CN

Network Devices

- Bridge

A device that connects and filters traffic between two network segments, often within the same local area network (LAN).

-Switch

A device that connects multiple devices within a LAN, directing data to specific devices by using MAC addresses.

-Router

A device that directs data between different networks, using IP addresses to determine the best path for data.

-Gateway

A device that acts as a translator between networks with different protocols, enabling communication across disparate networks.

-Access Point

A device that allows wireless devices to connect to a wired network, typically within a Wi-Fi network.

Topologies

1] Star Topology:

Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer. The central computer is known as a server, and the peripheral devices attached to the server are known as clients. Coaxial cable or RJ-45 cables are used to connect the computers. Hubs or Switches are mainly used as connection devices in a physical star topology. Star topology is the most popular topology in network implementation.

Adv	Dis-Adv
-Efficient troubleshooting -Network control -Limited failure -Familiar technology	-A Central point of failure -Cable

-Easily expandable -Cost effective -High data speeds	

Application:

-Home Networks

-Offices and Small Businesses

-Data Centres

2] Ring Topology:

Ring topology is like a bus topology, but with connected ends. The node that receives the message from the previous computer will retransmit to the next node. The data flows in one direction, i.e., it is unidirectional. The data in a ring topology flow in a clockwise direction.

Adv	Dis-Adv
-Network Management -Product availability -Cost -Reliable	-Difficult troubleshooting -Failure -Reconfiguration difficult -Delay

Application:

-Fiber Distributed Data Interface (FDDI)

-Industrial Networks

3] Bus Topology

The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable. Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable. When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not. The configuration of a bus topology is quite simpler as compared to other topologies.

Adv	Dis-Adv
-Low-cost cable	-Difficult troubleshooting

-Familiar technology -Moderate data speeds -Limited failure	-Extensive cabling -Attenuation -Signal Interference

Application:

-Older Ethernet Networks

-Broadcast Networks

-Wireless Networks

4] Mesh Topology

Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections. There are multiple paths from one computer to another computer. It does not contain the switch, hub or any central computer which acts as a central point of communication. The Internet is an example of the mesh topology. Mesh topology is mainly used for wireless networks.

Adv	Dis-Adv
-Reliable -Fast Communication -Easy Reconfiguration	-Cost -Management -Efficiency

Application:

-Internet backbone

-Wireless mesh network (WMN)

-Military Communication

Types of Networks

LAN – Local Area Network

It is designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

MAN - Metropolitan Area Network

It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.

Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.

PAN-Personal Area Network

PAN stands for personal area network, a network covering a very small area, usually a small room. PAN's can be wired or wireless. The best known wireless PAN network technology is Bluetooth, and the most popular wired PAN is USB. Wi-Fi also serves as a PAN technology, since Wi-Fi is also used over a small area.

Ad-hoc Networks

A wireless **ad hoc network** (WANET) or MANET is a decentralized type of wireless **network**. The **network** is **ad hoc** because it does not rely on a pre existing infrastructure, such as routers in wired **networks** or access points in managed (infrastructure) wireless **networks**.

Transmission Medium

Wired/Guided Media	Wireless/Unguided Media
-Twisted pair cable -Coaxial Cable -Fibre Optic Cable	-Radio waves -Microwaves -Infrared waves

OSI Model

OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

Layers	Description	Protocols
Physical layer	Defines the physical medium for data transmission, managing bit-level transmission across a network.	USB, IEEE 802.11 (Wi-Fi), Bluetooth, Ethernet, DSL, Hubs
Data Link	Ensures reliable node-to-node data transfer with error detection and correction.	Ethernet, PPP, HDLC, Frame Relay, ATM, ARP, MPLS, STP, LLDP
Network	Determines the best physical path for data, handling logical addressing, routing, and packet forwarding.	IP (IPv4/IPv6), ICMP, IGMP, OSPF, RIP
Transport	Provides reliable data transfer through flow control, error checking, and data segmentation	TCP, UDP, SCTP, DCCP, SPX
Session	Manages sessions or connections between applications, ensuring data is properly synchronized and maintained	NetBIOS, PPTP, SAP, RPC
Presentation	Translates data between application and network formats, handling encryption, compression, and data encoding	SSL/TLS, JPEG, MPEG, GIF, ASCII, EBCDIC, XDR
Application	Interfaces directly with end-user applications to provide services like email, file transfer, and web browsing.	HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, DNS, Telnet, SSH, NFS, TFTP

Sub-netting

Subnetting is the process of dividing a large network into smaller, more manageable sub-networks, or subnets. This improves network performance and security by limiting broadcast traffic within each subnet and providing better control over IP addressing. Subnetting allows efficient use of IP addresses and helps to organize a network into logical segments, each with its own range of IP addresses.

