SIT202: Computer Networks and Communication
Leaning Evidence for Active Class Task 10

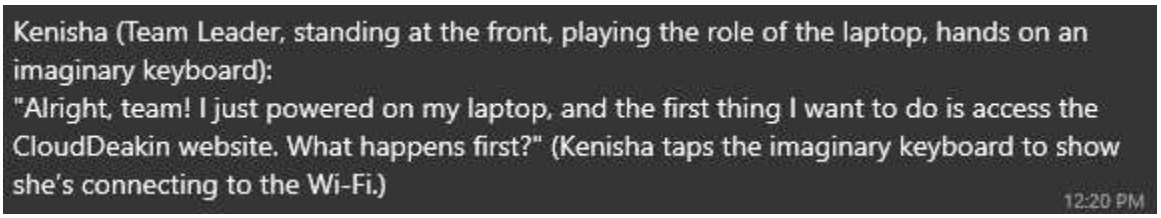
Name: Kenisha Corera
Student ID: C23020001

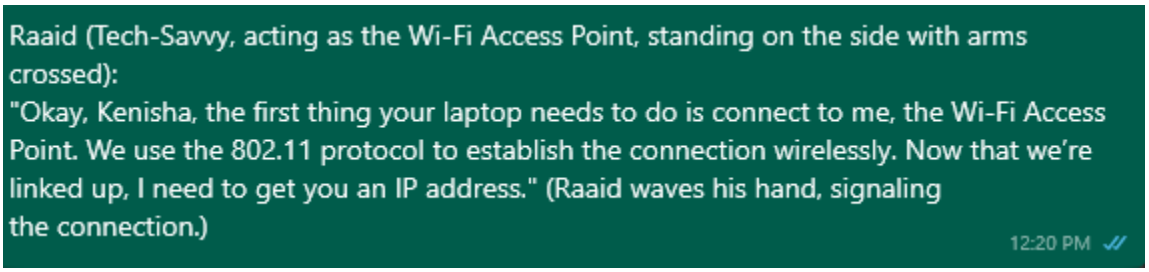
Members in this group activity task:

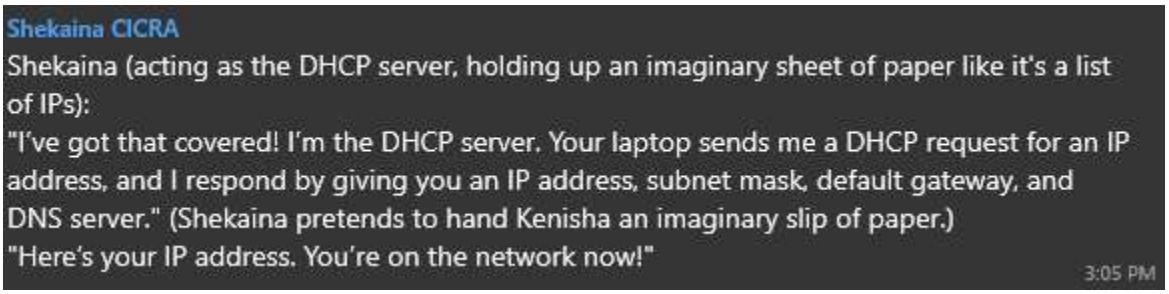
Nishad – C23110001
Kenisha – C23020001
Shekaina – C23110002
Raaid – C23020004
Pavithran – C22060015

Activity 1

1. Outline the major steps used by your laptop after it is first powered on until it downloads the page from CloudDeakin.
2. For each of the major steps you have outlined, identify the network protocols that are used and explain what functionality they provide in achieving the task.
3. Explain what would change in your answer to the above questions if your home network uses NAT.







Kenisha CICRA
Kenisha (still playing the laptop, holding the "IP address"):
"Thanks! Now I need to connect to the CloudDeakin website. I'll need the IP address of the server for 'd2l.deakin.edu.au'. Who's got that?" (Kenisha looks around.)
3:49 PM

Pavithran AIR
Pavithran (acting as the DNS server, waving like he's waiting for his turn):
"Over here! I'm the DNS server. You ask me for the IP address of 'd2l.deakin.edu.au'." (Pretending to search a database, Pavithran then points at Kenisha.)
"I found it! The IP address is 192.168.1.100. Now you can connect!"
3:55 PM

Kenisha CICRA
Kenisha (receiving the "IP address" from Pavithran):
"Awesome, got it! Now I need to establish a connection with the CloudDeakin server. Time for TCP to come into play. Nishad, I'm sending a SYN packet to you!" (Kenisha mimics sending a data packet.)
4:14 PM

Nishad
Nishad (acting as the CloudDeakin server, giving a nod and holding out his hand to catch the 'SYN' packet):
"I got your SYN! Here's my SYN-ACK response!" (Nishad tosses an imaginary packet back to Kenisha.)
5:24 PM

Kenisha CICRA
Kenisha (pretending to catch the packet, and quickly responding):
"And here's my ACK! Now we have a reliable connection, Nishad." (Kenisha does a small celebratory move.)
"Now, Nishad, I'm requesting the web page from you using HTTPS."
5:32 PM

Nishad
Nishad (as the server, crossing his arms, standing confidently):
"I'm on it! Since you're using HTTPS, I'll make sure everything's secure and encrypted." (Pretending to hold up a secured lock.)
"Here's the web page data—encrypted, of course." (Tosses the 'data packets' back to Kenisha.)
5:33 PM

Kenisha CICRA
Kenisha (pretending to receive the data packets and act like the page loads on her "laptop" screen):
"And boom! The SIT202 CloudDeakin page is loaded. Looks good, right?" (Gestures to the others as if showing the web page on a laptop.)
5:33 PM

Raaid (raising a hand, excited):
"Hold on, Kenisha. What if your home network was using NAT? What would change?" (Smirking, challenging the situation.)
3:03 AM ✓✓

Pavithran CICRA

Pavithran (stepping forward, acting as the home router with NAT):
"Good question! If I, the home router, am using NAT, then instead of your private IP address being sent to Nishad, I'd replace it with my own public IP address before forwarding the request." (He points at Nishad, indicating how he's hiding Kenisha's real IP address.)
"When Nishad replies, I swap my public IP back for your private IP and pass it back to you. This way, all devices in the home network share my single public IP address."

