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:

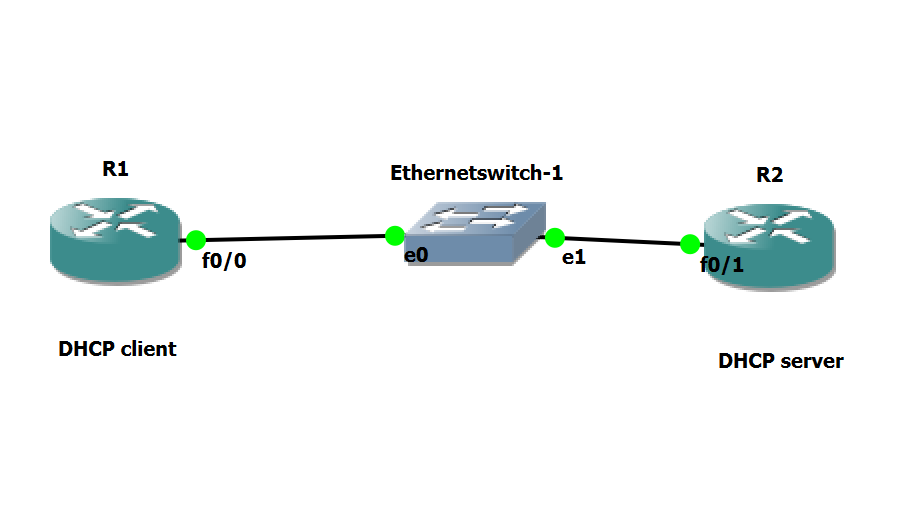


Fig.1

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

A black screen with white text

Description automatically generated

1. 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)

Between the Switch and the DHCP-Client(R1).

1. 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, because DHCP operates at the application layer. The IP address is necessary for DHCP communication, allowing the DHCP server to send and receive DHCP messages.

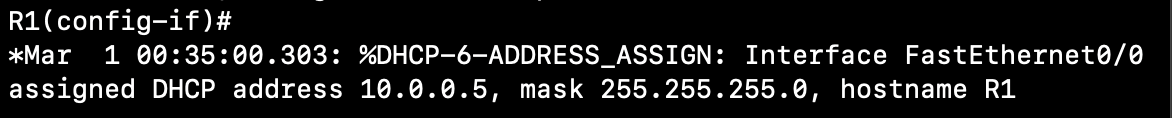
1. Having made sure you started Wireshark capture in Step 3, now configure R2 to be a DHCP server. Paste a screenshot of the configuration you made on R2. **[5 points]**

A computer screen shot of a computer program

Description automatically generated

I can set the default gateway as the router’s IP address and exclude it from the dhcp pool. I did this in the next objective.

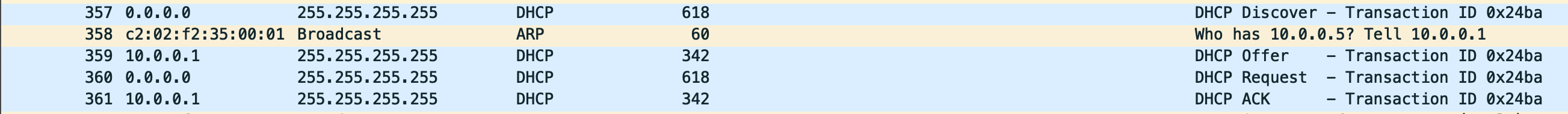
1. Did you get an IP address on R1? Indicate from its CLI that it got a DHCP address. How do you know this? **[2 points]**



A computer screen with white text

Description automatically generated

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

The following DHCP messages are broadcast at Layer 3:

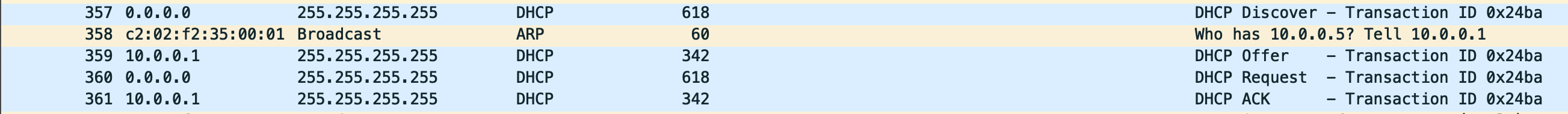
* DHCPDISCOVER
* DHCPOFFER
* DHCPREQUEST
* DHCPACK

The following DHCP messages are broadcast at Layer 2:

* DHCPDISCOVER
* DHCPOFFER

1. 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]**

****

A screenshot of a computer program

Description automatically generated

The ARP between DHCP Discover (client) and DHCP Offer (server) is the server checking whether the IP address is in use before offering.

