**SPIDER SOFTWARE TASK-2**

**COMPUTER NETWORKING**

**LEVEL - 1**

1. **Transmission Control Protocol (TCP):**

TCP is a network protocol that ensures reliable data transmission between devices over a network. It establishes a connection before data is sent. It ensures that there is no data loss during the transmission. It

adjusts the rate of data transmission based on network traffic conditions. It is used to transfer files, emails and also used in in web browsing.

1. **User Datagram Protocol (UDP):**

UDP is a connectionless protocol that sends data packets without establishing a connection between the host and the receiver. Each packet that is sent is independent, with no need to track connections. It does not guarantee complete data transfer or error checking. It is used at places where faster communication is required and complete data transfer is not cared about.

Differences between TCP and UDP:

TCP is a connection-oriented protocol that ensures reliable data transmission through error checking, flow control, and acknowledgment of packets. It establishes a connection between the sender and receiver before data transfer begins, making it suitable for applications where complete data transfer is crucial. In contrast, UDP is a connectionless protocol that sends data packets without establishing a connection and without proper delivery, order, or error correction.

1. **Internet Control Message Protocol (ICMP):**

The Internet Control Message Protocol (ICMP) is a network security protocol used for error reporting, diagnostics within networks. It serves as a crucial tool for network management and troubleshooting. It is used by network devices like routers for sending error messages and operations information. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.

1. **Hypertext Transfer Protocol (HTTP/HTTPS):**

HTTP is the protocol used for transferring web pages on the internet. HTTPS is the secure version of HTTP, using TLS/SSL for encryption.

**5.Internet Protocol (IP):**

Internet Protocol is a protocol through which data is sent from one host to another over the internet. It is used for addressing and routing data packets so that they can reach their destination. IP provides the addressing mechanism that allows each device on a network to be uniquely identified. IP works in conjunction with higher level protocols like TCP and UDP to ensure data is delivered correctly, handling tasks such as packet fragmentation, reassembly, and error checking.

**6.File Transfer Protocol (FTP):**

FTP is used for transferring files between a client and server over a network. It allows users to download files, programs and web pages available in other services.

**7.Simple Mail Transfer Protocol (SMTP):**

Simple Mail Transfer Protocol (SMTP) is a network protocol used for sending emails across the Internet. It follows a store and forward model, where emails are temporarily stored on intermediate servers before reaching their final destination.

**8.Post Office Protocol (POP3):**

POP3 is a network protocol that enables a server to retrieve emails from a remote server and download them to the local device. Whenever the client connects to the server via TCP, it automatically downloads all the new messages to it, making them accessible to the user both online and off-line.

Difference between SMTP and POP3:

SMTP is responsible for sending outgoing emails from a sender's email client or server to the receiver's email server. It initiates the email transfer process by connecting to the receiver's mail server and delivering the email. In contrast, POP3 is used by email clients to retrieve emails from a mail server to a local device, mainly downloading and deleting emails from the server.

**9.Simple Network Management Protocol (SNMP):**

SNMP is an application layer protocol that’s used to collect management information from devices such as computers, routers, switchers, firewalls and printers. Network monitoring platforms often use SNMP to monitor the performance and status of devices throughout a network in real time.

**10.Dynamic Host Configuration Protocol (DHCP):**

DHCP is a network management protocol used to automatically assign IP addresses and other network configuration parameters (subnet mask, default gateway, DNS servers) to devices on a network. DHCP prevents manually configuring each device on a network and supports dynamic IP address allocation and network reconfiguration as devices connect and disconnect from the network.

