

COURSE: CLOUD AND NETORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

**EXAMINE TCP/IP AND OSI MODELS IN ACTION WITH
CISCO PACKET TRACER**

Contents

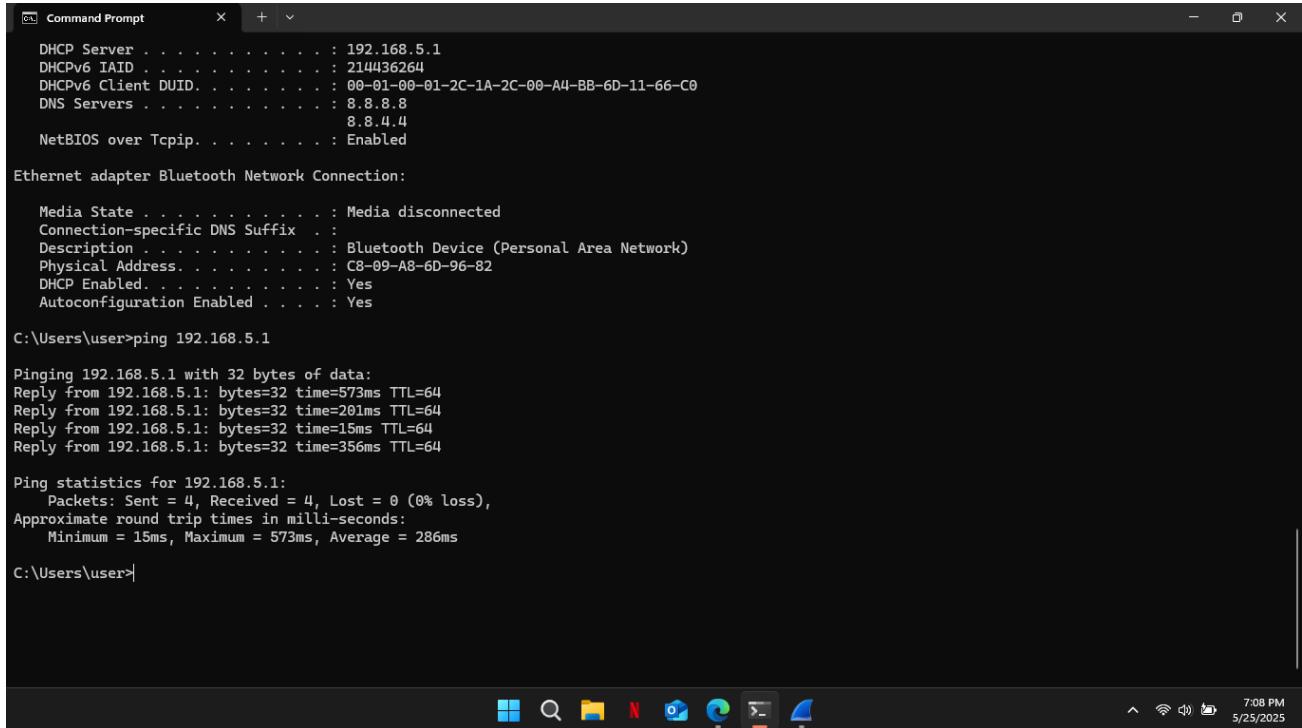
INTRODUCTION.....	3
USE WIRESHARK TO EXAMINE NETWORK TRAFFIC.....	4
EXAMINING THE CAPTURED DATA	5
PING THE FOLLOWING WEBSITE URLs	6
CONCLUSION	8

INTRODUCTION

In this activity, we used the ping command and Wireshark to understand how computers communicate over a network. The goal was to see how our computer finds the MAC address of another device when we ping it and to observe what actually happens on the network during that process. We also tested pinging different websites to compare how local network traffic differs from internet traffic. By applying filters like ICMP in Wireshark, we could clearly see how our computer sends and receives packets, and how it gets the MAC address using ARP when needed.

