Module Code & Module Title

Level 5-CT5052NP & Network Operating System

Assessment Type

Extra Credit Lab: IP Lab

Semester

2024/25 Spring/Autumn

Student Name: Arij Lamichhane

London Met ID: 22085885

Assignment Due Date: 5 January 2025

Assignment Submission Date: 5 January 2025

Submitted To: Mr. Prashant Adhikari

I confirm that I understand my proposal needs to be submitted online via College's MST PORTAL under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Introduction:

By dynamically allocating IP addresses to networked devices, the Dynamic Host Configuration Protocol (DHCP) streamlines network administration. Devices can now easily join a network since manual configuration is no longer necessary. The OSI model, IP addressing ideas, and the DHCP process are thoroughly examined in this paper. Wireshark data is used to show the DHCP exchange and its elements. Furthermore, examined is the procedure for acquiring IP, MAC addresses, and gateway configurations for online connection, highlighting the need of DHCP for effective network operations.

1.What is the OSI Model? How many layers are there in the OSI Model/ What is the function of each layer?

Ans: The Open Systems interconnection model (OSI) model is a conceptual framework that

Standardizes the functions of a telecommunication or computing system into seven layers. This model assists in understanding and designing network protocols to facilitate working together without being specially configured to do so between different systems and networks.

The seven layers of the OSI model are:

1.Physical Layer: This layer is responsible for the transmission and reception of unstructured raw data between a device and a physical transmission medium. It defines hardware components like equipment, cabling, and wiring.

2.Data Link Layer: Provides node to node data transfer a link between two directly connected nodes. It detects and possibly corrects errors that may occur in the physical layer.

3.Network Layer: Handles the routing of data by determining the best physical path for the data to reach its destination. It manages logical addressing and translates logical addresses into physical addresses.

4.Transport Layer: Ensures complete data transfer. It provides error detection and recovery, as well as flow control to ensure that data is sent at a rate that matches the receiving device's capacity.

5. Session Layer: Manages sessions between applications. It establishes, manages, and terminates the connection between local and remote applications.

6. Presentation Layer: Translates data between the application layer and the network. It ensures that data is usable format and is where data encryption occurs.

7.Application Layer: Server as the window for users and application processes to access network services. It provides network services directly to end-user applications.

2.What is an IP Address? How many bits does an IP Address have (IPV4)? Define network bits, host bits, subnet address, and subnet mask. Provide an example.

Ans: An internet Protocol (IP) address is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IPV4 address is a 32-bit number, typically expressed in dotted decimal notation, divided into four 8-bit octets.

Definitions:

- Network Bits: The portion of the IP address that identifies the specific network on which a device resides.

- Host Bits: The portion of the IP address that identifies the specific device (or host) on the network.

- Subnet Adress: A subdivision of an IP network that creates multiple distinct networks within a single network address space.

- Subnet Mask: A 32-bit number that masks an IP address and divides the IP address into network and host portions. It is written in the same notation as an IP address.

Example:

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0

3. What is Default Gateway?

Ans: A Network node (typically a router) that serves as an access point to other networks. It facilitates communication between different networks. It allows devices on separate networks to connect and communicate with one another seamlessly. It acts as the exit point from local network. Example: 192.168.1.1 in a home network.

The primary function of default gateway is to act as forwarding host when no specific route for the destination Internet Protocol (IP) address is specified. Additionally, it can serve as an intermediary between multiple devices connected to a shared subnet.

4.How does a computer on a network get the IP address, subnet mask, and default gateway?

Ans: A computer obtains its IP address, Subnet mask, and default gateway through the Dynamic Host Configuration Protocol (DHCP). The process involves:

1.DHCP Discover: The client broadcast message to identify available DHCP servers.

2.DHCP Offer: A DHCP server responds with an offer, including an IP address, subnet mask, default gateway, and lease duration.

3.DHCP Request: The client replies, indicating acceptance of the parameters offered.

4. DHCP Acknowledgement: The server sends a final acknowledgement, and the client configures its network interface with the provided settings.

5. Show a DHCP Exchange on Wireshark and Explain the Process.

Ans: Below is the process of DHCP Exchange on Wireshark with explanation.

1.DHCP Release (Packet 1389)

Time: 57.782089

Source: 192.168.18.41 (Client)

Destination: 192.168.18.1 (Server)

Length: 342 bytes

- computer actively releases its current IP address
- Usually when you run ipconfig /release or disconnect from network
- Tells the DHCP server this IP is now available for other clients

2.DHCP Discover (Packet 1410)

Time: 65.998499

Source: 0.0.0.0 (Client has no IP)

Destination: 255.255.255.255 (Broadcast)

Length: 342 bytes

Transaction ID: 0x873c35eb

- Client broadcasts "Hey, I need an IP address!"
- Uses 0.0.0.0 because it has no IP yet
- Broadcast ensures all DHCP servers can hear the request

3.DHCP Offer (Packet 1474)

Time: 68.087240

Source: 192.168.18.1 (DHCP Server)

Destination: 192.168.18.41

Length: 590 bytes

- Server responds with "Here's an IP you can use"

Includes:

- Offered IP address
- Subnet mask
- Default gateway
- DNS servers
- Lease duration

4.DHCP Request (Packet 1475)

Time: 68.089049

Source: 0.0.0.0 (Client)

Destination: 255.255.255.255 (Broadcast)

Length: 356 bytes

- Client broadcasts "Yes, I want that IP!"
- Still broadcasts in case multiple DHCP servers responded
- Uses same Transaction ID to match the offer

5.DHCP ACK (Packet 1480)

Time: 68.194058

Source: 192.168.18.1 (Server)

Destination: 192.168.18.41

Length: 590 bytes

- Server says "OK, it's yours!"
- Confirms all configuration details
- Client can now use the IP address
- Lease timer starts

Key Details in Your Capture:

- Total exchange took about 10 seconds (57s to 68s)
- Local network is using 192.168.18.x addressing
- DHCP server is at 192.168.18.1 (typical for home routers)
- Transaction ID 0x873c35eb remains consistent through the process
- Packet sizes vary (342-590 bytes) depending on message type and included options

Conclusion:

Using Wireshark packet captures, this paper illustrates the crucial role that DHCP plays in automating IP address management. Network communication requires the OSI model, IP addressing, and associated procedures. While DNS and ARP protocols facilitate seamless data flow over the internet, DHCP's effectiveness guarantees that devices connect with ease. When combined, these technologies highlight how crucial reliable network protocols are to contemporary computing.

Reference:

RFC 2131 - Dynamic Host Configuration Protocol (ietf.org)

Wireshark Documentation (wireshark.org)

Open Systems Interconnection Model - ISO (iso.org)