

Computer Network and Data Communication



School of Information Technology and Software Engineering (SITE)

Table of Contents

1.	Introduction to Data Communications and Computer networks	4
1.1	Introduction:	4
1.2	Basic components of communication networks.....	4
1.3	Types of Transmission mode	5
1.4	Fundamentals of Information Transmission Media and Coding.....	7
1.5	Types of Computer Networks	7
i.	Local Area Network.....	8
ii.	Wireless Area Network	9
iii.	Wide Area Network.....	9
iv.	Metropolitan Area Network	9
v.	Campus Area Network	10
1.6	Data Communication Hardware	10
1.7	Types of Network Topologies	12
2.	OSI 7 Layers and Concept of Open standard	17
2.1	Application Layer	19
2.2	Presentation Layer	19
2.3	Session Layer	20
2.4	Transport Layer	21
2.5	Network Layer	21
2.6	Data Link Layer	21
2.7	Physical Layer	22
2.8	Advantages of OSI Model.....	22
2.2	OSI vs. TCP/IP Model.....	22

Figure 1 Data Communication Component	5
Figure 2 Simplex Transmission mode	5
Figure 3 Half Duplex Transmission Mode.....	6
Figure 4 Full Duplex Transmission Mode.....	6
Figure 5 All the transmission Mode.....	7
Figure 6 LAN Network	8
Figure 7 WLAN Network.....	9
Figure 8 WAN Network	9
Figure 9 Point-to-point topology diagram.....	12
Figure 10 Bus Topology Network.....	13
Figure 11 Ring Topology	14
Figure 12 Star Topology	15
Figure 13 Partial Mesh	16
Figure 14 Full Mesh topology.....	16
Figure 15 Summary of OSI Model functionality	18

Chapter One

1. Introduction to Data Communications and Computer networks

1.1 Introduction:

Data Commutation deals with the transmission (sending and receiving) of information between two locations by means of electrical signals. The two types of electric signals may be either analog or digital. Digital Data communication is the name given to the communication where exchange of information takes place in the form of 0s and 1s over some transmission medium like a wire or wireless.

The effectiveness of a data communication system depends on three fundamental characteristics:

- ✓ **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended devices or user and only by that devices or user.
- ✓ **Accuracy:** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected must not be used.
- ✓ **Timeliness:** The system must deliver the data in time. The data delivered late are useless. For example, in the case of audio and video, timely deliver means delivering the data as they are produced in the same order of production and without significant delay. This type of delivery is called real-time transmission (live streaming)

1.2 Basic components of communication networks

To make the communication effective, every network use five components:

