

CSCI 5010 – Fundamentals of Data Communications

Lab 7

Applications:
DHCP and DNS

University of Colorado Boulder
Department of Computer Science
Network Engineering

Levi Perigo, Ph.D.

Objectives

- Learn DHCP configuration and concepts.
- Learn DNS basic configuration and concepts.

Summary:

As networks scale, we need applications to help manage our IP addresses and configuration of devices. Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) are applications used for better network management. You will use GNS3 in this lab to implement these protocols. You will be examining the messages on Wireshark at the packet level to get a deeper understanding about the protocol mechanics. This lab covers many interview questions that you will be asked when you're applying for internships and jobs. The main goal of the lab is to help you gain protocol knowledge and basic implementation skills to be able to configure these services on networking devices.

Objective-1: Getting started with DHCP

1. Startup GNS3 and initialize the following topology:

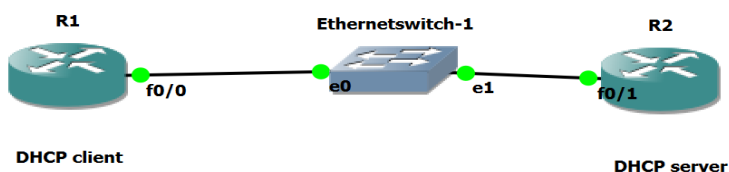
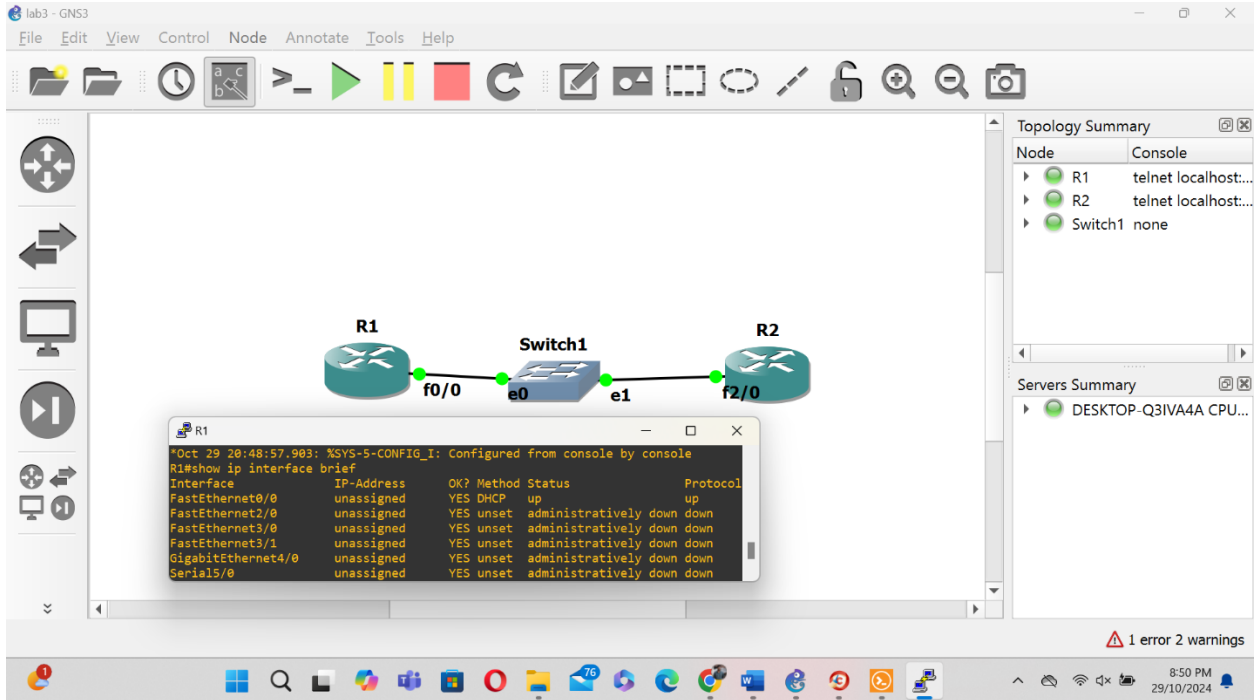


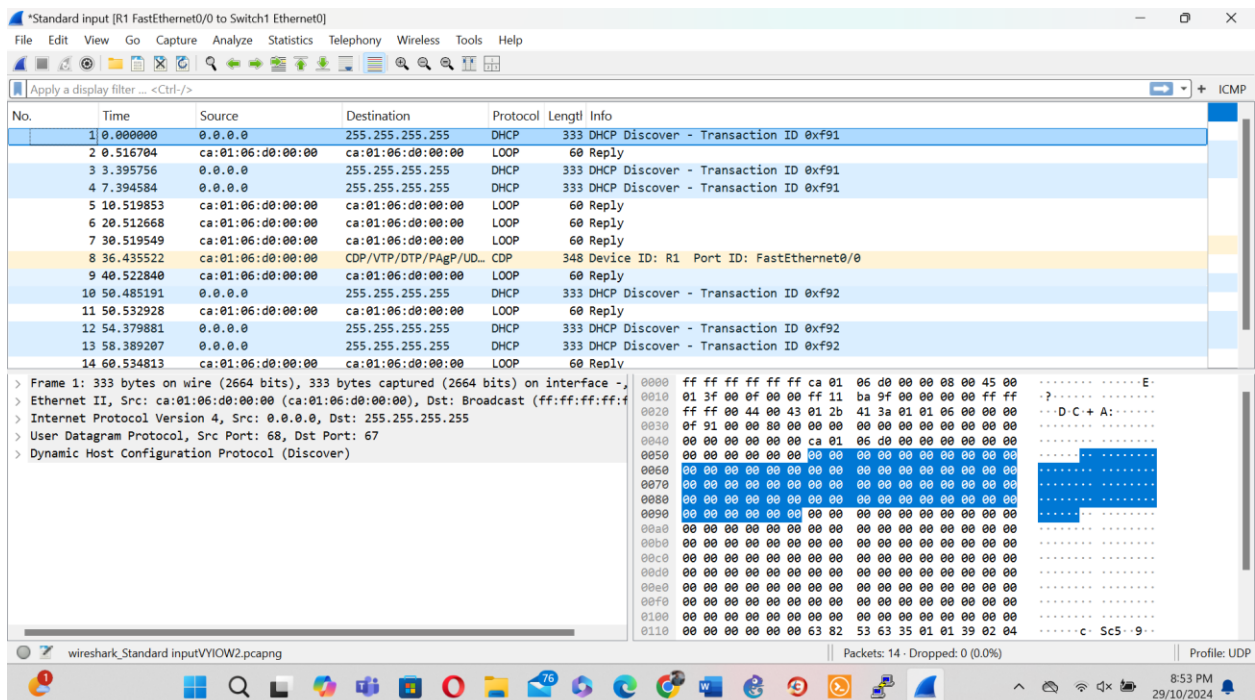
Fig.1

2. Configure R1's f0/0 interface to obtain its IP address from DHCP. Paste a screenshot of the interface configuration. **[3 points]**



3. Start a Wireshark capture in this step to capture all DHCP messages that will be exchanged in the next step. In the above topology, where would you initiate a Wireshark capture? [1 point]
 (Hint: To start a capture on Wireshark, right click on an interface and click start capture)

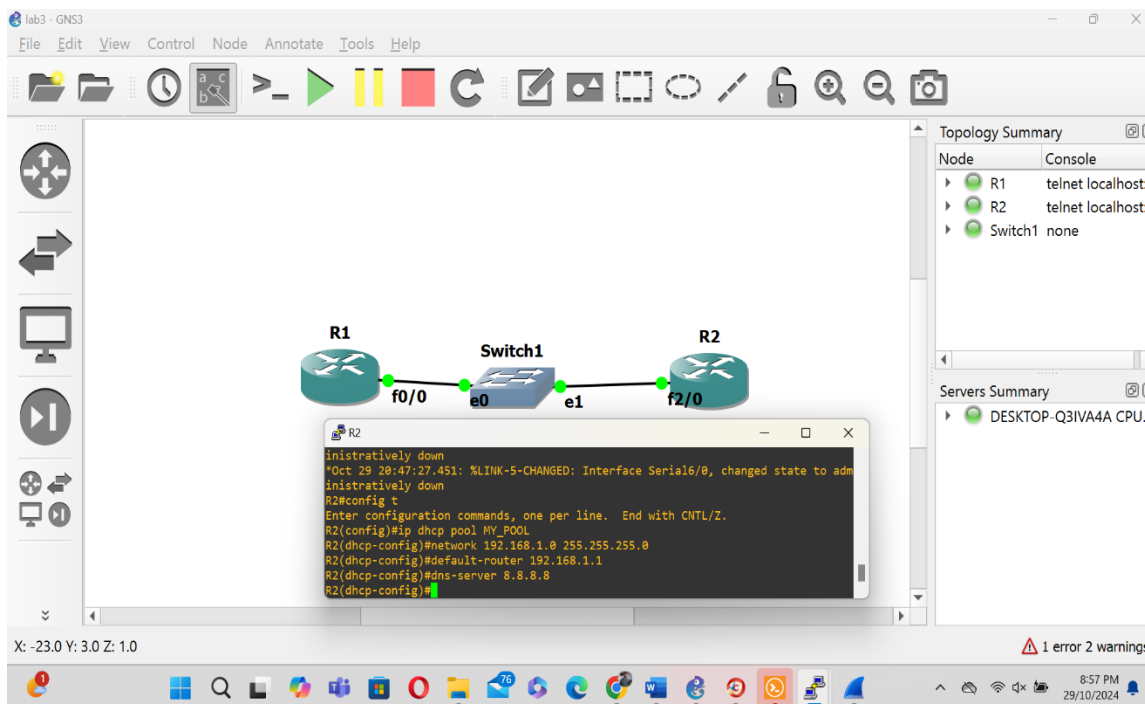
We can start the Wireshark capture in the e0 interface on the switch-1 because that is where we can see the DHCP packets exchanged with client and server.



4. If R2 is only a DHCP server, do you need any other basic configuration on R2 besides the configuration of a DHCP pool? Explain if the f0/1 interface of R2 needs to have an IP address. Justify your answer. **[5 points]**

Yes, R2 is only acting as a DHCP server, we do need some additional basic configuration particularly on the fa2/0 interface. The R2 should have the IP address within the same subnet as the DHCP pool, in this case 192.168.1.0/24. So, I have assigned IP address as 198.168.1.1 to fa2/0 allows R2 to act as default gateway for DHCP clients on the network and I have specified the default-router in the DHCP pool configuration. DHCP clients (R1) send DHCP Discover messages as broadcasts to identify available DHCP servers. R2 needs the same IP address within the subnet to listen to broadcasts and respond and act as a default gateway.