8:07 PM

Shekaina CICRA

Shekaina (nodding along, stepping up to Kenisha, pretending to look over the "laptop screen"):
"So, Nishad only sees the public IP address, not Kenisha's actual private one. And the NAT does all this behind the scenes. Pretty cool!"

8:31 PM

Nishad CICRA

Nishad (crossing his arms, confidently):
"Yeah, and from my perspective as the server, I have no idea how many devices are using that public IP. It's like talking to one person, but there are actually many behind the scenes."

8:56 PM

Kenisha CICRA

Kenisha (nodding, arms crossed, addressing everyone):
"Exactly! NAT allows us to have multiple devices on a network, all using one public IP address. It's an efficient way of managing connections. So, with NAT or without, we can still access the CloudDeakin page. Mission accomplished, team!" (She smiles at the group.)

8:56 PM

Pavithran CICRA

Pavithran (with a smile, giving a thumbs up):
"Great teamwork! We just walked through the entire process of accessing a web page, covering all the major protocols—802.11, DHCP, DNS, TCP, HTTPS, and NAT."

8:56 PM

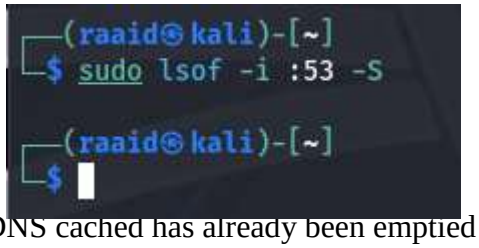
Kenisha CICRA

Kenisha (wrapping up, hands on hips):
"Fantastic job, everyone! I think we've got this networking thing down!" (Everyone cheers or gives high-fives.)

8:56 PM

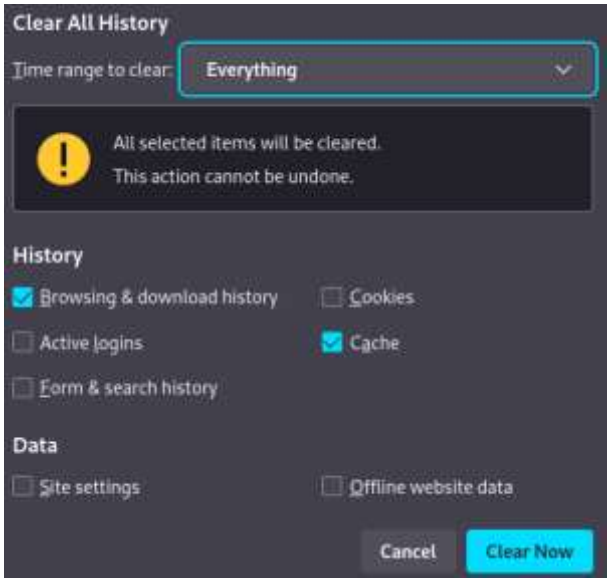
Activity 2

1. Use ipconfig in your command prompt/ terminal to empty the DNS cache in your host using ipconfig /flushdns. (MacOS Mojave use: sudo killall -HUP mDNSResponder)



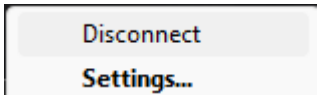
DNS cached has already been emptied

2. Open Google Chrome and empty your browser cache



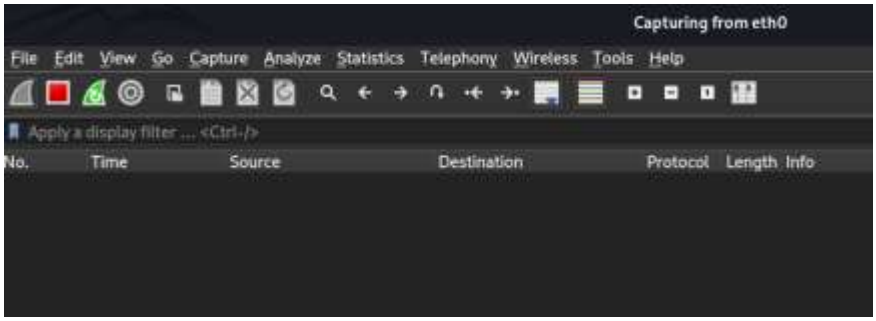
Browser cache has been cleared

3. Turn off your network connection (turn your WiFi off or disconnect your ethernet cable)

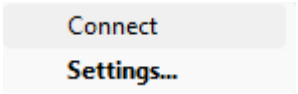


Switching off network connection in my Virtual Machine

4. Open Wireshark and start packet capture (remember to select your typical network interface). You will see an empty window.

