

Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

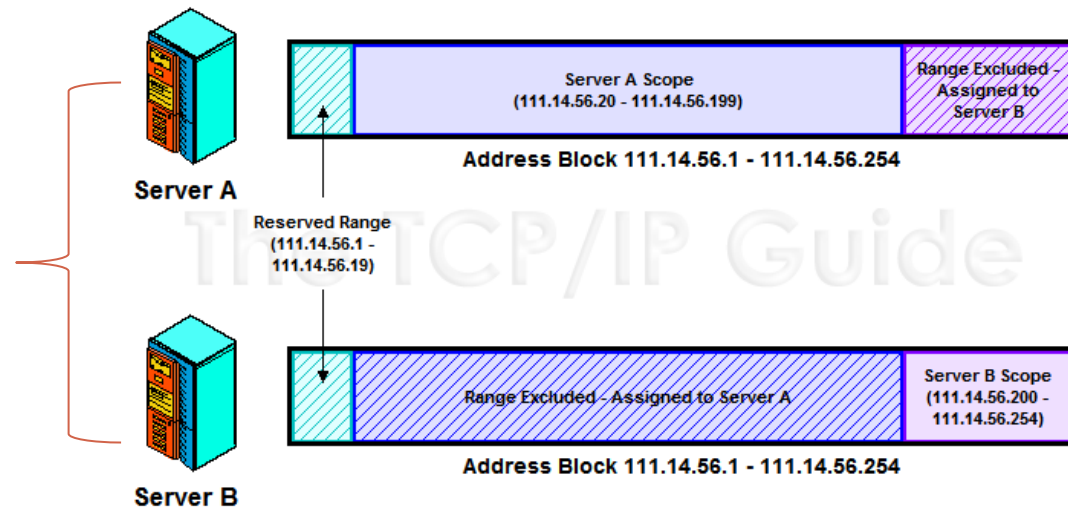
Save Settings Cancel Changes

Cisco Systems

DHCP SERVIS

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

DHCP SERVIS



DHCP SERVER - DETEKCIJA KONFLIKTA

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

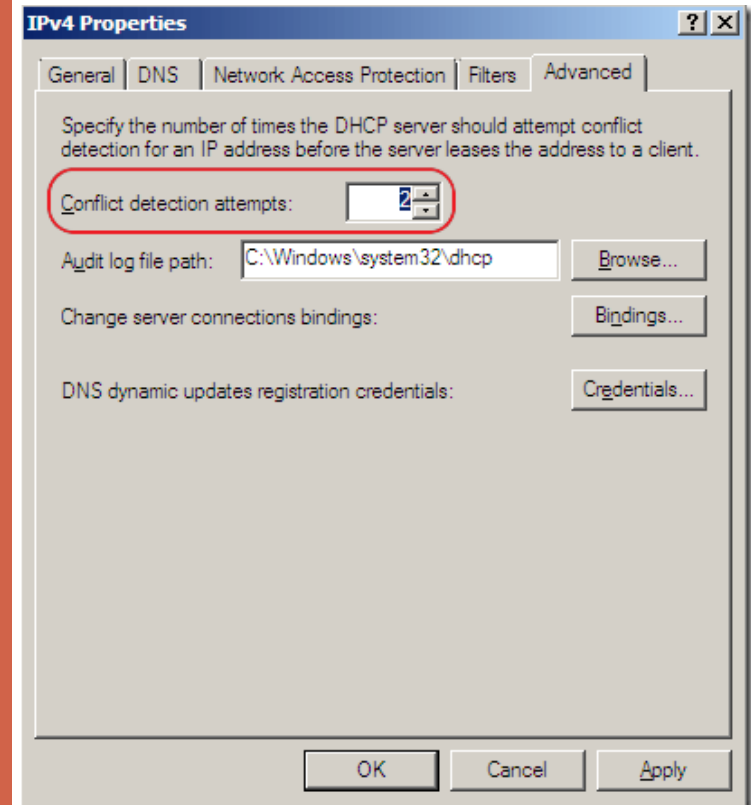
Podrazumevano, ova opcija je isključena

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 SERVIS



DHCP KLIJENT

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 Tcpiip. . . . . : Enabled
```

DHCP
konfiguracioni
parametri

DHCP SERVIS



DHCP KLIJENT

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 . . . . . :
```

DHCP RELEASE UNICAST PORUKA

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 SERVIS



DHCP KLIJENT

```
C:\Users\Korisnik>ipconfig /renew lan } — Zahtev za IP adresom
Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . :
    Link-local IPv6 Address . . . . . : fe80::51a8:395a:a2d4:58db%12
    IPv4 Address. . . . . : 10.1.1.17
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.1.1

Ethernet adapter LAN:

    Connection-specific DNS Suffix . . : vts.local
    Link-local IPv6 Address . . . . . : fe80::ac5d:98b4:f651:284f%10
    IPv4 Address. . . . . : 160.99.37.203
    Subnet Mask . . . . . : 255.255.255.128
    Default Gateway . . . . . : 160.99.37.129
```

DHCP SERVIS



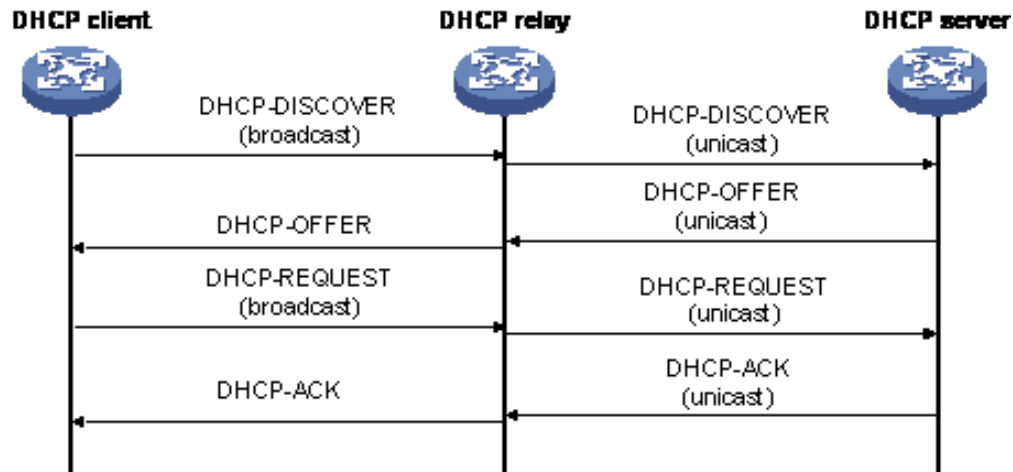
DHCP RELAY AGENT

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?