- ✓ Messages
- ✓ Sender
- ✓ Receiver
- ✓ Medium and
- ✓ Protocol

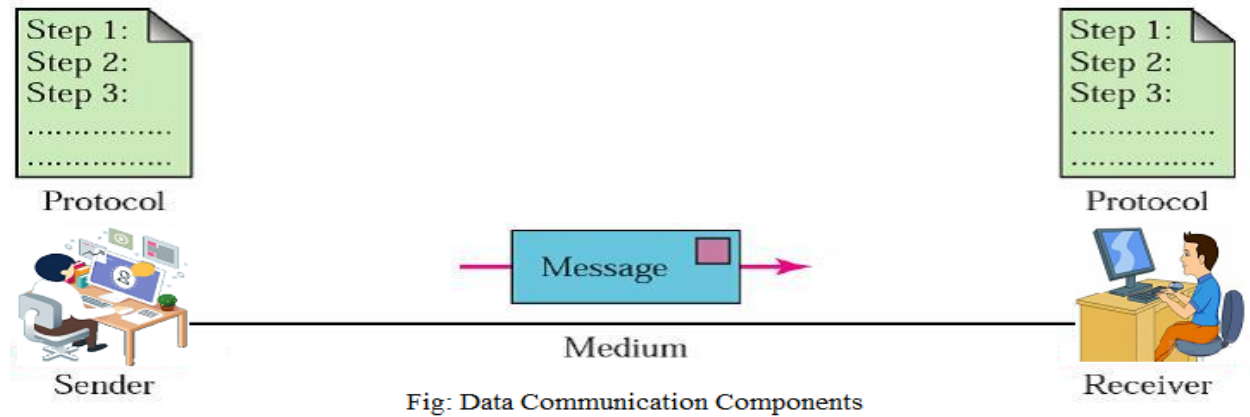


Figure 1 Data Communication Component

- i. **Message:** The message is the data information to be communicated. It can be text, audio, numbers, video or any combination of these types.
- ii. **Sender:** The sender is the devices that sends the data message. It can be a computer, workstation, telephone or video camera.
- iii. **Receiver:** The receiver is the devices that receives the message. It can be computer, workstation, or phone.
- iv. **Medium:** The transmission medium is the physical path by which a message travels from send to receiver. It should be a twisted-pair, co-axial cable, fiber optic cable or Radio waves.
- v. **Protocol:** A protocol is a set of rules that govern the data communications. It represents arrangement between the communicating devices. Without a protocol, two devices may be connected but cannot communicate.

1.3 Types of Transmission mode

The term transmission mode is used to define the direction of signal flow between two linked devices. There are three types of transmission modes. They are ***simplex, Half Duplex and Full duplex***

Simplex: In simplex mode communication is unidirectional, i.e only one of the two devices on the link can transmit data and the other will only receive the data. Take an example of Computer and Monitor. The compute will send data to the monitor and the monitor will only display it.



Figure 2 Simplex Transmission mode

So, simplex data transfer is Uni-directional. And monitor will never send data back to the computer. Same is true between computer and key board. Keyboard receive data from computer but computer will never receive data from key board.

Half Duplex: In half Duplex both the linked device can transmit and receive the data. But not at the same time. i.e when the first device is sending the data the second will only receive, similarly when the second is sending the data the first will be receive. Example the use of a walkie-talkie is a half-duplex.

In a half-Duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the same time.

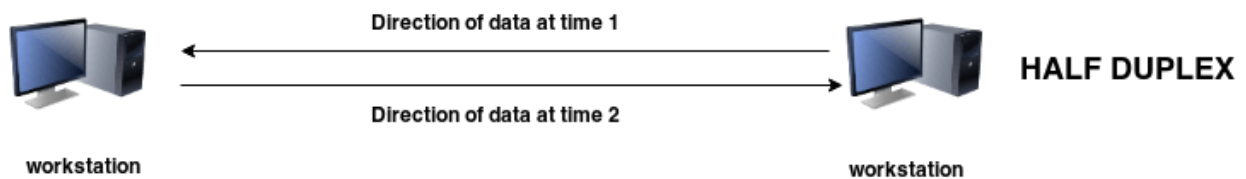


Figure 3 Half Duplex Transmission Mode

Full Duplex: In full duplex mode (Duplex) both the linked device can transmit and receive the data at the same time. The one example is mobile phone or telephone line between two users. Both users can talk and hear at the same time. The signals going in either direction share the capacity of the link. This sharing can occur in two ways. Either the link contains two physically separate transmission paths. One for sending and the other for receiving or the capacity of the channel is divided between signals travelling in both directions.