Class	Range	Subnet Mask	Purpose
A	1 – 126	255.0.0.0	Large network
B	128 – 191	255.255.0.0	Medium network
C	192 – 223	255.255.255.0	Small network
D	224 – 239	N/A	Multicasting
E	240 - 255	N/A	Experimental/future use

Socket Programming

A **socket** is an endpoint in network communication, a combination of an IP address and port number that allows data exchange between devices over a network. Sockets serve as the connecting point for applications on different machines or within the same machine to communicate using protocols like TCP or UDP.

Socket programming is the process of writing code to enable communication between devices over a network using sockets. It allows developers to create applications that send and receive data over networks (e.g., client-server applications).

TCP Client: This is the device or program that initiates the connection by sending a request to the TCP server.

TCP Server: This is the device or program that listens for incoming connection requests from clients on a specific port.

UDP Client: The client sends data (in the form of packets, called datagrams) to a UDP server without establishing a direct connection.

UDP Server: The UDP server listens for incoming datagrams on a specified port but does not establish a connection with the client. It receives packets as they arrive and processes them, but it does not confirm receipt or manage retransmissions if packets are lost.

UDP is commonly used for applications where speed is prioritized over reliability, such as live video streaming, online gaming

Protocols

1. HTTP (HyperText Transfer Protocol)

-A protocol used for transferring web pages over the internet.

-Facilitates the retrieval of resources (HTML files, images, etc.) from a web server.

-Used in web browsing; it is stateless and enables communication between web browsers and servers.

2. HTTPS (HyperText Transfer Protocol Secure)

-A secure version of HTTP.

-Encrypts data between the web server and client using SSL/TLS to prevent eavesdropping.

-Used in secure online transactions (e.g., banking, shopping) to protect sensitive data.

3. FTP (File Transfer Protocol)

-A protocol for transferring files between computers over a network.

-Allows users to upload and download files from remote servers.

-Used in file sharing, website management, and backup services. FTP can be insecure unless encrypted (FTPS).

4. RIP (Routing Information Protocol)

-A distance-vector routing protocol.

-Helps routers determine the best path to route data by counting the number of hops (maximum 15).

-Used in small to medium-sized networks, but has limitations like slower convergence and a maximum hop count.

5. OSPF (Open Shortest Path First)

-A link-state routing protocol.

-Helps routers exchange routing information, selecting the most efficient path using a shortest path first algorithm.

-Used in larger networks as it scales better than RIP, supports hierarchical routing, and converges quickly.

6. BGP (Border Gateway Protocol)

-A path vector protocol used for routing between autonomous systems (AS).

-Determines the best path for data between different networks on the internet.

-Used by internet service providers (ISPs) and large organizations for inter-domain routing and managing internet traffic.

7. DHCP (Dynamic Host Configuration Protocol)

-A protocol that automatically assigns IP addresses to devices on a network.

-Dynamically provides IP addresses, subnet masks, gateways, and other network configuration to clients.

-Used in home and enterprise networks to simplify IP address management and reduce configuration errors.

8. DNS (Domain Name System)

-A system for translating human-readable domain names into IP addresses.

-Resolves domain names (e.g., www.example.com) to their corresponding IP addresses for network communication.

-Used across the internet to enable easy access to websites and services by name instead of IP address.

9. SSL (Secure Sockets Layer)

-A protocol for encrypting data between a client and server.

-Provides a secure connection by encrypting the data to prevent interception.

-Used for secure web browsing (HTTPS) and online transactions, although now largely replaced by TLS.

10. TCP (Transmission Control Protocol)

-A connection-oriented protocol in the transport layer.

-Ensures reliable, ordered delivery of data between devices, with error correction and retransmission.

-Used for applications requiring reliable data transfer, like web browsing, email, and file transfer.

11. UDP (User Datagram Protocol)

-A connectionless, unreliable transport layer protocol.

-Sends data in packets without ensuring delivery or order, providing faster communication.

-Used in real-time applications like video streaming, online gaming, and VoIP where speed is more critical than reliability.

12. POP3 (Post Office Protocol version 3)

-A protocol for retrieving email from a mail server.

-Downloads emails to a client, removing them from the server (unless configured to leave a copy).

-Used in email clients like Outlook or Thunderbird for downloading emails for offline access.