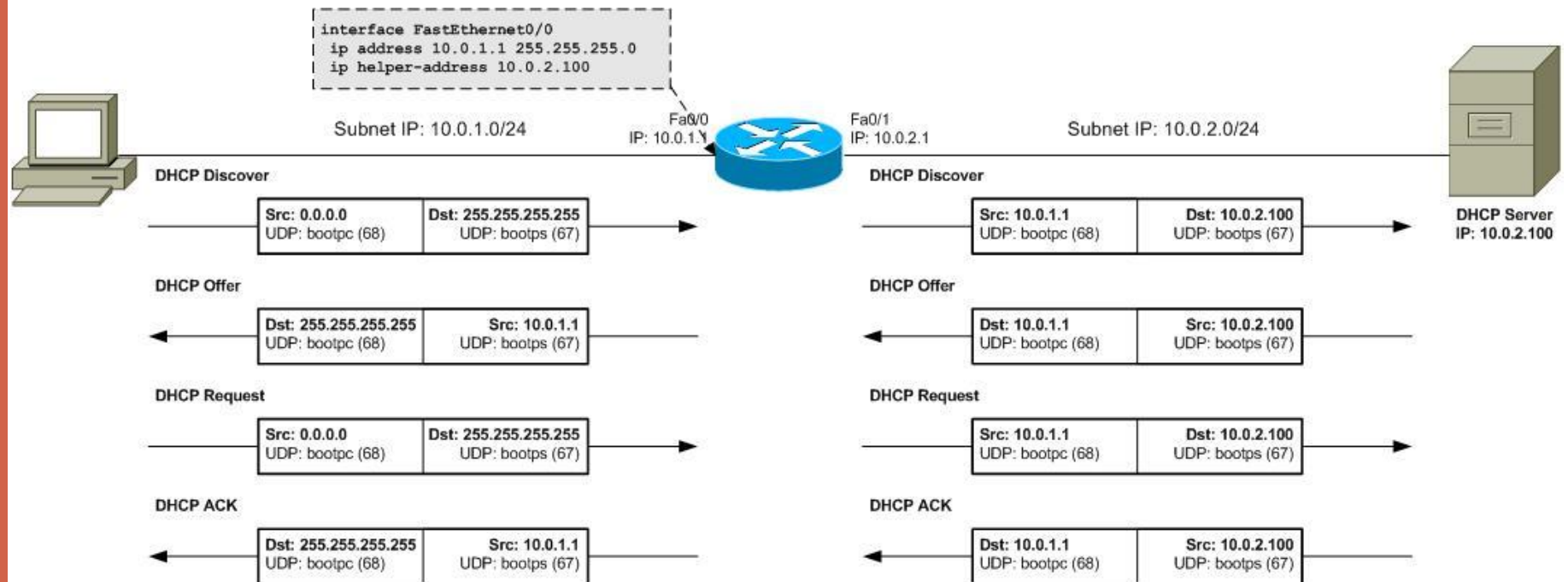
Ruteri ne prosleđuju broadcast poruke u drugim mrežama

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



DHCP SERVIS

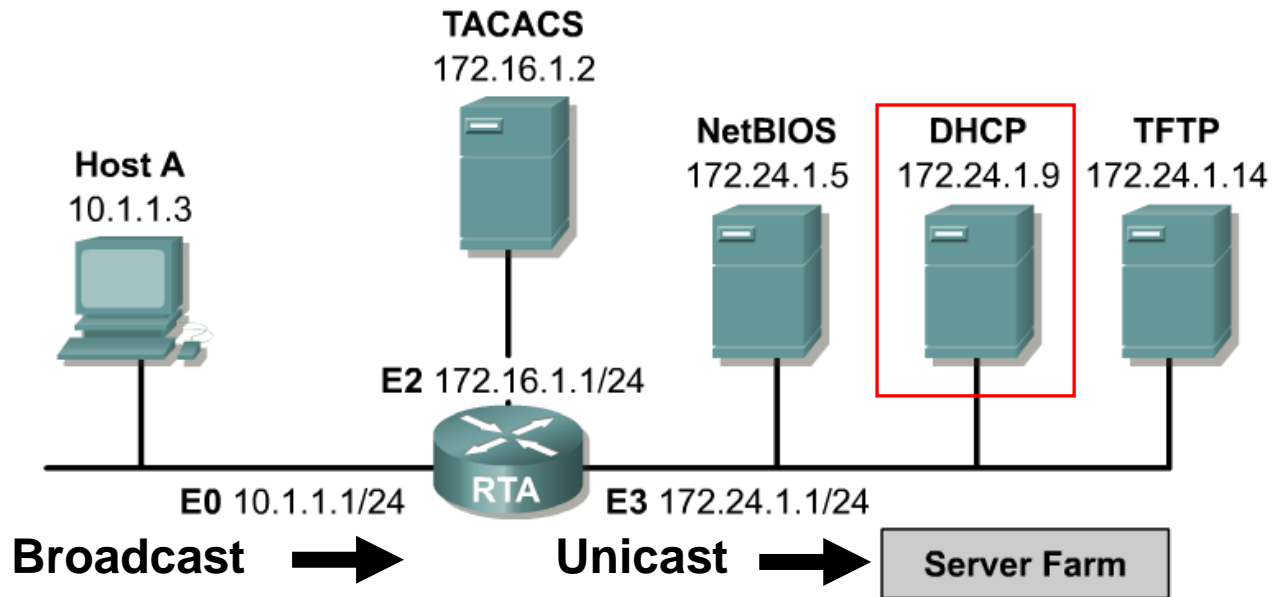
DHCP KOMUNIKACIJA PREKO RELAY AGENT-a



DHCP SERVIS



DHCP RELAY AGENT



```
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
```