5. Having made sure you started Wireshark capture in Step 3, now configure R2 to be a DHCP server. Paste a screenshot of the configuration you made on R2. **[5 points]**

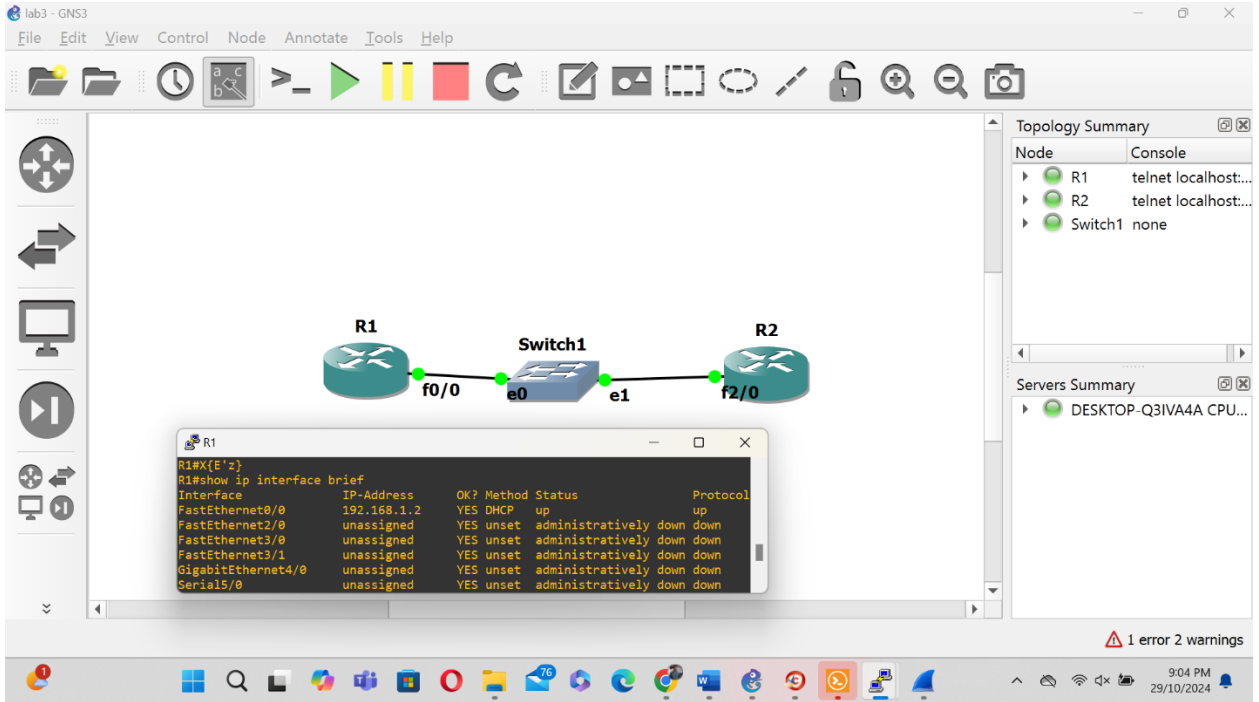


6. Did you get an IP address on R1? Indicate from its CLI that it got a DHCP address. How do you know this? **[2 points]**

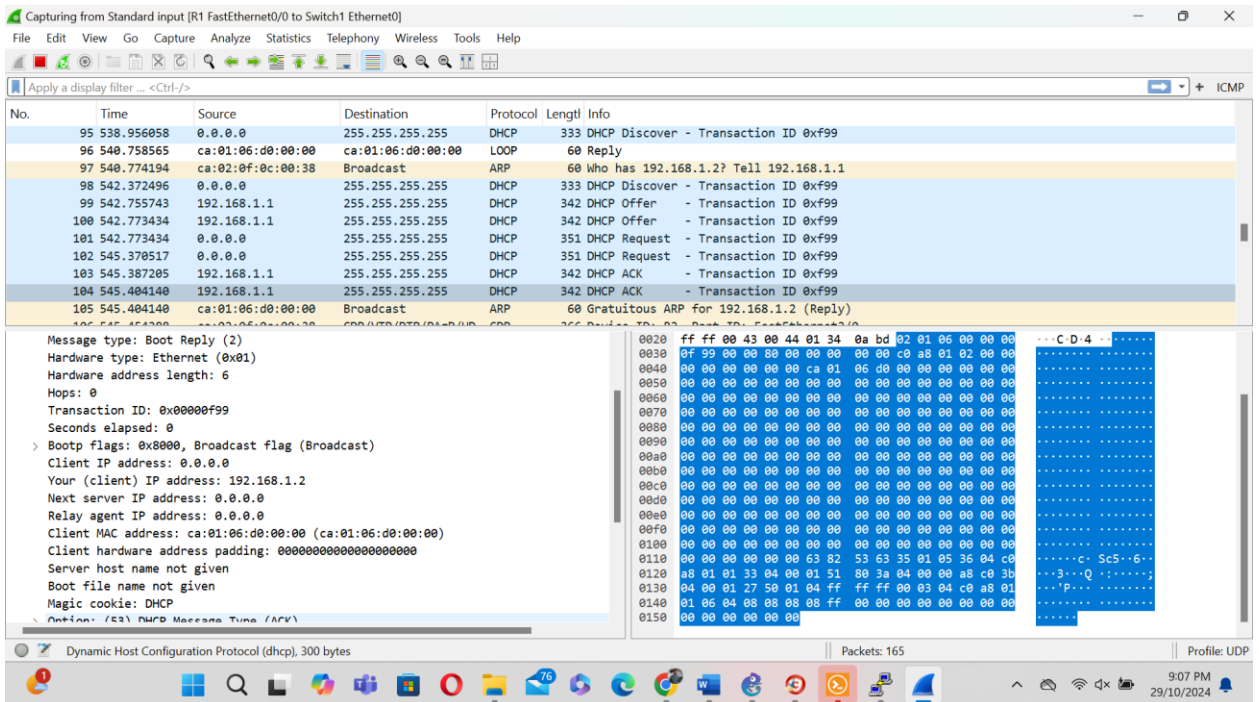
To verify that R1 successfully obtained an IP address via DHCP. We can go to R1 and enter the following command on R1.

Show ip interface brief

From the below figure it indicates that R1 obtained the IP address and it is 192.168.1.2 on fa0/0 and status and protocol shows “up”.



- In the above step, capture the DHCP messages that were exchanged. Explain in detail the four messages. For each of these messages, mention the Source IP, Destination IP, Source MAC and Destination MAC that you see. [10 points]



1.DHCP Discover

The purpose of DHCP Discover message is that it sends by the client (R1) to find any available DHCP servers on the network.

Source IP:0.0.0.0(Since client doesn't have an ip address yet)

Destination:255.255.255.255(Broadcast to all the devices on the local network)

Source MAC Address: ca:01:06:d0:00:00

Destination MAC address: ff:ff:ff:ff:ff:ff (broadcast MAC address)

The client broadcast this message to discover DHCP servers in the network that can assign IP addresses.

2.DHCP Offer

The purpose of DHCP Offer message is to send by DHCP server (R2) in response to DHCP Discover, offering an IP address to the client.

Source IP:192.168.1.1 (R2 IP address)

Destination:255.255.255.255(Broadcast to all the devices on the local network)

Source MAC Address: ca:02:0f:0c:00:38

Destination MAC address: ff:ff:ff:ff:ff:ff (broadcast MAC address)

The Server offers an IP address 192.168.1.2 and addition configurations.

3.DHCP Request

The purpose of DHCP Request message is sent by the client to request the offered Ip address from the DHCP server. Sometimes if the router already had a IP address, it may ask its preferred IP address back.

Source IP:0.0.0.0 (Since the client hasn't fully configured its IP)

Destination:255.255.255.255(Broadcast to all the devices on the local network)

Source MAC Address: ca:01:06:d0:00:00

Destination MAC address: ff:ff:ff:ff:ff:ff (broadcast MAC address)

The Client accepts the IP address offered by the DHCP server and request to formally lease it.

4.DHCP Acknowledgement

The purpose of DHCP Acknowledgment message is sent by the server to confirm that IP address has been given to the client.

Source IP:192.168.1.1 (R2 IP address)

Destination: 192.168.1.2 (the newly assigned IP address of R1)

Source MAC Address: ca:02:0f:0c:00:38 (R2 MAC address)

Destination MAC address: ca:01:06:d0:00:00 (R1 MAC address)

The client finalizes and uses the IP address 192.168.1.2 on its interface.

8. Which of the DHCP messages are broadcast at Layer 3? Which of the DHCP messages are broadcast at Layer 2? **[2 points]**

In layer 3, the DHCP discover and DHCP Request are Broadcast at layer 3 . DHCP Discover because the client does know the IP address of the DHCP server so the destination IP (255.255.255.255). DHCP requests are also broadcast as the client formally requests the offered IP address from the DHCP server.

In layer 2, both DHCP Discover and Request does broadcast to ensure all the devices on the local network see the message.

- Are there any other messages you expect to see during the above process except DHCP messages? (Eg: From your theoretical knowledge of DHCP, postulate if you would see any ARP, ICMP or any other messages. Now verify the same on Wireshark)

Explain if you see any of these messages. Why or why not? [5 points]

ICMP messages, such as pings may appear after IP assignment to check the connectivity. There are no ICMP messages shown in the capture since I haven't done any ping. ICMP messages would appear if a connectivity test was initiated using ping.

ARP is expected as part of the DHCP process to check that the IP address is unique on the network. Once the DHCP assigns an IP address to the client it typically performs an ARP check to confirm that assigned IP address is unique on the network and not in use. The message can be Gratuitous ARP or standard ARP. The Gratuitous ARP for newly assigned IP (192.168.1.2) confirms that the client ensures no IP conflicts.

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays the following key entries:

No.	Time	Source	Destination	Protocol	Length	Info
89	490.959533	ca:02:0f:0c:00:38	ca:01:06:d0:00:00	CDP	366	Device ID: R2 Port ID: FastEthernet2/0
90	500.756824	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
91	510.748472	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
92	513.171161	ca:01:06:d0:00:00	ca:01:06:d0:00:00	CDP	348	Device ID: R1 Port ID: FastEthernet0/0
93	520.748177	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
94	530.756539	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
95	538.956058	0.0.0.0	255.255.255.255	DHCP	333	DHCP Discover - Transaction ID 0xf99
96	540.758565	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
97	540.774194	ca:02:0f:0c:00:38	Broadcast	ARP	60	Who has 192.168.1.2? Tell 192.168.1.1
98	542.372496	0.0.0.0	255.255.255.255	DHCP	333	DHCP Discover - Transaction ID 0xf99
99	542.755743	192.168.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xf99
100	542.773434	192.168.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xf99
101	542.773434	0.0.0.0	255.255.255.255	DHCP	351	DHCP Request - Transaction ID 0xf99
102	545.370517	0.0.0.0	255.255.255.255	DHCP	351	DHCP Request - Transaction ID 0xf99
103	545.387205	192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xf99
104	545.404140	192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xf99
105	545.404140	ca:01:06:d0:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.2 (Reply)
106	545.454288	ca:02:0f:0c:00:38	ca:01:06:d0:00:00	CDP	366	Device ID: R2 Port ID: FastEthernet2/0
107	548.454455	ca:01:06:d0:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.2 (Reply)
108	548.501498	ca:01:06:d0:00:00	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.2
109	548.518062	ca:02:0f:0c:00:38	ca:01:06:d0:00:00	ARP	60	192.168.1.1 is at ca:02:0f:0c:00:38
110	550.756822	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
111	560.762140	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply
112	565.924510	ca:01:06:d0:00:00	ca:01:06:d0:00:00	CDP	366	Device ID: R1 Port ID: FastEthernet0/0
113	570.767052	ca:01:06:d0:00:00	ca:01:06:d0:00:00	LOOP	60	Reply

The packet details pane for the selected DHCP Discover packet (No. 95) shows:

- Ethernet II, Src: ca:02:0f:0c:00:38 (ca:02:0f:0c:00:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255
- User Datagram Protocol, Src Port: 67, Dst Port: 68

The packet bytes pane shows the hexadecimal representation of the packet data.

