**The Data Packets**

***Resources from Microsoft Copilot***

When we send information (like emails, images, videos...etc) from one source to a destination, what we are actually sending are data packets. What are data packets? you can think of data packets are a series of 1s and 0s numeric digits. When you send information (data packets) from a source to a destination, the data pakets will gone through a series of processing (or layers) to actually arrive to the destination. Below briefly describe each layers.

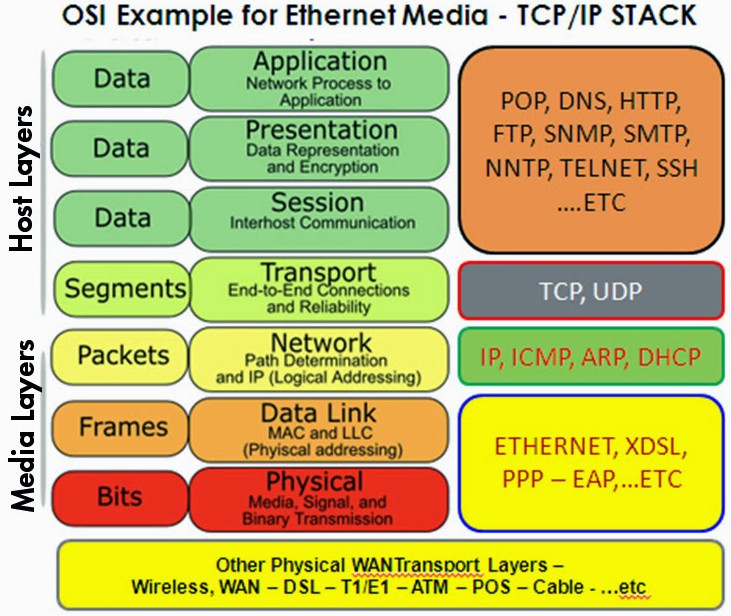
Sending data packets across a network involves several layers, each with its specific role. These layers are part of the OSI (Open Systems Interconnection) model, which standardizes the functions of a telecommunication or computing system. Here are the seven layers:

1. Application Layer: This is the top layer, where end-user applications interact with the network. It provides network services to applications such as web browsers, email clients, and file transfer programs. Protocols at this layer include HTTP, FTP, SMTP, and DNS.
2. Presentation Layer: This layer translates data between the application layer and the network. It handles data formatting, encryption, and compression. It ensures that data sent by the application layer of one device is understandable by the application layer of another device.
3. Session Layer: This layer manages sessions or connections between applications. It establishes, maintains, and terminates communication sessions. It also handles synchronization and dialog control to ensure proper data exchange.
4. Transport Layer: This layer ensures reliable data transmission between devices by managing end-to-end communication. It provides error detection, flow control, and data sequencing. Key protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
5. Network Layer: This layer determines the best path for data packets to travel across multiple networks. It handles logical addressing and routing. The most well-known protocol here is the Internet Protocol (IP), which assigns IP addresses to devices and routes packets.
6. Data Link Layer: This layer is responsible for establishing a reliable link between directly connected nodes. It packages raw bits into frames, handles error detection and correction, and manages access to the physical medium. Key protocols include Ethernet and Wi-Fi.
7. Physical Layer: This is the lowest layer and deals with the physical connection between devices. It includes hardware components like cables, switches, and network interfaces, as well as the transmission of raw binary data (bits) over the physical medium.

Below lists the summary in table form:

|  |  |  |
| --- | --- | --- |
| **Layer** | **Function** | **Examples** |
| Application | Network services for applications | HTTP, FTP, SMTP, DNS |
| Presentation | Data translation, encryption, compression | SSL/TLS, JPEG, ASCII |
| Session | Session management, synchronization, dialog control | N/A |
| Transport | End-to-end communication, error detection, sequencing | TCP, UDP |
| Network | Logical addressing, routing | IP |
| Data Link | Reliable link, error detection/correction, framing | Ethernet, Wi-Fi |
| Physical | Transmission of raw data bits over a physical medium | Cables, Switches, Network Interfaces, Optical Fiber |

Below illustrate the process of each layers:



### **Process of Sending and Receiving Data Packets**

1. Packetization:
   * At the sender's end, the data is divided into smaller packets. Each packet contains a portion of the data, along with header information such as source and destination addresses, sequence numbers, and error-checking codes.
2. Transmission:
   * The packets are transmitted over the network. They may take different paths to reach the destination, depending on the network routing algorithms.
3. Reception:
   * At the receiver's end, packets are received, possibly out of order and from different paths.
4. Reassembly:
   * The receiver uses the sequence numbers in the packet headers to reassemble the packets in the correct order to reconstruct the original data.
5. Error Detection and Correction:
   * The receiver checks for errors using the error-checking codes in the packet headers. If errors are detected, the receiver can request the sender to retransmit the affected packets.

### **Methods for Ensuring Correct and Secure Reception**

1. TCP (Transmission Control Protocol):
   * Reliability: TCP ensures reliable transmission by using acknowledgments (ACKs) and retransmissions. The receiver sends an ACK for each successfully received packet. If the sender does not receive an ACK within a certain time, it retransmits the packet.
   * Flow Control: TCP uses flow control to prevent overwhelming the receiver by adjusting the rate of data transmission based on the receiver's capacity.
   * Error Checking: TCP uses checksums to detect errors in the packets.
2. UDP (User Datagram Protocol):
   * Simplicity: Unlike TCP, UDP is connectionless and does not guarantee reliable delivery. It is used for applications where speed is more critical than reliability (e.g., streaming video).
   * Error Checking: UDP also uses checksums for error detection, but it does not provide retransmission mechanisms.
3. Encryption:
   * TLS/SSL (Transport Layer Security/Secure Sockets Layer): These protocols encrypt data packets to ensure confidentiality and integrity during transmission. They are commonly used in secure web communications (HTTPS).
4. IPSec (Internet Protocol Security):
   * Authentication and Encryption: IPSec provides authentication and encryption at the IP layer, ensuring secure data transmission over potentially insecure networks.
5. Error Correction Codes (ECC):
   * Forward Error Correction (FEC): This technique involves adding redundant data to the packets. The receiver can use this redundant data to detect and correct errors without needing retransmissions.