NAPAD NA DHCP SERVIS

LAŽNI DHCP SERVER (DHCP SPOOF ATTACK)

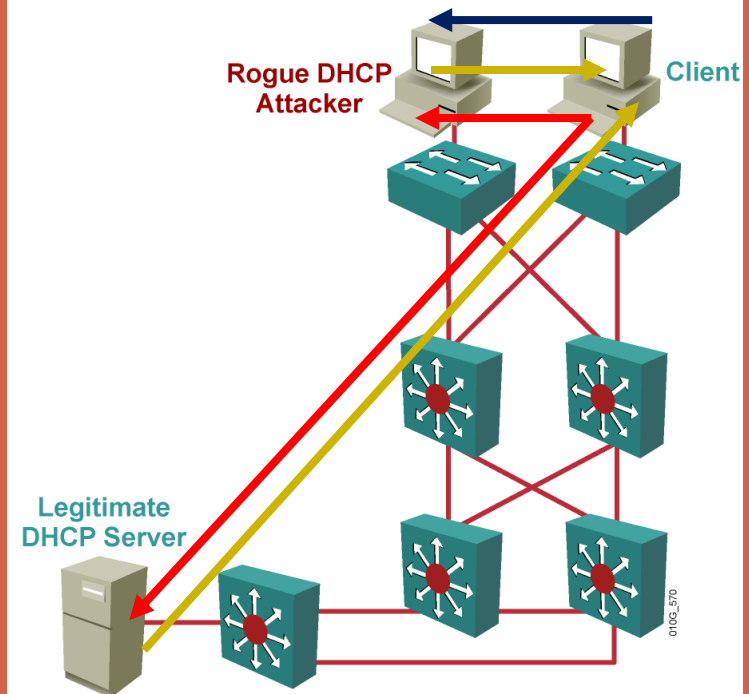
- Lažni DHCP server odgovara klijentima sa DHCP requests porukom na isti način na koji to radi legitimni DHCP server.
- Lažni DHCP server DHCP klijentima može da ponudi:

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**

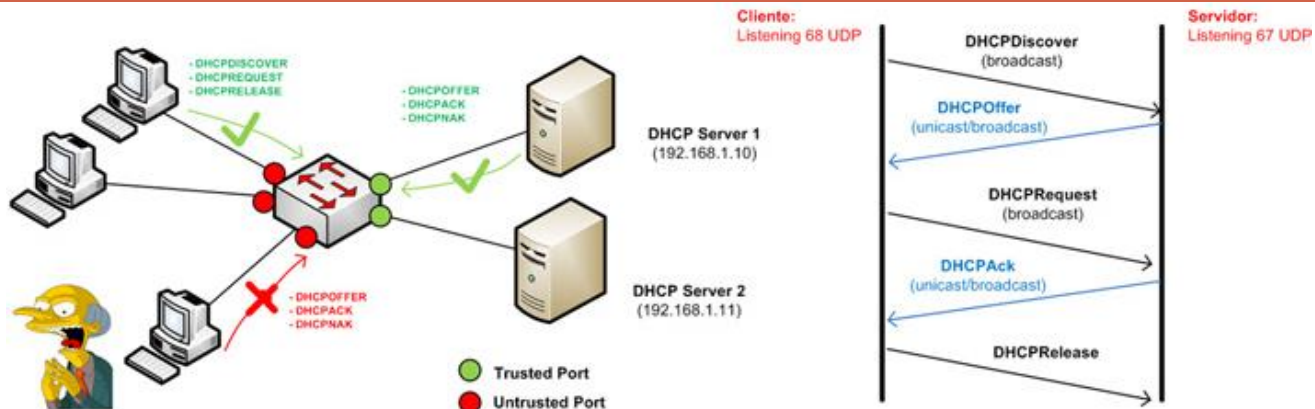


DHCP SERVIS



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** blokiraju DHCP poruke koje šalju DHCP serveri tzv. **DHCP response** poruke (DHCP OFFER, DHCP ACK ili DHCP NAK)

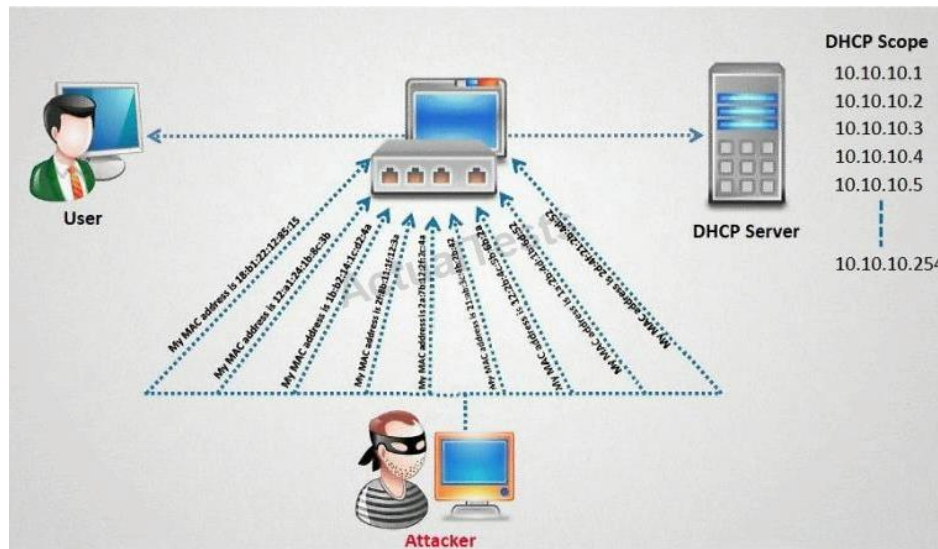


DHCP SERVIS



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 ovog napada je da legitimni PC oстане bez konfiguracionih parametra.



