**TCP (Transmission Control Protocol):**

TCP, an acronym for Transmission Control Protocol, represents a connection-oriented approach to network communication. It establishes a reliable and ordered delivery mechanism for data transmission across the internet. Suited for applications prioritizing high reliability, such as HTTP, FTP, and SMTP, TCP ensures that data transferred remains intact and arrives in the same order it was sent. It rearranges data packets in the specified order and implements flow control and error recovery mechanisms. However, this reliability comes at the cost of speed, as TCP's header size is larger at 20 bytes, and it requires a three-packet handshake to set up a socket connection. Despite its heavyweight nature, TCP serves as a cornerstone for critical network operations, offering absolute assurance of data integrity and delivery.

**UDP (User Datagram Protocol):**

UDP, short for User Datagram Protocol, embodies a connectionless approach to network communication. Unlike TCP, UDP does not establish continuous connections and operates without the overhead of reliability mechanisms. Instead, it focuses on fast and efficient transmission, making it ideal for applications like games and servers handling numerous small queries. While TCP guarantees data integrity and ordered delivery, UDP offers no such assurances, as it simply discards erroneous packets without attempting recovery. With a smaller header size of 8 bytes and no flow control or error recovery options, UDP prioritizes speed over reliability. Its lightweight design and stateless nature enable rapid data transmission, making it a preferred choice for time-sensitive applications where occasional packet loss is acceptable.

**How TCP and UDP work**

A TCP connection begins with a three-way handshake, a process where the client and server exchange synchronization (SYN) and acknowledgment (ACK) packets to establish a connection. Upon successful handshake completion, data transfer between the two parties can commence. Following the transmission of data, the connection is terminated by closing all established virtual circuits, ensuring the orderly conclusion of the communication session. This structured approach to connection establishment and termination is fundamental to the reliability and orderliness characteristic of TCP communications.

UDP employs a straightforward transmission model devoid of implicit handshaking dialogues to ensure reliability, ordering, or data integrity. Consequently, UDP offers an unreliable service where datagrams may arrive out of order, appear duplicated, or vanish without warning. UDP operates under the assumption that error checking and correction are unnecessary or handled at the application layer, thus circumventing the overhead associated with network interface-level processing. Unlike TCP, UDP supports packet broadcasts and multicasting, facilitating communication to multiple recipients simultaneously within a local network.

**Working of HTTP**

HTTP (Hypertext Transfer Protocol) is the foundation of data communication for the World Wide Web. It operates as a request-response protocol, where a client sends a request to a server, typically to retrieve a web page, and the server responds with the requested information. HTTP

operates over TCP (Transmission Control Protocol) port 80 by default and is stateless, meaning each request is independent and unrelated to previous requests..

**Working of HTTPS**

HTTPS (Hypertext Transfer Protocol Secure) is the secure version of HTTP, providing encrypted communication between a client and a server. HTTPS uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption to secure data transmission, ensuring privacy and integrity. It operates over TCP port 443 and is commonly used for secure transactions, such as online banking, e-commerce, and sensitive data transfer.

**Working of ICMP**

ICMP (Internet Control Message Protocol) is a supporting protocol used for diagnostic and control purposes within IP networks. ICMP messages are typically used for network management functions, such as error reporting, network troubleshooting, and congestion control. Common uses of ICMP include the "ping" command, which sends ICMP echo request messages to test network connectivity, and the "traceroute" command, which uses ICMP Time Exceeded messages to trace the route packets take across an IP network. ICMP operates at the network layer of the OSI model and is an integral part of the TCP/IP protocol suite.

**(Karan Tolambiya)**

**15-05-2025**