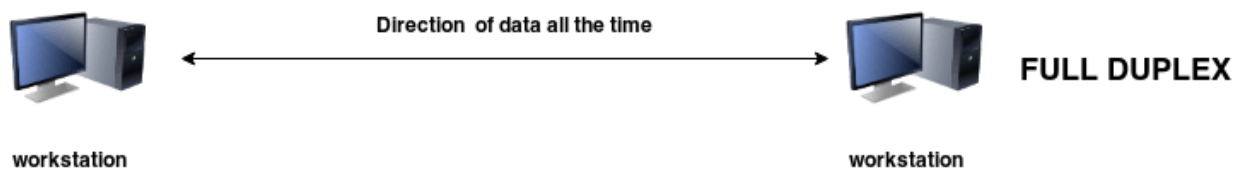


Figure 4 Full Duplex Transmission Mode

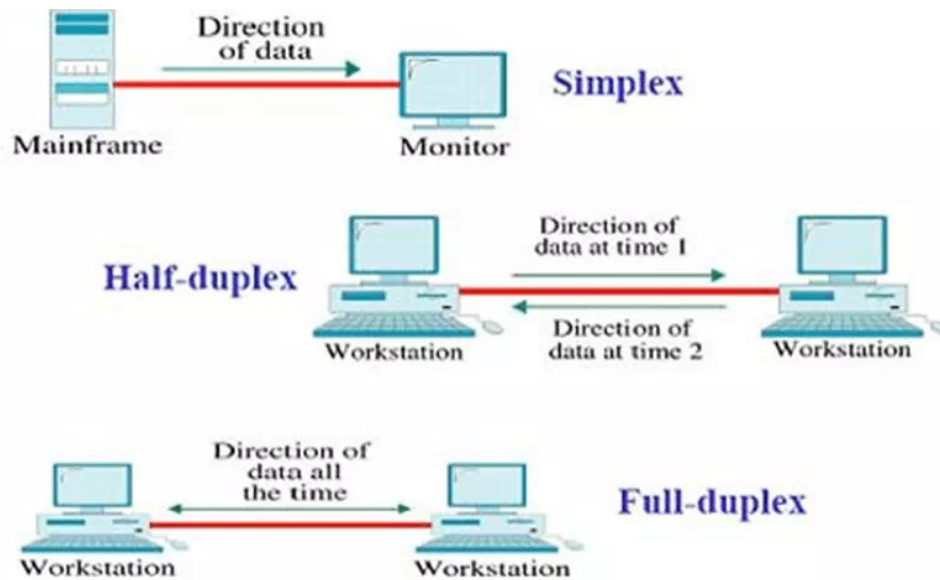


Figure 5 All the transmission Mode

1.4 Fundamentals of Information Transmission Media and Coding

In the process of data communication, the data must be transformed into signals to send them from one place to another. Data stored in a computer is in the form of 0s and 1s. to transform this data from one place to another place, it must be converted into digital signals. This is called Encoding digital data into digital signals or digital to digital conversion.

- ✓ And the process of converting analog signal into digital signal is called analog to digital conversion or digitizing an analog signal.
- ✓ The process of converting the digital signal into analog signal is called digital to analog conversion or modulating a digital signal.
- ✓ The process of sending an analog signal over long distances using high frequency carrier signal is called analog to analog conversion or modulating an analog signal.

1.5 Types of Computer Networks

There are different type of network, however these are the basic and commonly used ones:

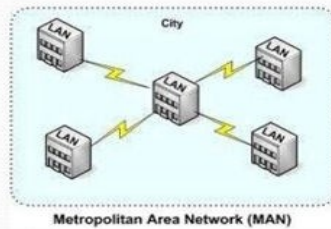
- ✓ Local Area Network (LAN)
- ✓ WLAN (Wireless LAN)
- ✓ WAN (Wide Area Network)
- ✓ MAN (Metropolitan Area Network)
- ✓ CAN (Campus Area Network)

There are different types of network:

- LAN(Local Area Networking)
- WLAN(Wireless Local Area Networks)
- WAN(Wide Area Networks)
- MAN(Metropolitan Area Networks)
- CAN(Campus Area Networks)



WAN



MAN



CAN

i. Local Area Network

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.

Regardless of size, a LAN's single defining characteristic is that it connects devices that are in a single, limited area.

