**Data communication and computer networks Lab**

**Semester:6th**



**Lab Report # 4**

**Submitted By:** *Zainab Khalid*

**Registration No:***19PWCSE1743*

**Section: A**

**Submitted to:** *Engr Faiz Ullah*

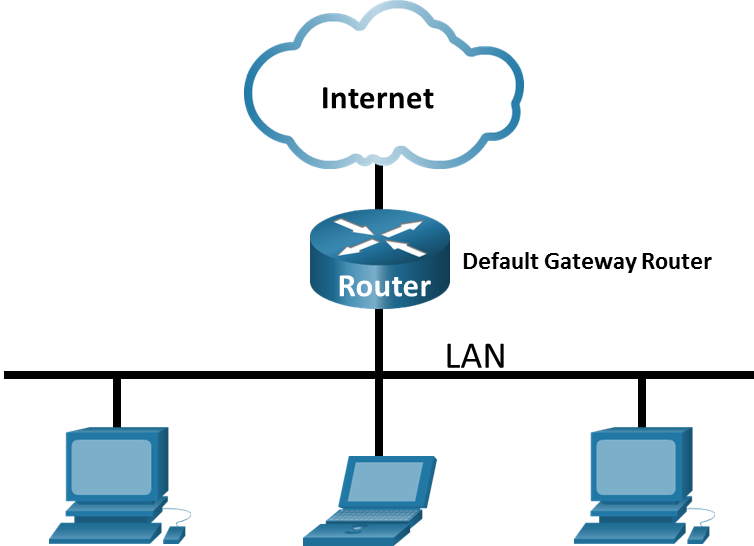
**Department of Computer Systems Engineering**

**University of Engineering and Technology Peshawar**

# Title:

Use Wireshark to View Network Traffic Topology

**ICMP (Internet Control Message Protocol) is an error-reporting protocol that network devices such as routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets.**



# Objectives:

* *Capture and Analyze Local ICMP Data in Wireshark*
* *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.

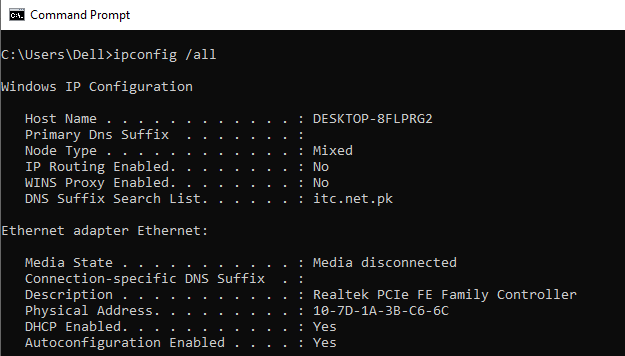
# Required Resources:

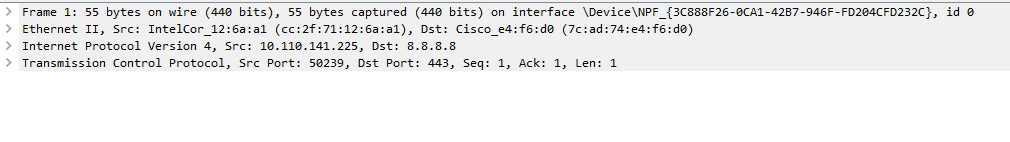
* 1 PC (Windows with internet access)
* Additional PCs on a local-area network (LAN) will be used to reply to ping requests.

# Capture and Analyze Local ICMP Data in Wireshark

1. **Question # 01:**
2. ***Does the source MAC address match your PC interface?***
3. **Answer:**

***Yes the source MAC address match with PC interface.***





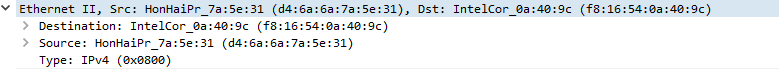
**Question # 02:**

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

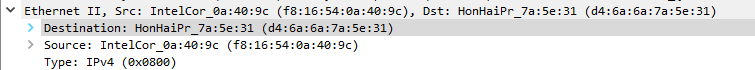
**Answer:**

***Yes, the destination MAC address in Wireshark match with our team member MAC address.***

**Request:**



**Reply:**

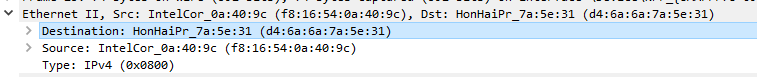


**Question # 03**

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

**Answer:**

***MAC address of the pinged PC obtained by entering ipconfig/all command in command prompt.***



## **Capture and Analyze Remote ICMP Data in Wireshark**

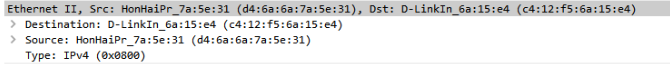
**Question # 01:**

1. ***List the destination IP and MAC addresses for all three locations in the space provided.***
2. **www.yahoo.com**

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



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

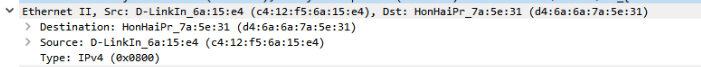


1. **www.cisco.com**:

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



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

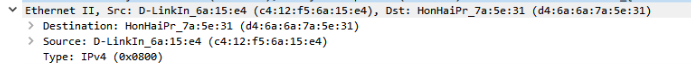


1. **www.google.com:**

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



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



**Question # 02:**

***What is significant about this information?***

**Answer:**

***We just ping any other local host’s IP address and we get MAC address of that local host in Wireshark on my PC.***

**Question # 03:**

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

**Answer:**

***This information is different from the local ping information in such a way that, the MAC address of the local hosts are same because they are on the same network, but the MAC address for the remote hosts are not same because they are not on the same network.***

**Question # 04:**

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

**Answer:**

***Wireshark show the actual MAC address of the local hosts because local hosts are on the same network, but not the actual MAC address for the remote hosts because they are not on the same network.***