Objective-2: DHCP server with multiple clients

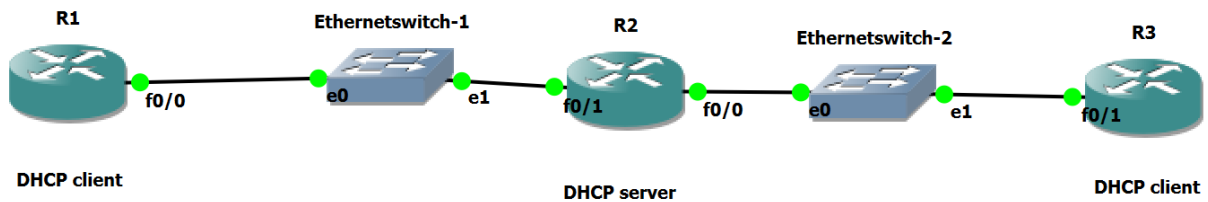


Fig.2

1. Refer to figure 2. Could this network design work? Can a single DHCP server serve two different DHCP clients as shown in the figure? If yes, explain what configuration changes you will need to do on R2 to make this work, and why you would have to make these modifications. Paste the configuration change you made on R2 to make it work.

[10 points]

Yes, a single DHCP server can serve multiple clients on different subnets. To make this work, we need to configure R2 with multiple DHCP pools, each corresponding to different subnets. R2 should know which DHCP pool to use based on the subnet it receives from the DHCP discover message. From the below screenshot is the configuration I made, the R1 pool serves IPs to client in the 192.168.1.0/24 network and R3 pool serves Ips to clients in the 192.168.2.0/24 network.

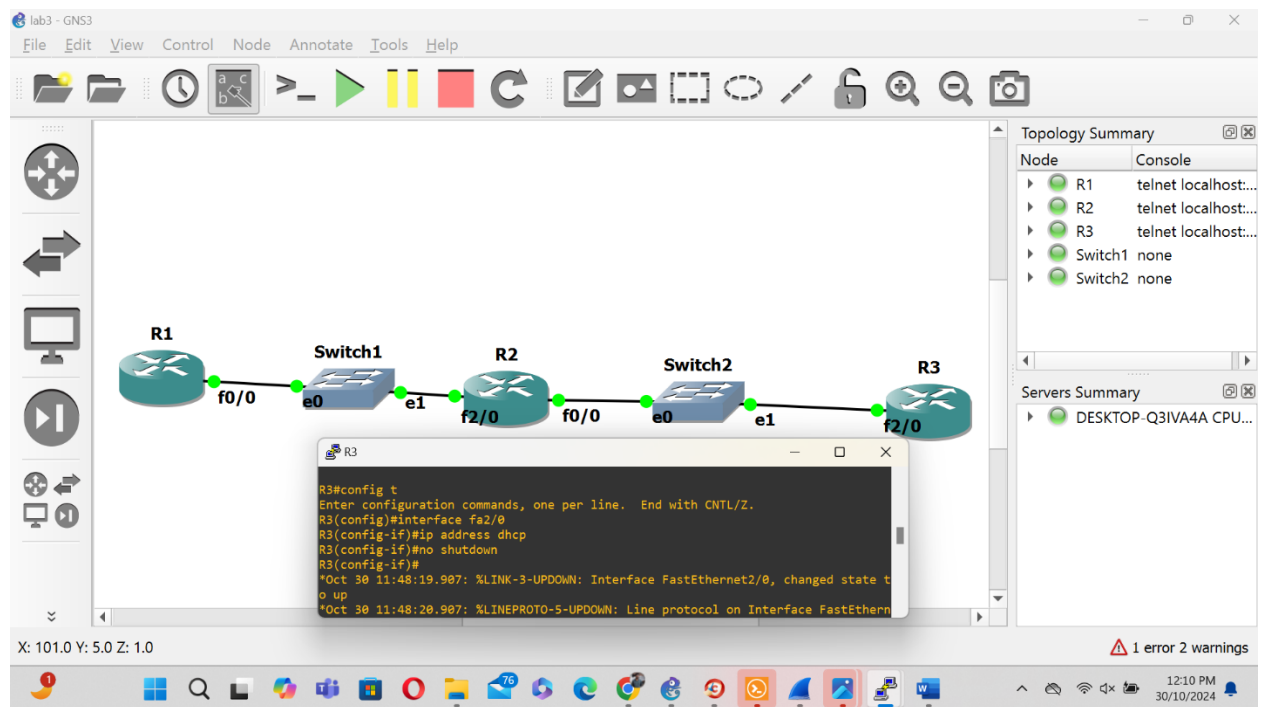
```
lab3 - GNS3
R2
R2(config-if)#show running-config | section dhcp
^
% Invalid input detected at '^' marker.

R2(config-if)#exit
R2(config)#exit
R2#show running-config | section dhcp
*Oct 29 21:00:36.935: %SYS-5-CONFIG_I: Configured from console by console
R2#show running-config | section dhcp
ip dhcp pool MY_POOL
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 8.8.8.8
R2#}z
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp pool R3_POOL
R2(dhcp-config)#network 192.168.2.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.2.1
R2(dhcp-config)#dns-server 8.8.8.8
R2(dhcp-config)#X{E'z}
R2#R}p
*Oct 29 23:09:15.563: %SYS-5-CONFIG_I: Configured from console by console
```

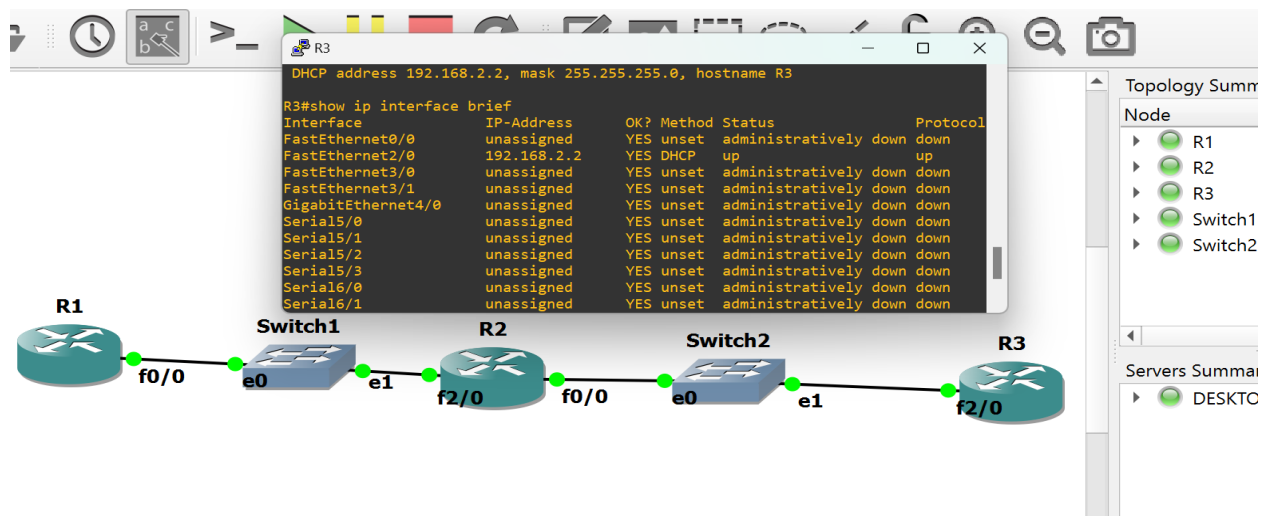

2. Now configure R3 as a DHCP client and R2 configured to also be the DHCP server for R3. Paste screenshots of DHCP messages exchanged and R3 getting the IP via DHCP.

[10 points]

The below screenshot shows the configuration I made to configure as R3 as a client.



From the below screenshot if I give the command show ip interface brief it shows that fa2/0 is assigned with IP address 192.168.2.2 by DHCP and status and protocol is “up”.



3. When R1 and R3 sent DHCP DISCOVER packets, how did R2 choose which IP to assign? How does R2 know which DHCP pool to use to loan IPs, if there are multiple pools configured on R2. **[10 points]**

When R1 and R3 send DHCP Discover packets, R2 decides which IP to assign by checking the interface on which the request was received. Each interface on R2 is associated with a specific subnet, and R2 has a DHCP pool configured for each subnet.

If R2 receives a Discover packet on its f0/0 interface, it is connected to 192.168.2.0/24 subnet and it assigns an IP from R3 pool and it gave 192.168.2.2 as the IP address.

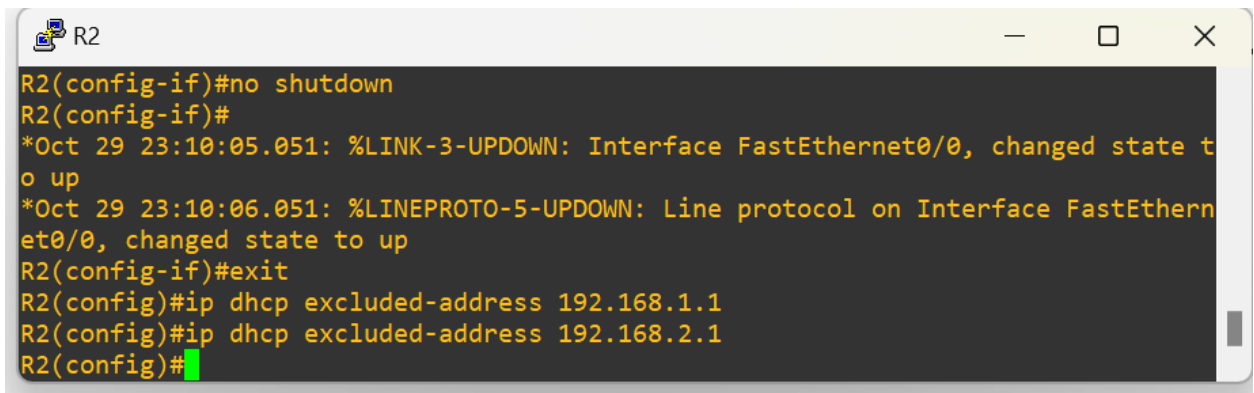
If R2 receives a Discover packet on its fa2/0 interface, it is connected to 192.168.1.0/24 subnet and it assigns an IP from R1 pool and it gave 192.168.1.2 as the IP address.