13. IMAP (Internet Message Access Protocol)

-A protocol for retrieving emails from a server.

-Allows emails to be stored on the server and accessed from multiple devices without removing them.

-Used in modern email systems where users want access to their emails from multiple devices.

14. SMTP (Simple Mail Transfer Protocol)

-A protocol for sending emails between servers.

-Defines how email messages are sent from the sender’s client to the email server and from server to server.

-Used by mail servers to send and relay emails across the internet.

15. SNMP (Simple Network Management Protocol)

-A protocol for managing and monitoring network devices.

-Collects data from devices like routers, switches, and servers for network performance management.

-Used in network management systems for monitoring the health and status of devices.

16. TELNET (Telecommunication Network)

-A text-based protocol used to remotely access a device.

-Provides terminal emulation to control remote devices via command-line interface.

-Used in legacy systems and network troubleshooting, though largely replaced by more secure protocols like SSH.

Wireshark

Wireshark is an open-source network protocol analyzer used for capturing and analyzing network traffic in real-time. It allows users to see what's happening on a network at a microscopic level, enabling detailed inspection of packets and data exchanged between devices. It is widely used by network engineers, security experts, and developers to monitor, analyze, and debug network traffic.

13. To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

->

What is the purpose of using Wireshark in this experiment?

Wireshark is used to capture and analyze the network packets transmitted between the client (web browser) and the server when visiting an SSL-secured website. By inspecting these packets, we can study the encryption process, how SSL works, and the handshakes involved in establishing a secure connection.

What do you expect to observe in Wireshark while capturing packets from an SSL-secured website?

In Wireshark, the captured packets should show an encrypted communication between the client and the server. Initially, you'll observe the **SSL/TLS handshake**, which includes the exchange of certificates, public keys, and cipher suites. After the handshake, the data packets will be encrypted, and the content of the communication will not be visible without the decryption keys.

What is the SSL handshake?

The SSL handshake is a process that occurs when a secure connection is established between a client and a server. During the handshake, the client and server exchange information, such as:

1.Cipher Suite Selection: The encryption algorithms to be used.

2.Server Certificate: The server sends its SSL certificate to authenticate itself.

3.Session Keys: Both parties agree on symmetric session keys to encrypt the data.

4.The exchange ensures that both parties can securely communicate.

What is the difference between SSL and TLS?

TLS (Transport Layer Security) is the successor to SSL. TLS is more secure and efficient than SSL and is used in modern applications. Although the terms "SSL" and "TLS" are often used interchangeably, SSL is now considered outdated and insecure, while TLS is the recommended protocol for secure communication.

Can SSL be used for any type of communication?

SSL is primarily used for securing web traffic (HTTP), but it can also be used to secure other types of communication such as email (SMTP, IMAP, POP3), FTP, and more. It is widely used in any application that requires secure data transmission.

14. Capture packets using Wireshark and accomplish the following and

save the output in file:

a. Capture all TCP traffic to/from Facebook, during the time when you log in to your

Facebook account. Capture all HTTP traffic to/from Facebook (other website), when you

log in to your Facebook account

b. Write a DISPLAY filter expression to count all TCP packets captured under item #1) that have the flags SYN, PSH, and RST set. Show the fraction of packets that had each flag set.

c. Count how many TCP packets you received from / sent to Facebook (other website), and how many of each were also HTTP packets.

->

1. What is the purpose of capturing TCP and HTTP traffic in Wireshark?

Capturing TCP and HTTP traffic allows us to analyze the network communication between the client (user's browser) and the server (Facebook or other websites). By monitoring the packets, we can study the network protocols involved (TCP for reliable communication and HTTP for web traffic) during user actions like logging into Facebook.

2. How do you capture TCP traffic to/from Facebook in Wireshark?

To capture TCP traffic to/from Facebook, you can use the Wireshark capture filter tcp and host facebook.com. This filter ensures that only TCP packets related to Facebook are captured. To log in to Facebook and capture the traffic during the session, you would start the capture session before logging in and stop it after the login process.

3. What does the capture filter tcp and host facebook.com do?

The filter tcp and host facebook.com captures only the TCP traffic between the client and the server at the IP address of facebook.com. The "tcp" ensures that only TCP packets are captured, and "host" limits the capture to traffic to or from the specific website.

4. How would you capture HTTP traffic to/from Facebook when logging in to your Facebook account?

To capture HTTP traffic, you can use the display filter http and host facebook.com. Since HTTP operates over TCP port 80 (or HTTPS over port 443), the filter ensures that you capture HTTP traffic (not HTTPS, which is encrypted and cannot be inspected without special configurations) to/from Facebook.

