**NAME:JOHN ONDIMU  
REG NUMBER: BIT/0069/21  
COURSE CODE: BIT223**

**1.Functions of protocols:**

i) DNS (Domain Name System): Resolves domain names to IP addresses.

ii) FTP (File Transfer Protocol): Facilitates the transfer of files between a client and a server over a network.

iii) HTTP (Hypertext Transfer Protocol): Allows for the transfer of hypertext requests and information on the World Wide Web.

**2.Difference between TCP and UDP protocols:**

TCP (Transmission Control Protocol) provides reliable, connection-oriented communication, ensuring that all data packets arrive intact and in order. It includes mechanisms for error detection, flow control, and congestion control. Examples include web browsing and email.

UDP (User Datagram Protocol) provides unreliable, connectionless communication, where data packets may be lost or arrive out of order. It offers low overhead and is used for applications where speed is more critical than reliability, such as video streaming and online gaming.

3.Network vulnerabilities on a LAN:

( i) Unauthorized Access: Weak passwords or misconfigured access controls can allow unauthorized users to gain access to the network.

(ii) Malware Attacks: Malicious software like viruses, worms, and Trojans can infect devices on the LAN, compromising security and causing damage.

( iii) Denial of Service (DoS) Attacks: Attackers may flood the network with excessive traffic, disrupting normal operations and rendering services unavailable.

(iv) Insider Threats: Authorized users with malicious intent can misuse their privileges to access sensitive information or disrupt network services.

**4.Explanation of IP addressing classes:**

i) Class B: Class B addresses use the first two octets to identify the network portion and the remaining two octets for hosts. They provide medium-sized networks with a large number of hosts.

ii) Class C: Class C addresses use the first three octets for network identification and the last octet for hosts. They are suitable for small networks with fewer hosts but offer a larger number of networks compared to Class B.

**5.Fields of an IP packet header:**

(i) Source IP Address: Specifies the sender's IP address.

(ii) Destination IP Address: Specifies the recipient's IP address.

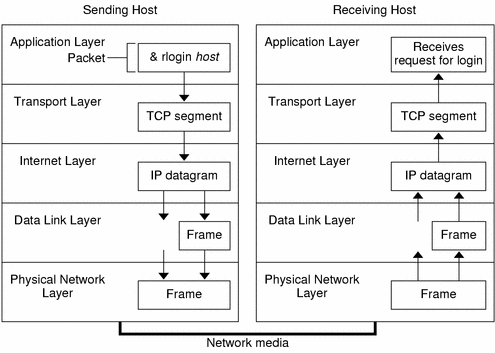
(iii) Protocol: Identifies the protocol used in the data portion of the packet (e.g., TCP, UDP).

(iv) Time-to-Live (TTL): Specifies the maximum number of hops (routers) the packet can traverse before being discarded.

**6.Network topologies**:

i) Hybrid Topology: Combination of two or more different basic network topologies, such as star and mesh. ii) Tree Topology: Hierarchical structure where nodes are arranged in a tree-like structure with a root node, branches, and leaf nodes.

**7. TCP/IP packet header:**



The TCP/IP packet header contains various fields that provide essential information for the transmission of data over a network using the Transmission Control Protocol (TCP) or Internet Protocol (IP).

(i)Source Port: This field indicates the port number of the sender's application or service.

(ii) Destination Port: Specifies the port number of the recipient's application or service.

(iii) Sequence Number: Used to order and reassemble the segments at the destination. It represents the byte in the data stream.

(iv) Acknowledgment Number: Indicates the next expected sequence number the sender of the segment is expecting to receive.

(v) Header Length: Specifies the length of the TCP header in 32-bit words. This field is necessary because the TCP header length can vary due to the presence of optional fields.

(vi)Checksum: Used for error detection. It ensures the integrity of the TCP header and data by calculating a checksum based on the contents of the packet.

(vii)Urgent Pointer: If the URG flag is set, this field specifies the offset from the sequence number indicating the last urgent data byte.

Data: This field contains the actual payload or data being transmitted.

**8.Default subnet masks:**

(i) 177.100.18.4 - Default subnet mask for Class B: 255.255.0.0

(ii) 119.18.45.0 - Default subnet mask for Class A: 255.0.0.0

(iii) 191.249.234.191 - Default subnet mask for Class B: 255.255.0.0

(iv) 223.23.223.109 - Default subnet mask for Class C: 255.255.255.0