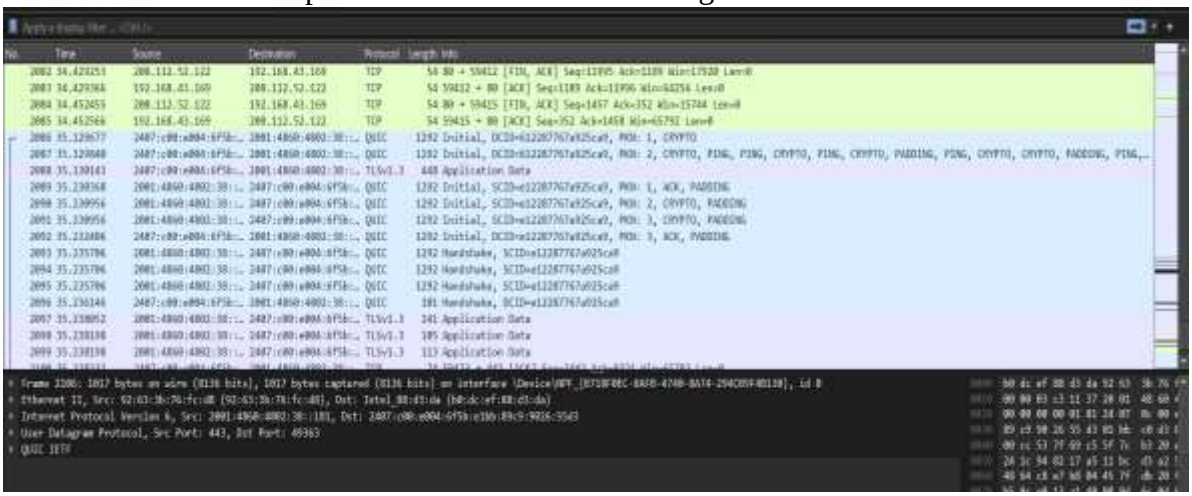


5. Turn on your network connection again.



6. Open your browser, visit the web page: http://www.discoverourtown.com and stop packet capture.

7. Now, you can start analyzing the packet capture.
    a) List down the order of protocols used and their messages.



1. QUIC (Quick UDP Internet Connections)

    - QUIC Client Hello: Client Hello, which is a message containing the client cipher and supported protocol versions by the client to the server is created to ensure a secure connection.
    - QUIC ACK: In order to confirm acknowledgement regarding received packets, both the client and server send ACK. Since it runs on UDP, it has its mechanism of ensuring data delivery in the connection to avoid instances where data is delivered unsuccessfully.
    - QUIC Data Packets: After the handshake, packets in the QUIC protocol are employed by both the client and the server to transfer encrypted data items such as requests and response to webpage.

2. TCP (Transmission Control Protocol)

    - SYN (Synchronize): The client initiates a connection by sending the server a message called SYN for connection.
    - SYN-ACK (Synchronize-Acknowledge): The request is accepted by the server; in reply the server sends a packet with SYN and ACK flags set.
    - ACK (Acknowledge): When the three way handshakes are over and the TCP connection has been established the client sends an ACK message back.
    - TCP Data Packets: Data residing at the client and server side are transmitted in the form of TCP segments after the connection has been made using the HTTP protocol.

3. TLSv1.3 (Transport Layer Security)

    - TLS Client Hello: Once the QUIC or TCP connection is successfully established then the client raises its hand by sending a Client Hello message that contains encryption preference and other session related information.
    - TLS Handshake: Both the client and the server share the encryption keys and decide upon secure sessions parameters.
    - TLS Encrypted Data: Once the handshake is done, any data is exchanged over the TCP or QUIC connection are encrypted by TLS to ensure the security of the data as it transmitted.

b) Explain the use of each protocol indicating the layer that they belong to.

1. QUIC (Quick UDP Internet Connections):

    - Purpose: QUIC may help clients and servers convey quicker and more safely. It ensures a minimal level of delays are acceptable while ensuring data encryption for security is upheld.
    - Layer: Unlike other protocols it adopts the UDP as the lower transport layer but works in the Fourth layer of the OSI model like TCP.

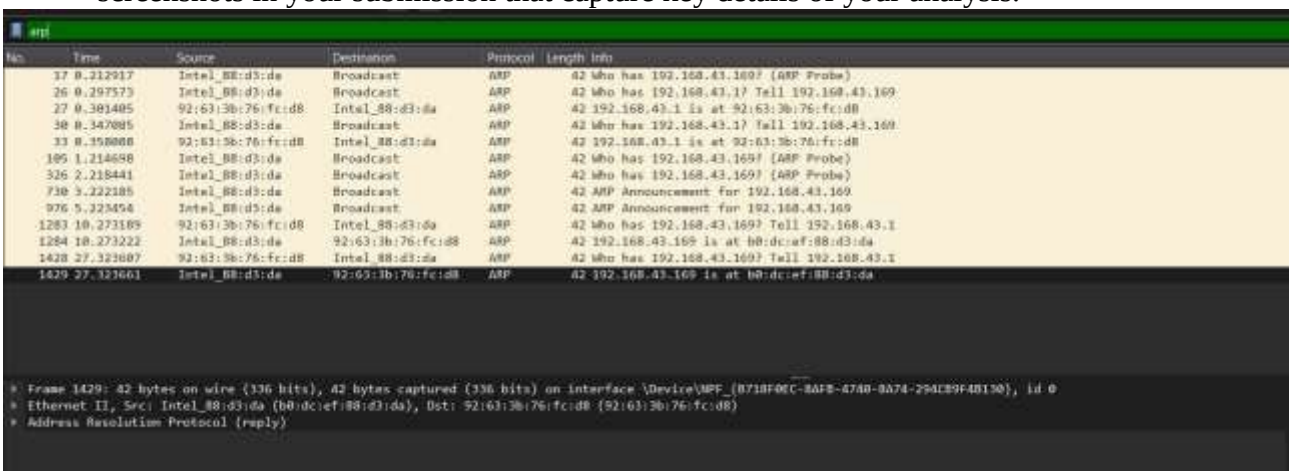
2. TCP (Transmission Control Protocol):

    - Purpose: By featuring control of data flow, error checking and retransmissions, TCP guarantees accurate message transmission by providing devices with reliable and timely information transfer.
    - Layer: WANs provide reliable data transmission at layer four also known as the Transport layer.

3. TLSv1.3 (Transport Layer Security):

    - Purpose: TLS encrypts data flow between clients and servers to ensure direct and indirect communications are secure and private.
    - Layer: HTTP, when used with TCP or QUIC, TLS runs at The Application Layer (Layer 7).

