

**Use Wireshark to View Network Traffic Topology**  
**LAB # 06**



**Spring 2025**

Submitted by: **Mohsin Sajjad**  
Registration No: **22pwsce2149**

**Class Section: A**

“On my honor, as student of University of Engineering and Technology, I have neither given nor received unauthorized assistance on this academic work.”

A handwritten signature in black ink that reads "Mohsin Sajjad".

Student Signature: \_\_\_\_\_

Submitted to:  
**Dr. Yasir Saleem Afridi**  
Month Day, Year (22 04, 2025)

Department of Computer Systems Engineering  
University of Engineering and Technology, Peshawar

---

## CSE 303L: Data Communication and Computer Networks

---

Credit Hours: 1

Demonstration of Concepts	Poor (Does not meet expectation (1))  The student failed to demonstrate a clear understanding of the assignment concepts	Fair (Meet Expectation (2-3))  The student demonstrated a clear understanding of some of the assignment concepts	Good (Exceeds Expectation (4-5))  The student demonstrated a clear understanding of the assignment concepts	Score  30%
Accuracy	The student mis-configured enough network settings that the lab computer couldn't function properly on the network	The student configured enough network settings that the lab computer partially functioned on the network	The student configured the network settings that the lab computer fully functioned on the network	30%
Following Directions	The student clearly failed to follow the verbal and written instructions to successfully complete the lab	The student failed to follow the some of the verbal and written instructions to successfully complete all requirements of the lab	The student followed the verbal and written instructions to successfully complete requirements of the lab	20%
Time Utilization	The student failed to complete even part of the lab in the allotted amount of time	The student failed to complete the entire lab in the allotted amount of time	The student completed the lab in its entirety in the al	20%

# Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

## Instructions

### Part 1: Capture and Analyze Local ICMP Data in Wireshark

In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

#### Step 1: Retrieve your PC interface addresses.

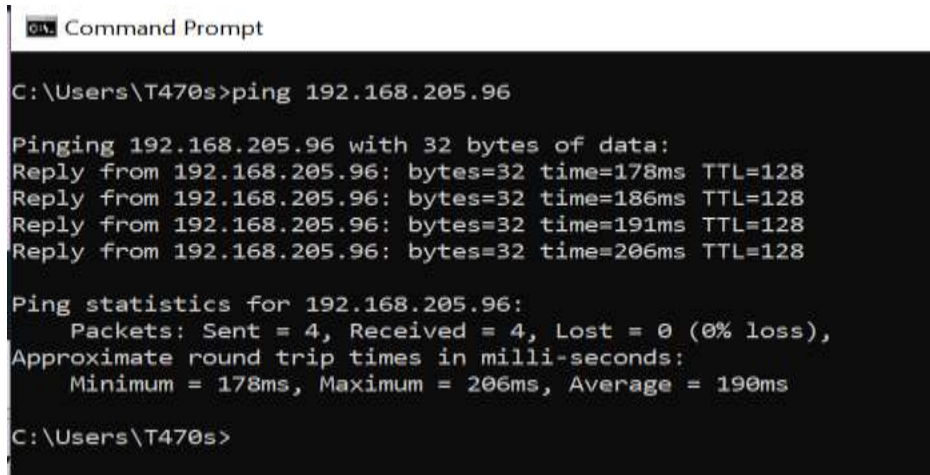
For this lab, you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

- a. In a command prompt window, enter **ipconfig /all**, to the IP address of your PC interface, its description, and its MAC (physical) address.