DHCP SERVIS



DHCP IZGLADNJIVANJE SERVERA (DHCP STARVATION)

DHCP Snooping je dovoljno pametan da uporedi 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.

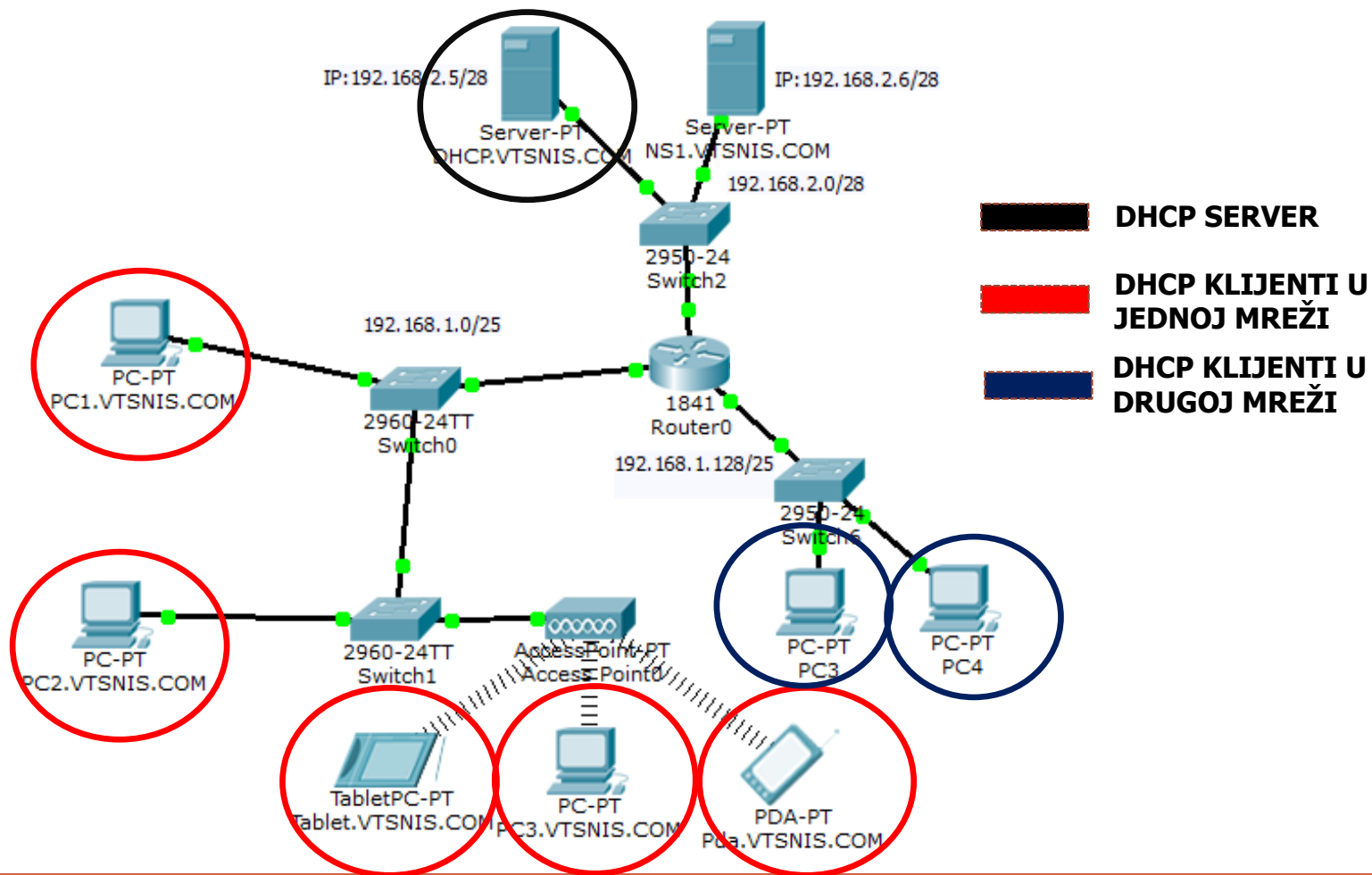
No.	Time	Source	Destination	Protocol	Length	Info
90:13:e8:eb:f7:cf	104.823241	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover -
90:13:e8:eb:f7:cf	106.825364	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover -
90:13:e8:eb:f7:cf	108.827849	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover -
90:13:e8:eb:f7:cf	111.798249	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover -
90:13:e8:eb:f7:cf	113.800161	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover -
90:13:e8:eb:f7:cf	117.562072	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover -

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: 00:16:36:c5:55:ab (00:16:36:c5:55:ab)
Client hardware address padding: 00000000000000000000

