WEEK 3

The Transport and Application Layers

Quiz : The Five Layer Model

Physical layer. The physical device that interconnects the computers, their specification and how the signal is sent over this connection all comes in the physical layer.
• Data link layer. It is basically all about defining a common way to interpret these signals so that a device can communicate with each other. The most common protocol used here is Ethernet.
• Network layer. It allows different networks to communicate with each other using devices called routers
• Transport layer. The transport layer finds which client and server programs are supposed to get that data. The most common protocol used here is TCP/IP
. • MAC address. It is the address embedded in your hardware device (which will constitute a node of the network) permanently during its manufacturing.
• IP address. Unlike the Mac address, it is not permanent and not embedded on any hardware it is the address of the network it might change when you are at home connected with the wifi and different when you are connected with the railway station's wifi even the devices in both cases are the same.
• TCP port. A port is a 16-bit number that's used to direct traffic to specific services running on a networked computer. For example, port 80 is a port in which a web server listens for the web request.
• Checksum check. It is a method used to check the correctness of data during the transmission from one place to another.
• Routing table. It is a table in which the router device used to locate the destination IP address.
• TTL or time to leave is the value assigned in the TTL field which tells the data when to leave the network. Let's begin our journey. Suppose there are two networks Network A and Network B with network space 9.5.4.0/24 and 125.5.45.0/24 respectively. These two networks are connected to the same router with two network interfaces having IP 9.5.4.1(on network A) and 125.5.45.1(on network B). Now suppose a laptop or desktop which is a client in this case which is a part of the Network A having IP 9.5.4.23. Again assume that a server which is connected to Network B has IP address 125.5.45.34 and has a web server which is listening on port 80. Now our clients want to access a website whose IP address is 125.5.45.34. He opens any browser and enters this IP address in the search bar and hits enter. The browser then communicates with the local networking stack, which is the part OS responsible for managing networking functions. Browser tells that it wants to establish a TCP connection with the server 125.5.45.34 through port 80. Then the networking stack will check its own subnet and find that 125.5.45.34 is on another network so the client has to send data through its gateway which has the network interface of 9.5.4.1. Then the client checks its ARP table to find out what is the MAC address of its gateway. There are two possibilities: It finds the MAC address. It doesn't find the MAC address. If it didn't find it first it will get it through an ARP request and then continue as described below : Our client then makes an ARP request for IP 9.5.4.1 which is sent to all devices connected to the same network having the same hardware broadcast ID of all Fs. When the router on this network receives this request it knows that it is for me and sends an ARP response with its own MAC address

to the client(9.5.4.23). Here our client gets the MAC to address its gateway & ready to send the outbound packet. The operating system opens an ephemeral port suppose 51355 and opens a socket connecting the browser through this port. The networking stack starts to form TCP segments. It completes all the header fields like source port (51355) and destination port(80), sequence number filled, SYN flag is assigned to 1 and finally, the checksum is calculated and filled in the corresponding checksum field. This TCP segment is now given to the IP layer of the networking stack. Here IP header is filled with source IP 9.5.4.23 and destination IP 125.5.45.34, Time to leave or TTL is set to 64. Now the earlier formed TCP segment is put as payload for IP datagram. Then checksum is calculated and filled. Now comes the turn of Ethernet frame all its field like source and destination MAC address are filled & then IP datagram formed earlier is inserted as the payload of ethernet frame and checksum value is calculated and filled. Now it is ready to be sent across the physical layer.It is sent through the wire connecting the client and the switch. The switch receives it & it already knows where this MAc address is which finally sends all the entire Ethernet frame to the router. After this router does the following task: Receives frame Recognise address Calculate checksum Compare checksum Match detected Following these tasks, it then removes the Ethernet frame with the only datagram left & then performs a checksum again to ensure the correctness of data. It then searches its Routing table and finds the destination IP address125.5.45.34 is connected via the local network. Now it decrements the TTL field by one (now 63) calculate the new checksum and makes new IP datagram which is again encapsulated by ethernet frame with destination and source MAC address filled which is finally sent to the Network B where the switch identifies the destination mac address and send it to the server. This is the complete process of one-time connection with SYN field set to 1.This process is again repeated from the server side with ACK (Acknowledgement) set to one. These processes are repeated again and again until the data is completely sent and a connection is closed.

Quiz : The Transport and Application Layer

1) Ports 1024-49151 are known as **registered** ports.
2) The instantiation of an endpoint in a potential TCP connection is known as a **socket.**
3) HTTP is an example of a(n) **application** layer protocol**.**
4) Application layer data lives in the **Data payload** section of transport layer protocol.
5) The concept of taking traffic that's all aimed at the same node and delivering it to the proper receiving service is known as : **demultiplexing**
6) The transport layer handles multiplexing and demultiplexing through what type of device : **Ports**
7) A Transmission Control Protocol (TCP) connection is in working order and both sides can send each other data. What is the TCP socket state : **ESTABLISHED**
8) Which field in a Transmission Control Protocol (TCP) header is chosen from ephemeral ports - **Source Port**
9) Which field in a Transmission Control Protocol (TCP) header is not typically used in modern networking - **Checksum.**
10) How many bits are in the checksum field in a Transmission Control Protocol (TCP) header - **16**
11) Connection-oriented protocols protect against dropped data by forming connections and using what type of constant stream- **Acknowledgements.**

WEEK 3

12) How many Transmission Control Protocol (TCP) control flags are there -**5**
13) One side in a Transmission Control Protocol (TCP) connection has not been able to properly recover from a series of malformed segments. Which Transmission Control Protocol (TCP) flag will be used - **RST.**
14) Which Transmission Control Protocol (TCP) flag is used to make sure the receiving end knows how to examine the sequence number field - **SYN**