Task – 10.1 P Physical layer :

- **Evidence:**
- **Exercises:**
- **Activities week 10:**
- **Activity 1: Behind the scenes process of a web page request**

Major steps and Network protocols:

1. Power on and connect to wifi --

Turning on the laptop and connecting to the home Wi-Fi network.

Protocols used: IEEE 802.11—Used for wireless networking (wi-fi) to establish a connection between the laptop and the wireless router.

DHCP(Dynamic host configuration protocol) – It assigns an IP address to laptop from the router.

2.DNS Resolution:

Laptop resolves the domain name d2l.deakin.edu.au to an IP address.

Protocol used: DNS(Domain name system)—It translates domain name to an IP address.

3.Establishing a TCP Connection:

The laptop establishes a TCP connection with the CloudDeakin server.

Protocol: TCP(Transmission control protocol) -- Provides reliable, ordered, and error-checked delivery of data between the laptop and the server.

4.HTTP request and response: The laptop sends an HTTP request to the CloudDeakin server and receives an HTTP response.

Protocol: HTTP(Hypertext transfer protocol) -- Used for transmitting web pages over the internet.

5.Downloading the web page : Laptop downloads the web page content from the CloudDeakin server.

Protocol used: TCP/IP - Ensures the data packets are transmitted reliably.

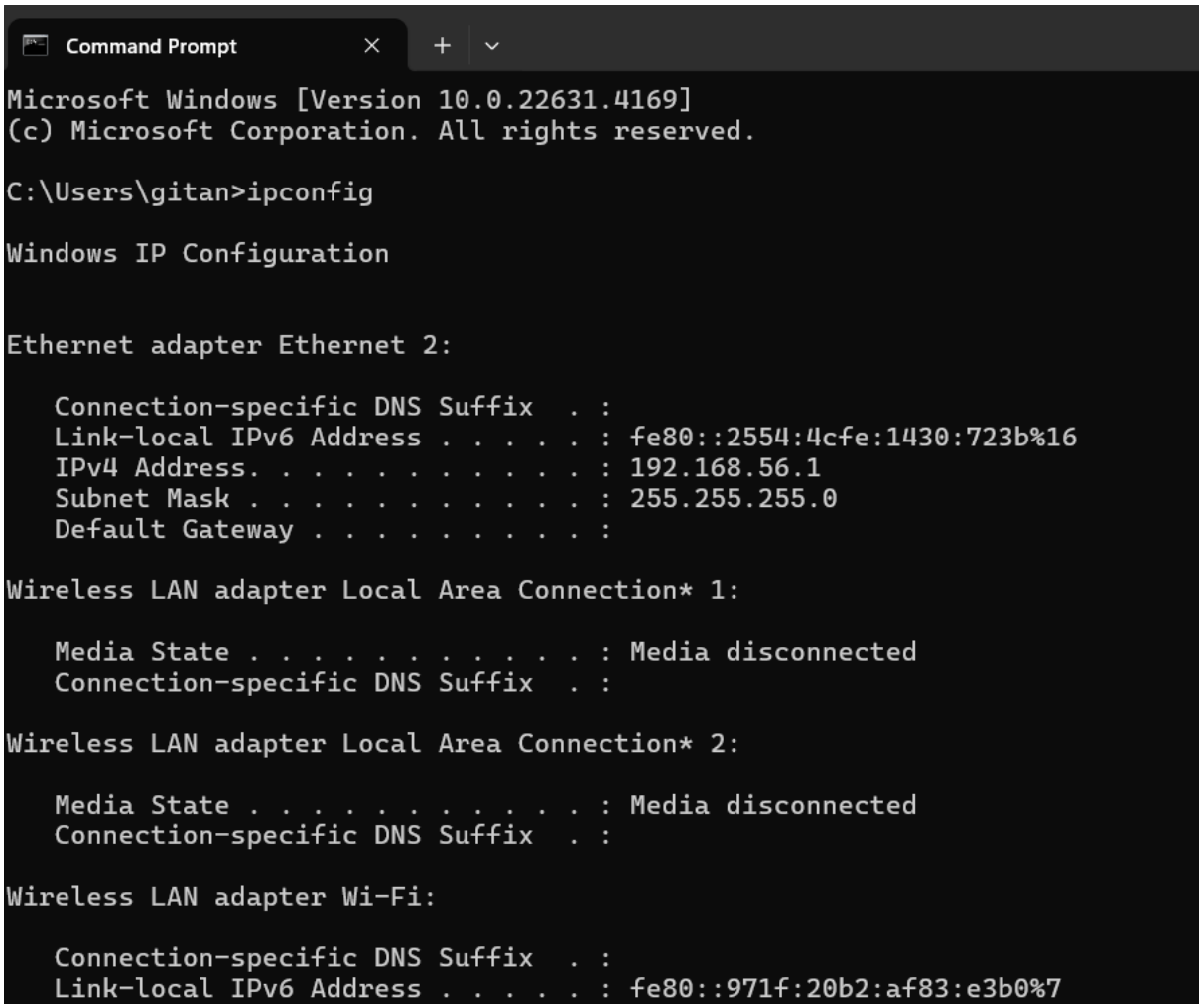
HTTP/HTTPS - Ensures the web page content is transmitted securely if using HTTPS.

Changes with NAT:

1. DHCP assignment: The router would assign a private IP address to the laptop.
2. NAT Translation: When laptop sends a request to clouddeakin server , router translates the private IP address to a public IP address.