USE WIRESHARK TO EXAMINE NETWORK TRAFFIC

We ping the other computer in the network



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the following output:

```
DHCP Server . . . . . : 192.168.5.1
DHCPv6 IAID . . . . . : 214436264
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-1A-2C-00-A4-BB-6D-11-66-C0
DNS Servers . . . . . : 8.8.8.8
                           8.8.4.4
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : C8-09-A8-6D-96-82
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

C:\Users\user>ping 192.168.5.1

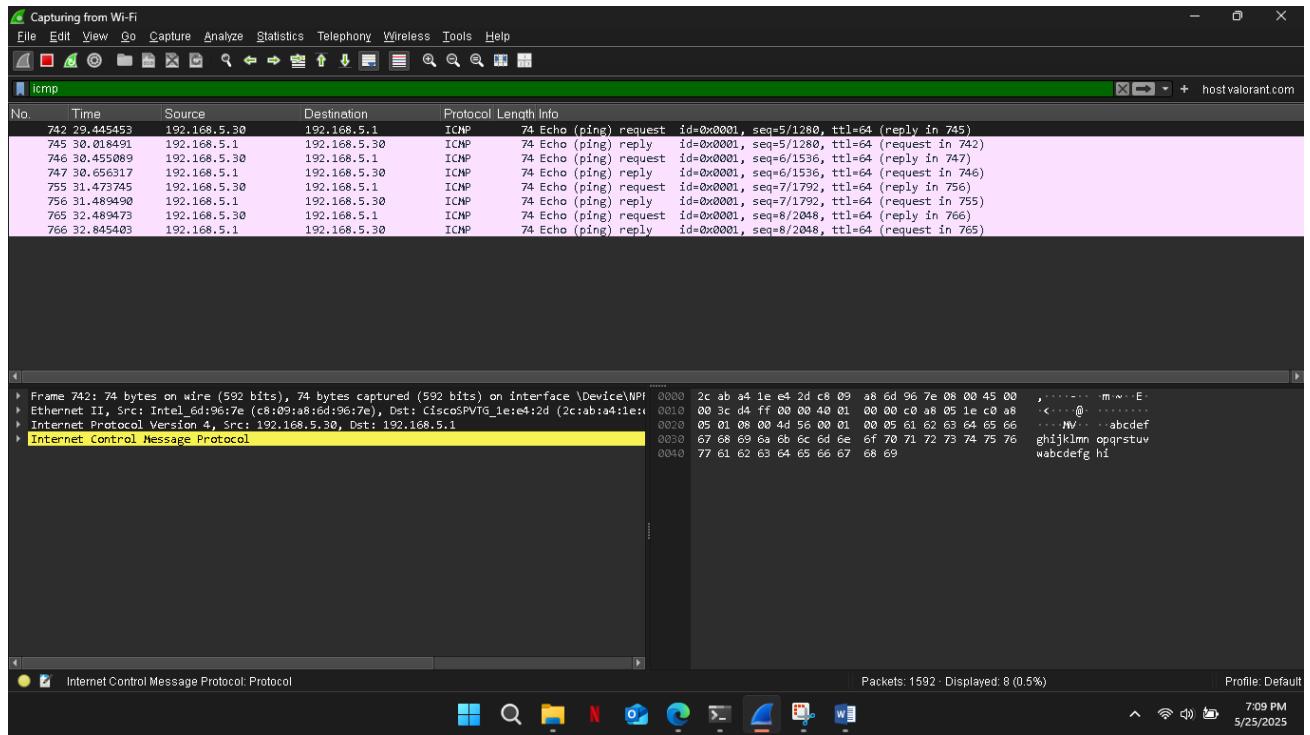
Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=573ms TTL=64
Reply from 192.168.5.1: bytes=32 time=201ms TTL=64
Reply from 192.168.5.1: bytes=32 time=15ms TTL=64
Reply from 192.168.5.1: bytes=32 time=356ms TTL=64

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 573ms, Average = 286ms

C:\Users\user>
```

The taskbar at the bottom of the screen includes icons for File Explorer, Search, Task View, and others, along with system status indicators like battery level and signal strength. The date and time (5/25/2025, 7:08 PM) are also visible.