Objective-2: DHCP server with multiple clients

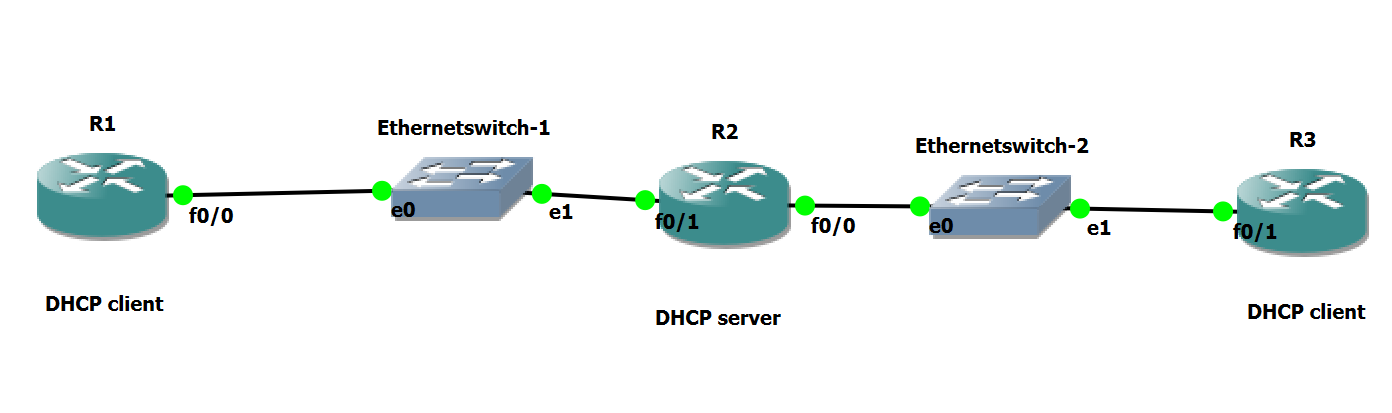


Fig.2

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]**

A computer screen shot of white text

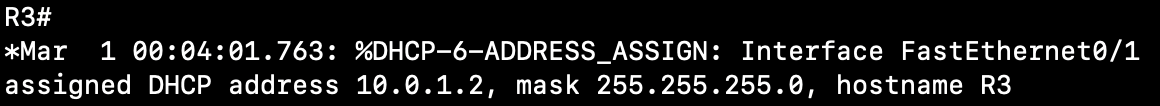
Description automatically generated

Yes, the network design can work, and a single DHCP server (R2) can serve two different DHCP clients (R1 and R3).

Routers separate the broadcast domains. The changes are needed to enable R2 as a DHCP server for multiple subnets. Configuring distinct DHCP pools ensures correct IP allocation.

1. 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]**



A computer screen with white text

Description automatically generated

1. 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]**

* R2 has multiple network interfaces, each connected to a different subnet or network segment.
* Each subnet corresponds to a specific DHCP pool with a range of available IP addresses.
* When R2 receives a DHCP DISCOVER packet, it knows the incoming interface through which the packet arrived.
* The DHCP server (R2) has a configuration that associates each network interface with a specific DHCP pool or subnet.
* R2 uses this association to determine which DHCP pool to use for assigning an IP address.
* The decision is based on the network segment or subnet of the incoming DHCP DISCOVER packet.
* R2 allocates an IP address from the chosen DHCP pool for the client (R1 or R3).