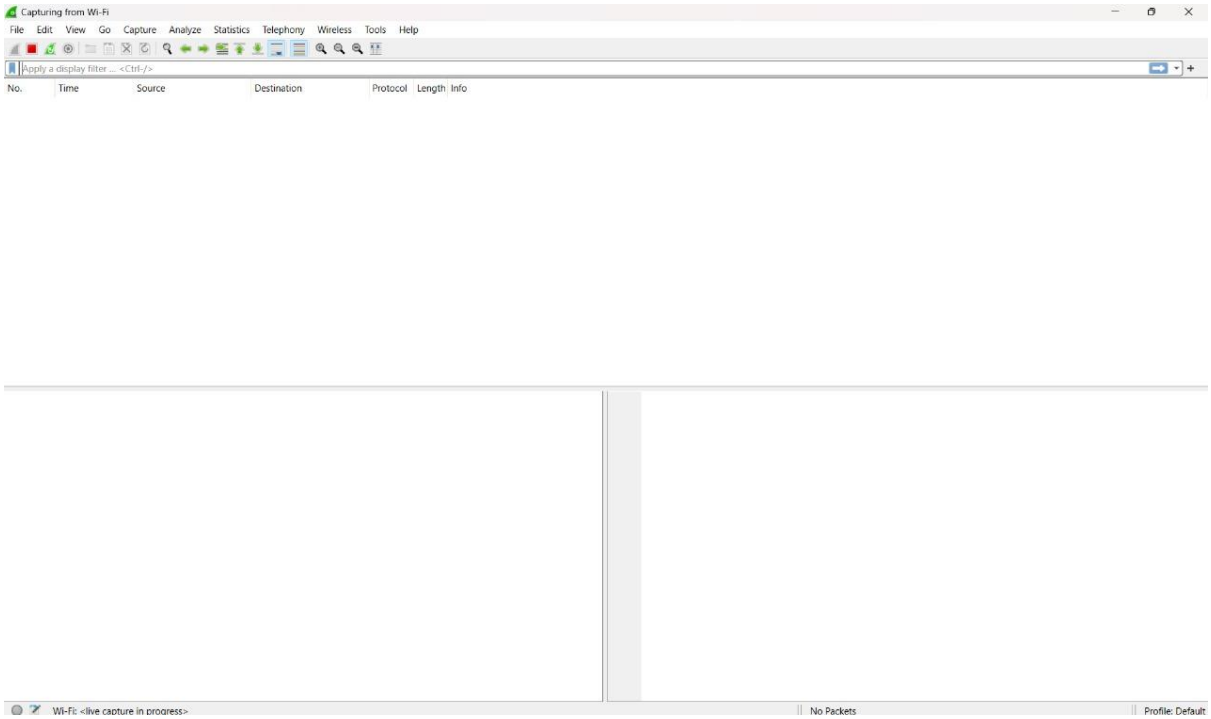
3. Port forwarding : Router keeps track of outgoing request and ensures that response from server is forwarded to correct device on the local network.

Activity 2: Wireshark, explain the process

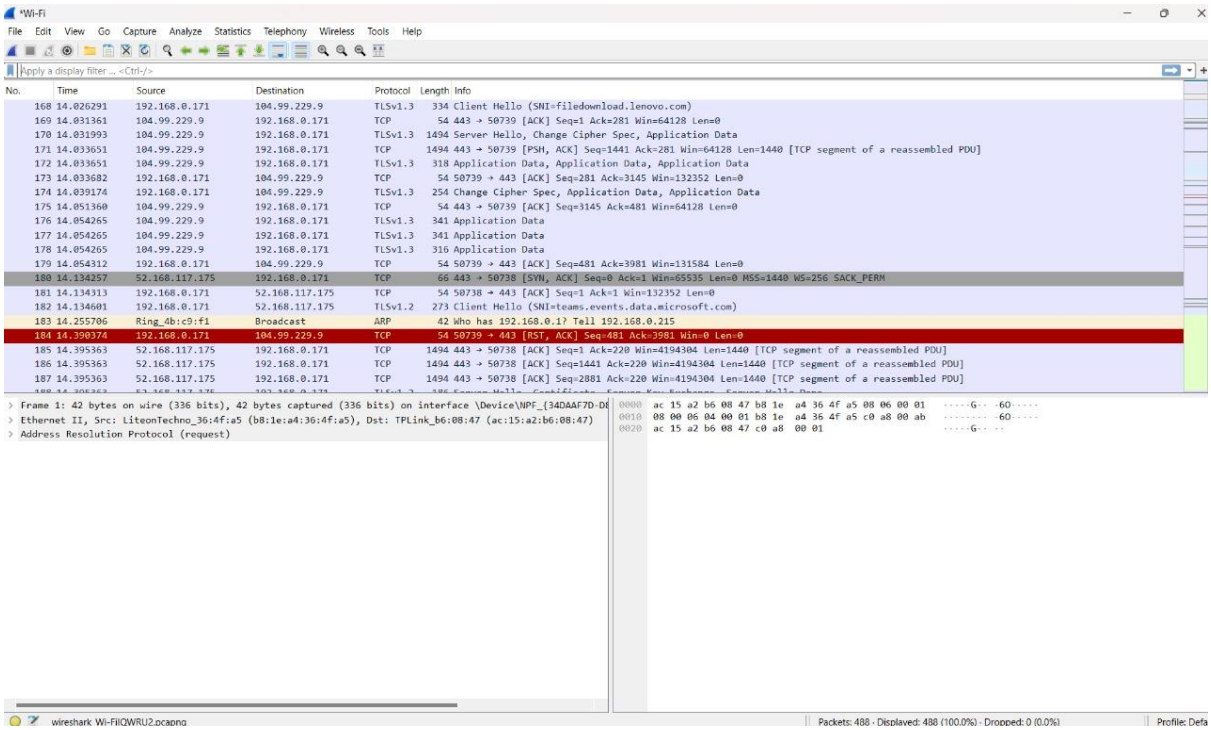


When I turned off the wifi,wireshark will not capture any packets .The window will be empty.