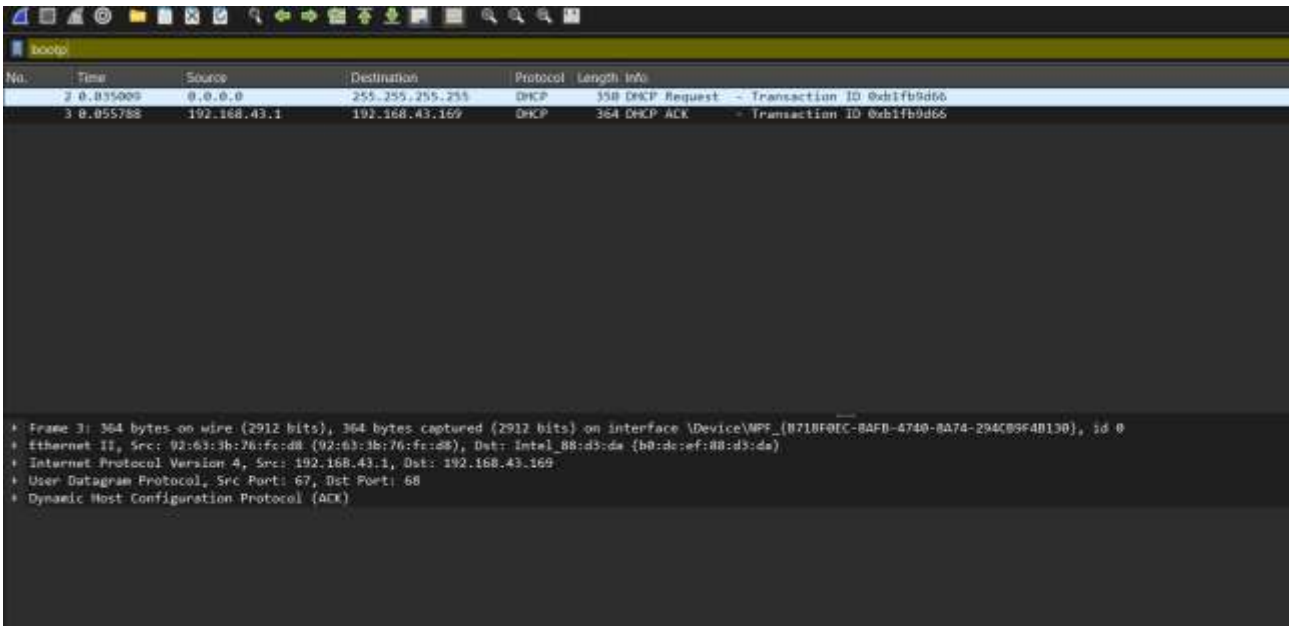
c) Check the details of each packet such as ARP, DHCP, DNS, and HTTP. Make sure you include screenshots in your submission that capture key details of your analysis.



The packet is an ARP Probe (or ARP Request) where the device with MAC address Intel_88:d3:da is asking the local network which device has the IP address 192.168.43.169.

- Address Resolution: Telecommunicating with an IP address of 192.168.43.169 means converting the IP address ad MAC address in the devices.
- Broadcast Request: This request is transmitted to all devices on the sending device network since the Address Resolution Protocol is unknown to the MAC address.

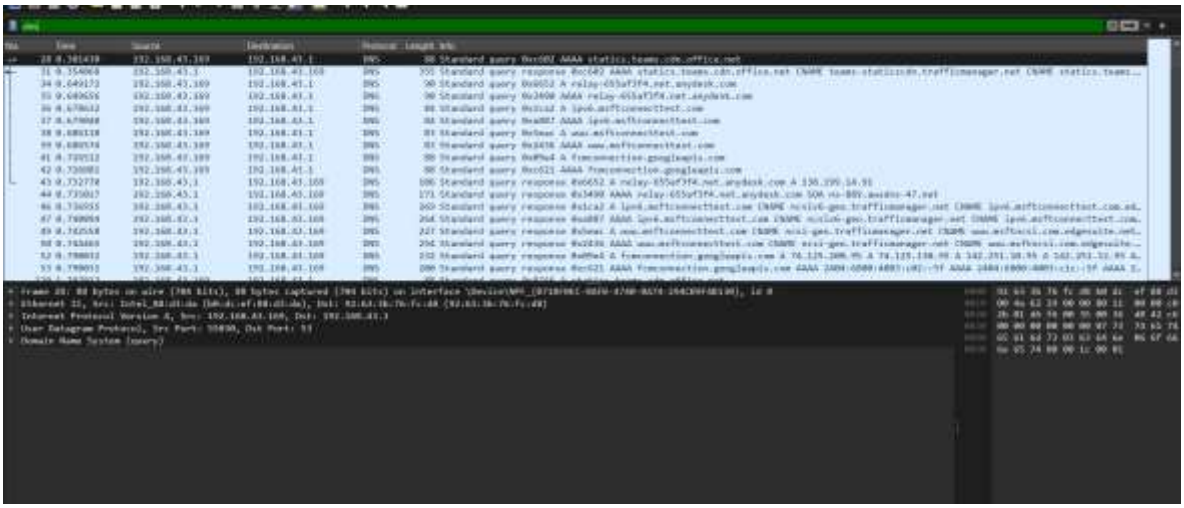
The device that controls IP address 192.168.43.169 will respond to this ARP Probe with MAC address. This is a network level query in a way to search for the MAC address equivalent to the given IP address.