1. 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]**

Excluded DHCP addresses are IP addresses within a DHCP pool range that the DHCP server avoids assigning. They are typically reserved for devices with static IP configurations. In my topology on R2, I excluded 10.0.0.1 and 10.0.1.1, which are the interfaces facing R1 and R3. This prevents the DHCP server from assigning these addresses dynamically, ensuring they are reserved for the routers' interfaces.

1. 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]**

A black background with white text

Description automatically generated

A black background with white text

Description automatically generated

Yes, R1's f0/0 can communicate with R3's f0/1 without additional static routes because both routers are directly connected to R2, which routes the traffic between them by default.

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

**Differences between TCP and UDP:**

**Connection:**

* + **TCP:** Connection-oriented.
  + **UDP:** Connectionless.

**Reliability:**

* + **TCP:** Reliable, ensures data integrity.
  + **UDP:** Unreliable, no guarantees.

**Flow Control:**

* + **TCP:** Implements flow control.
  + **UDP:** No inherent flow control.

**Order of Delivery:**

* + **TCP:** In-order delivery.
  + **UDP:** No guaranteed order.

**Advantages and Disadvantages:**

**TCP:**

**Advantages:**

* Reliable data delivery.
* Error recovery.

**Disadvantages:**

* Higher overhead.
* Slower transmission.

**UDP:**

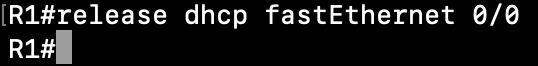
**Advantages:**

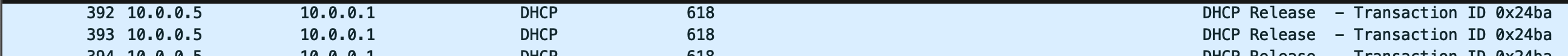
* Faster transmission.
* Lightweight.

**Disadvantages:**

* Unreliable.
* No error recovery.

1. 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]**





1. 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]**

**Clear ip dhcp binding <ip address>**

A computer screen with white text

Description automatically generated

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



1. 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]**

A computer code with white text

Description automatically generated

A computer screen shot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

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]**

A black background with white text

Description automatically generated

A computer screen shot of a black screen

Description automatically generated

A screenshot of a computer

Description automatically generated

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



This command enables the router to perform domain lookups using the configured DNS server.

1. 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]**

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. 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 R3” command. **[10 points]**

Placed the packet analyzer between R1 and Switch1

Ping R3:



Request:

A screenshot of a computer program

Description automatically generated

Response:

A screenshot of a computer

Description automatically generated

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

**Message 1(R1 to R2):**

Router 1(10.0.0.6) sends a DNS query to Router 2(10.0.0.1) for the type `A` record of the domain name `R3`. The query is sent using the User Datagram Protocol (UDP) on port 53.

**Message 2(R2 to R1):**

Router 2(10.0.0.1) resolves the query and returns the IP address of Router 3(10.0.1.4) to Router 1(10.0.0.6). The response is sent using UDP on port 60147(random port).

1. 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 my case, DNS used UDP as the transport layer protocol. This is typical for most DNS queries because UDP is efficient for small responses. However, DNS might switch to TCP in scenarios like large responses that exceed the UDP packet size limit, during zone transfers, or when specific TCP-only queries are involved. So, while UDP is the standard choice for DNS, TCP may be used in certain situations.

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](http://www.google.com)
2. What IP is your laptop using as the DNS server? How do you know this? **[2 points]**

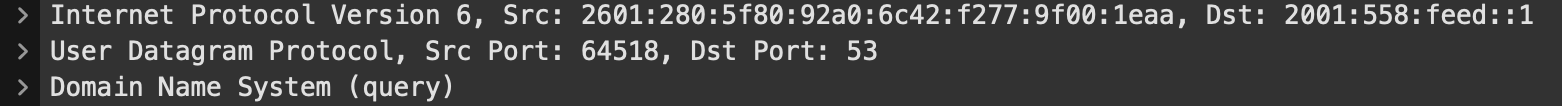
A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