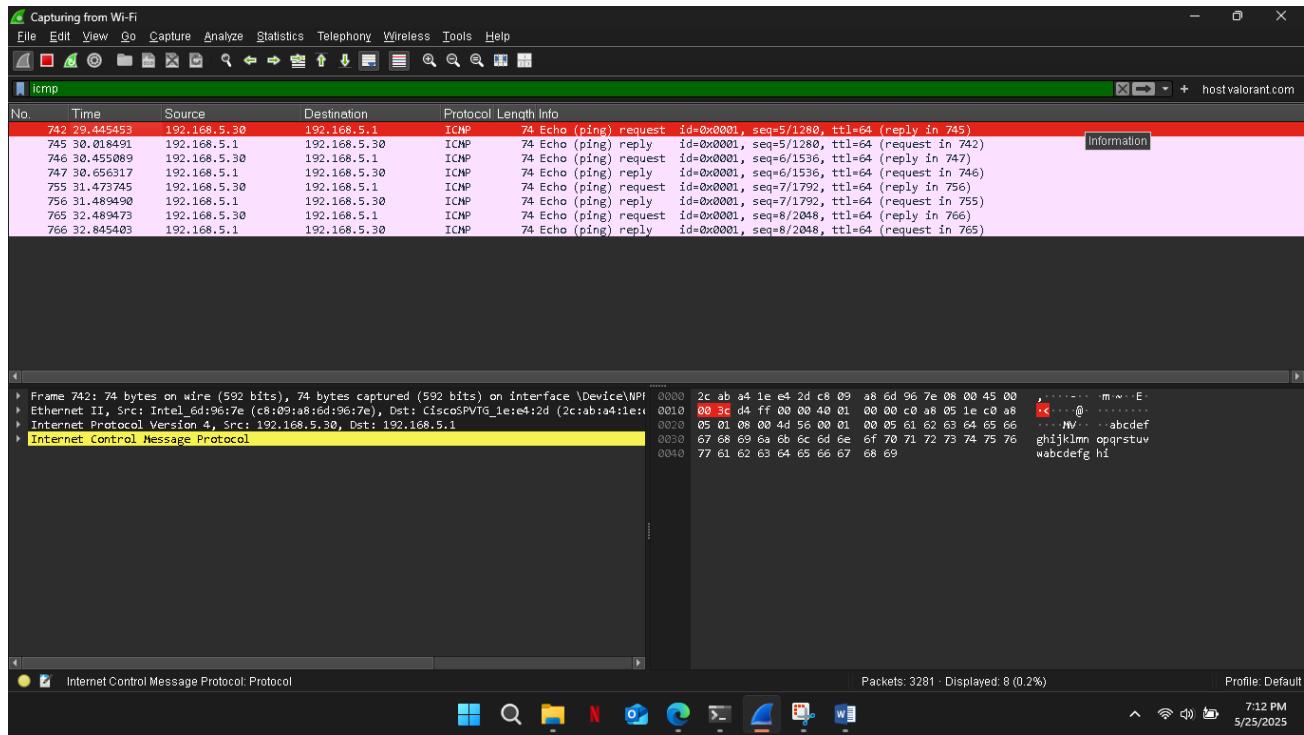
The output that we get on wireshark, this is after adding a filter ICMP (ping) PDUS.



EXAMINING THE CAPTURED DATA

Does the source mac address match your pcs mac address? YES!

Does the destination mac address match the destination mac address? YES!