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

DHCP SERVIS

DHCP KONFIGURACIJA – PACKET TRACER



DHCP SERVIS

DHCP KONFIGURACIJA – PACKET TRACER

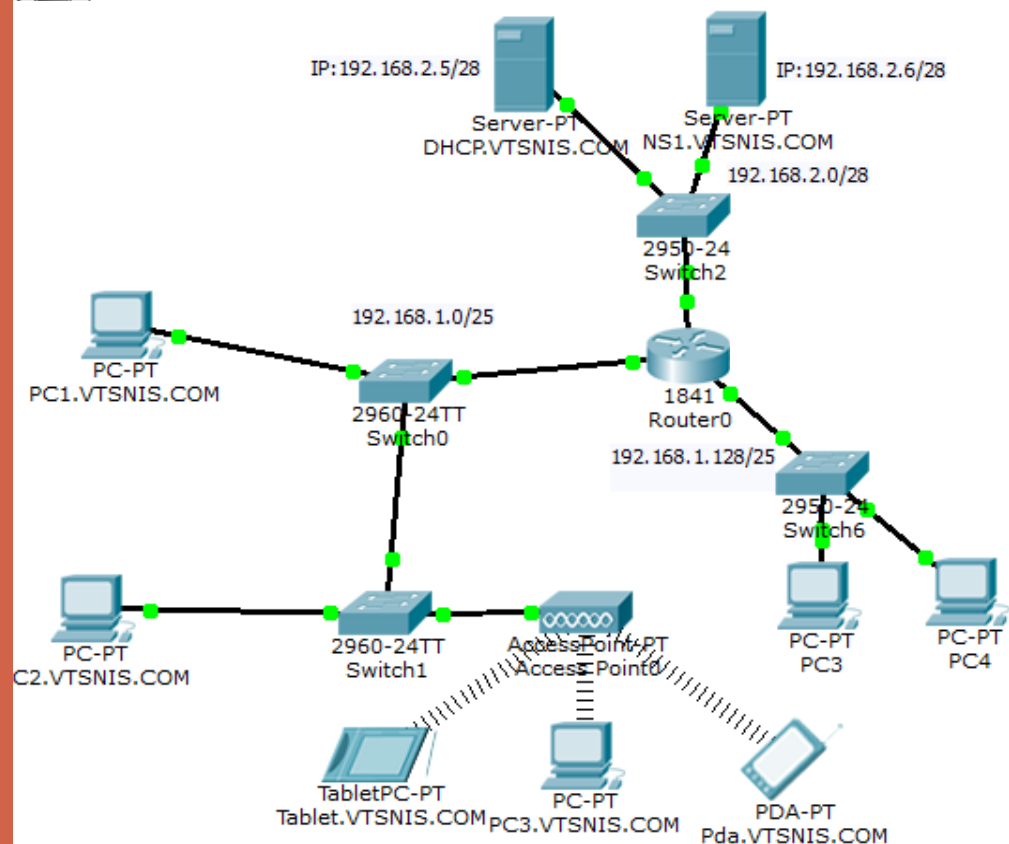
DHCP server opslužuje dve IP mreže.

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



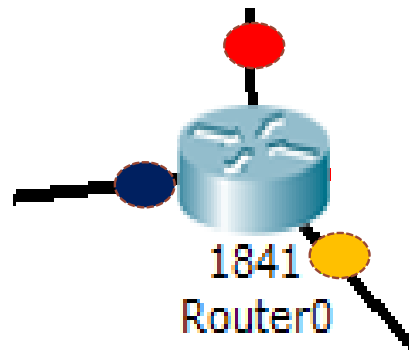
DHCP SERVIS



KONFIGURACIJA IP ADRESA NA RUTERU

FastEthernet0/0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto
<input type="radio"/> 10 Mbps	<input checked="" type="radio"/> 100 Mbps
Duplex	<input checked="" type="checkbox"/> Auto
<input checked="" type="radio"/> Full Duplex	<input type="radio"/> Half Duplex
MAC Address	0009.7C42.2101
IP Address	192.168.1.1
Subnet Mask	255.255.255.128
Tx Ring Limit	10

FastEthernet0/1	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="checkbox"/> Auto
<input type="radio"/> 10 Mbps	<input checked="" type="radio"/> 100 Mbps
Duplex	<input checked="" type="checkbox"/> Auto
<input checked="" type="radio"/> Full Duplex	<input type="radio"/> Half Duplex
MAC Address	0009.7C42.2102
IP Address	192.168.2.1
Subnet Mask	255.255.255.240
Tx Ring Limit	10



```
VIS>enable
VIS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VIS(config)#interface vlan 1
VIS(config-if)#ip address 192.168.1.129 255.255.255.128
VIS(config-if)#
```

DHCP SERVIS

KONFIGURACIJA STATIČKE IP ADRESE NA DHCP SERVERU

The image displays a network diagram on the left and a configuration window on the right. The network diagram shows a central 184 Router connected to a 2950-Switch. The 2950-Switch is connected to a 2960-24TT Switch0, which is further connected to a 2960-24TT Switch1. The 2960-24TT Switch1 is connected to an Access Point. The network includes several devices: PC-PT PC1.VTSNIS.COM (IP: 192.168.1.0/25), PC-PT PC2.VTSNIS.COM, TabletPC-PT Tablet.VTSNIS.COM, PC-PT PC3.VTSNIS.COM, and a Server-PT (IP: 192.168.2.5/28) with DHCP.VTSNIS.COM DNS1.V. The configuration window, titled "IP Configuration", shows the "FastEthernet0" interface configured with "Static" IP. The IP Address is 192.168.2.5, the Subnet Mask is 255.255.255.240, and the Default Gateway is 192.168.2.1. The IPv6 Configuration section shows "Static" selected, with an IPv6 Address field and a Link Local Address of FE80::240:BFF:FE6A:88D0.