R2 uses the source interface of the incoming DHCP request to select the corresponding DHCP pool and allocate the correct IP address for each subnet.

4. Explain excluded DHCP addresses are and why you would use them. Did you configure this on R2? If so, what are some of the DHCP excluded addresses on R2 in your topology? **[3 points]**

Exclude DHCP addresses are specific IP addresses within the DHCP pools range and that are reserved and not assigned to clients by the DHCP server. Excluded addresses prevent conflicts from statically assigned IP and dynamically assigned IP. For instance, the default gateway should typically be excluded to avoid accidental assignments to clients.

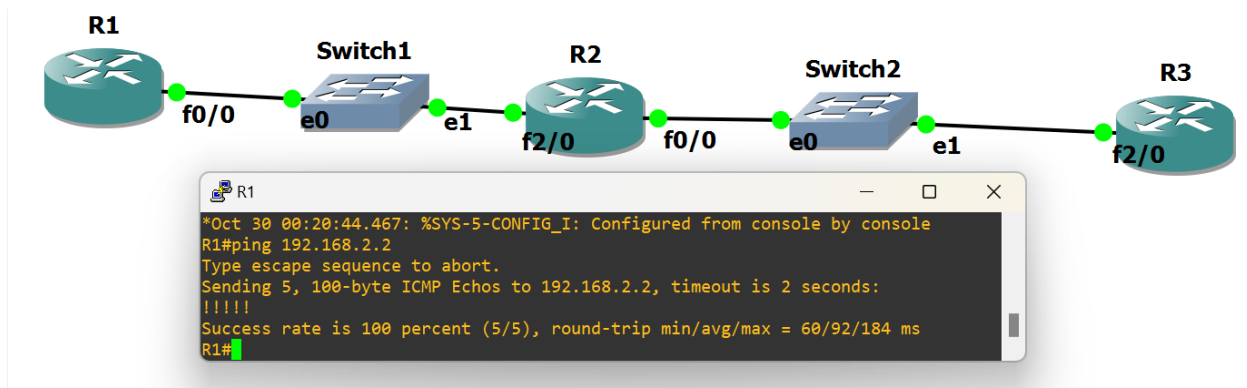
Yes, I have configured an excluded address on R2 which is 192.168.1.1 and 192.168.2.1 which is default gateway on the subnet R1 and R3. By excluding these addresses, R2 ensures that they are not assigned to DHCP clients, reserving them for gateway purposes.



```
R2
R2(config-if)#no shutdown
R2(config-if)#
*Oct 29 23:10:05.051: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Oct 29 23:10:06.051: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config-if)#exit
R2(config)#ip dhcp excluded-address 192.168.1.1
R2(config)#ip dhcp excluded-address 192.168.2.1
R2(config)#
```

5. Can R1's f0/0 interface communicate with R3's f0/1 interface? If yes, how? Make this work without adding any static routes on any of the routers. Paste screenshots of what you did to make it work and the successful ping. **[3 points]**

Yes, R1 interface fa0/0 can communicate with R3 fa0/1 interface because R2 interface is directly connected with R1 and R3. When R1 sends a packet to R2 it has route R3 which is directly connected. Therefore, it will route the packets to R3 and doesn't require static routes on any routes.



6. Explain four differences between TCP and UDP. Mention two advantages and disadvantages of both. [5 points]

- TCP is connection oriented, it establishes a connection before data transfer and ensures reliable communication.
- UDP is connectionless, it sends out data without establishing a connection, making it faster but less reliable.
- TCP provides reliability through error checking and acknowledgment of packets and retransmission of lost packets.
- UDP does not guarantee delivery, order, or error-checking, which makes it faster but less dependable.
- TCP includes flow control mechanisms to manage data transmission rates between sender and receiver.
- UDP does not have flow control mechanisms, allowing data to be sent continuously without adjustments.
- TCP is suitable for application reliable data transfer such as web browsing (HTTP) and email (SMTP).
- UDP is used in applications where speed is critical such as video streaming, gaming and VoIP.

Advantages of TCP

1. Reliable data transfer due to acknowledgment and retransmission.
2. Ensures data is received in the right order.

Disadvantages of TCP

1. High latency due connection setup and acknowledgement.
2. More overhead leading to slower performance.

Advantages of UDP

1. Faster data transmission with lower latency and suitable for real-time applications.
2. Less overhead making it lightweight and efficient.

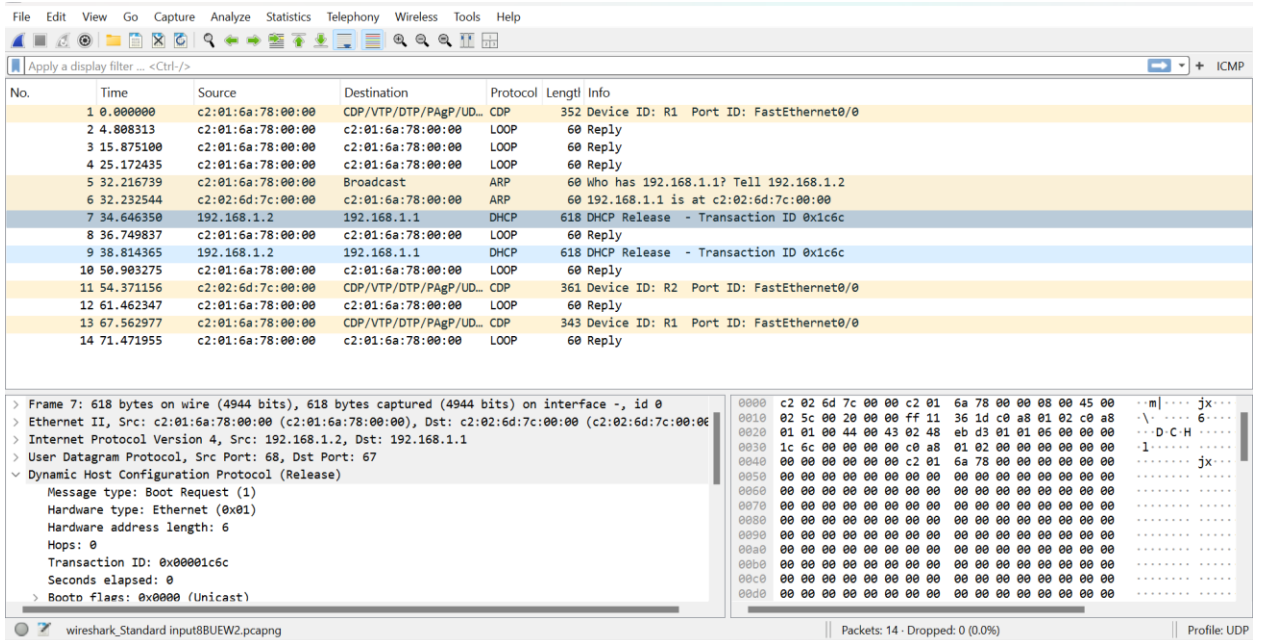
Disadvantages of UDP

1. If a packet is lost there is no retransmission therefore no reliability

2. Packets may arrive out of order, they don't have the mechanism to keep it in right order.

7. Release the DHCP IP from the client R1. What command did you use? Paste the screenshot of the packet capture on Wireshark where these DHCP messages are captured. [5 points]

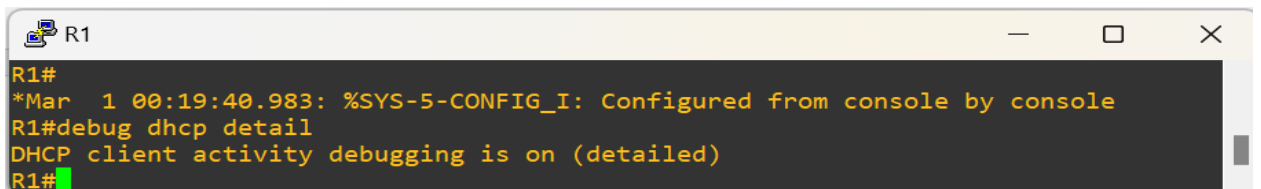
I gave the command "no ip address dhcp" to release the dhcp IP from the client and captured the traffic between R1 client and R2 server.



8. Can the server also retrieve the DHCP IP back from the client before the lease time is over? If yes, what command can you use on the server to do this? [5 points]

Yes, the DHCP server can retrieve or a free DHCP-assigned IP address from the client before the release time is over by using clear ip dhcp binding 192.168.1.2. This action effectively removes the IP address assignment from the servers DHCP release table making it available for reassignment. This command only clears the DHCP lease from the server side, the client may still retain the IP address until it refreshes or releases the lease on its own. The client needs to release the IP, we need to perform dhcp release action on the client device.

9. Now turn on DHCP debugging on R1 and R3. What commands did you use? [3 points]



```

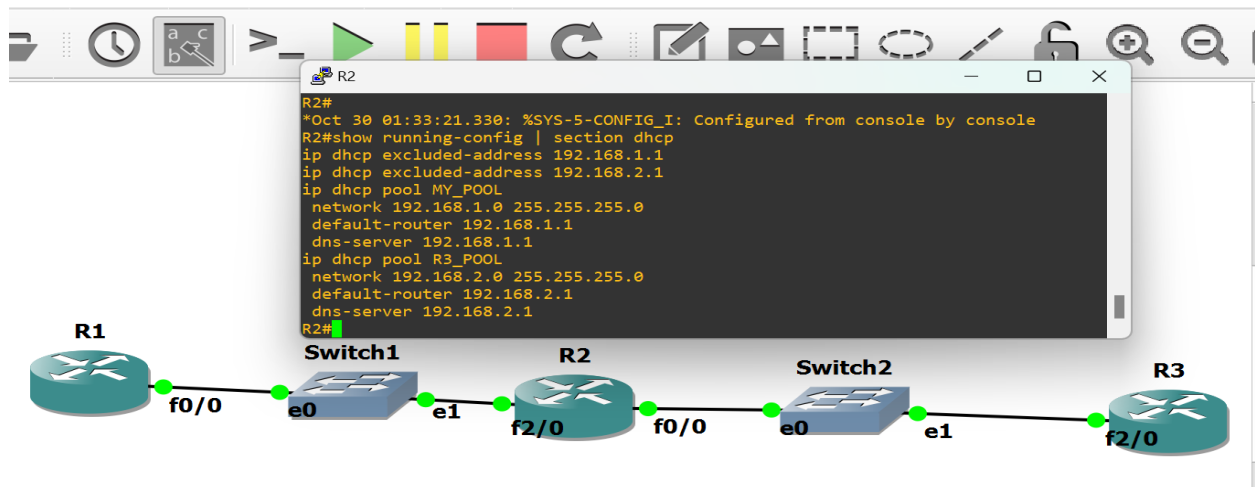
R3#debug dhcp detail
DHCP client activity debugging is on (detailed)
R3#

```

- Update the configuration on R2 to provide extra DHCP option for DNS. The DNS server you are using should be R2 itself. Include the appropriate IP address(es) to use in the DHCP configuration. Paste a screenshot of updated DHCP configuration on R2.