#### Step 2: Start Wireshark and begin capturing data.

- a. Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic.
- b. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark.



```
Command Prompt
C:\Users\T470s>ping 192.168.205.96

Pinging 192.168.205.96 with 32 bytes of data:
Reply from 192.168.205.96: bytes=32 time=178ms TTL=128
Reply from 192.168.205.96: bytes=32 time=186ms TTL=128
Reply from 192.168.205.96: bytes=32 time=191ms TTL=128
Reply from 192.168.205.96: bytes=32 time=206ms TTL=128

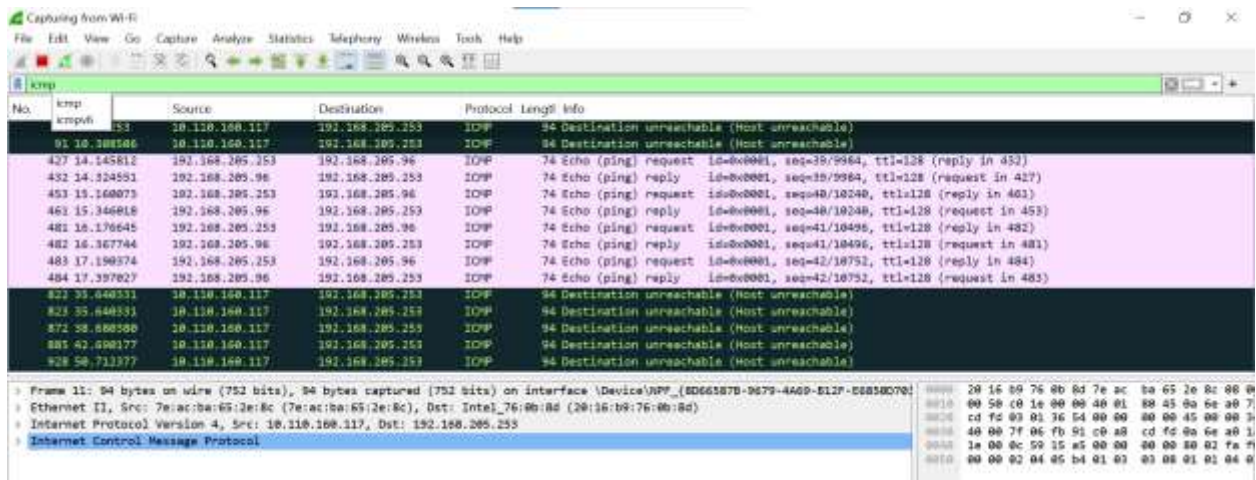
Ping statistics for 192.168.205.96:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 178ms, Maximum = 206ms, Average = 190ms

C:\Users\T470s>
```

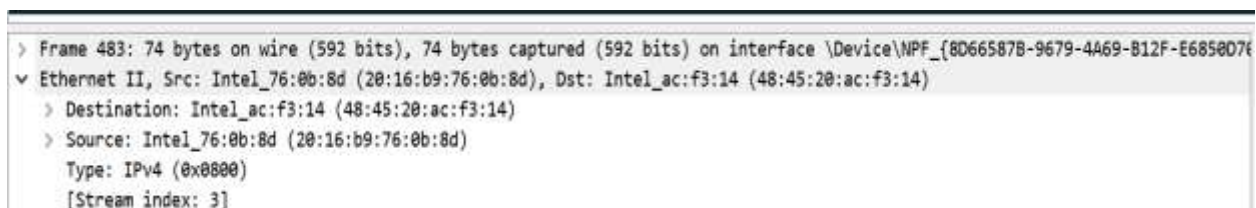
### Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed; 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers; and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

- Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the **Source** column has your PC IP address, and the **Destination** column contains the IP address of the teammate PC that you pinged.



- With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the destination and source MAC addresses.



### Question:

Does the source MAC address match your PC interface?

### Answer:

Yes the mac address is same .

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Dual Band Wireless-AC 8260
Physical Address. . . . . : 20-16-B9-76-0B-8D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9dc6:b9f4:1da7:872e%11(Preferred)
IPv4 Address. . . . . : 192.168.205.253(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, 22 April 2025 11:31:12 pm
Lease Expires . . . . . : Wednesday, 23 April 2025 12:31:10 am
Default Gateway . . . . . : 192.168.205.114
DHCP Server . . . . . : 192.168.205.114
DHCPv6 IAID . . . . . : 136320697
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-86-17-6E-8C-16-45-E2-71-14
DNS Servers . . . . . : 192.168.205.114
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

```

Does the destination MAC address in Wireshark match your team member MAC address?

**Answer:**

Yes the mac is same.

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Dual Band Wireless-N 7265
Physical Address. . . . . : 48-45-20-AC-F3-14
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7356:f195:d4e3:4097%6(Preferred)
IPv4 Address. . . . . : 192.168.205.96(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, April 22, 2025 11:30:54 PM
Lease Expires . . . . . : Wednesday, April 23, 2025 12:30:53 AM
Default Gateway . . . . . : 192.168.205.114
DHCP Server . . . . . : 192.168.205.114
DHCPv6 IAID . . . . . : 88622368
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-85-2F-E9-00-0C-29-54-3A-70
DNS Servers . . . . . : 192.168.205.114
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Admin>_

```

How is the MAC address of the pinged PC obtained by your PC?

