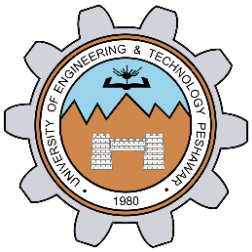
USE WIRESHARK TO VIEW NETWORK TRAFFIC TOPOLOGY

Lab #05



Spring 2021

CSE303L Data Communication and Networks Lab

Submitted by: **Shah Raza**

Registration No. : **18PWCSE1658**

Class Section: **B**

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

Student Signature: _____

Submitted to:

Engr. Faiz Ullah

Friday, June 25, 2021

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

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and MAC addresses.

Required Resources

- 1 PC (Windows with internet access)
- Additional PCs on a local-area network (LAN) will be used to reply to ping requests.

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.

```
C:\Users\Shah Raza>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-T3I4Q71
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
```

```
   Physical Address. . . . . . . . . : F8-CA-B8-5B-DC-18
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 00-1E-64-FA-C2-7A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
#2
   Physical Address. . . . . . . . . : 02-1E-64-FA-C2-79
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for
VMnet1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.144.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for
VMnet8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.192.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3160
   Physical Address. . . . . . . . . : 00-1E-64-FA-C2-79
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.43.182(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, June 25, 2021 7:18:44 PM
   Lease Expires . . . . . . . . . . : Friday, June 25, 2021 8:18:44 PM
   Default Gateway . . . . . . . . . : 192.168.43.1
   DHCP Server . . . . . . . . . . . : 192.168.43.1
   DNS Servers . . . . . . . . . . . : 192.168.43.1
```

```
   NetBIOS over Tcpip. . . . . : Enabled
```

b. Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time.

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.

For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the **Filter** box at the top of Wireshark and press **Enter,** or click the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.

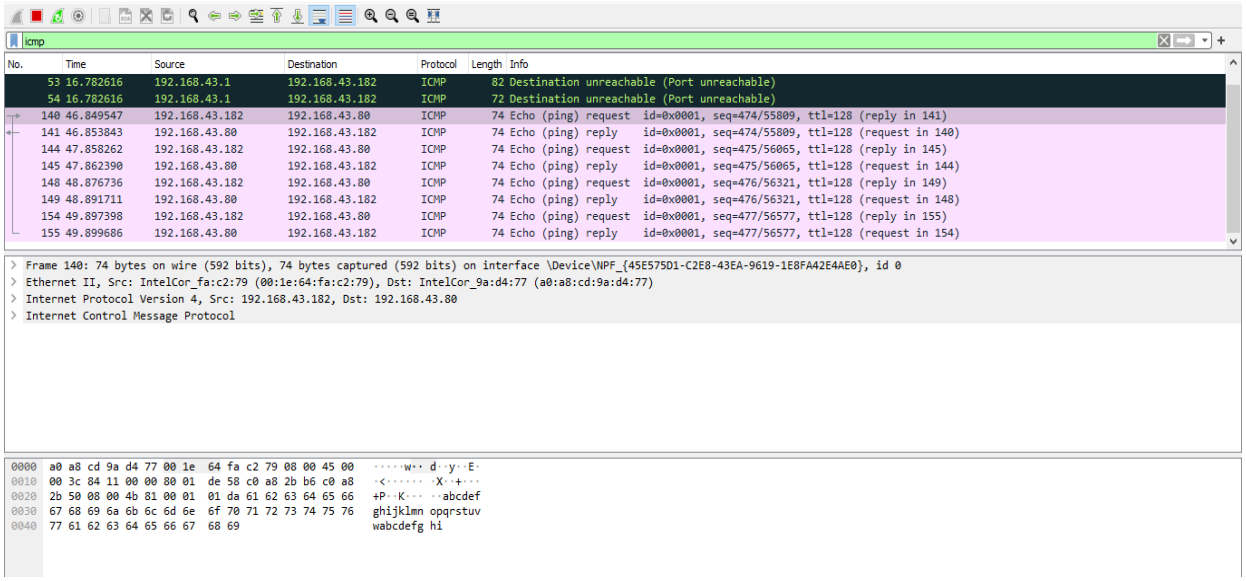
c. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Navigate to a command prompt window and ping the IP address that you received from your team member.

```
C:\Users\Shah Raza>ping 192.168.43.80

Pinging 192.168.43.80 with 32 bytes of data:
Reply from 192.168.43.80: bytes=32 time=4ms TTL=128
Reply from 192.168.43.80: bytes=32 time=4ms TTL=128
Reply from 192.168.43.80: bytes=32 time=15ms TTL=128
Reply from 192.168.43.80: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.43.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 15ms, Average = 6ms
```

Notice that you start seeing data appear in the top window of Wireshark again.



d. Stop capturing data by clicking the **Stop Capture** icon.

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.

a. 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.

b. 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.

Questions:

Does the source MAC address match your PC interface?
Yes! The source MAC address matches my PC interface.

Does the destination MAC address in Wireshark match your team member MAC address?
Yes! The destination MAC address in Wireshark matches my team member MAC address.

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

It is obtained through an ARP Request.

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.

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**:

87.248.100.215

MAC address for **www.yahoo.com**:

7c:ad:74:e4:f6:d1

IP address for **www.cisco.com**:

23.10.231.118

MAC address for **www.cisco.com**:

7c:ad:74:e4:f6:d1

IP address for **www.google.com**:

142.250.185.36

MAC address for **www.google.com**:

7c:ad:74:e4:f6:d1

What is significant about this information?

As we can see, the MAC address of all three destinations is same.

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

A ping to a local host returns the MAC address of the PC NIC. A ping to a remote host returns the MAC address of the default gateway LAN interface.

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

MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.