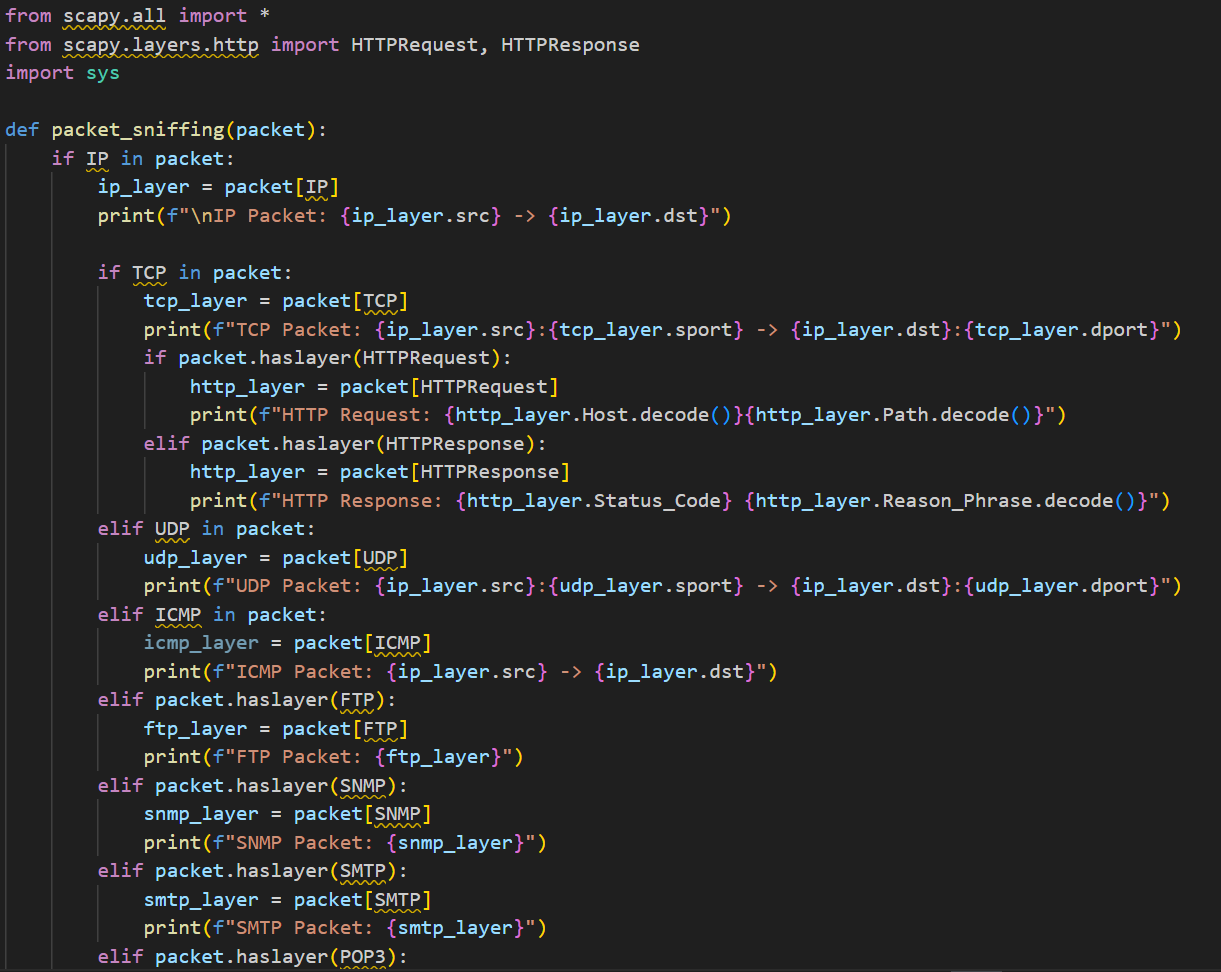
**11.Address Resolution Protocol (ARP):**

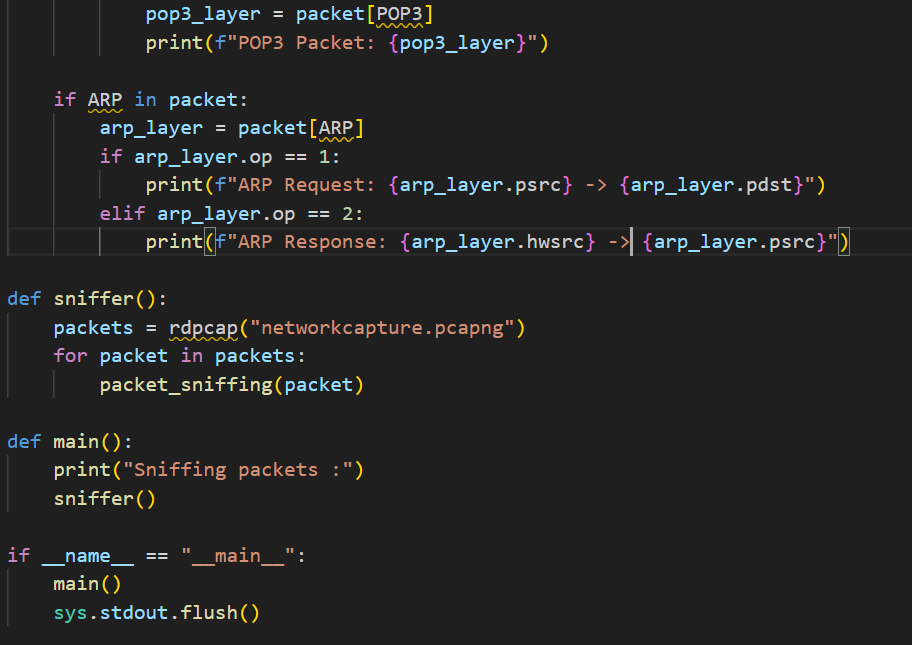
ARP is a fundamental networking protocol used to map IP addresses to MAC addresses within a local network. When a device wants to communicate with another device on the same subnet, it uses ARP to discover the MAC address associated with the IP address of the destination. ARP operates at the data link layer (Layer 2) of the OSI model and is essential for the proper functioning of ethernet networks.

**12.Telnet:**

Telnet is a network protocol and application that allows a user to remotely access and interact with another computer or device over a network. During telnet operation, whatever is performed on the connected computer will be displayed in the computer that provides the connection. Telnet operates on a client-server principle.

**PACKET SNIFFING TOOL:**





**LEVEL – 2**

Setting up the network topology and testing the tool’s ability to capture packets in the GNS3 environment is done and the results are present in the video attached.