5. How would you save the captured output in a file?

In Wireshark, you can save the captured packets by going to **File > Save As** and choosing a location and file format (such as .pcap or .pcapng). This allows you to store the captured data for later analysis.

6. What is the role of the DISPLAY filter in Wireshark?

A DISPLAY filter in Wireshark is used to show or hide specific packets after they have been captured. Unlike capture filters, which limit what packets are captured, display filters allow you to filter and analyze the already captured traffic based on specific criteria such as protocol type, IP address, flags, etc.

7. What is the display filter expression for counting TCP packets with SYN, PSH, and RST flags set?

The display filter expression to count TCP packets with SYN, PSH, and RST flags set would be:

Copy code

tcp.flags.syn == 1 and tcp.flags.psh == 1 and tcp.flags.rst == 1

This filter expression captures packets where the SYN, PSH, and RST flags are all set. You can apply it in the Wireshark display filter bar to see only those packets.

8. How would you show the fraction of packets that had each flag (SYN, PSH, RST) set in Wireshark?

After applying the display filter for each individual flag, you can use the **Statistics > Packet Lengths** or **Statistics > TCP Stream Graphs** options to analyze the distribution of packets. You can manually count the occurrences of each flag and then calculate the fraction (e.g., total packets with each flag divided by the total captured packets).

9. How do you count the total number of TCP packets captured?

In Wireshark, you can count the total number of TCP packets by going to **Statistics > Protocol Hierarchy**. This will give you a breakdown of the different protocols present in the capture, including TCP. Alternatively, you can use the display filter tcp and then look at the packet count displayed at the bottom of the Wireshark window.

10. How do you count how many of the TCP packets are HTTP packets?

To count how many of the TCP packets are HTTP packets, you can use the display filter http to filter out the HTTP packets from the total TCP packets. Then, use **Statistics > Protocol Hierarchy** to get the number of HTTP packets specifically.

11. What is the significance of the SYN, PSH, and RST flags in TCP packets?

The SYN, PSH, and RST flags in TCP packets are used for specific control purposes:

- **SYN (Synchronize)**: Used to initiate a connection in the TCP handshake.
- **PSH (Push)**: Instructs the receiver to push the buffered data to the application immediately.
- **RST (Reset)**: Used to reset a connection due to an error or abnormal condition.

12. Why is the PSH flag important in HTTP communication?

The PSH flag is often used in HTTP communication to signal that data should be delivered to the application layer immediately. This is important for ensuring that HTTP requests and responses are handled promptly without unnecessary buffering.

13. Why might the RST flag be set in TCP packets during your capture?

The RST flag is typically set when a connection is reset, either due to an error or if the server or client decides to abort the connection. It can be seen in cases of interrupted communication or failed connections.

14. What are the challenges you may face when capturing encrypted traffic (HTTPS) in Wireshark?

Since HTTPS traffic is encrypted, you cannot directly view the content of the packets in Wireshark. To capture and analyze HTTPS traffic, you would need to have access to the SSL keys or use tools like SSL decryption (if configured) or SSL proxying tools, which allow decrypting the encrypted traffic.

15. How would you filter out non-TCP traffic in your capture?

To filter out non-TCP traffic, you can apply a capture or display filter like tcp. This will ensure that only TCP packets are displayed or captured, removing other protocols such as UDP, ICMP, etc., from the analysis.

16. How do you differentiate between regular TCP packets and HTTP packets in Wireshark?

HTTP packets are a subset of TCP packets, specifically using port 80 (for HTTP) or 443 (for HTTPS). In Wireshark, you can use the filter http to view only HTTP traffic. Additionally, in the packet details, the HTTP protocol is displayed explicitly when the packet contains HTTP headers or data.

17. Why is it important to capture HTTP traffic to/from Facebook or other websites during login?

Capturing HTTP traffic during login allows us to observe the details of the authentication process, such as the exchange of credentials, cookies, and session tokens. It also helps in understanding how secure the login process is and if sensitive data is transmitted in plaintext (in case of HTTP instead of HTTPS).

18. What can you learn about network performance by analyzing TCP and HTTP traffic?

By analyzing TCP traffic, we can learn about the reliability of the connection, the presence of retransmissions, and the efficiency of data transfer. HTTP traffic analysis can show how quickly resources are loaded, how HTTP requests and responses are handled, and how long the login process takes.