**Answer:**

The MAC address of the pinged PC is obtained via the Address Resolution Protocol (ARP), where your PC sends an ARP request to resolve the IP address to a MAC address. The destination PC replies with its MAC address, allowing communication.

## Part 2: Capture and Analyze Remote ICMP Data in Wireshark

In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

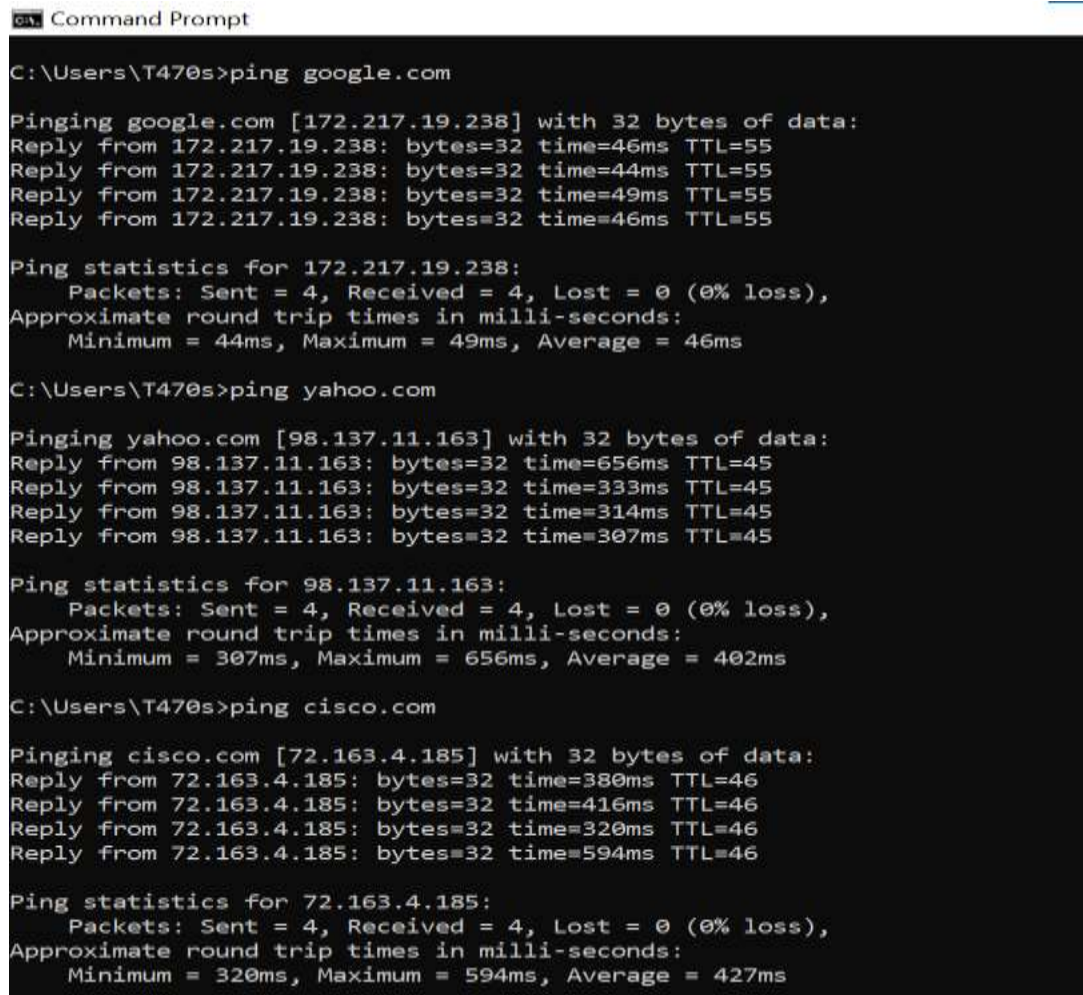
Step 1: Start capturing data on the interface.