[10 points]

To configure R2 as the DNS server in the DHCP settings, we need to add a DNS server options within the DHCP pool configuration. Clients R1 and R3 will receive the respective IP address of R2 as their DNS server along with their IP lease allowing them to resolve domain names using R2's IP. R2 IP addresses are 192.168.1.1 in f2/0 interface and 192.168.2.1 in f0/0 interface.



- After DHCP is successful, paste screenshots of debug messages you captured on R1 and R3 indicating the success. **[10 points]**

```

R1
R1(config-if)#
*Mar 1 00:35:36.035: DHCP: DHCP client process started: 10
*Mar 1 00:35:36.035: RAC: Starting DHCP discover on FastEthernet0/0
*Mar 1 00:35:36.035: DHCP: Try 1 to acquire address for FastEthernet0/0
*Mar 1 00:35:36.047: DHCP: allocate request
*Mar 1 00:35:36.047: DHCP: new entry. add to queue, interface FastEthernet0/0
*Mar 1 00:35:36.051: DHCP: SDiscover attempt # 1 for entry:
*Mar 1 00:35:36.051: Temp IP addr: 0.0.0.0 for peer on Interface: FastEthernet
0/0
*Mar 1 00:35:36.051: Temp sub net mask: 0.0.0.0
*Mar 1 00:35:36.051: DHCP Lease server: 0.0.0.0, state: 3 Selecting
*Mar 1 00:35:36.055: DHCP transaction id: AE9
R1(config-if)#
*Mar 1 00:35:36.055: Lease: 0 secs, Renewal: 0 secs, Rebind: 0 secs
*Mar 1 00:35:36.055: Next timer fires after: 00:00:04
*Mar 1 00:35:36.055: Retry count: 1 Client-ID: cisco-c201.6860.0000-Fa0/0
*Mar 1 00:35:36.055: Client-ID hex dump: 636973636F2D633230312E363836302E
303030302D4661302F30
*Mar 1 00:35:36.063: Hostname: R1
*Mar 1 00:35:36.067: DHCP: SDiscover: sending 291 byte length DHCP packet
*Mar 1 00:35:36.067: DHCP: SDiscover 291 bytes
*Mar 1 00:35:36.067: B'cast on FastEthernet0/0 interface from 0.0.0.0

```

```
R1
nd secs: 75600
*Mar 1 00:35:38.119: DHCP: Server ID Option: 192.168.1.1
*Mar 1 00:35:38.119: DHCP: offer received from 192.168.1.1
*Mar 1 00:35:38.123: DHCP: SRequest attempt # 1 for entry:
*Mar 1 00:35:38.123: Temp IP addr: 192.168.1.3 for peer on Interface: FastEthernet0/0
*Mar 1 00:35:38.123: Temp sub net mask: 255.255.255.0
*Mar 1 00:35:38.123: DHCP Lease server: 192.168.1.1, state: 4 Requesting
*Mar 1 00:35:38.127: DHCP transaction id: AE9
*Mar 1 00:35:38.127: Lease: 86400 secs, Renewal: 0 secs, Rebind: 0 secs
*Mar 1 00:35:38.127: Next timer fires after: 00:00:03
*Mar 1 00:35:38.127: Retry count: 1 Client-ID: cisco-c201.6860.0000-Fa0/0
*Mar 1 00:35:38.127: Client-ID hex dump: 636973636F2D633230312E363836302E
*Mar 1 00:35:38.135: 303030302D4661302F30
*Mar 1 00:35:38.139: Hostname: R1
*Mar 1 00:35:38.139: DHCP: SRequest- Server ID option: 192.168.1.1
*Mar 1 00:35:38.139: DHCP: SRequest- Requested IP addr option: 192.168.1.3
*Mar 1 00:35:38.139: DHCP: SRequest placed lease len option: 86400
*Mar 1 00:35:38.139: DHCP: SRequest: 309 bytes
*Mar 1 00:35:38.143: DHCP: SRequest: 309 bytes
*Mar 1 00:35:38.143: B'cast on FastEthernet0/0 interface from 0.0.0.0
*Mar 1 00:35:38.183: DHCP: Received a BOOTREP pkt
```

```
R1
*Mar 1 00:35:38.183: DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Mar 1 00:35:38.183: DHCP server identifier: 192.168.1.1
*Mar 1 00:35:38.183: xid: AE9, secs: 0, flags: 8000
*Mar 1 00:35:38.183: client: 0.0.0.0, your: 192.168.1.3
*Mar 1 00:35:38.183: srvr: 0.0.0.0, gw: 0.0.0.0
*Mar 1 00:35:38.183: options block length: 60
*Mar 1 00:35:38.183: DHCP Ack Message
*Mar 1 00:35:38.183: DHCP: Lease Seconds: 86400 Renewal secs: 43200 Rebind secs: 75600
*Mar 1 00:35:38.183: DHCP: Server ID Option: 192.168.1.1
*Mar 1 00:35:41.183: DHCP: Releasing ipl options:
*Mar 1 00:35:41.183: DHCP: Applying DHCP options:
*Mar 1 00:35:41.183: Setting default_gateway to 192.168.1.1
*Mar 1 00:35:41.183: Adding default route 192.168.1.1
*Mar 1 00:35:42.183: DHCP Client Pooling: ***Allocated IP address: 192.168.1.3
*Mar 1 00:35:42.243: Allocated IP address = 192.168.1.3 255.255.255.0
*Mar 1 00:35:42.243: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 192.168.1.3, mask 255.255.255.0, hostname R1
R1(config-if)#
R1(config-if)#
```



```

R3
R3(config-if)#
*Mar 1 00:24:39.231: DHCP: DHCP client process started: 10
*Mar 1 00:24:39.243: RAC: Starting DHCP discover on FastEthernet0/1
*Mar 1 00:24:39.243: DHCP: Try 1 to acquire address for FastEthernet0/1
*Mar 1 00:24:39.259: DHCP: allocate request
*Mar 1 00:24:39.259: DHCP: new entry. add to queue, interface FastEthernet0/1
*Mar 1 00:24:39.259: DHCP: SDiscover attempt # 1 for entry:
*Mar 1 00:24:39.263: Temp IP addr: 0.0.0.0 for peer on Interface: FastEthernet0/1
*Mar 1 00:24:39.263: Temp sub net mask: 0.0.0.0
*Mar 1 00:24:39.263: DHCP Lease server: 0.0.0.0, state: 3 Selecting
*Mar 1 00:24:39.263: DHCP transaction id: D23
R3(config-if)#
*Mar 1 00:24:39.263: Lease: 0 secs, Renewal: 0 secs, Rebind: 0 secs
*Mar 1 00:24:39.267: Next timer fires after: 00:00:04
*Mar 1 00:24:39.267: Retry count: 1 Client-ID: cisco-c203.5ea0.0001-Fa0/1
*Mar 1 00:24:39.267: Client-ID hex dump: 636973636F2D6332303332E356561302E
*Mar 1 00:24:39.275: 303030312D4661302F31
*Mar 1 00:24:39.275: Hostname: R3
*Mar 1 00:24:39.279: DHCP: SDiscover: sending 291 byte length DHCP packet
*Mar 1 00:24:39.279: DHCP: SDiscover 291 bytes
*Mar 1 00:24:39.279: B'cast on FastEthernet0/1 interface from 0.0.0.0

```

```

R3
.0
R3(config-if)#
*Mar 1 00:24:41.563: DHCP: Received a BOOTREP pkt
*Mar 1 00:24:41.563: DHCP: Scan: Message type: DHCP Offer
*Mar 1 00:24:41.567: DHCP: Scan: Server ID Option: 192.168.2.1 = C0A80201
*Mar 1 00:24:41.567: DHCP: Scan: Lease Time: 86400
*Mar 1 00:24:41.567: DHCP: Scan: Renewal time: 43200
*Mar 1 00:24:41.567: DHCP: Scan: Rebind time: 75600
*Mar 1 00:24:41.567: DHCP: Scan: Subnet Address Option: 255.255.255.0
*Mar 1 00:24:41.567: DHCP: Scan: Router Option: 192.168.2.1
*Mar 1 00:24:41.571: DHCP: rcvd pkt source: 192.168.2.1, destination: 255.255.255.255
*Mar 1 00:24:41.571: UDP sport: 43, dport: 44, length: 308
*Mar 1 00:24:41.571: DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Mar 1 00:24:41.571: DHCP server identifier: 192.168.2.1
*Mar 1 00:24:41.571: xid: D23, secs: 0, flags: 8000
*Mar 1 00:24:41.575: client: 0.0.0.0, your: 192.168.2.3
*Mar 1 00:24:41.575: srvr: 0.0.0.0, gw: 0.0.0.0
*Mar 1 00:24:41.575: options block length: 60
*Mar 1 00:24:41.575: DHCP Offer Message Offered Address: 192.168.2.3
*Mar 1 00:24:41.579: DHCP: Lease Seconds: 86400 Renewal secs: 43200 Rebind secs: 75600

```

```

R3
nd secs: 75600
*Mar 1 00:24:41.579: DHCP: Server ID Option: 192.168.2.1
*Mar 1 00:24:41.579: DHCP: offer received from 192.168.2.1
*Mar 1 00:24:41.579: DHCP: SRequest attempt # 1 for entry:
*Mar 1 00:24:41.579: Temp IP addr: 192.168.2.3 for peer on Interface: FastEthernet0/1
*Mar 1 00:24:41.583: Temp sub net mask: 255.255.255.0
*Mar 1 00:24:41.583: DHCP Lease server: 192.168.2.1, state: 4 Requesting
*Mar 1 00:24:41.583: DHCP transaction id: D23
*Mar 1 00:24:41.583: Lease: 86400 secs, Renewal: 0 secs, Rebind: 0 secs
*Mar 1 00:24:41.587: Next timer fires after: 00:00:03
*Mar 1 00:24:41.587: Retry count: 1 Client-ID: cisco-c203.5ea0.0001-Fa0/1
*Mar 1 00:24:41.587: Client-ID hex dump: 636973636F2D6332303332E356561302E
*Mar 1 00:24:41.591: 303030312D4661302F31
*Mar 1 00:24:41.595: Hostname: R3
*Mar 1 00:24:41.595: DHCP: SRequest- Server ID option: 192.168.2.1
*Mar 1 00:24:41.599: DHCP: SRequest- Requested IP addr option: 192.168.2.3
*Mar 1 00:24:41.599: DHCP: SRequest placed lease len option: 86400
*Mar 1 00:24:41.599: DHCP: SRequest: 309 bytes
*Mar 1 00:24:41.599: DHCP: SRequest: 309 bytes
*Mar 1 00:24:41.603: B'cast on FastEthernet0/1 interface from 0.0.0.0
.0
*Mar 1 00:24:41.711: DHCP: Received a BOOTREP pkt