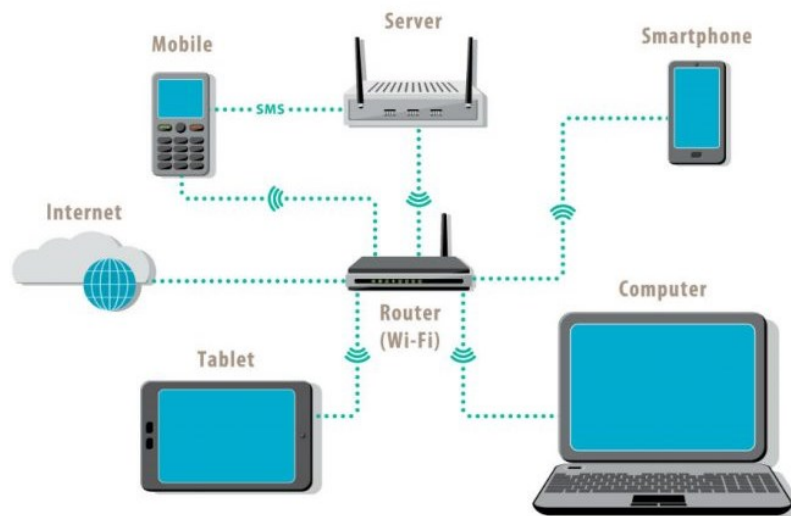


Figure 6 LAN Network

ii. Wireless Area Network

A wireless local area network (WLAN) is a wireless distribution method for two or more devices. WLANs use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection. A WLAN is sometimes called a local area wireless network (LAWN).



Figure 7 WLAN Network

iii. Wide Area Network

In its simplest form, a wide-area network (WAN) is a **collection of local-area networks (LANs) or other networks that communicate with one another**. A WAN is essentially a network of networks, with the Internet the world's largest WAN.

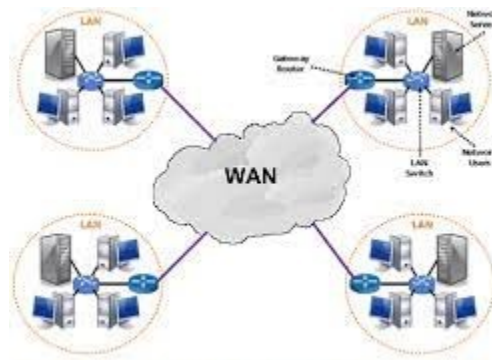


Figure 8 WAN Network

iv. Metropolitan Area Network

A metropolitan area network (MAN) is a **computer network that connects computers within a metropolitan area**, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN).

v. Campus Area Network

A campus area network (CAN) is a **computer network that spans a limited geographic area**. CANs interconnect multiple local area networks (LAN) within an educational or corporate campus. ... CANs are smaller than metropolitan area networks (MAN) and wide area networks (WAN), which stretch over large geographic areas.

1.6 Data Communication Hardware

In data communication, the integration of hardware and software must be done meticulously so that the intended outcome will be achieved. Below is some of the hardware component for data communication over the network:

NIC: Network Interface Card

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Network Cables: there are different types of cables that will be used to connect the network equipment. That could be between the network device or network device with end user device. Below is the most basic cable types, characteristics, benefits and it features:

Twisted-pair cable. You probably see this during your lap session and the name itself comes from the type of cable inside the shield. This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green, and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

In the **UTP (Unshielded twisted-pair)** cable, all pairs are wrapped in a single plastic sheath.

In the **STP (Shielded twisted-pair)** cable, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

Similarities and differences between STP and UTP cables

- ✓ Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- ✓ Since the STP cable contains more materials, it is more expensive than the UTP cable.
- ✓ Both cables use the same RJ-45 (registered jack) modular connectors.
- ✓ The STP provides more noise and EMI resistance than the UTP cable.
- ✓ The maximum segment length for both cables is 100 meters or 328 feet.
- ✓ Both cables can accommodate a maximum of 1024 nodes in each segment.

Fiber Optic Cable

This cable consists of a core, cladding, buffer, and jacket. The core is made from thin strands of glass or plastic that can carry data over a long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.

SMF (Single-mode fiber) optical cable

This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable

This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used for shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.

Switch: Switch is where you end user lives. All end user device like computer, laptop, printer, CCTV camera, IP Phone... etc will be connected to these devices. There is different type of switch which is access switch, distribution switch and core switch. Based on its functionality, the layer where each switch will be presented is different. It operates at layer two of the OSI model and uses MAC address as source and destination address for communication purpose.

Router: Unlike switch which will broadcast its traffic to all its port to find the destination devices, router is a bit intelligent and decide where to send the traffic based on the destination IP address of the devices. It uses routing table and exit interface to decide where to send the data. It operates at layer 3 of the OSI model.

