Detailed Study on Basic Networking and Wireshark

1. IP Address

An IP Address (Internet Protocol Address) is a unique numerical identifier assigned to every device connected to a network. It helps devices locate and communicate with each other over the internet or local network. There are two main versions: IPv4 and IPv6.

2. MAC Address

A MAC Address (Media Access Control Address) is a permanent hardware address assigned to a network interface card. It is used for communication within the same local network and cannot be changed easily.

3. DNS (Domain Name System)

DNS is a system that translates human-readable domain names into IP addresses. When a user enters a website name in a browser, DNS servers help find the correct IP address of that website.

4. TCP (Transmission Control Protocol)

TCP is a connection-oriented protocol that ensures reliable data transmission. It checks for errors, retransmits lost packets, and ensures data arrives in the correct order.

5. UDP (User Datagram Protocol)

UDP is a connectionless protocol used for fast communication. It does not guarantee delivery or order of packets, making it suitable for streaming and gaming.

6. Wireshark Tool

Wireshark is a network packet analyzer that captures and displays network traffic in real time. It helps in learning networking concepts, troubleshooting network issues, and analyzing security threats.

7. Packet Capture

Packet capture is the process of collecting data packets traveling through a network interface. Each packet contains source, destination, protocol, and data information.

8. Packet Filtering

Packet filtering in Wireshark allows users to display specific packets based on protocols or conditions. Common filters include HTTP, DNS, and TCP.

9. TCP Three-Way Handshake

The TCP three-way handshake establishes a connection between client and server. It consists of SYN, SYN-ACK, and ACK packets, ensuring both sides are ready to communicate.

10. Plain-text Traffic

Plain-text traffic sends information in readable format. Protocols like HTTP transmit data without encryption, making them insecure.

11. Encrypted Traffic

Encrypted traffic protects data using encryption techniques. Protocols like HTTPS secure communication by hiding sensitive information.

12. DNS Queries

A DNS query is a request sent by a client to a DNS server asking for the IP address of a domain name. Wireshark can be used to observe these queries.

13. PCAP Files

PCAP files store captured network packets for later analysis. They are useful for documentation, learning, and forensic investigations.

Conclusion

This practical study helps in understanding how network communication works. Wireshark plays an important role in visualizing real-time network data and improving networking knowledge.