```



```
R3
*Mar 1 00:24:41.711: DHCP: Received a BOOTREP pkt
*Mar 1 00:24:41.711: DHCP: Scan: Message type: DHCP Ack
*Mar 1 00:24:41.711: DHCP: Scan: Server ID Option: 192.168.2.1 = C0A80201
*Mar 1 00:24:41.715: DHCP: Scan: Lease Time: 86400
*Mar 1 00:24:41.715: DHCP: Scan: Renewal time: 43200
*Mar 1 00:24:41.715: DHCP: Scan: Rebind time: 75600
*Mar 1 00:24:41.715: DHCP: Scan: Subnet Address Option: 255.255.255.0
*Mar 1 00:24:41.715: DHCP: Scan: Router Option: 192.168.2.1
*Mar 1 00:24:41.715: DHCP: rcvd pkt source: 192.168.2.1, destination: 255.255.255.255
*Mar 1 00:24:41.719:     UDP sport: 43, dport: 44, length: 308
*Mar 1 00:24:41.719:     DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Mar 1 00:24:41.719:     DHCP server identifier: 192.168.2.1
*Mar 1 00:24:41.719:     xid: D23, secs: 0, flags: 8000
*Mar 1 00:24:41.719:     client: 0.0.0.0, your: 192.168.2.3
*Mar 1 00:24:41.723:     srvr: 0.0.0.0, gw: 0.0.0.0
*Mar 1 00:24:41.723:     options block length: 60

*Mar 1 00:24:41.723: DHCP Ack Message
*Mar 1 00:24:41.723: DHCP: Lease Seconds: 86400      Renewal secs: 43200      Rebind secs: 75600
*Mar 1 00:24:41.727: DHCP: Server ID Option: 192.168.2.1
*Mar 1 00:24:44.743: DHCP: Releasing ipl options:
```

```
R3
*Mar 1 00:24:41.719:     DHCP op: 2, htype: 1, hlen: 6, hops: 0
*Mar 1 00:24:41.719:     DHCP server identifier: 192.168.2.1
*Mar 1 00:24:41.719:     xid: D23, secs: 0, flags: 8000
*Mar 1 00:24:41.719:     client: 0.0.0.0, your: 192.168.2.3
*Mar 1 00:24:41.723:     srvr: 0.0.0.0, gw: 0.0.0.0
*Mar 1 00:24:41.723:     options block length: 60

*Mar 1 00:24:41.723: DHCP Ack Message
*Mar 1 00:24:41.723: DHCP: Lease Seconds: 86400      Renewal secs: 43200      Rebind secs: 75600
*Mar 1 00:24:41.727: DHCP: Server ID Option: 192.168.2.1
*Mar 1 00:24:44.743: DHCP: Releasing ipl options:
*Mar 1 00:24:44.743: DHCP: Applying DHCP options:
*Mar 1 00:24:44.747:     Setting default_gateway to 192.168.2.1
*Mar 1 00:24:44.747:     Adding default route 192.168.2.1
*Mar 1 00:24:45.747: DHCP Client Pooling: ***Allocated IP address: 192.168.2.3
*Mar 1 00:24:45.851: Allocated IP address = 192.168.2.3 255.255.255.0

*Mar 1 00:24:45.851: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1 assigned
DHCP address 192.168.2.3, mask 255.255.255.0, hostname R3

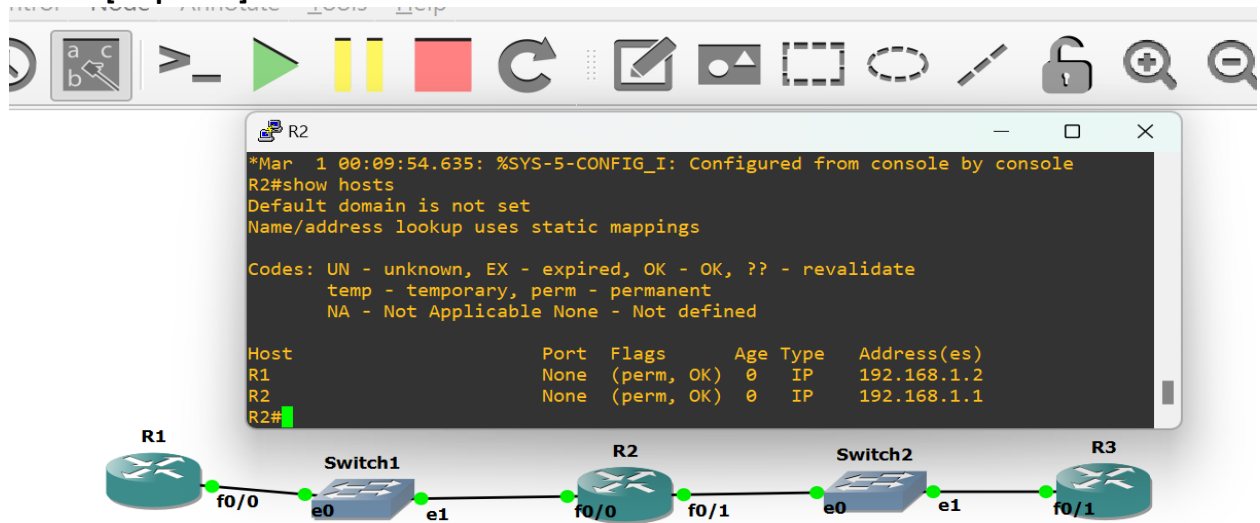
R3(config-if)#
R3(config-if)#
```

Objective-3: Getting started with DNS

1. Now configure R2 as the DNS server. Below are the mappings you will add on the DNS server:

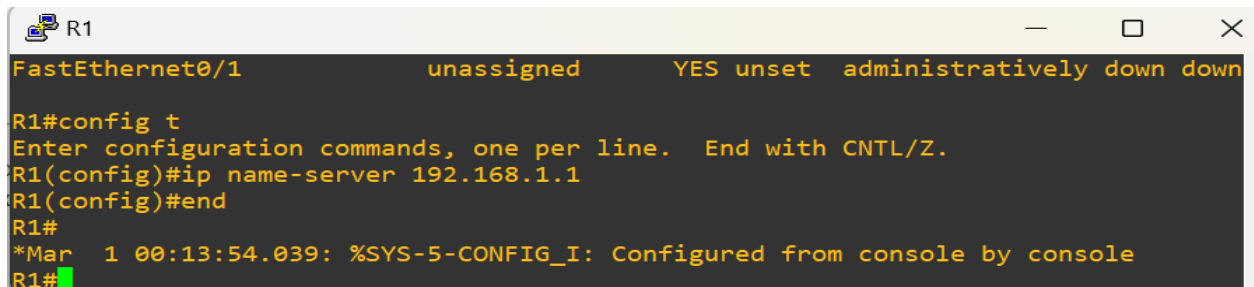
Hostname	IP address
R1	R1's interface IP
R2	R2's interface IP

Paste a screenshot of the configuration on R2 indicating the hostname configurations.
[10 points]



2. To implement DNS, do you need any additional configuration on R1 and R3? If yes, explain and paste screenshots. If not, explain. **[5 points]**

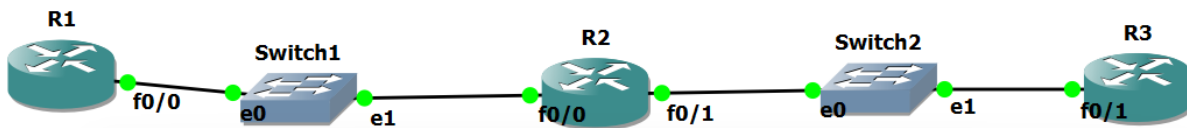
Yes, additional configuration is needed on R1 and R3 to specify R2 is DNS server enabling them to resolve hostnames.



```
R3
% Invalid input detected at '^' marker.

R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip name-server 192.168.2.1
R3(config)#end
R3#
*Mar  1 00:13:40.795: %SYS-5-CONFIG_I: Configured from console by console
R3#
```

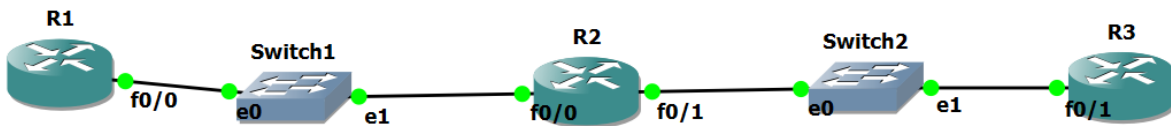
3. If DNS is successfully configured, from R1 you should be able to issue the command “ping R2” and on R2 use the command “ping R1”. Show screenshots of the ping working. [10 points]



```
R1
R1#
*Mar  1 00:43:25.783: %SYS-5-CONFIG_I: Configured from console by console
R1#ping R2

Translating "R2"...domain server (192.168.1.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/36/64 ms
R1#
```



```
R2
R2#ping R1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/31/48 ms
R2#
```

- Initiate a Wireshark capture in your topology. Where would you initiate the capture?
Paste a screenshot of the Wireshark capture of the DNS messages that are exchanged when you issue either “ping R1” or “ping R2” command. **[10 points]**

Since DNS request flow between R1 and R2 the ideal location to capture the traffic is the link between R1 and R2.

```

R1#
*Mar 1 00:43:25.783: %SYS-5-CONFIG_I: Configured from console by console
R1#ping R2

Translating "R2"...domain server (192.168.1.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/36/64 ms
R1#

```

The screenshot shows a Wireshark capture on the link between R1 and R2. The packet list pane shows the following traffic:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	c2:01:6a:78:00:00	c2:01:6a:78:00:00	LOOP	60	Reply
2	11.185760	c2:01:6a:78:00:00	c2:01:6a:78:00:00	LOOP	60	Reply
3	15.261415	192.168.1.2	192.168.1.1	DNS	62	Standard query 0x9a34 A R2
4	15.277023	192.168.1.1	192.168.1.2	DNS	78	Standard query response 0x9a34 A R2 A 192.168.1.1
5	15.293036	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) request id=0x0002, seq=0/0, ttl=255 (reply in 6)
6	15.308752	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) reply id=0x0002, seq=0/0, ttl=255 (request in 5)
7	15.324746	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) request id=0x0002, seq=1/256, ttl=255 (reply in 8)
8	15.340483	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) reply id=0x0002, seq=1/256, ttl=255 (request in 7)
9	15.355998	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) request id=0x0002, seq=2/512, ttl=255 (reply in 10)
10	15.371722	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) reply id=0x0002, seq=2/512, ttl=255 (request in 9)
11	15.387572	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) request id=0x0002, seq=3/768, ttl=255 (reply in 12)
12	15.403292	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) reply id=0x0002, seq=3/768, ttl=255 (request in 11)
13	15.419098	192.168.1.2	192.168.1.1	ICMP	114	Echo (ping) request id=0x0002, seq=4/1024, ttl=255 (reply in 14)
14	15.434727	192.168.1.1	192.168.1.2	ICMP	114	Echo (ping) reply id=0x0002, seq=4/1024, ttl=255 (request in 13)
15	20.543240	c2:01:6a:78:00:00	c2:01:6a:78:00:00	LOOP	60	Reply

The packet details pane for the selected packet (No. 3) shows:

```

> Ethernet II, Src: c2:01:6a:78:00:00 (c2:01:6a:78:00:00), Dst: c2:02:6d:7c:00:00 (c2:02:6d:7c:00:00)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 55611, Dst Port: 53
> Domain Name System (query)

```

The packet bytes pane shows the raw data of the DNS query packet.

