Follow the Packet:

Application Layer:

- When I (the source) click “send” on the messaging platform, the messaging application (mail applications, chat applications etc) prepares my message.
- They use an application protocol like HTTP or HTTPS to communicate with my friend’s machine.
- But we do not know the destination IP address, since humans (in this case, me) do not put the destination IP address in the message.
- This is where the DNS lookup or DNS resolution comes into play. It helps us find the destination IP address, which, in this case, is my German friend’s IP.
- The app checks its local cache to find if the destination IP address is stored there. If yes, it will add it to the HTTP header and send it down to the Transport Layer. If not, then it will contact a recursive DNS resolver, which is usually my ISP’s DNS server.
- The recursive DNS resolver will also check its own cache. If the domain is not there, it sends the DNS query on to the root DNS server (13 sets globally).
- The root DNS server doesn’t know the exact IP, but it will check for the TLD- Top Level Domain (example .com, .in etc) and point to the TLD DNS server.
- The resolver then queries the Top-Level Domain (TLD) server for the destination IP. It gives the resolver the IP of the authoritative name server for that domain.
- Finally, the DNS query gets the final answer from the authoritative DNS server. For example- 172.217.22.14 is my final destination IP address.
- Now, since the DNS is resolved, the application asks the OS to create a socket, which acts as a network endpoint. Sockets consist of an IP address along with a port number.
- A socket is created on the source and the receiver’s side, ready for connection.

Transport Layer:

- Since now the device knows where to send the data, the problem is how to send the data.
- There are two main ways data can be transmitted: TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
- If it uses TCP, first a 3-way handshake occurs to establish a connection. A SYN segment goes from my side to the server. The server sends back its own SYN segment along with the acknowledgement (ACK) for the SYN segment I had sent. To establish a connection, acknowledgement (ACK) for the SYN the server had sent is given to the server from my side. This ensures that the communication flow is both ways and the server and client are ready to send/receive data.
- It can also be sent through UDP, which is a connectionless, slightly unreliable but faster network protocol. It does not establish a persistent connection or perform handshakes, it just sends the segments directly.
- After TCP and UDP are performed, each segment is sent to the Network Layer.

Network Layer:

- At this level, each TCP/UDP segment is converted into an IP packet.
- Each IP packet has: Source IP, Destination IP and other header information.
- Once the transport layer sends its segments to the network layer, my computer sends the packet to the default gateway, which in most cases, is the router.
- The router replaces my private IP address with the public IP assigned to it by the ISP. This allows multiple devices on the network to have the same public common IP address. This technique is called NAT, which stands for Network Address Translation.
- Then, my data packet enters the ISP's internal routers. These routers determine the next hop using routing tables.
- Once the packet leaves the ISP's domain, it moves across multiple Autonomous Systems (AS). An Autonomous System is a network under a single administrative control that uses a common routing policy.
- Routers between different ASes route information using BGP (Border Gateway Patrol). It helps decide the best path to each destination network based on a set of policies.

- BGP ensures that my packet follows the most efficient path across the world to reach the destination.

Data Link Layer:

- It defines how data is formatted for transmission over the local network.
- Data packets are converted into frames here, with the MAC (Media Access Control) address of my device and my router.
- When travelling across different ISP's, the corresponding MAC address changes at every hop.

Physical Layer:

- Converts digital signals into electrical, radio or light signals.]
- These signals may pass through repeaters, switches, and routers to maintain signal strength.

Reverse Path:

- When my friend receives the data, they send back a response packet back to my IP address.
- A similar process to what I have mentioned above occurs again, this time using the source IP as destination IP and vice versa.
- Note that routers do not use the same path they sent the original message from. Instead, they use routing tables, which may be different from the original path.
- The application displays the reply.

Routing in ISP vs Autonomous Systems:

- They both basically use a different set of protocols.
- For example, Intra-AS routing uses Interior Gateway Protocols (IGPs) and Inter-AS routing uses Border Gateway Protocol.

The effect of congestion or packet loss:

- If the channel is congested and the routers are overloaded, packets may be dropped (packet loss) or sometimes errors appear in the data.
- TCP detects packet loss and retransmits the lost packet.

How HTTPS modifies or secures the exchange:

- HTTPS is just regular HTTP running over a secure TLS layer that encrypts and authenticates communication before any data is exchanged.
- After the TCP connection, the client and server perform a TLS handshake: exchanging certificates and generating a shared encryption key.
- Encryption: All HTTP requests and responses are encrypted using symmetric encryption or asymmetric encryption. There are multiple encryption and decryption algorithms.
- Secure Communication Channel: Once established, all HTTP data travels through this encrypted tunnel, ensuring privacy.