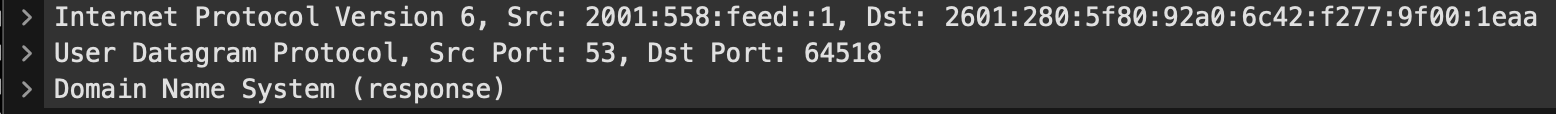
1. For a DNS query, what is the source and destination port numbers? **[2 points]**



Source port: 64518

Destination port: 53

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



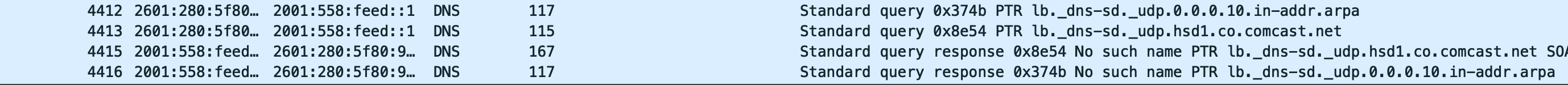
Source port: 53

Destination port: 64518

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

****

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



It used UDP.

1. 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]**
2. The DNS client sends a query to its **recursive resolver**.
3. The **recursive resolver** queries the **root nameservers** for the top-level domain (TLD) of the domain name being resolved.
4. The root nameservers respond with the addresses of the TLD nameservers for the domain name being resolved.
5. The **recursive resolver** queries the **TLD nameservers** for the authoritative nameservers for the domain name being resolved.
6. The TLD nameservers respond with the addresses of the authoritative nameservers for the domain name being resolved.
7. The **recursive resolver** queries the **authoritative nameservers** for the IP address of the domain name being resolved.
8. The authoritative nameservers respond with the IP address of the domain name being resolved.
9. The recursive resolver caches the obtained information for a specified time and returns the IP address to the DNS client.
10. Explain briefly the different type of DNS records. **[5 points]**
    * **A Record:** Maps a domain to an IPv4 address.
    * **AAAA Record:** Maps a domain to an IPv6 address.
    * **CNAME Record:** Creates an alias for a domain.
    * **MX Record:** Specifies mail servers for a domain.
    * **PTR Record:** Used for reverse DNS lookups.
    * **TXT Record:** Holds arbitrary text information.
    * **NS Record:** Specifies authoritative DNS servers.
    * **SOA Record:** Contains domain and zone information.
    * **SRV Record:** Specifies information about available services.
    * **CAA Record:** Specifies authorized certificate authorities.
11. 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]**

**Types of DNS nameservers:**

* Root nameservers
* Top-level domain (TLD) nameservers
* Authoritative nameservers
* Recursive resolvers
* Caching Nameservers

Yes, I can configure my laptop to be a DNS server. It can be either a recursive nameserver or an authoritative nameserver.

**Authoritative Nameserver:**

* If I host a domain on my laptop and configure it to store authoritative DNS records for that domain, my laptop becomes an authoritative nameserver for that specific domain.

**Recursive Nameserver:**

* If my laptop performs the entire DNS resolution process on behalf of the clients, providing the final resolved IP address, it acts as a recursive nameserver.

1. Explain briefly the HTTP Error Messages with their status code. **[2 points]**
2. **200 OK:** Successful request.
3. **400 Bad Request:** Client error, malformed request.
4. **401 Unauthorized:** Lack of valid authentication.
5. **403 Forbidden:** Server refuses to authorize.
6. **404 Not Found:** Requested resource not found.
7. **500 Internal Server Error:** Unexpected server condition.
8. Explain briefly the different types of HTTP requests. **[2 points]**
9. **GET:** Retrieve data from a resource.
10. **POST:** Submit data to be processed.
11. **PUT:** Update or create a resource.
12. **DELETE:** Delete a specified resource.
13. **PATCH:** Apply partial modifications to a resource.
14. **HEAD:** Retrieve only headers, not data.
15. **CONNECT:** Establish a tunnel to a specified server.
16. What is a proxy web server? Mention any four advantages of using a proxy webserver.