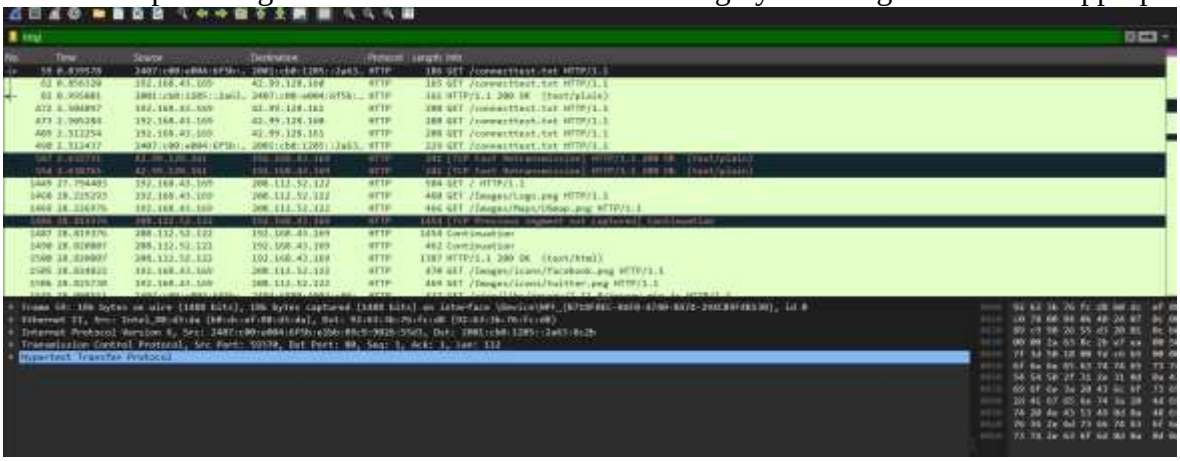
- This DHCP packet shows the result of a DHCP Request message that a client sends to ask for an IP address.

- Client Initialization: Right now, the client is attempting to get an IP address by connecting to a DHCP server mostly. The client does not possess an IP address yet, and thus the client broadcast for an IP address using the broadcast address of 255.255.255.255 so as to reach any and all DHCP servers.
- Transaction ID: 0xb1fb9d66 is used to keep track of the particular request in relation to the server's matching DHCP Offer or ACK.

This packet is a broadcast DHCP Request indicating that a client is trying to obtain an IP address configuration from any available DHCP server on the local network.



The DNS response is effectively redirecting requests from activity.windows.com to activity-consumer.trafficmanager.net and providing authoritative information about the DNS zone. This redirection helps manage domain names and load balancing by directing traffic to the appropriate servers.



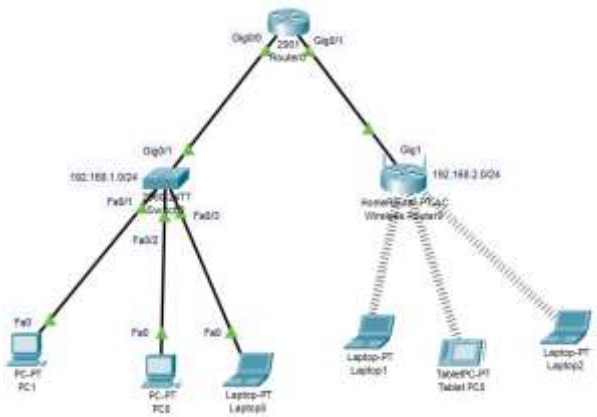
The packet with [TCP Fast Retransmission] indicates that a previously sent HTTP response (with a 200 OK status) was retransmitted due to a network issue or packet loss. The content of this packet is text/plain, which means it's a simple text file or response.

8. Compare the results of your analysis in the above step (7) with the findings of Activity 1.

- In the present activity, readers come to understand the function of networking protocols in the communication process as offered by activity 1 and 2. Activity 1 involves an interactive simulation of server, QUIC, TCP and TLS along with other components including Laptops, Wi-Fi Access Points, and NAT. The second activity is an extensive Packet Capture Analysis which is based purely on TCP, QUIC and TLS and displays how these protocols are relevant in the specific cases of website browsing.
- In brief, Activity 1 gives a general exposure of the networking paradigm, as in Activity 2, more details are added with regards to the packet level; therefore, both activities help enrich the knowledge on networking paradigms and their functionalities. Understanding of how these protocols work is facilitated by Activity 1, and Activity 2 provides a technical perspective of their objectives and levels of operation.

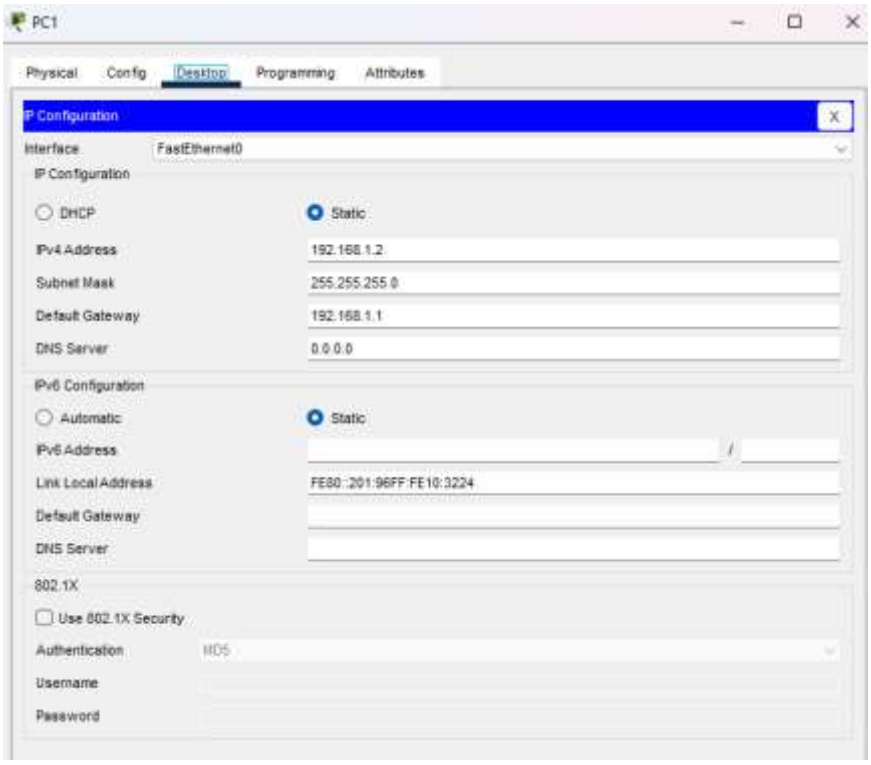
Activity 3

In this activity, you explore more on wired and wireless LANs. Implement the above network in Cisco Packet Tracer. You need to use static IP configuration to configure hosts and router interfaces. Make sure to take screenshots of your findings as you need to include the evidence in the task submissions

