

Laboratorul 6 - Protocolul DHCP

În acest laborator vom studia protocolul DHCP. Știm că DHCP (Dynamic Host Configuration Protocol) este folosit mult în rețele corporatiste, de universități și în LAN-uri, pentru a atribui în mod dinamic adrese IP și pentru a configura rețeaua.

Prin intermediul protocolului DHCP calculatoarele dintr-o rețea pot obține automat o adresă IP, printr-o cerere către serverul DHCP. Serverul poate să furnizeze stației respective toate informațiile de configurare necesare, inclusiv adresa IP, masca de subrețea, default gateway, adresa serverului DNS, etc.

Astfel, când serverul primește o cerere de la o stație, selectează adresa IP și un set de informații asociate dintr-o mulțime de adrese predefinite care sunt păstrate într-o baza de date. Odată ce adresa IP este selectată, serverul DHCP oferă aceste valori stației care a efectuat cererea. Dacă stația acceptă oferta, serverul DHCP îi împrumută adresa IP pentru o perioadă, după care o regenerează.

Generarea adreselor IP prin serverul DHCP este o metodă utilizată pe scară largă în administrarea rețelelor de mari dimensiuni.

Folosirea unui server DHCP simplifică administrarea unei rețele pentru că software-ul ține evidenta adreselor IP. În plus, este exclusă posibilitatea de a atribui adrese IP invalide sau duplicate.

Vom examina doar pachetele DHCP capturate de un computer. Dacă aveți acces ca administrator la serverul vostru DHCP, puteți extinde laboratorul după ce faceți câteva schimbări (de exemplu "lease time"). Dacă aveți un router acasă, vă puteți configura și acolo serverul DHCP. Deoarece multe mașini Unix/Linux (mai ales cele cu mulți utilizatori) au o adresă IP statică și deoarece pentru a manipula DHCP pe astfel de mașini vă trebuie privilegii de superuser, laboratorul acesta va fi prezentat doar pentru Windows.

Experimentul 1

Vom scrie câteva comenzi în legătura cu DHCP și vom captura mesajele DHCP schimbate după aceste comenzi. Procedați la următoarele comenzi:

1. Deschideți Command Prompt și scrieți "*ipconfig /release*". Această comandă va elibera adresa IP pe care o aveți acum (curentă), astfel încât adresa IP a computerului dvs devine 0.0.0.0.
2. Porniți captura Wireshark.

3. Scrieți acum *“ipconfig /renew”*. Acum computerul va obține o configurație de rețea și o nouă adresă IP. În figura 1 computerul obține adresa 192.168.1.108.