Physical Config Desktop Software/Services

IP Configuration

Interface: FastEthernet0

IP Configuration

DHCP Static

IP Address: 192.168.2.5

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.2.1

DNS Server:

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address: /

Link Local Address: FE80::240:BFF:FE6A:88D0

IPv6 Gateway:

IPv6 DNS Server:

DHCP SERVIS

KONFIGURACIJA ADRESNOG POOL-a NA DHCP SERVERU

The image displays a network diagram on the left and a DHCP configuration window on the right. The network diagram shows a central 2950-24TT Switch connected to a Server-PT (DHCP.VTSNIS.COM, IP: 192.168.2.5/28) and a 2960-24TT Switch0. Switch0 is connected to a 1841 Router (IP: 192.168.1.1) and another 2960-24TT Switch1. Switch1 is connected to PC-PT PC1.VTSNIS.COM (IP: 192.168.1.0/25), PC-PT PC2.VTSNIS.COM, TabletPC-PT Tablet.VTSNIS.COM, and PC-PT PC3.VTSNIS.COM. An Access Point-PT is also connected to Switch1.

The DHCP configuration window (DHCP.VTSNIS.COM) shows the following settings:

- Service: On
- Pool Name: LAN2
- Default Gateway: 192.168.1.129
- DNS Server: 0.0.0.0
- Start IP Address: 192.168.1.150
- Subnet Mask: 255.255.255.128
- Maximum number of Users: 30
- TFTP Server: 0.0.0.0

The configuration window also includes a table of existing DHCP pools:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max Num
LAN2	192.168.1.129	0.0.0.0	192.168.1.150	255.255.255.128	30
serverPool	192.168.1.1	0.0.0.0	192.168.1.10	255.255.255.128	30

DHCP SERVIS

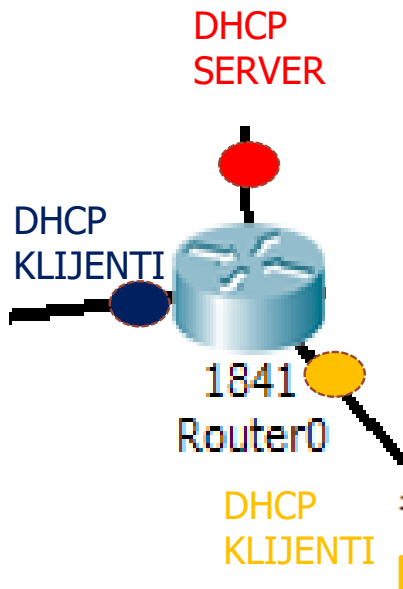
KONFIGURACIJA RELAY-AGENT NA RUTERU

DHCP klijenti koriste IP broadcast za pronalaženje DHCP servera u mreži

Routeri ne prosleđuju broadcast poruke u drugim mrežama

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

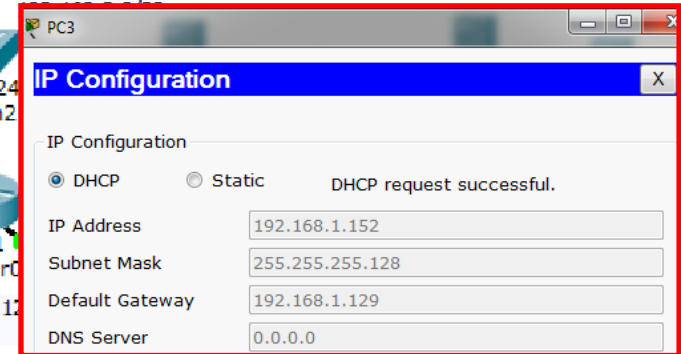
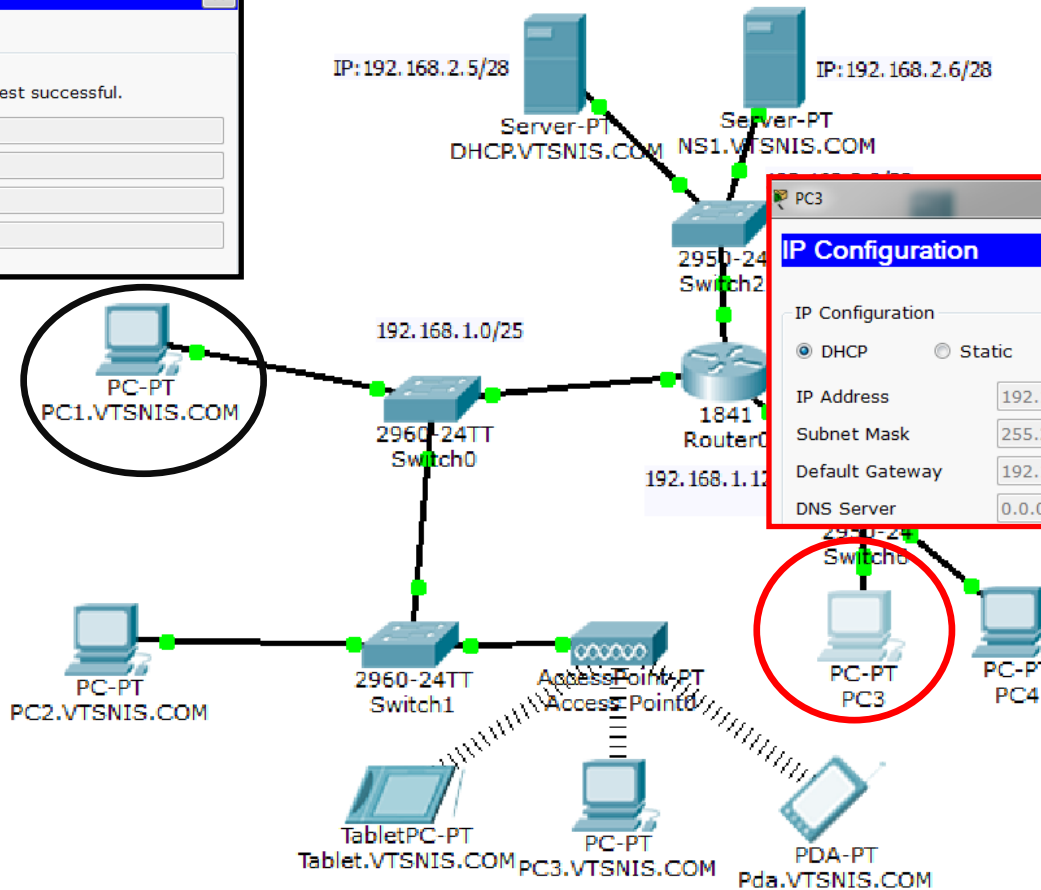
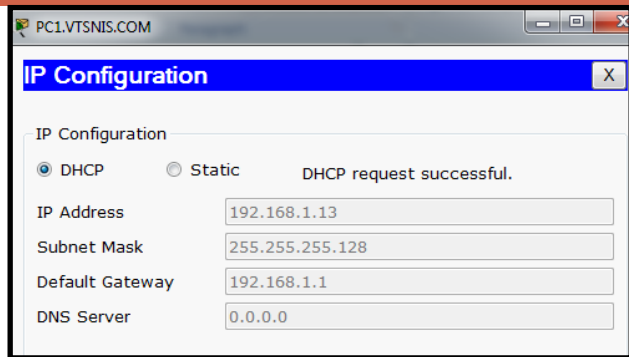
```
interface FastEthernet0/0  
ip address 192.168.1.1 255.255.255.128  
ip helper-address 192.168.2.5  
duplex auto  
speed auto
```



```
interface Vlan1  
ip address 192.168.1.129 255.255.255.128  
ip helper-address 192.168.2.5
```