Firewall: At your network premises, you might have different application such as website at DMZ, mailbox sever at server farm, or edge server at DMZ or FTP server. If you want to protect those servers from being access by unauthorized person, you need to deploy firewall at the edge of your network and

create rules or policy to enforce who can access the resource with specific ports. It operates both at Layer 3 and Layer 4 of OSI model.

1.7 Types of Network Topologies

Point to Point: Point-to-point topology is the easiest of all the network topologies. In this method, the network consists of a direct link between two computers.

Advantages:

- ✓ This is faster and highly reliable than other types of connections since there is a direct connection.
- ✓ No need for a network operating system
- ✓ Does not need an expensive server as individual workstations are used to access the files
- ✓ No need for any dedicated network technicians because each user sets their permissions

Disadvantages:

- ✓ The biggest drawback is that it only be used for small areas where computers are in close proximity.
- ✓ You can't back up files and folders centrally
- ✓ There is no security besides the permissions. Users often do not require to log onto their workstations.

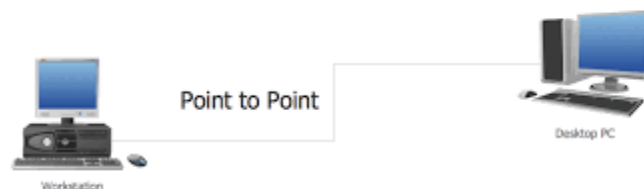


Figure 9 Point-to-point topology diagram

Bus Topology

Bus topology uses a single cable which connects all the included nodes. The main cable acts as a spine for the entire network. One of the computers in the network acts as the computer server. When it has two endpoints, it is known as a linear bus topology.

Advantages:

Here are pros/benefits of using a bus topology:

- ✓ Cost of the cable is very less as compared to other topology, so it is widely used to build small networks.
- ✓ Famous for LAN network because they are inexpensive and easy to install.
- ✓ It is widely used when a network installation is small, simple, or temporary.
- ✓ It is one of the passive topologies. So, computers on the bus only listen for data being sent, that are not responsible for moving the data from one computer to others.

Disadvantages:

Here are the cons/drawbacks of bus topology:

- ✓ In case if the common cable fails, then the entire system will crash down.
- ✓ When network traffic is heavy, it develops collisions in the network.
- ✓ Whenever network traffic is heavy, or nodes are too many, the performance time of the network significantly decreases.
- ✓ Cables are always of a limited length.

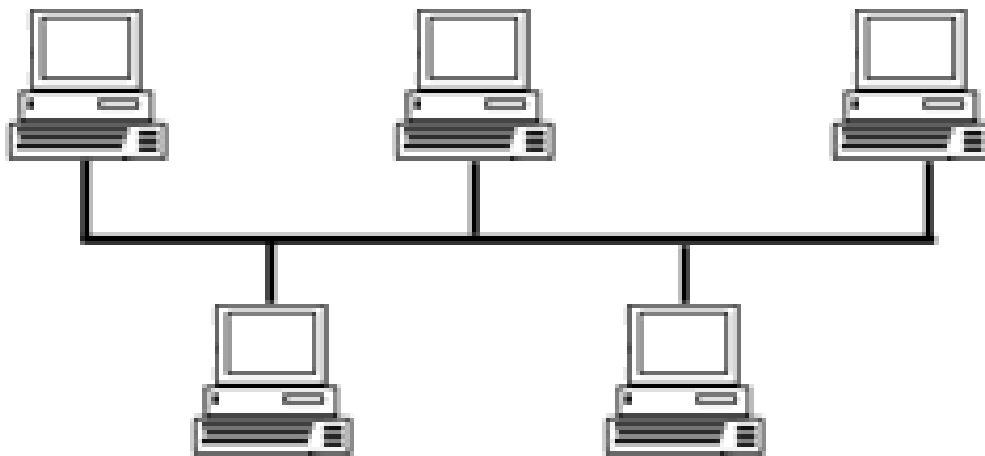


Figure 10 Bus Topology Network

Ring Topology

In a ring network, every device has exactly two neighboring devices for communication purpose. It is called a ring topology as its formation is like a ring. In this topology, every computer is connected to another computer. Here, the last node is combined with a first one.