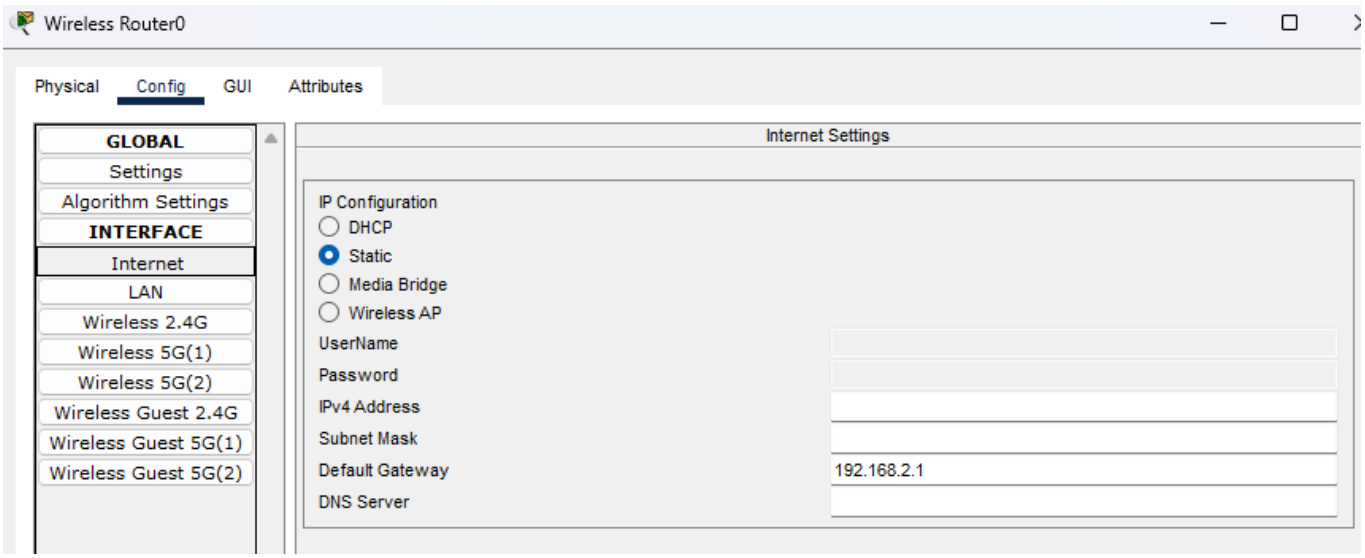


Implemented Network Architecture

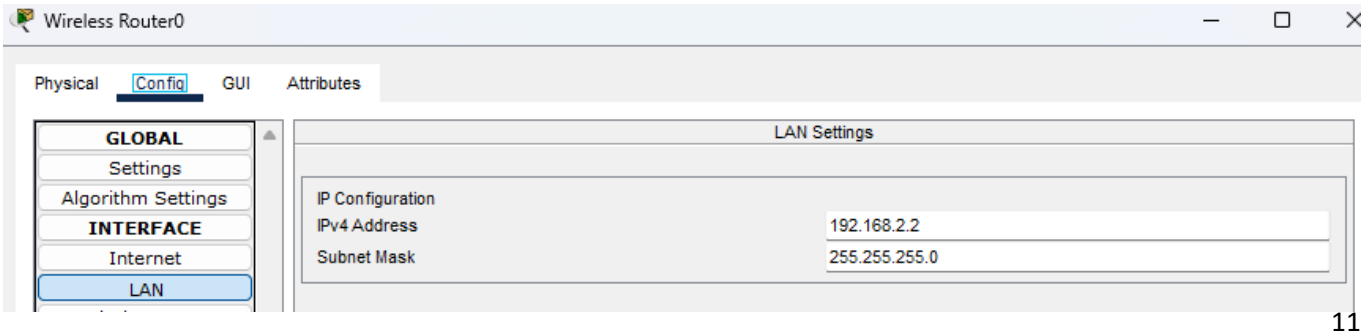
```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Router#exit
```

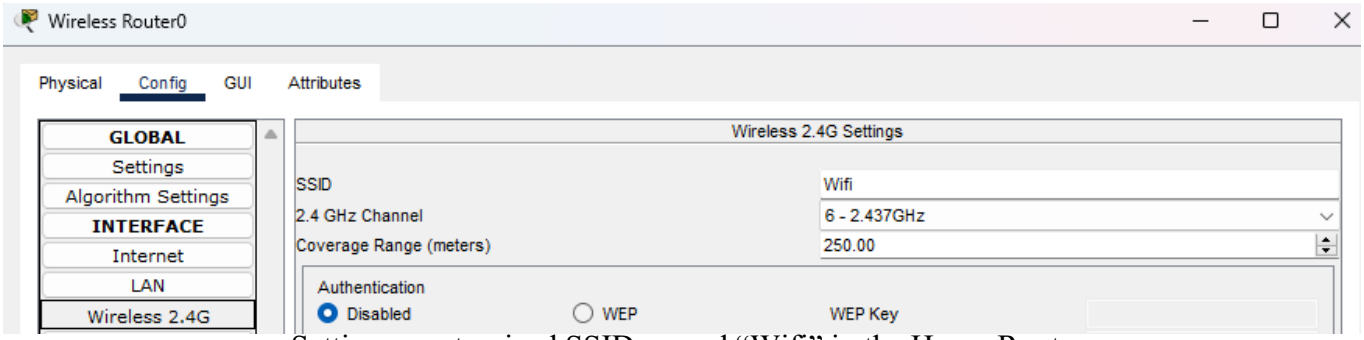


Setting up static connections with all end devices in both subnets as seen now in PC1