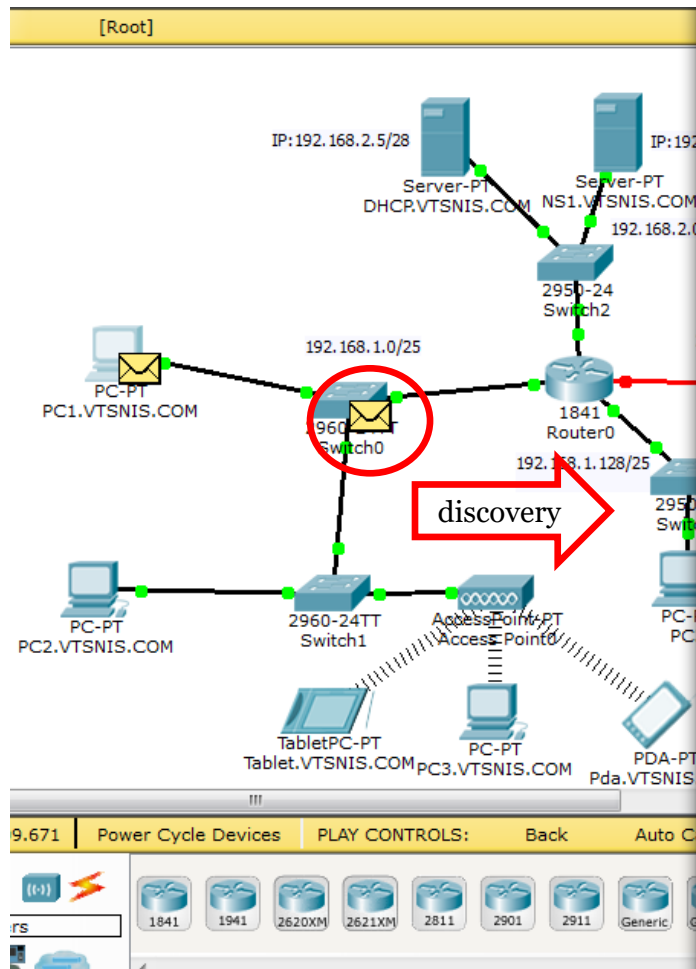
DHCP SERVIS

KONFIGURACIJA DHCP KLIJENTA



DHCP SERVIS

SIMULACIJA PRAĆENJA DHCP PORUKA



PDU Formats

PREAMBLE: 101010...1011	DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 0040.0B58.4ADD
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 62		
ID: 0xa		0x0	0x0		
TTL: 128	PRO: 0x11	CHKSUM			
SRC IP: 0.0.0.0					
DST IP: 255.255.255.255					
OPT: 0x0			0x0		
DATA (VARIABLE LENGTH)					

UDP

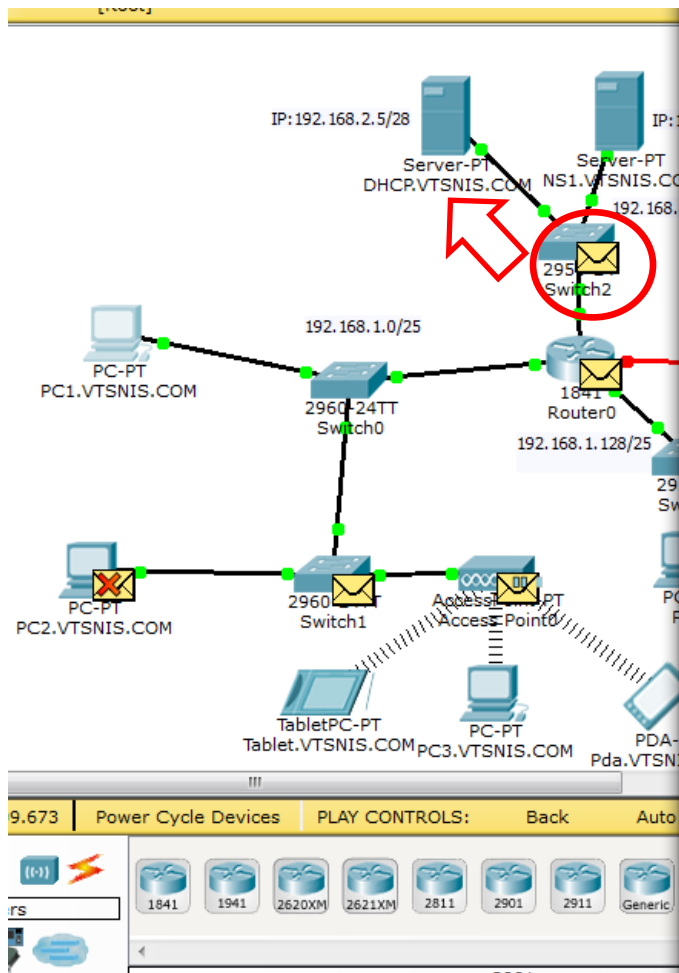
0	16	31 Bits
SRC PORT: 68		DEST PORT: 67
LENGTH: 0x2a	CHECKSUM: 0x0	
DATA (VARIABLE)		