This topology uses token to pass the information from one computer to another. In this topology, all the messages travel through a ring in the same direction.

Advantages:

Here are pros/benefits of ring topology:

- ✓ Easy to install and reconfigure.
- ✓ Adding or deleting a device in-ring topology needs you to move only two connections.
- ✓ The troubleshooting process is difficult in a ring topology.
- ✓ Failure of one computer can disturb the whole network.
- ✓ Offers equal access to all the computers of the networks
- ✓ Faster error checking and acknowledgment.

Disadvantages:

Here are drawbacks/cons of ring topology:

- ✓ Unidirectional traffic.
- ✓ Break in a single ring can risk the breaking of the entire network
- ✓ Modern days high-speed LANs made this topology less popular.
- ✓ In the ring, topology signals are circulating at all times, which develops unwanted power consumption.
- ✓ It is very difficult to troubleshoot the ring network.
- ✓ Adding or removing the computers can disturb the network activity.



Figure 11 Ring Topology

Star Topology

In the star topology, all the computers connect with the help of a hub. This cable is called a central node, and all other nodes are connected using this central node. It is most popular on LAN networks as they are inexpensive and easy to install.

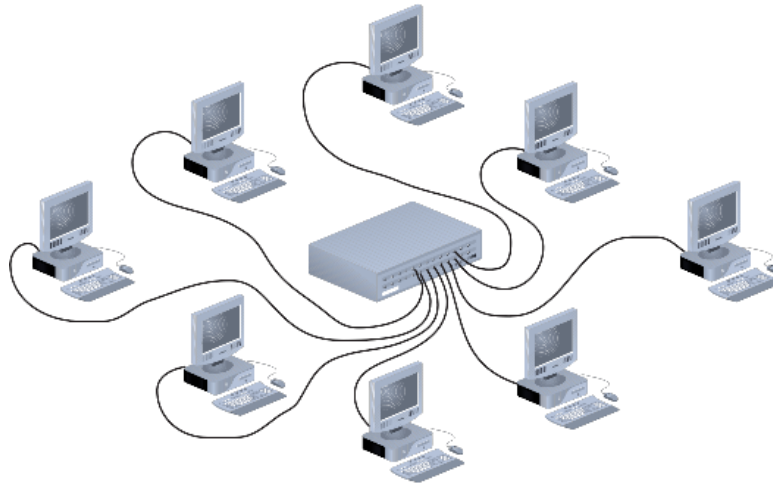


Figure 12 Star Topology

Advantages:

Here are pros/benefits of start topology:

- ✓ Easy to troubleshoot, set up, and modify.
- ✓ Only those nodes are affected, that has failed. Other nodes still work.
- ✓ Fast performance with few nodes and very low network traffic.
- ✓ In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages:

Here are cons/drawbacks of using Star:

- ✓ If the hub or concentrator fails, attached nodes are disabled.
- ✓ Cost of installation of star topology is costly.
- ✓ Heavy network traffic can sometimes slow the bus considerably.
- ✓ Performance depends on the hub's capacity
- ✓ A damaged cable or lack of proper termination may bring the network down.

Mesh Topology

The mesh topology has a unique network design in which each computer on the network connects to every other. It is developing a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, still data has an alternative path to reach its destination.

Types of Mesh Topology:

- **Partial Mesh Topology:** In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices.