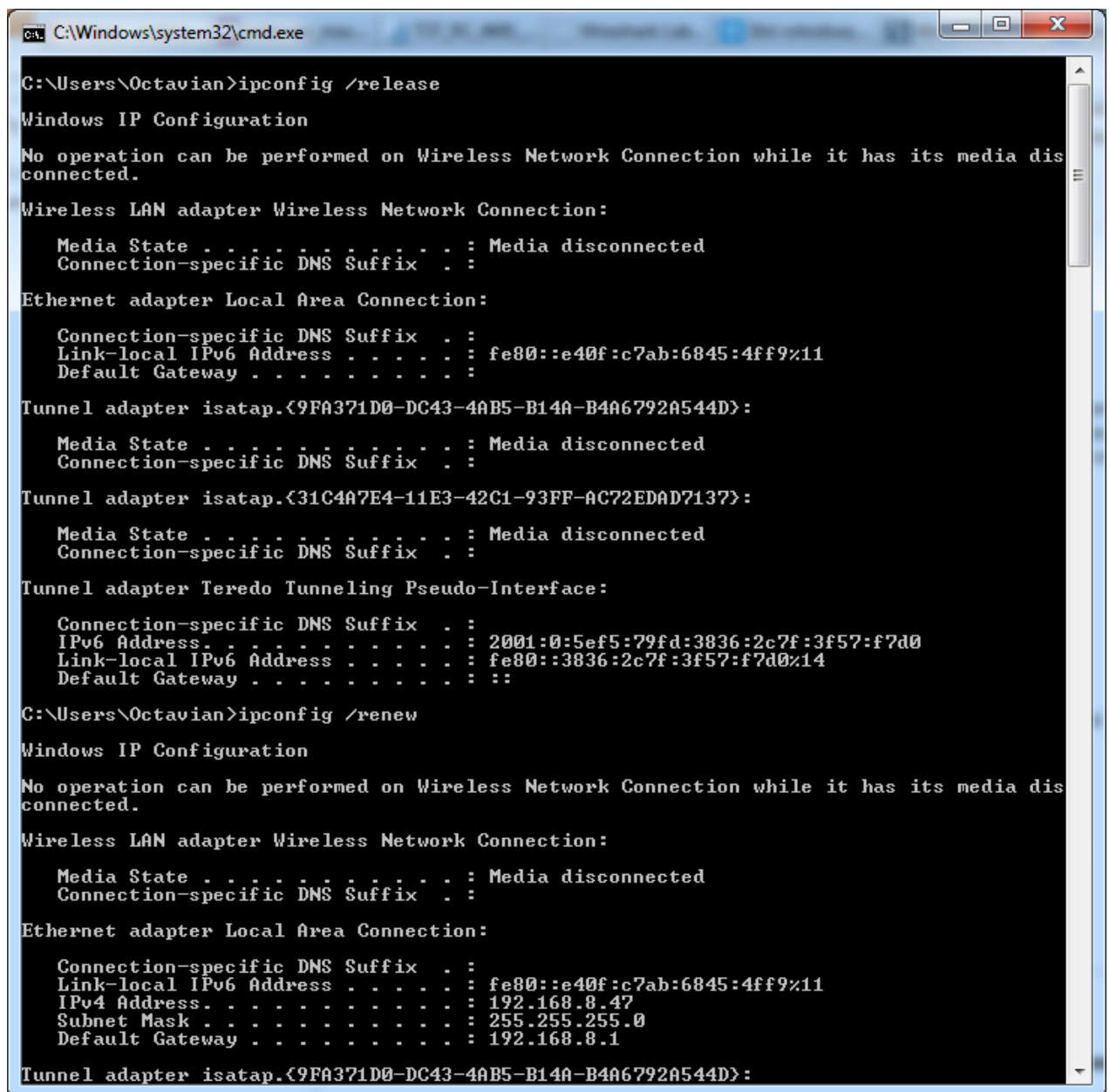
4. Așteptați până când *“ipconfig /renew”* se termina. Apoi scrieți *“ipconfig /renew”* din nou.

5. După ce al doilea *“ipconfig /renew”* se termină, scrieți *“ipconfig /release”* pentru a elibera adresa IP precedentă.

6. Acum scrieți *“ipconfig/renew”* din nou pentru a va fi alocată o adresă IP.

7. Opriți Wireshark.

(Nota: dacă nu vă merge Wireshark, folosiți fișierul *dhcp-ethereal-1* de pe CD).



```
C:\Windows\system32\cmd.exe

C:\Users\Octavian>ipconfig /release

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media dis
connected.

Wireless LAN adapter Wireless Network Connection:

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

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::e40f:c7ab:6845:4ff9%11
    Default Gateway . . . . . :

Tunnel adapter isatap.{9FA371D0-DC43-4AB5-B14A-B4A6792A544D}:

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

Tunnel adapter isatap.{31C4A7E4-11E3-42C1-93FF-AC72EDAD7137}:

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

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . :
    IPv6 Address . . . . . : 2001:0:5ef5:79fd:3836:2c7f:3f57:f7d0
    Link-local IPv6 Address . . . . . : fe80::3836:2c7f:3f57:f7d0%14
    Default Gateway . . . . . :

C:\Users\Octavian>ipconfig /renew

Windows IP Configuration

No operation can be performed on Wireless Network Connection while it has its media dis
connected.

Wireless LAN adapter Wireless Network Connection:

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

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::e40f:c7ab:6845:4ff9%11
    IPv4 Address. . . . . : 192.168.8.47
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.8.1

Tunnel adapter isatap.{9FA371D0-DC43-4AB5-B14A-B4A6792A544D}:
```

Figura 1 - Obținerea unei noi adrese și eliberarea adresei precedente

Pentru a vedea doar pachete DHCP, scrieți *“bootp”* la filtru (DHCP provine

dintr-un protocol mai vechi (*Bootstrap Protocol*) numit BOOTP. Ambele protocoale folosesc aceleași porturi, 67 și 68).