DHCP

0	8	16	31 Bits
OP: 0x1	HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)			
SECS		FLAGS	
CLIENT ADDRESS: 0.0.0.0			
"YOUR" CLIENT ADDRESS: 0.0.0.0			
SERVER ADDRESS: 0.0.0.0			
RELAY AGENT ADDRESS			
CLIENT HARDWARE ADDRESS: 0040.0B58.4ADD			

DHCP SERVIS

SIMULACIJA PRAĆENJA DHCP PORUKA



PDU Formats

PREAMBLE: 101010...1011		DEST MAC: 0040.0B6A.88D0	SRC MAC: 0009.7C42.2102
TYPE: 0x800	DATA (VARIABLE LENGTH)		FCS: 0x0

IP

0				4				8				16				19				31 Bits			
4		IHL	DSCP: 0x0		TL: 62																		
ID: 0xa		0x0		0x0																			
TTL: 128		PRO: 0x11		CHKSUM																			
SRC IP: 192.168.1.1																							
DST IP: 192.168.2.5																							
OPT: 0x0		0x0																					
DATA (VARIABLE LENGTH)																							

UDP

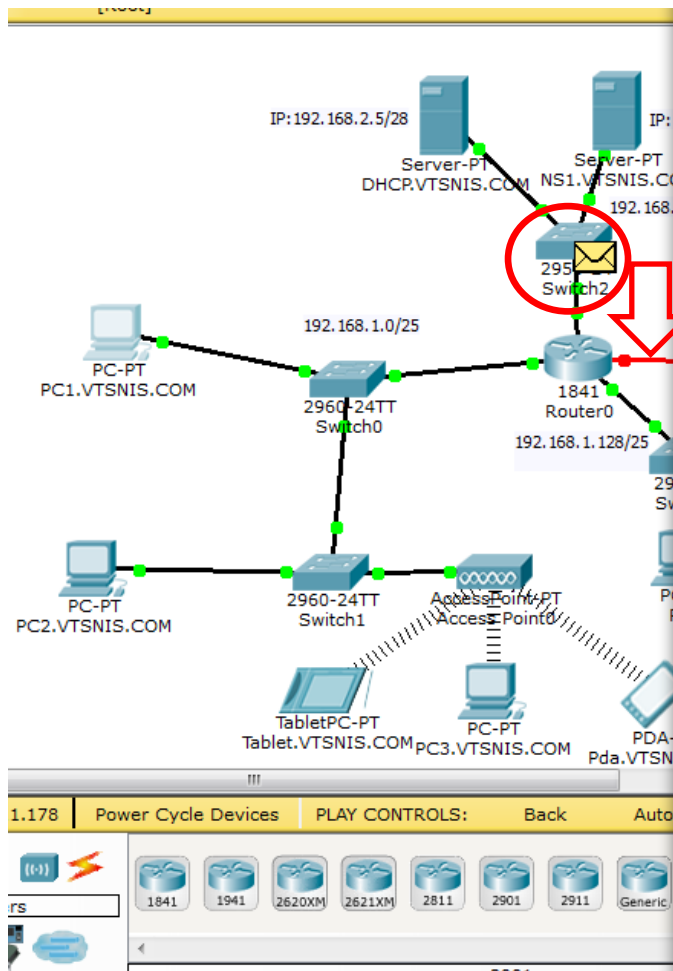
0		16		31 Bits	
SRC PORT: 68		DEST PORT: 67			
LENGTH: 0x2a		CHECKSUM: 0x0			
DATA (VARIABLE)					

DHCP

0		8		16		31 Bits	
OP: 0x1		HW TYPE		HW LEN		HOPS	
TRANSACTION ID (4 BYTES)							
SECS				FLAGS			
CLIENT ADDRESS: 0.0.0.0							
"YOUR" CLIENT ADDRESS: 0.0.0.0							
SERVER ADDRESS: 0.0.0.0							
RELAY AGENT ADDRESS							
CLIENT HARDWARE ADDRESS: 0040.0B58.4ADD							

DHCP SERVIS

SIMULACIJA PRAĆENJA DHCP PORUKA



PDU Formats

PREAMBLE: 101010...1011	DEST MAC: 0009.7C42.2102	SRC MAC: 0040.0B6A.88D0
TYPE: 0x800	DATA (VARIABLE LENGTH)	FCS: 0x0

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 62		
ID: 0x25		0x0	0x0		
TTL: 128	PRO: 0x11	CHKSUM			
SRC IP: 192.168.2.5					
DST IP: 192.168.1.1					
OPT: 0x0			0x0		
DATA (VARIABLE LENGTH)					

UDP

0	16	31 Bits
SRC PORT: 67		DEST PORT: 67
LENGTH: 0x2a	CHECKSUM: 0x0	
DATA (VARIABLE)		

DHCP

0	8	16	31 Bits
OP: 0x2	HW TYPE	HW LEN	HOPS
TRANSACTION ID (4 BYTES)			
SECS		FLAGS	
CLIENT ADDRESS: 0.0.0.0			
"YOUR" CLIENT ADDRESS: 192.168.1.15			
SERVER ADDRESS: 192.168.2.5			
RELAY AGENT ADDRESS			
CLIENT HARDWARE ADDRESS: 0040.0B58.4ADD			