**[3 points]**

A proxy web server acts as an intermediary between a user's device and the internet. It forwards requests from users to websites and returns the requested information back to the users.

**Advantages:**

* **Privacy and Anonymity:** Masks user IP addresses for increased privacy.
* **Content Filtering:** Blocks or filters specific websites or content categories.
* **Bandwidth Savings:** Caches frequently requested content, reducing the need for repeated downloads.
* **Security:** Acts as a barrier against malicious content and provides access control measures.

1. You are trying to connect to [www.bbc.com](http://www.bbc.com) but the page does not load and keeps buffering. So now you try to connect to [www.cnn.com](http://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]**

**REASONS:**

* **Server Issues:**The BBC server may be experiencing high traffic, maintenance, or technical difficulties.
* **Geographical Content Delivery:**BBC and CNN may use different servers for content delivery, and your location might be closer to servers used by CNN.
* **DNS Issues:** Domain Name System (DNS) resolution issues might be affecting the connection to www.bbc.com.
* **Browser Compatibility with Website Technology:** Website www.bbc.com may use certain technologies or features that are not fully compatible with the browser you are using.

**TROUBLESHOOTING:**

**Geographical Content Delivery:**

* + Use a VPN to change location and retry.

**DNS Issues:**

* + Change DNS server (e.g., Google DNS).
  + Flush DNS cache on your computer.

**Browser Compatibility:**

* + Try a different browser.
  + Ensure your browser is updated.

**Server Issues:**

* + Check other websites.
  + Try accessing later.

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

A major disadvantage of using HTTP is the lack of encryption, exposing data to security threats. **HTTPS** addresses this issue by securing the communication between clients and servers, ensuring data confidentiality and integrity.