Name – jasveena Student id-224001588

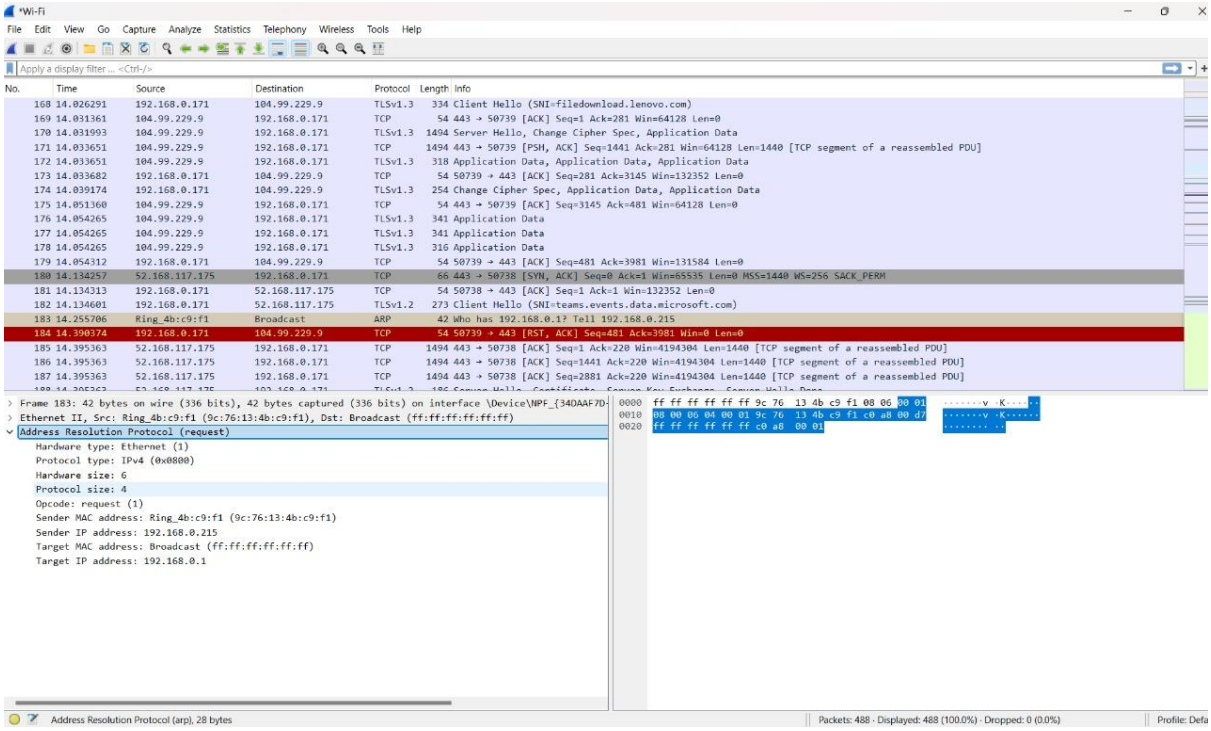


Wireshark capturing of http://www.discoverourtown.com.