- Explain in detail the sequence of DNS messages that are exchanged. **[8 points]**

When we issue a command like ping R2 on R1, the device needs to resolve the IP address of the hostname R2 before it proceeds for ping. So, it sends a DNS query, since R2 is used as a DNS server it will send a DNS query packet to R2. The source IP is 192.168.1.2 (R1) and the Destination IP is 192.168.1.1 (R2). The message contains the hostname R2 that R1 is trying to resolve and indicates a request for an IP address.

R2 receives the DNS query from R1 on its IP address 192.168.1.1. Since R2 has been configured as the DNS server and has static hostname mapping for R2, it checks its local hostname table. After R2 locates the IP address for R2, it sends a DNS response back to R1.

R2 sends a DNS response packet back to R1 with the resolved IP address. R1 receives a DNS response from R2. R1 reads the response and caches the IP address 192.168.1.1 for R2 and initiates a ping.

6. Did DNS use UDP or TCP as the transport layer protocol in this case? Will it ever use the other protocol? If yes, when? **[3 points]**

In this case DNS used UDP as a transport layer protocol for communication between R1 and R2. DNS typically uses UDP on port 53 because UDP is a lightweight protocol with lower overhead, making it faster for simple query-response exchanges.

Since most DNS queries are small, UDP is more efficient it doesn't require connection setup like TCP.

DNS will switch to TCP when there is large responses. If the DNS responses exceed 512 bytes it will use TCP for reliability. DNS uses TCP for zone transfers between DNS servers (when synchronizing records between primary and secondary DNS servers).

This ensures that large amounts of DNS data are transferred reliably, as TCP provides connection-oriented communication.

Objective-4: Report Questions

1. Run Wireshark on your laptop and start the capture on the interface going to the Internet. Ping www.google.com

2. What IP is your laptop using as the DNS server? How do you know this? **[2 points]**

While capturing traffic in Wireshark and filter out DNS, the DNS server IP is 128.138.129.76. It is mentioned in the DNS queries sent from the laptop's IP 10.200.205.253. I also verified in by giving a command ipconfig /all on my command prompt

3. For a DNS query, what is the source and destination port numbers? **[2 points]**

For a DNS query, the source port is typically a random port which was 59268 and the destination port=53 which is shown in UDP section.

4. For a DNS response what is the source and destination port numbers? **[2 points]**

For a DNS response, the source port is 53 and the destination port is 59268 that the client used to make the query.

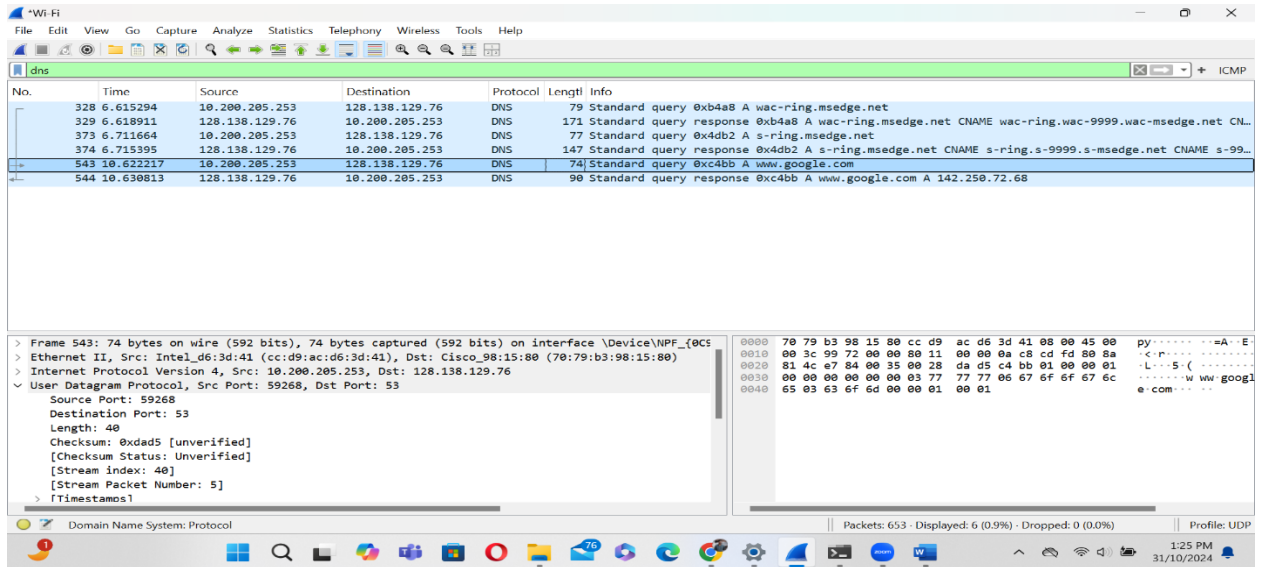
5. Clear any DNS cache on your laptop. How did you do this? Paste screenshot. **[2 points]**



```
C:\Users\abey>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\abey>
```

6. Paste a screenshot of the DNS messages exchanged in this case. Did DNS use UDP or TCP in this case? **[2 points]**

From the screenshot, DNS is using UDP. DNS typically uses protocol for DNS queries and responses due to its lightweight and speed compared to TCP.



- You had your DNS cache cleared. Assume all DNS nameservers in the world have their DNS cache cleared. Now explain in theory how your DNS query is resolved. Assuming no caches exist, what levels of the hierarchy does the query need to propagate through to get resolved? Explain the sequence of events and the flow. **[10 points]**

The process begins with the client (laptop) sending a DNS query to its configured DNS server. Since there is no DNS cache there is no mapping for any of the hostnames so it will have to resolve the query by contacting the higher-level DNS servers. So, it contacts the Root Nameserver. Root nameservers are the highest level in DNS hierarchy and know all the IP address of the Top-level Domain (TLD) nameservers. The root nameserver doesn't know the final IP address of the domain but can direct the query to the TLD nameserver. The TLD nameserver doesn't know the exact answer but knows the Authoritative Nameserver which holds the information of the specific domain. The TLD nameserver responds with IP address of google authoritative nameserver. It returns the IP address to the local DNS server. The local DNS server now has the IP address for ww.google.com and responds to the client with the final IP address. The client uses this IP address to establish a connection to www.google.com.

- Explain briefly the different type of DNS records. **[5 points]**

The types are:-

A Record (address Record): This record maps a domain name to an IPv4 address, allowing the domain to be resolved to a specific IP address.

AAAA Record (IPv6 Address Record): Like an A record but maps a domain name to an IPv6 address instead of IPv4. This is used for domains that operate over IPv6 networks.

CNAME Record (Canonical Name Record): This record allows a domain to be an alias of another domain. It allows multiple domains to refer to the same IP address

MX Record (Mail Exchange Record): Used to specify the mail server responsible for receiving emails on behalf of a domain. MX records include priority values to manage multiple mail servers, directing email to the highest-priority server.

NS Record (Name Server Record): It specifies the authoritative name servers for a domain. These records indicate which DNS servers are responsible for managing and resolving queries for a specific domain. NS records delegate a domain to a set of DNS servers.

9. What are the different types of DNS nameservers? Could you configure your laptop to be a DNS server too? If yes, explain what type of DNS nameserver or nameservers it can be. **[5 points]**

Root Nameservers: The top-level DNS servers that hold information about Top-level Domain (TLD) servers such .com or .org. They provide referrals to TLD servers but do not resolve domain names directly.

Top-level Domain Servers: These servers manage specific domain suffixes, such as .com or .org. They provide referrals to authoritative nameservers for domain within that TLD.

Authoritative Nameservers: These servers store DNS records for specific domains. They respond to queries with authoritative answers, directly providing the requested IP addresses.

Yes, we can configure my laptop to act as a DNS server, typically as a Local Authoritative DNS server. The laptop can act as an authoritative DNS server for specific domains within the local network. We can configure it to respond with IP addresses for internal domain names, useful for small network for devices without external domain requirements.

10. Explain briefly the HTTP Error Messages with their status code. **[2 points]**

400 Bad Request: The server cannot process the request due to client-side issues, such as malformed syntax or invalid request parameters.

401 Unauthorized: The request lacks valid authentication credentials, requiring the client to authenticate to access the resource.

403 Forbidden: the server understands the request but refuses to authorize it. The client does not have permission to access the resource.

404 Not found: the server cannot find the requested resource. This is a common error when the URL is incorrect, or the resource has been moved or deleted.

505 Internal Server Error: A generic error indicating the server encountered an unexpected condition that prevented it from fulfilling the request.

11. Explain briefly the different types of HTTP requests. **[2 points]**

GET: Requests data from a server without modifying it. Commonly used to load web pages. The data requested is appended to the URL, making it visible at the address.

POST: Sends data to the server to create or update a resource. Commonly used in form submissions. Data is sent in the body of the request, making it more secure than GET for sensitive information.

PUT: Used to update an existing resource or create a resource if it does not exist. Typically idempotent, meaning repeated PUT requests result in the same state.

DELETE: Used to remove resource from the server. Often requires authentication, as it modifies server data.

HEAD: Like GET, but only retrieves the headers of a resource, not the body. Often used to check if a resource exists or to inspect metadata.

12. What is a proxy web server? Mention any four advantages of using a proxy webserver. **[3 points]**

A proxy server is an intermediary server between a client and the internet. It forwards client requests to external servers and returns responses to the client. The advantage is that it provides improved security, it can mask client IPs, protecting user privacy.

Content filtering-Blocking access to certain websites for security or compliance.

Load balancing- Distributes requests to multiple servers, reducing server load.

Caching-Stores frequently accessed content, improving load times and reducing bandwidth usage.

13. You are trying to connect to www.bbc.com but the page does not load and keeps buffering. So now you try to connect to www.cnn.com and the page loads relatively faster. Brainstorm four possible reasons that could have led to this scenario. Mention the steps you will follow to troubleshoot this. **[10 points]**

We can try pinging both the websites with their IP address, if the ping is successful, it is a DNS issue that it is not able to resolve the hostname to IP address.

Run a traceroute to track the path to www.bbc.com if any hops are slow or unresponsive, indicating possible network issues.

Temporarily changing the DNS server to a reliable public DNS like google DNS (8.8.8.8), this change will help verify if the primary DNS server is causing the issue. After these steps we can verify that it is due to DNS resolution.

We can flush the local DNS cache to ensure the computer uses fresh DNS information by using command `ipconfig /flushdns`.

14. What is a major disadvantage in using HTTP? What is another protocol that would solve this issue? [2 points]

The disadvantage is that HTTP is not secure since it sends data in plaintext, making it vulnerable to interception.

By using HTTPS, which encrypts data using SSL/TLS, providing a secure connection.