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

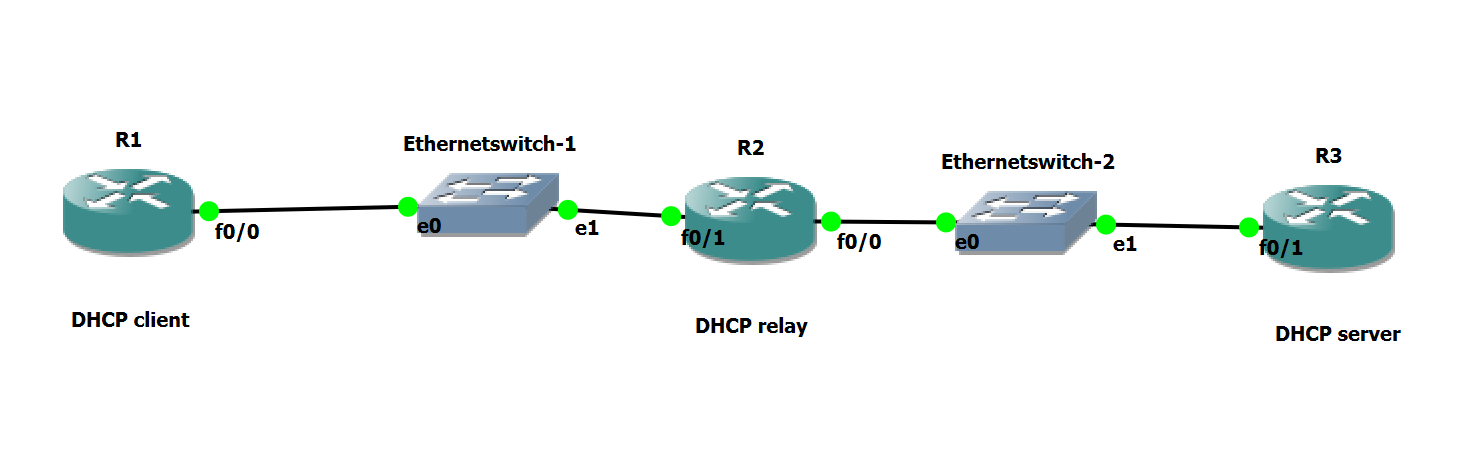


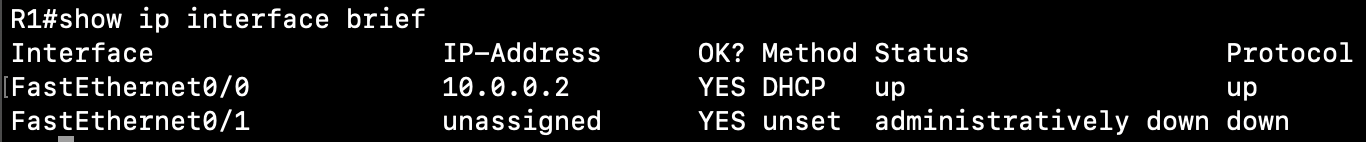
Fig.3

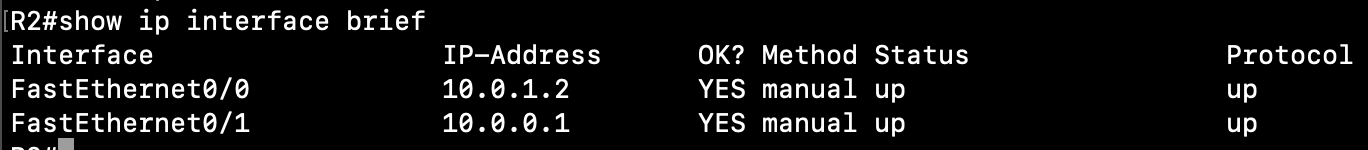
1. What is a DHCP relay? When would you use one? **[2 points]**

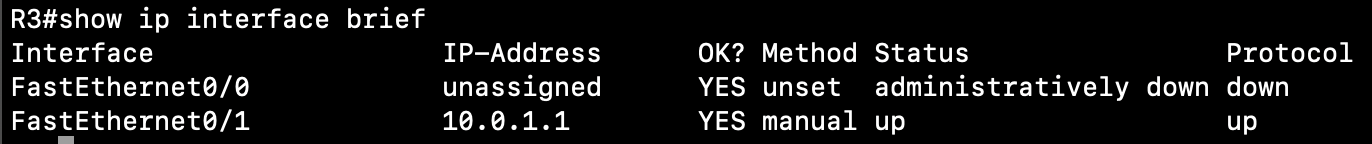
A DHCP relay (Dynamic Host Configuration Protocol relay) forwards DHCP messages between clients and servers across different subnets, facilitating centralized DHCP management in networks with multiple subnets. It's used when DHCP clients in one subnet need to obtain IP addresses from a DHCP server in another subnet, optimizing IP address assignment in complex network setups.

1. 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.
2. 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.
3. 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]**







A computer screen shot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

1. 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]**

* Enable DHCP relay on Router 2 with IP helper-address on the interface connected to DHCP clients.
* Set IP addresses on Router 2's interfaces connected to R1 and R3, and on Router 3's interface.
* Ensure Router 3 has a default gateway pointing to Router 2.

1. 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]**

DHCP Discover 0.0.0.0 255.255.255.255 c2:01:0b:a0:00:00 ff:ff:ff:ff:ff:ff Broad Broad

DHCP Offer 10.0.0.1 255.255.255.255 c2:01:0b:a7:00:01 ff:ff:ff:ff:ff:ff Broad Broad

DHCP Request 0.0.0.0 255.255.255.255 c2:01:0b:a0:00:00 ff:ff:ff:ff:ff:ff Broad Broad

DHCP Ack 10.0.0.1 255.255.255.255 c2:01:0b:a7:00:01 ff:ff:ff:ff:ff:ff Broad Broad

1. 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]**

DHCP Discover 10.0.0.1 10.0.1.1 c2:02:0b:a7:00:00 c2:03:0b:a9:00:01 uni uni

DHCP Offer 10.0.1.1 10.0.0.1 c2:03:0b:a9:00:01 c2:02:0b:a7:00:00 uni uni

DHCP Request. 10.0.0.1 10.0.1.1 c2:02:0b:a7:00:00 c2:03:0b:a9:00:01 uni uni

DHCP Ack 10.0.1.1 10.0.0.1 c2:03:0b:a9:00:01 c2:02:0b:a7:00:00 uni uni

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]