În imaginea de mai jos se vede că prima comandă *ipconfig* a forțat generarea a 4 pachete DHCP: un pachet DHCP Discover, un pachet DHCP Offer, un pachet DHCP Request și un pachet DHCP ACK.

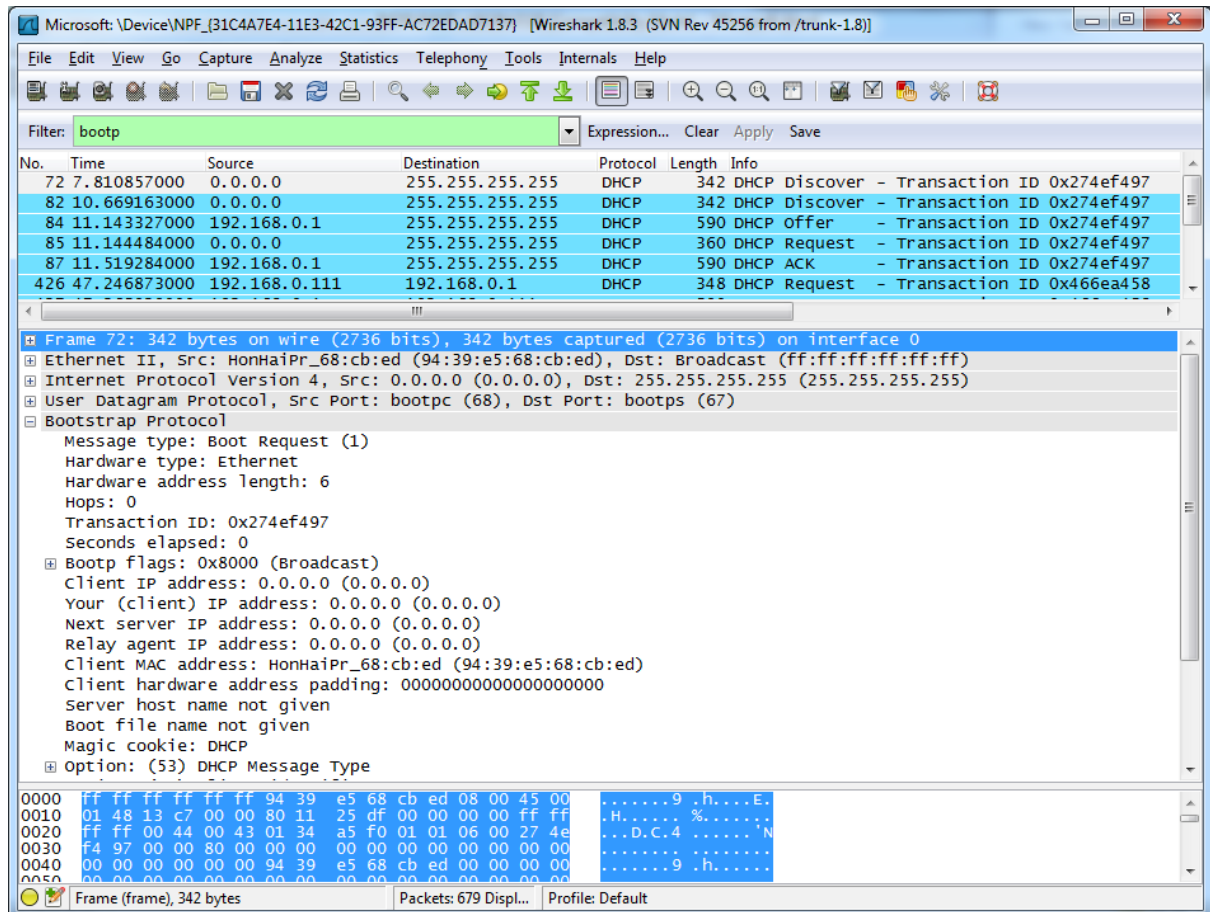


Figura 2 - Vizualizarea exclusivă a pachetelor DHCP

Nu uitați, înainte de a răspunde la întrebări, trebuie să aveți și un printout cu pachetele din trace-ul folosit. Justificați-vă fiecare răspuns pe printout. Pentru a tipări un pachet *File* → *Print*, alegeți *Selected packet only*, alegeți *Packet summary line*, și selectați doar detaliile pachetului de care aveți nevoie pentru a răspunde la întrebare.