- a. Start the data capture again.
- b. A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.
- c. With the capture active, ping the following three website URLs from a Windows command prompt:

- 1) www.yahoo.com
- 2) www.cisco.com
- 3) www.google.com

**Note:** When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

- d. You can stop capturing data by clicking the **Stop Capture** icon.



```
GA Command Prompt

C:\Users\T470s>ping google.com

Pinging google.com [172.217.19.238] with 32 bytes of data:
Reply from 172.217.19.238: bytes=32 time=46ms TTL=55
Reply from 172.217.19.238: bytes=32 time=44ms TTL=55
Reply from 172.217.19.238: bytes=32 time=49ms TTL=55
Reply from 172.217.19.238: bytes=32 time=46ms TTL=55

Ping statistics for 172.217.19.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 44ms, Maximum = 49ms, Average = 46ms

C:\Users\T470s>ping yahoo.com

Pinging yahoo.com [98.137.11.163] with 32 bytes of data:
Reply from 98.137.11.163: bytes=32 time=656ms TTL=45
Reply from 98.137.11.163: bytes=32 time=333ms TTL=45
Reply from 98.137.11.163: bytes=32 time=314ms TTL=45
Reply from 98.137.11.163: bytes=32 time=307ms TTL=45

Ping statistics for 98.137.11.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 307ms, Maximum = 656ms, Average = 402ms

C:\Users\T470s>ping cisco.com

Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=380ms TTL=46
Reply from 72.163.4.185: bytes=32 time=416ms TTL=46
Reply from 72.163.4.185: bytes=32 time=320ms TTL=46
Reply from 72.163.4.185: bytes=32 time=594ms TTL=46

Ping statistics for 72.163.4.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 320ms, Maximum = 594ms, Average = 427ms
```



## Step 2: Examining and analyzing the data from the remote hosts.

Review the captured data in Wireshark and examine the IP and MAC addresses of the three locations that you pinged.

List the destination IP and MAC addresses for all three locations in the space provided.

IP address for [www.yahoo.com](http://www.yahoo.com):

98.137.11.163

MAC address for [www.yahoo.com](http://www.yahoo.com):

7e:ac:ba:65:2e:8c

```
> Frame 137: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70}
  Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: 7e:ac:ba:65:2e:8c (7e:ac:ba:65:2e:8c)
    > Destination: 7e:ac:ba:65:2e:8c (7e:ac:ba:65:2e:8c)
    > Source: Intel_76:0b:8d (20:16:b9:76:0b:8d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  > Internet Protocol Version 4, Src: 192.168.205.253, Dst: 98.137.11.163
  > Internet Control Message Protocol
```

IP address for [www.cisco.com](http://www.cisco.com):

72.163.4.185

MAC address for [www.cisco.com](http://www.cisco.com):

7e:ac:ba:65:2e:8c

```
> Frame 269: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70}
  Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: 7e:ac:ba:65:2e:8c (7e:ac:ba:65:2e:8c)
    > Destination: 7e:ac:ba:65:2e:8c (7e:ac:ba:65:2e:8c)
    > Source: Intel_76:0b:8d (20:16:b9:76:0b:8d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  > Internet Protocol Version 4, Src: 192.168.205.253, Dst: 72.163.4.185
  > Internet Control Message Protocol
```

IP address for [www.google.com](http://www.google.com):

172.217.19.238

MAC address for [www.google.com](http://www.google.com):

7e:ac:ba:65:2e:8c

```
> Frame 47: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8D66587B-9679-4A69-B12F-E6850D70}
  Ethernet II, Src: Intel_76:0b:8d (20:16:b9:76:0b:8d), Dst: 7e:ac:ba:65:2e:8c (7e:ac:ba:65:2e:8c)
    > Destination: 7e:ac:ba:65:2e:8c (7e:ac:ba:65:2e:8c)
    > Source: Intel_76:0b:8d (20:16:b9:76:0b:8d)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  > Internet Protocol Version 4, Src: 192.168.205.253, Dst: 172.217.19.238
  > Internet Control Message Protocol
```

**What is significant about this information?**

**Answer:**

The significant part is that the local MAC addresses are directly related to devices within the same network, while remote MAC addresses are those of the routers or gateways handling the traffic.

**How does this information differ from the local ping information you received in Part 1?**

**Answer:**

In Part 1, the local ping shows the actual MAC addresses of the devices on the same network, while in Part 2, only the MAC address of the router/gateway is shown for remote hosts.

**Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?**

**Answer:**

Wireshark shows local MAC addresses because they are within the same local network, while remote hosts use routers, which only show the MAC address of the router, not the final destination.