1. Capture and analyze ARP packets using Wireshark. Inspect the ARP request and reply frames, and discuss the role of the sender's IP and MAC address in these packets.

ARP REQUEST:

A screenshot of a computer

AI-generated content may be incorrect.

ARP REPLY:

A screenshot of a computer

AI-generated content may be incorrect.

2.Using Packet Tracer, simulate an ARP spoofing attack. Analyze the behavior of devices on the network when they receive a malicious ARP response.

A diagram of a network

AI-generated content may be incorrect.

A close-up of a computer address

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

3.Manually configure static IPs on the client devices (like Pc or your mobile phone) and verify connectivity using ping.

Network topology:

A screenshot of a computer

AI-generated content may be incorrect.

Testing using ping:

A computer screen with a black background

AI-generated content may be incorrect.

A computer screen with a black background

AI-generated content may be incorrect.

4. Use Wireshark to capture DHCP Discover, Offer, Request, and Acknowledge messages and explain the process.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

5. Given an IP address range of 192.168.1.0/24, divide the network into 4 subnets.

Task: Manually calculate the new subnet mask and the range of valid IP addresses fo each subnet.

Assign IP addresses from these subnets to devices in Cisco Packet Tracer and verify connectivity using ping between them.

5. A hand holding a notebook with writing

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

6. You are given three IP addresses: 10.1.1.1, 172.16.5.10, and 192.168.1.5.

Task: Identify the class of each IP address (Class A, B, or C). What is the default subnet mask for each class?

Provide the range of IP addresses for each class.

IP Address Class Default Subnet Mask Class Range

10.1.1.1 Class A 255.0.0.0 1.0.0.0 – 126.255.255.255

172.16.5.10 Class B 255.255.0.0 128.0.0.0 – 191.255.255.255

192.168.1.5 Class 255.255.255.0 192.0.0.0 – 223.255.255.255