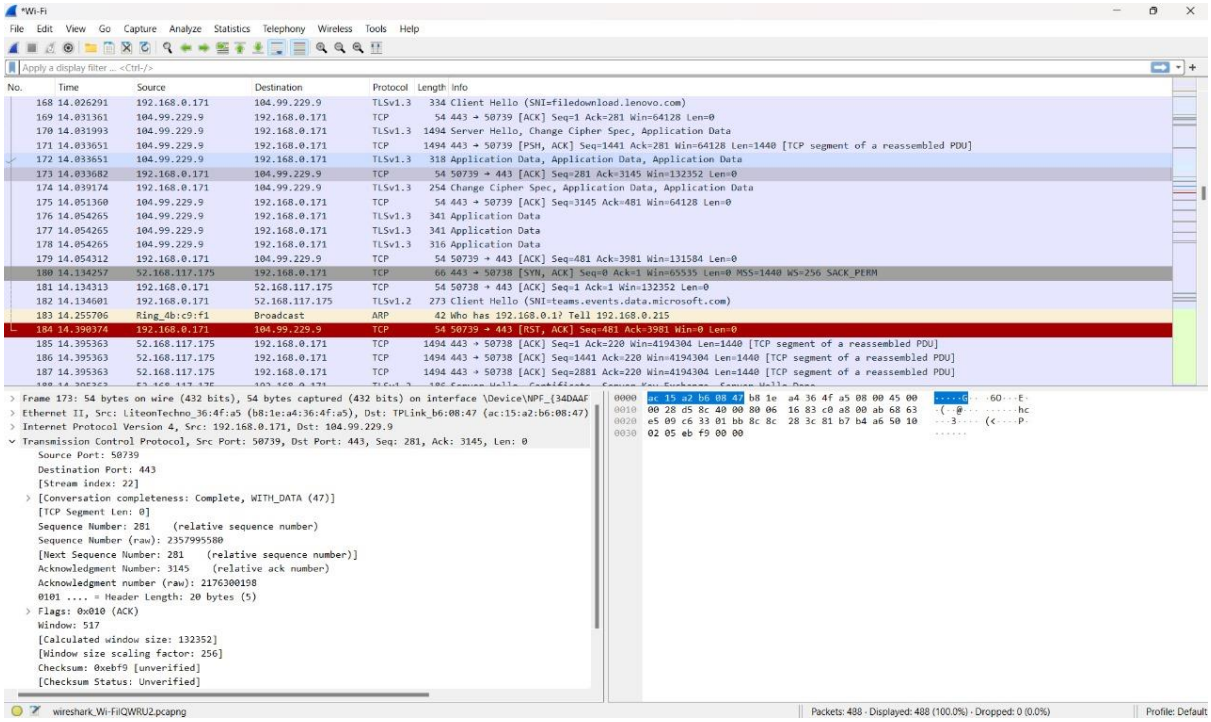


List and details of protocols and messages:

1. ARP (Address resolution protocol): It looks for ARP requests and resolves IP address to MAC addresses.
   It belongs to layer 2().

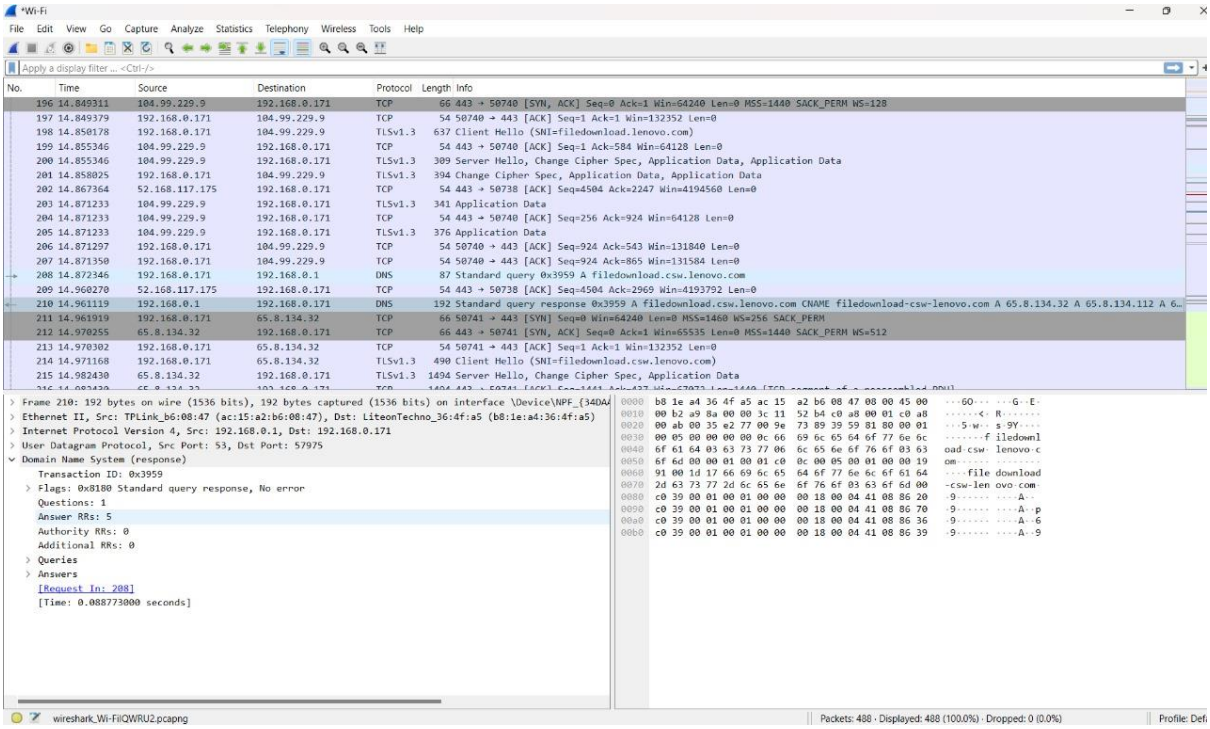


2. DHCP (Dynamic host configuration protocol): It offers,requests and assigns IP addresses to devices.
   It belongs to layer 7().



3.HTTP (Hypertext transfer protocol): It looks for HTTP Get requests and transmits web page data or HTTP responses.
It belongs to layer 7().

4.TCP (Transmission control protocol): It establishes a connection and ensures reliable data transfer
It belongs to layer 4.



Comparison:

Similarities:

ARP : Both activities involve ARP for MAC address resolution.

DHCP: Both activities involve DHCP for IP address assignment.

DNS: Both activities involve DNS for domain name resolution.

TCP: Both activities involve TCP for establishing a reliable connection.

HTTP: Both activities involve HTTP for web page data transmission.

Differences:

Network Connection Type: Activity 2 includes the additional step of toggling the network connection to capture packets.

Web page accessed: Different web pages are accessed in each activity, but the underlying protocols remain the same.