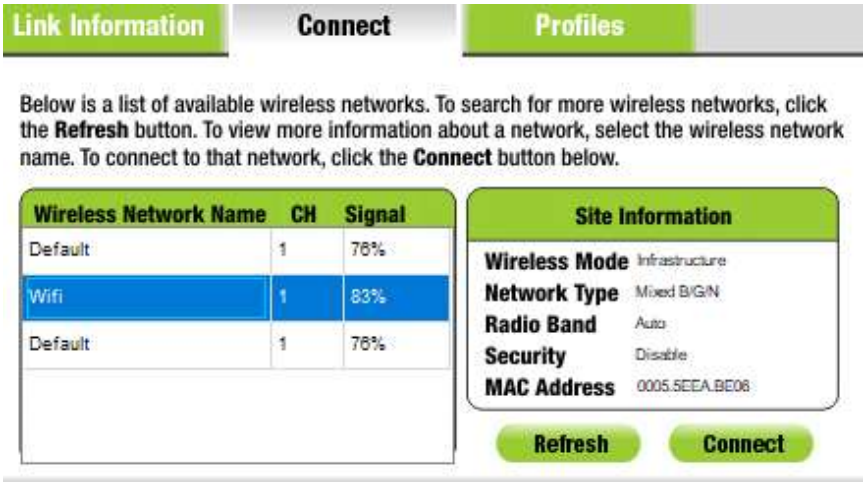


Configuring the Default Gateway for the Home Router



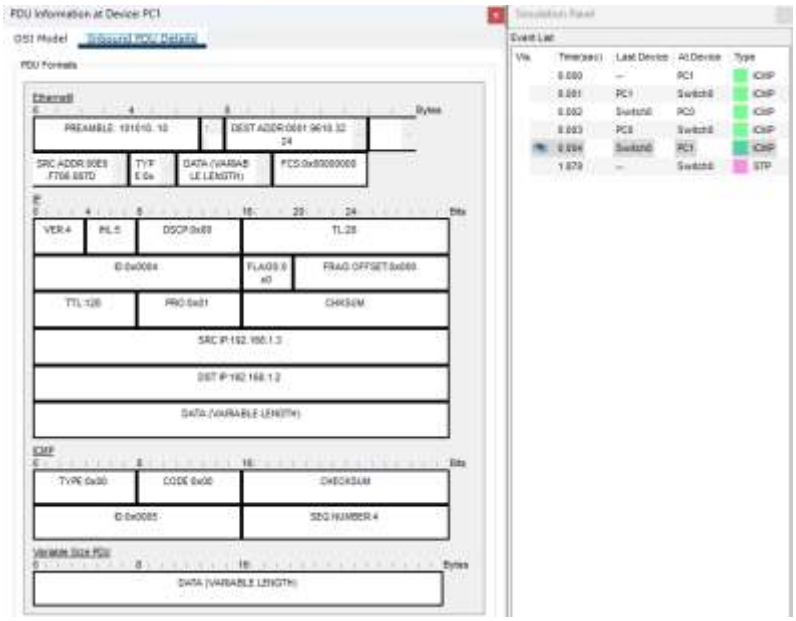


Setting a customized SSID named “Wifi” in the Home Router

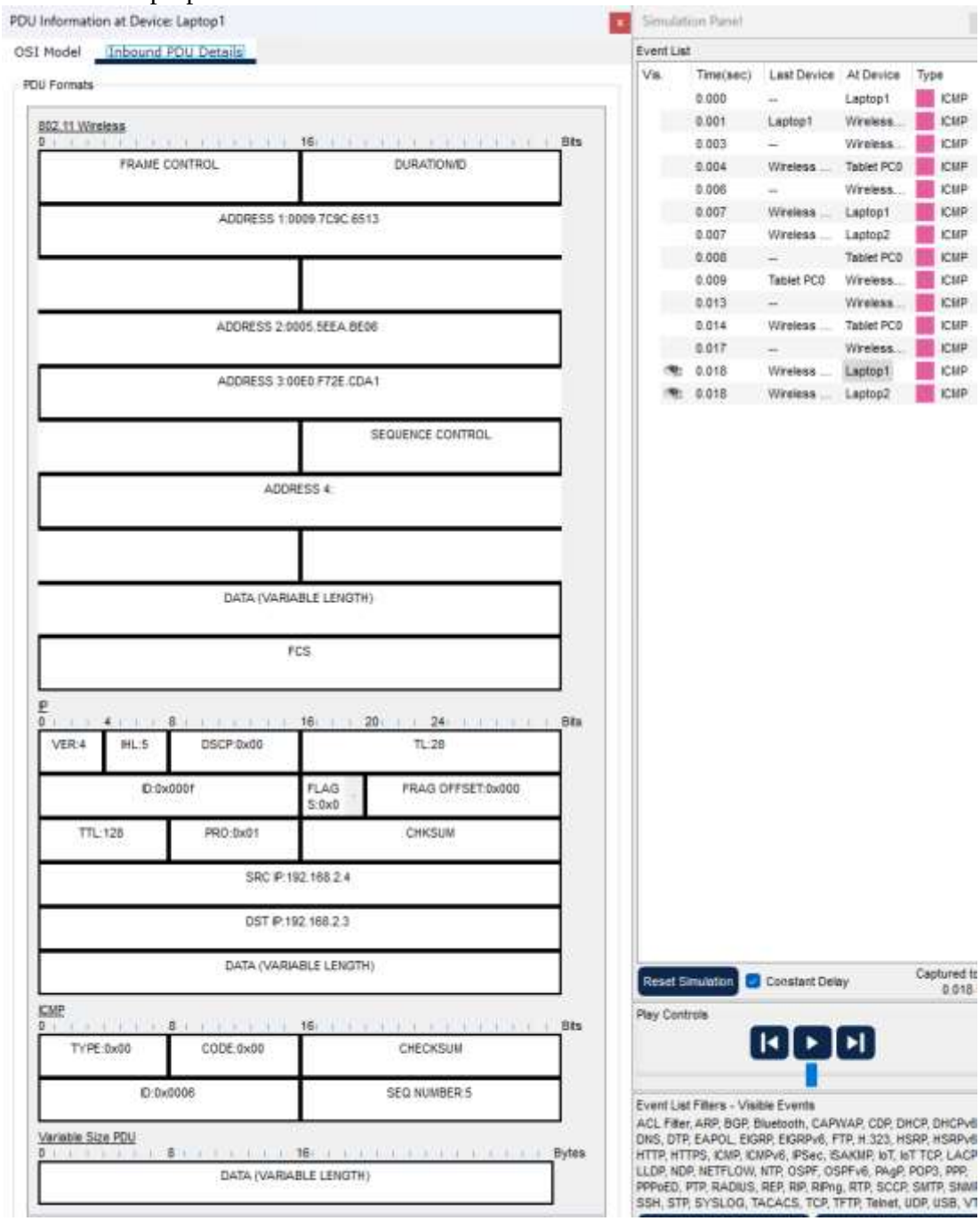


Going to each laptop to connect to the wireless Home Router with the specified SSID