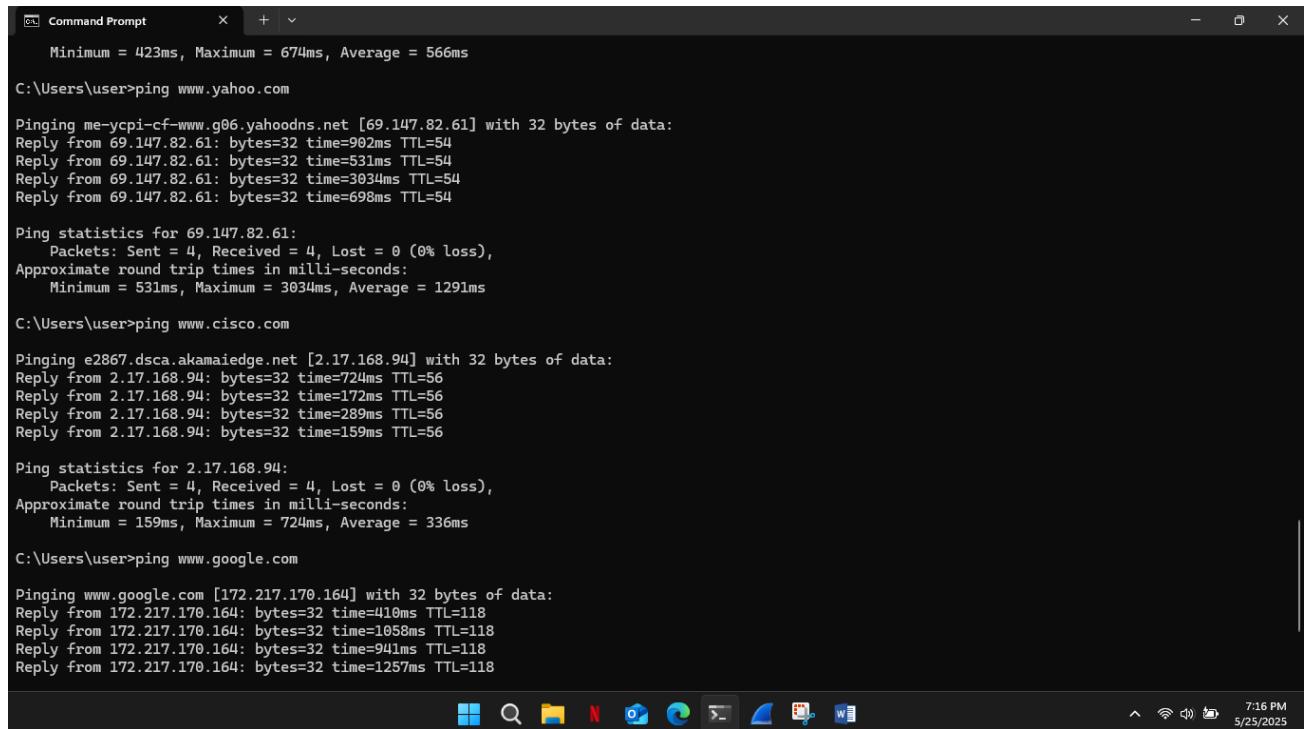


HOW IS THE MAC ADDRESS OF THE PINGED PC OBTAINED BY MY PC?

My computer first checks if it knows the MAC address linked to that IP. If it doesn't, it sends out an ARP (Address Resolution Protocol) request asking, "Who has this IP?" The target PC replies with its MAC address, and your computer stores it in the ARP cache for future use. Once it has the MAC address, it can send the ping (ICMP) packet directly to the right device over the network.

PING THE FOLLOWING WEBSITE URLs

1. YAHOO- IP ADDRESS 69.147.82.61
2. CISCO- - IP ADDRESS 2.17.168.94
3. GOOGLE- - IP ADDRESS 172.217.178.164



Command Prompt

```
Minimum = 423ms, Maximum = 674ms, Average = 566ms
C:\Users\user>ping www.yahoo.com

Pinging me-ycpi-cf-www.g06.yahoodns.net [69.147.82.61] with 32 bytes of data:
Reply from 69.147.82.61: bytes=32 time=902ms TTL=54
Reply from 69.147.82.61: bytes=32 time=531ms TTL=54
Reply from 69.147.82.61: bytes=32 time=3034ms TTL=54
Reply from 69.147.82.61: bytes=32 time=698ms TTL=54

Ping statistics for 69.147.82.61:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 531ms, Maximum = 3034ms, Average = 1291ms

C:\Users\user>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [2.17.168.94] with 32 bytes of data:
Reply from 2.17.168.94: bytes=32 time=724ms TTL=56
Reply from 2.17.168.94: bytes=32 time=172ms TTL=56
Reply from 2.17.168.94: bytes=32 time=289ms TTL=56
Reply from 2.17.168.94: bytes=32 time=159ms TTL=56

Ping statistics for 2.17.168.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 159ms, Maximum = 724ms, Average = 336ms

C:\Users\user>ping www.google.com

Pinging www.google.com [172.217.170.164] with 32 bytes of data:
Reply from 172.217.170.164: bytes=32 time=410ms TTL=118
Reply from 172.217.170.164: bytes=32 time=1058ms TTL=118
Reply from 172.217.170.164: bytes=32 time=941ms TTL=118
Reply from 172.217.170.164: bytes=32 time=1257ms TTL=118
```

In all the above we sent 4 packets and received 4 packets with 0 lost with their specific IP addresses.

When you ping websites like www.google.com or www.yahoo.com out on the internet, you don't get their MAC address — only their IP address shows up.

Because MAC addresses are only used inside local networks (like your home or office LAN). When your ping goes beyond your local network—say, across the internet—the MAC addresses of distant servers aren't visible or needed by your computer. Instead, your data travels through multiple routers, each with their own MAC addresses, but your computer only cares about the IP address to find the destination.

CONCLUSION

From this experiment, we learned that when pinging a device on the same local network, our computer uses ARP to find its MAC address. Once it gets that MAC address, it can send packets directly. However, when we ping websites on the internet, we don't see their MAC addresses—only their IP addresses. This is because MAC addresses are only used within a local network. On the internet, routers handle the communication between networks using IP addresses. This helped us understand the difference between local and global network communication.