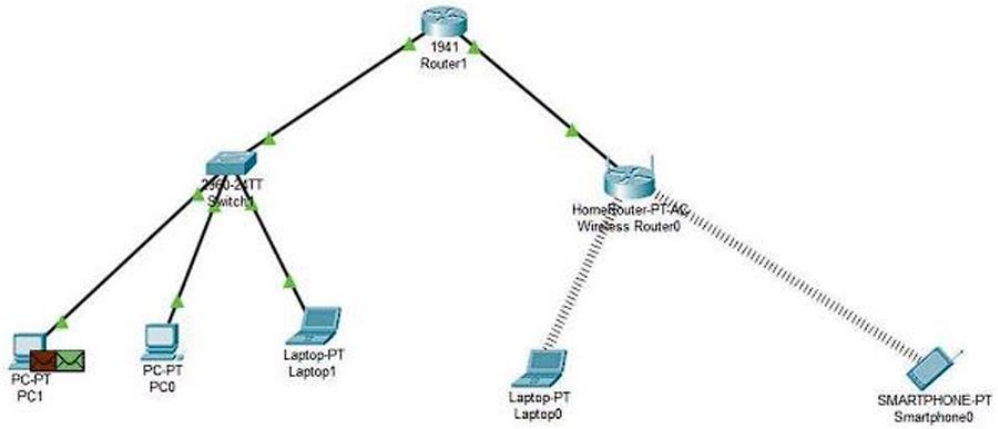
Packet capture analysis: Activity 2 provides a hands-on approach to observing the protocols in action.

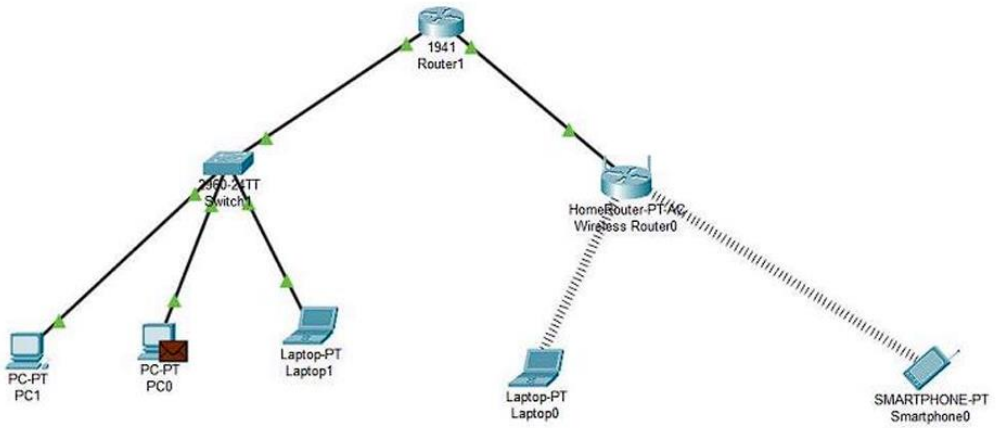
Conclusion: Both activities involve the same fundamental protocols (ARP, DHCP, DNS, TCP, HTTP) and their functions in the process of accessing a web page. The main difference lies in the practical aspect of capturing and analyzing packets in Activity 2, which provides a deeper understanding of the behind-the-scenes process.

