What is Circuit Switching?

Circuit switching is a communication method where a dedicated communication path, or circuit, is established between two devices before data transmission begins. The circuit remains dedicated to the communication for the duration of the session, and no other devices can use it while the session is in progress. Circuit switching is commonly used in voice communication and some types of data communication.

Advantages of Circuit Switching:

Guaranteed bandwidth: Circuit switching provides a dedicated path for communication, ensuring that bandwidth is guaranteed for the duration of the call.

Low latency: Circuit switching provides low latency because the path is predetermined, and there is no need to establish a connection for each packet.

Predictable performance: Circuit switching provides predictable performance because the bandwidth is reserved, and there is no competition for resources.

Suitable for real-time communication: Circuit switching is suitable for real-time communication, such as voice and video, because it provides low latency and predictable performance.

Disadvantages of Circuit Switching:

- **Inefficient use of bandwidth:** Circuit switching is inefficient because the bandwidth is reserved for the entire duration of the call, even when no data is being transmitted.
- **Limited scalability:** Circuit switching is limited in its scalability because the number of circuits that can be established is finite, which can limit the number of simultaneous calls that can be made.
- **High cost:** Circuit switching is expensive because it requires dedicated resources, such as hardware and bandwidth, for the duration of the call.

What is Packet Switching?

Packet switching is a communication method where data is divided into smaller units called packets and transmitted over the network. Each packet contains the source and destination addresses, as well as other information needed for routing. The packets may take different paths to reach their destination, and they may be transmitted out of order or delayed due to network congestion.

Advantages of Packet Switching:

- **Efficient use of bandwidth:** Packet switching is efficient because bandwidth is shared among multiple users, and resources are allocated only when data needs to be transmitted.
- **Flexible:** Packet switching is flexible and can handle a wide range of data rates and packet sizes.
- **Scalable:** Packet switching is highly scalable and can handle large amounts of traffic on a network.
- **Lower cost:** Packet switching is less expensive than circuit switching because resources are shared among multiple users.

Disadvantages of Packet Switching:

- **Higher latency:** Packet switching has higher latency than circuit switching because packets must be routed through multiple nodes, which can cause delay.
- **Limited QoS:** Packet switching provides limited QoS guarantees, meaning that different types of traffic may be treated equally.
- **Packet loss:** Packet switching can result in packet loss due to congestion on the network or errors in transmission.
- **Unsuitable for real-time communication:** Packet switching is not suitable for real-time communication, such as voice and video, because of the potential for latency and packet loss.

Reference Models in Computer Network

In the past couple of decades, many networks that were built used different hardware and software implementations as a result they were incompatible, and thus it became difficult for networks using different specifications to communicate with each other.

In order to address this problem: the incompatibility of networks and their inability to communicate with each other. The International Organization of Standardization (ISO) researched various network schemes. After that, they recognized there is a need to create a Network Model that will help vendors to create interoperable implementations of the network.

Let us now understand what is a Reference Model?

Reference Model

It is a conceptual layout mainly used to describe how the communication between devices should occur.

One of the main advantages of the reference model is that it defines the standards for building components of the network thereby permitting multiple-vendor development.

Reference models define which functions should be performed at each layer of the model and thus they promote standardization.

The most important reference models are:

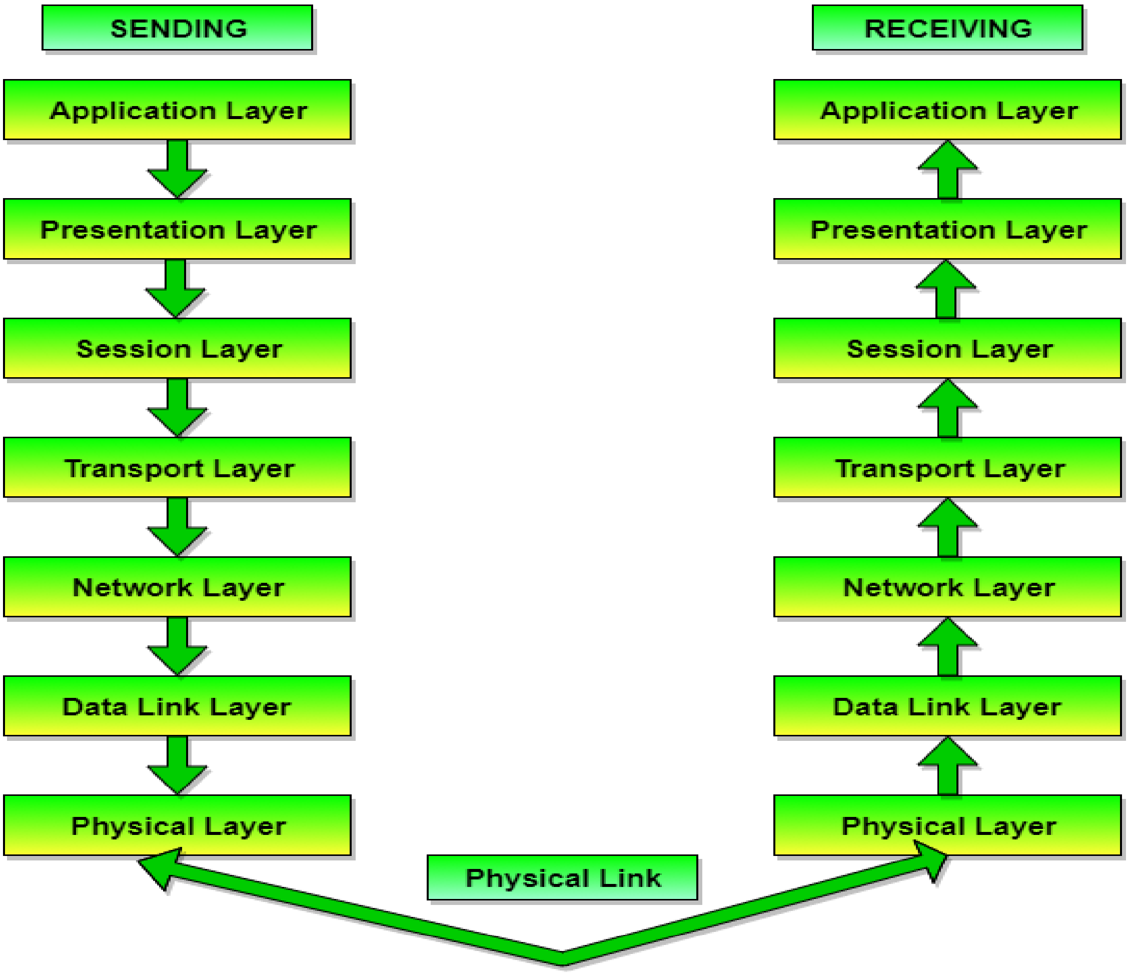
- OSI reference model.
- TCP/IP reference model.

Introduction to ISO-OSI Model

There are many users who use computer networks and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called an OSI model. OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system. These seven layers are interconnected to each other.

Seven Layers of the OSI Model are as follows:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer



Network Protocol

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

Similar to the way that speaking the same language simplifies communication between two people, network protocols make it possible for devices to interact with each other because of predetermined rules built into devices' software and hardware. Neither local area networks (LAN) nor wide area networks (WAN) could function the way they do today without the use of network protocols.

Types of Protocols

The protocols can be broadly classified into three major categories-

1. Communication
2. Management
3. Security

1. Communication

Communication protocols are really important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication.

- HTTP
- TCP
- UDP
- BGP
- ARP
- IP

2. Management

These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for troubleshooting connections between a host and a client.

Examples of Management Protocols:

- ICMP
- SNMP
- Gopher
- FTP
- POP3
- Telnet

3. Security

These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

Examples of Security Protocols:

SSL: It is a network security protocol mainly used for protecting sensitive data and securing internet connections. SSL allows both server-to-server and client-to-server communication. All the data transferred through SSL is encrypted thus stopping any unauthorized person from accessing it.

HTTPS: It is the secured version of HTTP; this protocol ensures secure communication between two computers where one sends the request through the browser and the other fetches the data from the web server.

TLS: It is a security protocol designed for data security and privacy over the internet, its functionality is encryption, checking the integrity of data i.e., whether it has been tampered with or not, and Authentication. It is generally used for encrypted communication between servers and web apps, like a web browser loading a website, it can also be used for encryption of messages, emails, and VoIP.

Spectrum

Spectrum refers to the entire range of frequencies right from the starting frequency (the lowest frequency) to the ending frequency (the highest frequency). Spectrum basically refers to the entire group of frequencies.

Example of spectrum- Electromagnetic Spectrum

The electromagnetic spectrum is one good example. The electromagnetic (EM) spectrum covers frequencies. Microwave radiations span in frequency from 300 MHz to 300 GHz.

Difference between spectrum and bandwidth?

The difference between spectrum and bandwidth is that spectrum refers to the 'entirety' while bandwidth is a 'sub-section' of the spectrum. Spectrum refers to the wholesome of the quantity while bandwidth, on the other hand, is a portion of the entire spectrum.

Example- difference between spectrum and bandwidth

If frequencies from **12 MHz up to 40 MHz** are allocated for an application, the spectrum refers to the entire range of frequencies right from 12 MHz to 40 MHz Therefore, the spectrum is (12 to 40) MHz in some cases, the entire allocated frequencies may not be used by the application. So, if only 17 MHz to 20 MHz is used by an application, then, those **range of frequencies** used is called the '**bandwidth**'.