1. Use the simulation mode and send a simple PDU,
    a. From PC1 to PC0



b. From Laptop 1 to Tablet 0



2. Note down the similarities and differences you observed in these to images. You may check the details of PDUs in each device. Explain the reasons behind the differences you observed.

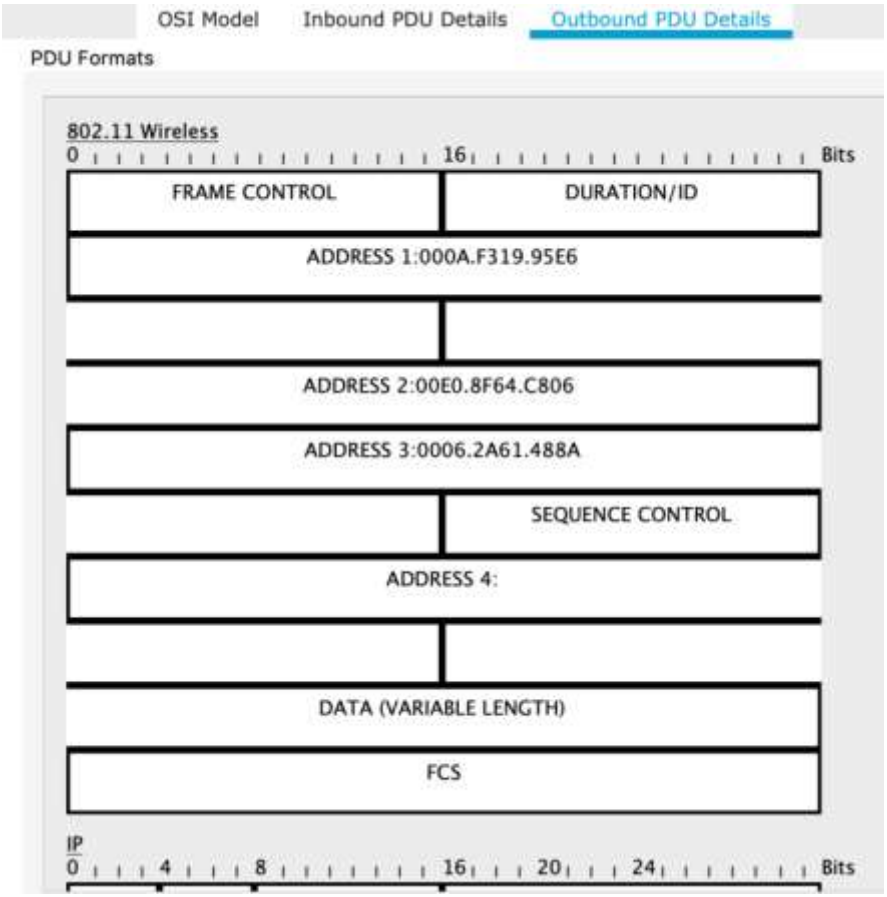
Similarities

- Both of the PDUs use portions of the IP Header by sharing the IPv4 version, header length, and DSCP, TL, and TTL parameters. This is set to 0x01 pointing to the fact that ICMP was used while the ICMP Header uses type 0x00 to show that an ICMP Echo Reply was responded to. In both scenarios there is a checksum present.

Differences

- Since the Data Link layer header of the PDU in Laptop1 has the word "802.11" Frame, which is Wireless Frame and has many address fields meaning there are various layers of addressing in the wireless setup, that means the mode of communication between Laptop1 and Tablet0 is wireless in the Data Link Layer (Layer 2). The communication link between PC1 and PC0 is via wire connection namely Ethernet.

3. Check the details of PDUs in both wired and wireless LANs. The PDUs of wired LAN, you can find source and destination MAC addresses. However, there are three MAC addresses listed in the PDUs of Wireless LAN as shown below.



4. Explain why there are three MAC addresses listed in 802.11 Wireless PDUs?

    - There are three MAC address in in this wireless PDU where;
        - Address 1 is the Destination Address – this is the MAC address of the final destination device.
        - Address 2 is the Source Address – this is the MAC address of the original sender of the packet.
        - The third MAC Address is the Basic Service Set Identifier which is the MAC address of the access point through which the wireless communication is routed.

There is a need to keep abreast three MAC addresses due to the following reasons; While on aspects of wireless network developments, the devices do not actually directly communicate; rather all broadcast communication are relayed through an AP. This leads to a multi hop scenario where a frame need to be routed from a source device to a AP and then to a target device.

Above and Beyond Tasks

There are two types of Ethernet cables used in computer network, i.e., straight through and crossover cables. Explain,

- What is a straight through Ethernet cable? When do we need to use a straight through Ethernet cable?
    - These include the straight through cables which are types of twisted pair cables used in local area network to connect devices like PCs with switches and routers with switches.

- What is a crossover Ethernet cable? When do we need to use a crossover Ethernet cable?
    - PC to PC, switch to switch or even a router to router can be directly connected to each other through a crossover connection.
- How do you identify the type of an Ethernet cable?
    - By the cable color Eth has distinguished between T568A and T568B wiring schedule. A cross over cable is one that implements both wiring patterns while a straight through is one that only implements one.