Activity 3: Wireless network vs wired networks/connectivity

1. **Use the simulation mode and send a simple PDU,**

a. From PC1 to PC0

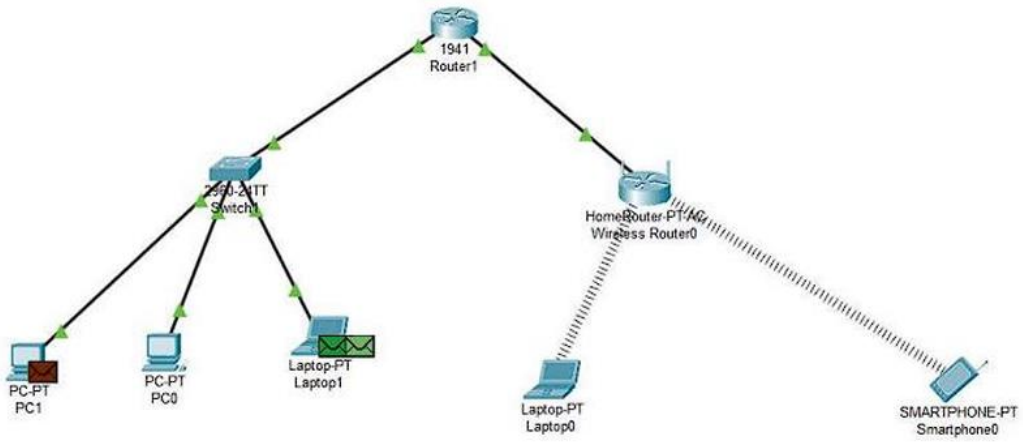


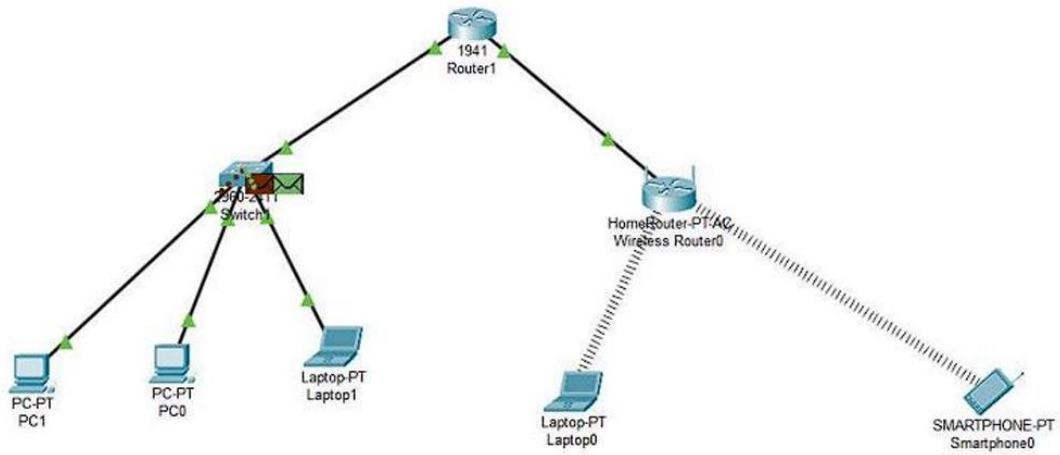


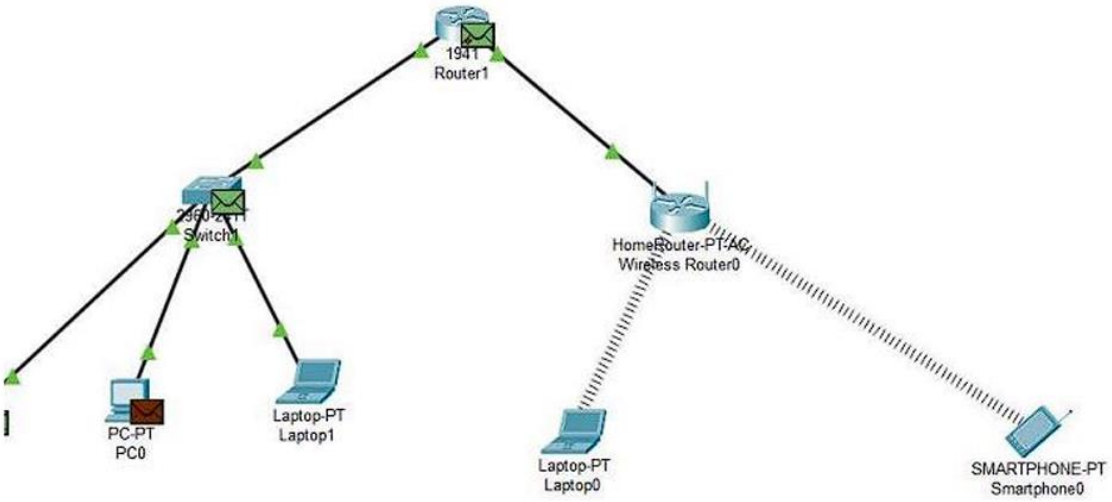
Pinging screenshot

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=17ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 17ms, Average = 11ms
```

b. From Laptop 1 to Tablet 0







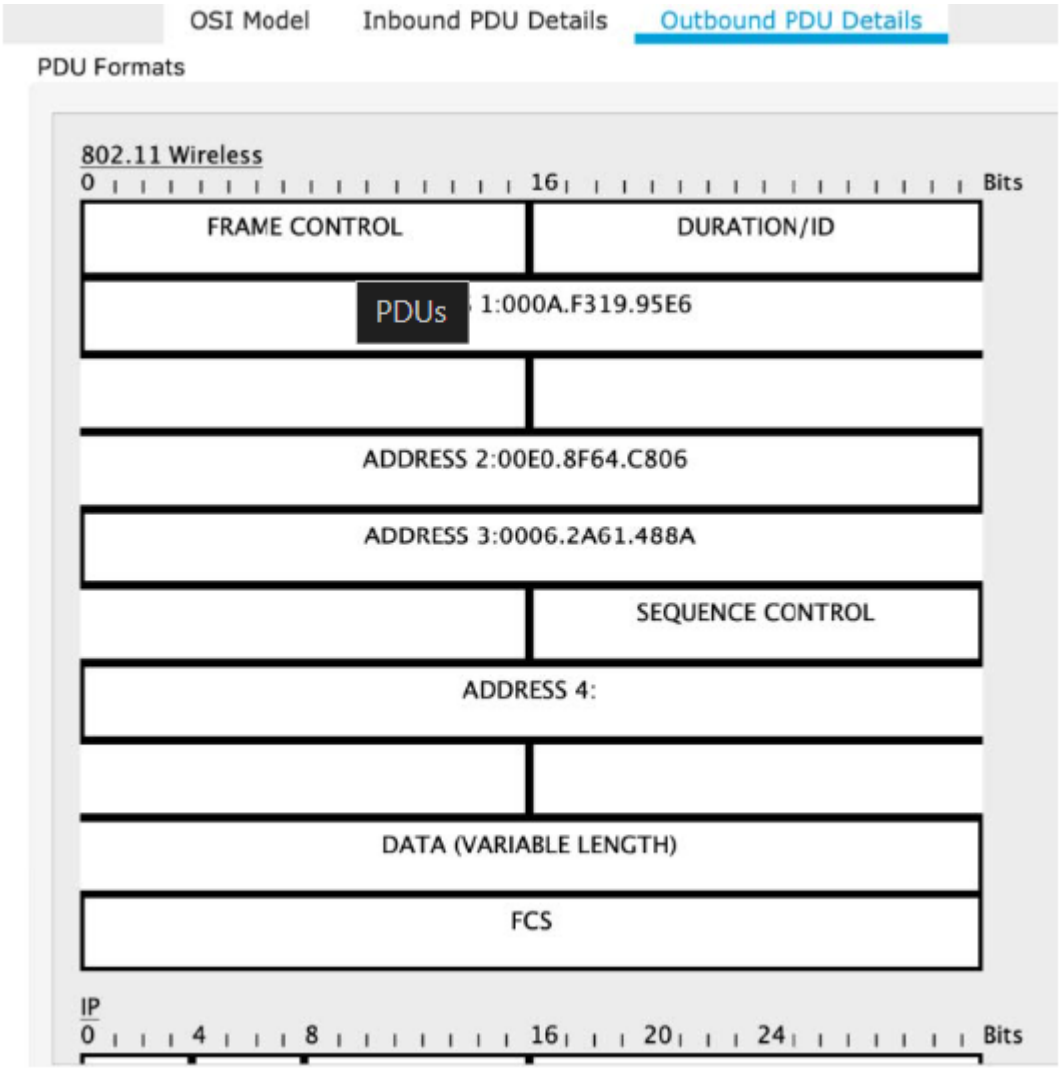
2. Note down the similarities and differences you observed in 1.a and 1.b. You may check the details of PDUs in each device. Explain the reasons behind the differences you observed.

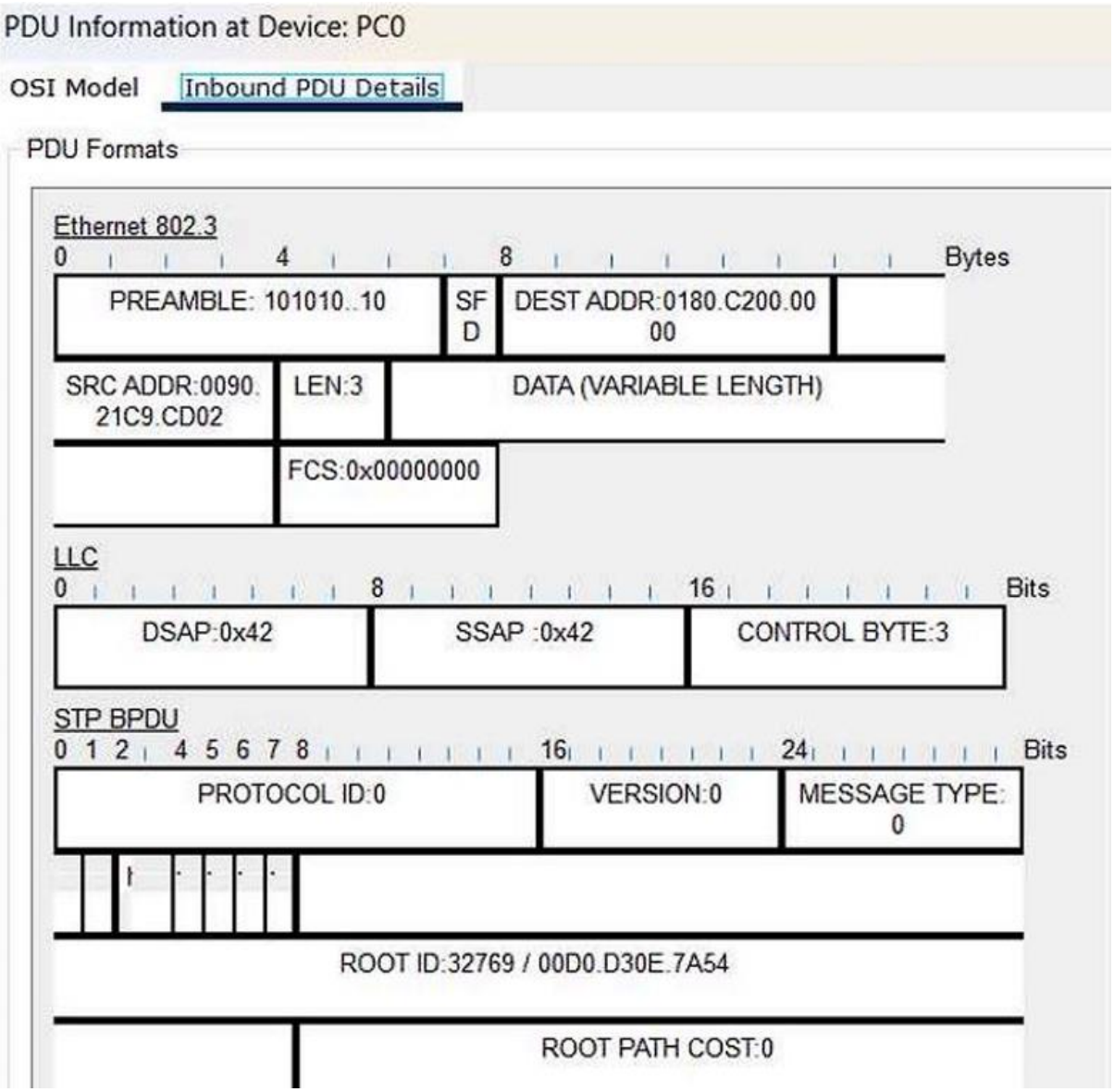
Similarities:
In both wired and wireless Local Area Networks (LANs), Protocol Data Units (PDUs) are transmitted using Layer 2 (Data Link Layer) and Layer 3 (Network Layer) protocols. In each scenario, devices within the same LAN are identified by their MAC addresses for the next-hop routing, while the destination is determined by IP addresses.