Răspundeți la următoarele întrebări:

1. Mesajele DHCP sunt trimise peste UDP sau peste TCP?
2. Desenați o datagramă temporală ilustrând succesiunea primelor 4 pachete Discover/Offer/Request/ACK DHCP între client și server. La fiecare pachet indicați

porturile sursă și destinație. Sunt aceleași porturi ca în exemplul de mai sus?

3. Care este adresa link-layer (de exemplu Ethernet) a computerului?
4. Ce valori din mesajul DHCP Discover diferențiază acest mesaj de mesajul DHCP Request?
5. Care este valoarea „Transaction-ID-ului” pentru fiecare dintre primele 4 mesaje (Discover/Offer/Request/ACK) DHCP ? Care este valoarea „Transaction-ID-ului” pentru al doilea set (Request/ACK) de mesaje DHCP? Care este scopul câmpului Transaction-ID?
6. Un computer folosește DHCP pentru a obține, printre altele, o adresă IP. Dar IP-ul unui computer nu este confirmat până la sfârșitul schimbului de 4 mesaje! Dacă adresa IP nu este setată până la sfârșitul schimbului celor 4 mesaje, atunci ce valori sunt folosite în datagramele IP în respectivul schimb? La fiecare dintre cele 4 mesaje DHCP (Discover/Offer/Request/ACK) indicați porturile sursă și destinație care sunt transportate în datagrama IP.
7. Care este adresa IP a serverului DHCP?
8. Ce adresă IP oferă serverul DHCP computerului dvs în mesajul DHCP Offer? Indicați care mesaj DHCP conține adresa IP oferită.
9. În imaginea de mai sus, nu există “relay agent” între computer și serverul DHCP. Care valori din trace indică absența unui “relay agent”? Există un “relay agent” în experiment? Dacă da, care este IP-ul lui?
10. Explicați scopul router-ului și a măștii din mesajul DHCP Offer.
11. În imaginile de mai sus, computerul cere adresa IP oferită în mesajul DHCP Request . Ce se întâmplă în experimentul vostru?
12. Ce scop are “lease time” (timpul de închiriere)? Cât de mare este el în experimentul dvs?
13. Care este scopul mesajului DHCP Release? Serverul DHCP oferă vreo confirmare a primirii cererii clientului? Ce s-ar întâmpla dacă mesajul DHCP release al clientului, s-ar pierde?
14. Ștergeți filtrul *bootp* din Wireshark. A fost vreun pachet ARP trimis sau primit în perioada schimbului de pachete DHCP? Dacă da, explicați scopul pentru care există aceste pachete ARP.

Notă

- DHCP Discover. Acest mesaj este transmis de client când el accesează o rețea

pentru a cere o adresă IP de la un server DHCP. Mesajul este transmis sub forma unui pachet difuzat (broadcast), cerând unui server DHCP un răspuns la acesta. Fiecare server DHCP, aflat în subrețeaua locală, primește pachetul, dar acesta nu trece prin router spre alte rețele sau subrețele deoarece este un packet broadcast.

- DHCP Offer. Acest mesaj este răspunsul la mesajul DHCP Discover și este transmis de unul sau mai multe servere DHCP și conține adresa de IP validă oferită spre închiriere, masca de rețea, adresa serverului DHCP care trimite pachetul, durata de închiriere a adresei, adresa pentru default gateway.

Deoarece clientul nu are încă o adresă de IP, pachetele “DHCP offer” sunt de tip broadcast și sunt transmise cu numărul de *port destinație* 68 care indică programele client DHCP.

- Mesajul DHCP Request arată că se cere o adresă IP particulară de către client, care realizează operațiile:
 - selectează prima ofertă primită;
 - trimite un “broadcast packet” în care anunță serverul că îi acceptă oferta;
 - cere informații suplimentare (masca, adresa de gateway, adresa de DNS, etc).