Objective-5: DHCP Relay- Extra Credit [+20]

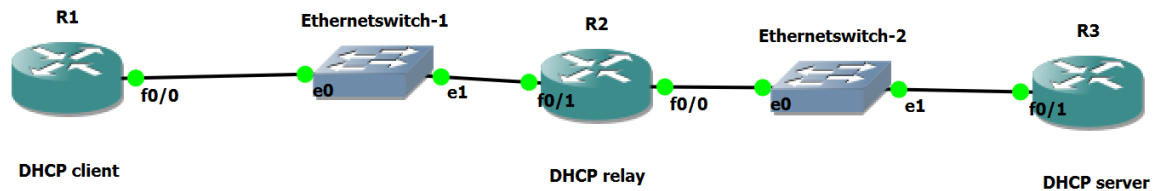


Fig.3

1. What is a DHCP relay? When would you use one? [2 points]

DHCP Relay is a function that allows router to forward DHCP messages between client and servers that are on different subnets. DHCP relay is used when the DHCP client and DHCP server are on different networks/subnets. Since DHCP messages are initially broadcasted (doesn't pass through routers), DHCP relay forwards these messages to ensure clients on different subnets can receive IP addresses from a centralized DHCP server.

2. Clear any previous configurations on your topology. Setup the topology shown in Fig3. Initiate a Wireshark capture on Switch-1 and a simultaneous Wireshark capture on Switch-2.
3. In this case, R1 should be configured as a DHCP client to get its IP from R3 which is the DHCP server. R2 is the DHCP relay.
4. Paste screenshot of DHCP and interface configurations on R1, R2 and R3 that will work. (Hint: show run | begin ip dhcp and sh ip int br) [5 points]

Router1:

```
R1
*Mar  1 01:08:00.023: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip int brief
Interface                IP-Address      OK? Method Status  Prot
ocol
Vlan1                    192.168.1.1    YES DHCP   up      up
FastEthernet0/0          192.168.1.1    YES DHCP   up      up
FastEthernet0/1          unassigned     YES unset  administratively down down
```


Router2:

```
R2
*Mar 1 00:04:24.927: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip int brief
Interface                IP-Address      OK? Method Status    Prot
ocol
FastEthernet0/0          192.168.3.2     YES manual up        up
FastEthernet0/1          192.168.1.2     YES manual up        up
R2#config t
```

```
R2
R2#show running-config
Building configuration...

Current configuration : 959 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no asa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
```

```
R2
!
archive
log config
hidekeys
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
ip address 192.168.3.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.1.2 255.255.255.0
ip helper-address 192.168.3.1
duplex auto
speed auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
```

Router3:

```
R3#show ip int brief
Interface                IP-Address      OK? Method Status        Prot
ocol
FastEthernet0/0          unassigned      YES unset  administratively down down
FastEthernet0/1          192.168.3.1    YES manual  up            up

R3#
```

```
R3#show running-config
Building configuration...

Current configuration : 1086 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip dhcp use vrf connected
!
ip dhcp pool CLIENT_POOL
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
```

```
R3#
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 192.168.1.0 255.255.255.0 192.168.3.2
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
control-plane
!
```

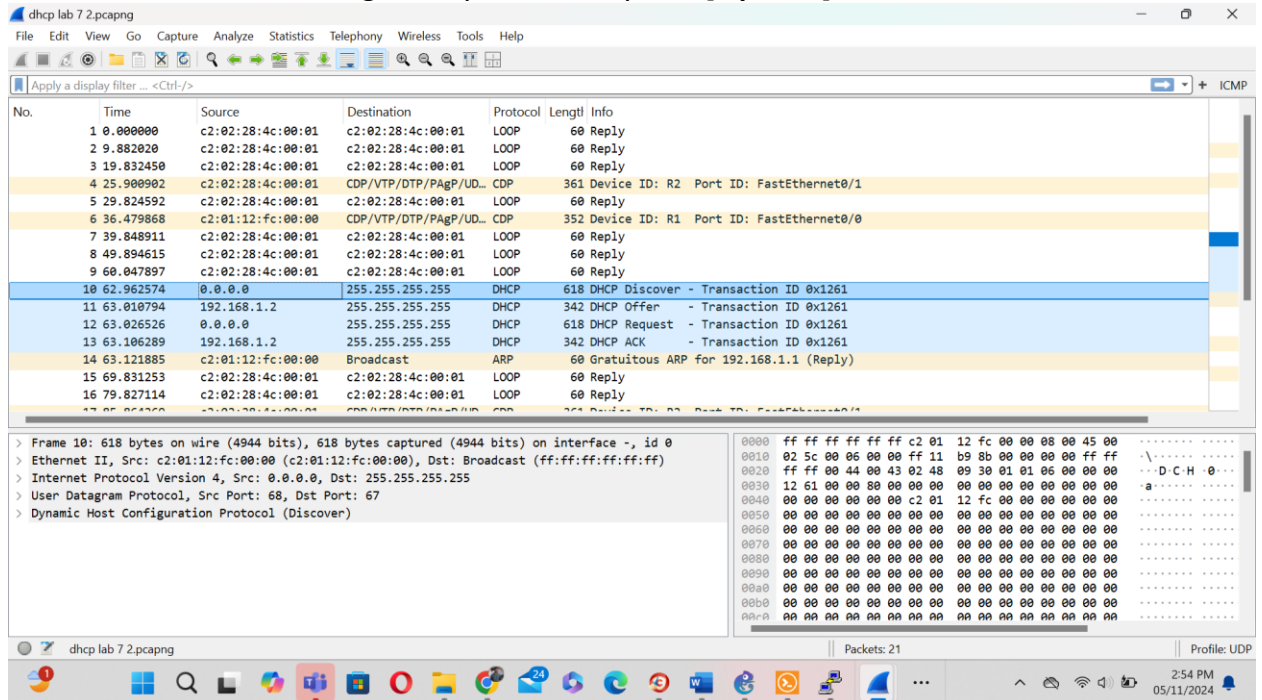
5. Is the configuration on DHCP server and DHCP client same as before? Or did you have to do anything extra in this case? If yes, mention the extra configuration you had to do.

[3 points]

The configuration of DHCP server and DHCP Client is essentially the same as in the basic DHCP setup, the extra setup was to configure DHCP relay to forward DHCP request from R1 to R3. In R2 interface I had configure ip helper-address to forward packets to R3. And configured a static route to R1 in R3 so the packets can be directed to Router-1.

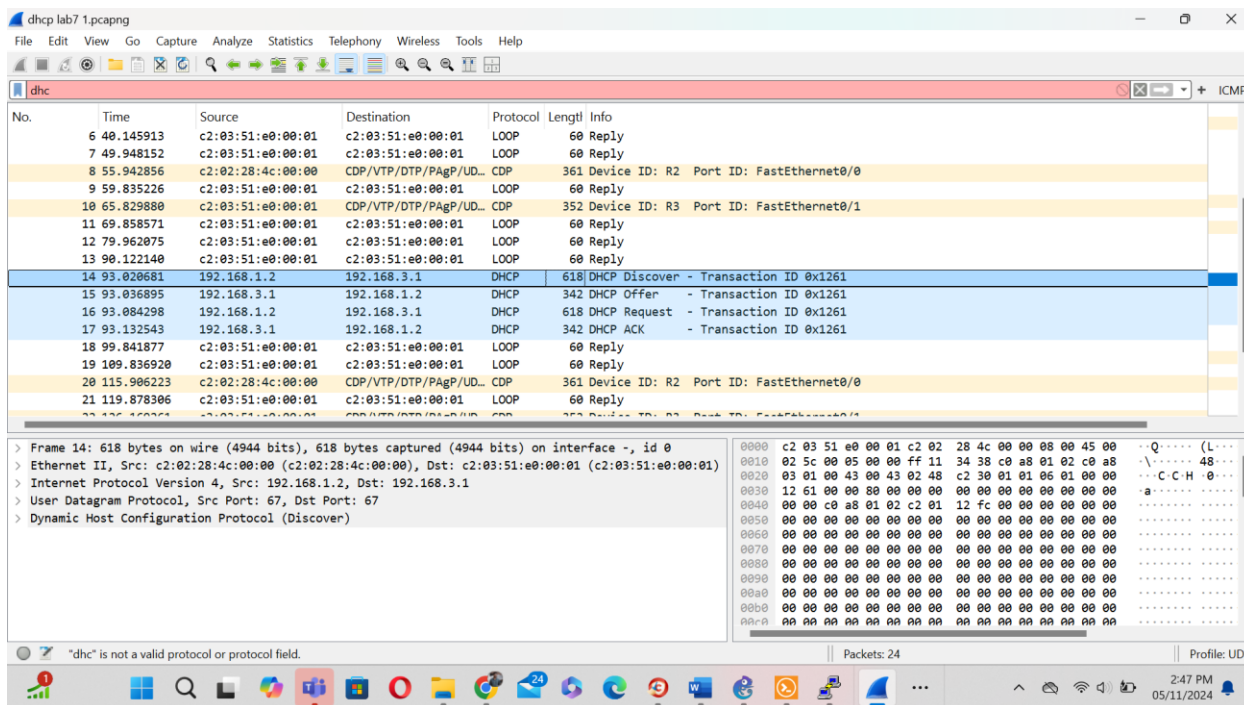
6. After successful DHCP, examine the Wireshark capture.

Mention Source IP, Dest IP, Source MAC and Dest MAC of all 4 DHCP messages for the capture on the Ethernet-1 switch interface. Also note if each individual message is a broadcast or unicast message at Layer-2 and Layer-3. **[5 points]**



	Src IP	Dest IP	Src MAC	Dest MAC	L2	L3
DHCP Discover	0.0.0.0	255.255.255.255	C2:01:12:fc:00:00	ff:ff:ff:ff:ff:ff	broadcast	broadcast
DHCP Offer	192.168.1.2	255.255.255.255	C2:02:28:4c:00:00	ff:ff:ff:ff:ff:ff	broadcast	broadcast
DHCP Request	0.0.0.0	255.255.255.255	C2:01:12:fc:00:00	ff:ff:ff:ff:ff:ff	broadcast	broadcast
DHCP Ack	192.168.1.2	255.255.255.255	C2:02:28:4c:00:00	ff:ff:ff:ff:ff:ff	broadcast	broadcast

7. Mention Source IP, Dest IP, Source MAC and Dest MAC of all 4 DHCP messages for the capture on the Ethernet-2 switch interface. Also note if each individual message is a broadcast or unicast message at Layer-2 and Layer-3. [5 points]



	Src IP	Dest IP	Src MAC	Dest MAC	L2	L3
DHCP Discover	192.168.1.2	192.168.3.1	C2:02:28:4c:00:00	C2:03:51:e0:00:01	Unicast	Unicast
DHCP Offer	192.168.3.1	192.168.1.2	C2:03:51:e0:00:01	C2:02:28:4c:00:00	Unicast	Unicast
DHCP Request	192.168.1.2	192.168.3.1	C2:02:28:4c:00:00	C2:03:51:e0:00:01	Unicast	Unicast
DHCP Ack	192.168.3.1	192.168.1.2	C2:03:51:e0:00:01	C2:02:28:4c:00:00	Unicast	Unicast

Format:

	Src IP	Dest IP	Src MAC	Dest MAC	L2	L3
DHCP Discover	XXXX	YYYY	abcd	efgh	uni/broadcast	uni/broadcast

.....

Score: _____ / 200 points [+20 points]