Differences:
In a Wired LAN (e.g., communication between PC1 and PC0), the transmission occurs directly between two devices within the same broadcast domain. As a result, Ethernet frames include two MAC addresses: the source MAC address and the destination MAC address.
Conversely, in a Wireless LAN (e.g., communication between Laptop 1 and Tablet 0), access points (APs) play a crucial role in forwarding frames. Consequently, 802.11 wireless frames incorporate three MAC addresses, reflecting the more complex nature of frame forwarding:

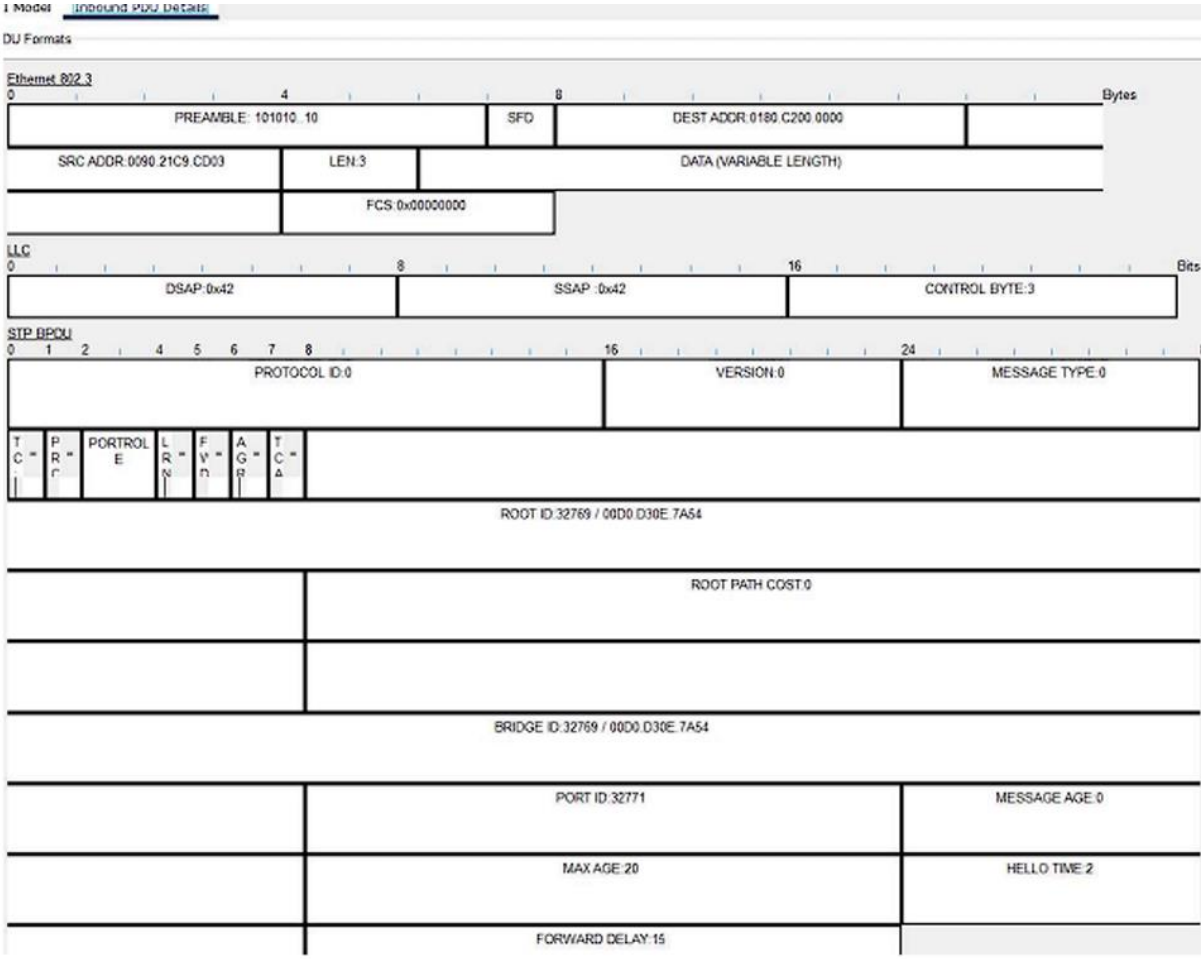
1. Source MAC Address: The MAC address of the device initiating the transmission (Laptop 1).
2. Destination MAC Address: The MAC address of the intended recipient device (Tablet 0).
3. BSSID (Basic Service Set Identifier): The MAC address of the access point managing the wireless network. This address is crucial when a wireless frame is sent from the laptop to the AP before being forwarded to the ultimate recipient.

1. 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.

Name – jasveena Student id-224001588




PDU Information at Device: PC0
OSI Model
Inbound PDU Details
PDU Formats
Ethernet 802.3
0
4
8
Bytes
PREAMBLE: 101010..10
SFD
DEST ADDR:0180.C200.0000
SRC ADDR:0090.21C9.CD02
LEN:3
DATA (VARIABLE LENGTH)
FCS:0x00000000
LLC
0
8
16
Bits
DSAP:0x42
SSAP :0x42
CONTROL BYTE:3
STP BPDU
0 1 2 4 5 6 7 8
16
24
Bits
PROTOCOL ID:0
VERSION:0
MESSAGE TYPE:0
ROOT ID:32769 / 00D0.D30E.7A54
ROOT PATH COST:0



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

   Transmitter Address (TA): This is the MAC address of the station (device) that is sending the frame.

   Receiver Address (RA): The RA is the MAC address of the station that should receive the frame. It's like the recipient's address on that same envelope. The RA tells the Wi-Fi network which device should process the incoming data.

   BSSID (Basic Service Set Identifier): The BSSID is a special MAC address associated with the access point (AP) that serves as the gateway to the wireless network.

Name – jasveena Student id-224001588