Toate celelalte servere DHCP care au făcut oferte primesc acest pachet; acestea află că au fost refuzate și că pot anula rezervările pe care le-au făcut pentru adresele oferite.

- Mesajul DHCP ACK este transmis de către serverul DHCP, clientului DHCP și reprezintă procesul prin care serverul DHCP asignează adresa IP clientului.

Într-o rețea rutată este nevoie de un Relay Agent pentru implementarea numai a unui server DHCP. Relay Agent este de fapt un protocol de rutare care permite clienților DHCP să obțină adrese IP de la un server DHCP dintr-o subrețea care nu este locală. Fără configurarea Relay Agent, clienții vor putea obține adrese IP numai de la serverul DHCP aflat în aceeași subrețea.

Pentru a transmite mesajele DHCP broadcast, fie se configurează routerele din rețea pentru mesaje de acest tip, fie se configurează Relay Agent.

Experimentul 2

Configurarea DHCP

1. Porniți Cisco Packet Tracer și deschideți fișierul DHCP-t1.

- Topologia diagramei:

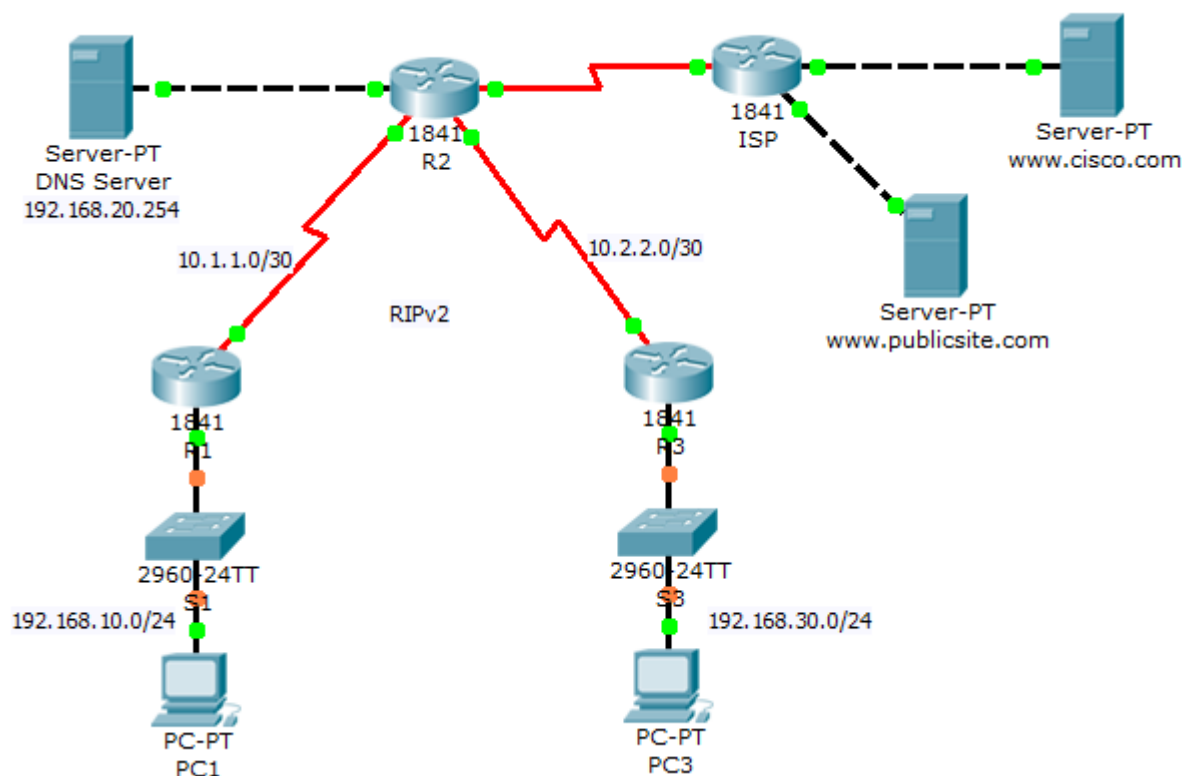


Figura 3 – Topologia diagramei din fișierul DHCP-t1

- Tabela de dirijare:

Device	Interface	IP Address	Subnet Mask
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

ISP	Fa 0/0	209.165.202.158	255.255.255.224
	Fa 0/1	209.165.202.129	255.255.255.224
	S 0/0/0	209.165.200.226	255.255.255.224

2. Realizati urmatoarele configurari pentru router R1:

- Interfata seriala a routerului R1 (s 0/0/0) are clock rate 64000
- R1(config)#router rip
- R1(config)#version 2
- R1(config_router)#network 192.168.10.0
- R1(config_router)#network 10.0.0.0

3. Realizati urmatoarele configurari pentru router R3:

- R3 (config)#router rip
- R3(config)#version 2
- R3(config_router)#network 10.0.0.0
- R3(config_router)#network 192.168.30.0

4. Realizati urmatoarele configurari pentru router R2:

- Interfata seriala a routerului R2 (s 0/0/1) are clock rate 64000 si este legata la interfata seriala s0/0/1 a routerului R3
- Interfata seriala a routerului R2 (s 0/0/0) este legata la interfata seriala s0/0/0 a routerului R1
- Interfata seriala a routerului R2 (s 0/1/0) este legata la interfata seriala s0/0/0 a routerului ISP.
- R2(config)#router rip
- R2(config)#version 2
- R2(config_router)#network 10.0.0.0

5. Realizati urmatoarele configurari pentru router ISP:

- Interfata seriala a routerului ISP (s 0/0/0) are clock rate 64000 si este legata la interfata seriala s0/1/0 a routerului R2.
- ISP(config)# ip route 10.0.0.0 255.0.0.0 Serial 0/0/0
- ISP(config)# ip route 192.168.0.0 255.255.0.0 Serial 0/0/0

6. Configurați router-ul R1:

- a) Se vor defini un set de adrese care vor fi rezervate pentru gazde (de exemplu: servere, routere, imprimante), care au nevoie de adrese statice. Aceste adrese nu sunt incluse în intervalul de adrese (pool of addresses) care sunt disponibile pentru asignarea clienților DHCP. Pentru routerele R1excludeți primele 9(nouă) adrese. Comanda prin care se face excluderea adreselor este:

R1(config)#**ip dhcp excluded-address A.B.C.D Low IP address**

- b) Definiți intervalul de adrese de unde DHCP atribuie adrese către clienții DHCP pe R1LAN. Adresele disponibile sunt toate adresele din rețeaua 192.168.10.0, cu excepția celor excluse de la pasul 2.a). Pentru router-ul R1 denumiți intervalul de adrese R1LAN. Specificați intervalul de adrese, poarta de acces implicită și serverul DNS care sunt atribuite fiecărui dispozitiv client care solicită serviciul DHCP.

R1(config)#**ip dhcp pool R1LAN**

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 192.168.20.254**

7. Configurați router-ul R3:

- a) Exclueți primele 9 (nouă) adrese.
- b) Pentru router-ul R3 denumiți intervalul de adrese R3LAN. Specificați intervalul de adrese, poarta de acces implicită și serverul DNS care sunt atribuite fiecărui dispozitiv client care solicită serviciul DHCP.

R3(config)#**ip dhcp pool R3LAN**

R3(dhcp-config)#**network 192.168.30.0 255.255.255.0**

R3(dhcp-config)#**default-router 192.168.30.1**

R3(dhcp-config)#**dns-server 192.168.20.254**

8. Configurați PC1 și PC3 pentru alocarea de adrese IP în modul DHCP.
9. Verificați funcționarea DHCP pe fiecare din cele două routere, R1 și R3 prin comanda **show ip dhcp binding**. Ce rezultat s-a afișat?
10. Configurați serverul DNS. Pentru a configura DNS-ul pe serverul DNS, faceți clic pe butonul DNS în tab-ul Config. Asigurați-vă că DNS este pornit, și introduceți următoarele intrări DNS:
- www.cisco.com 209.165.201.30
 - www.publicsite.com 209.165.202.158
11. Verificați dacă PC1 și PC2 se pot conecta la servere folosind numele de domeniu. Pentru PC1, deschideți browser-ul web și introduceți www.cisco.com în linia de adresă. Pentru PC2, introduceți www.publicsite.com.