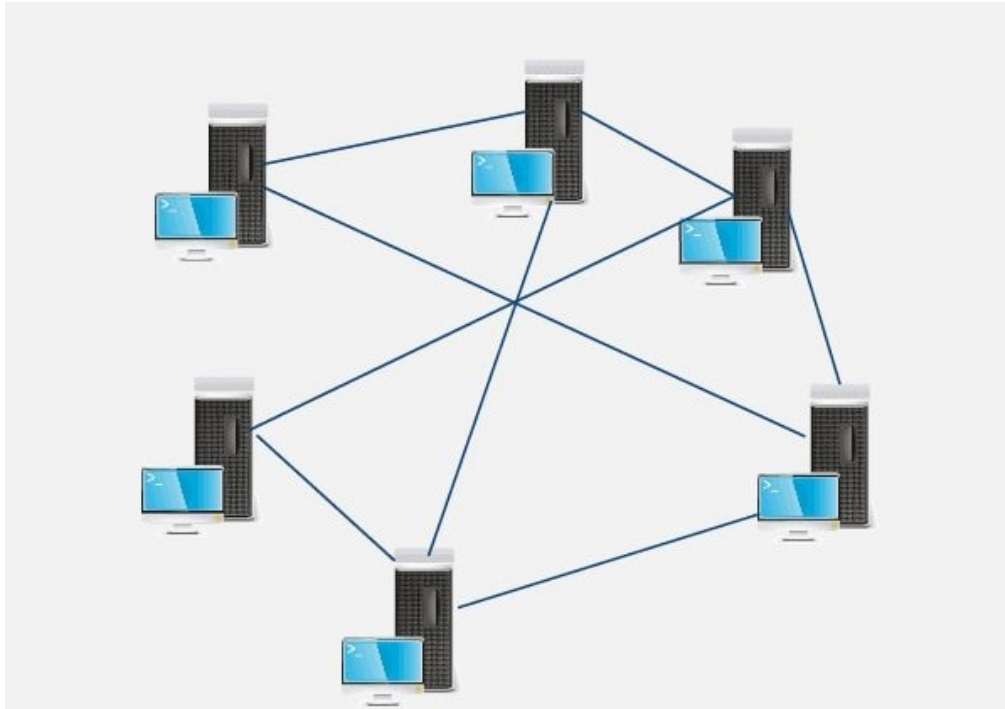


Figure 13 Partial Mesh

Full Mesh topology

In a full mesh topology, all nodes/devices are directly connected. The type of redundancy is increased in a full-mesh topology. These types of network topology are used in the backbone network. If there is high traffic between any nodes then other routes are chosen for traffic balancing.

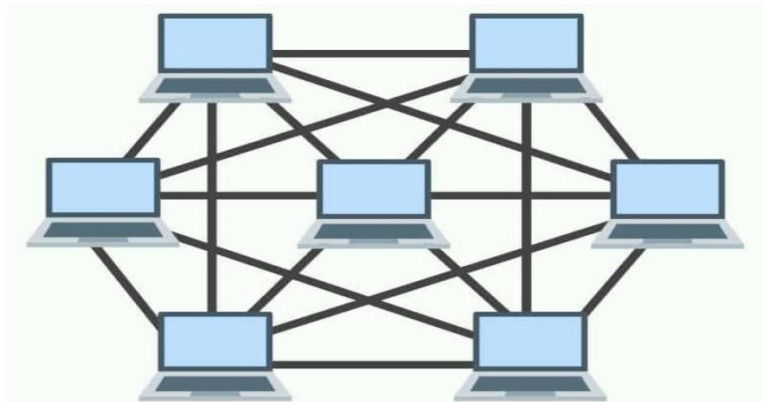


Figure 14 Full Mesh topology

Advantages:

Here, are pros/benefits of Mesh topology

- ✓ The network can be expanded without disrupting current users.
- ✓ Need extra capable compared with other LAN topologies.
- ✓ No traffic problem as nodes has dedicated links.
- ✓ Dedicated links help you to eliminate the traffic problem.
- ✓ A mesh topology is robust.
- ✓ It has multiple links, so if any single route is blocked, then other routes should be used for data communication.
- ✓ P2P links make the fault identification isolation process easy.
- ✓ It helps you to avoid the chances of network failure by connecting all the systems to a central node.
- ✓ Every system has its privacy and security.

Disadvantages:

- ✓ Installation is complex because every node is connected to every node.
- ✓ It is expensive due to the use of more cables. No proper utilization of systems.
- ✓ Complicated implementation.
- ✓ It requires more space for dedicated links.
- ✓ Because of the amount of cabling and the number of input-outputs, it is expensive to implement.
- ✓ It requires a large space to run the cables.

Chapter Two

2. OSI 7 Layers and Concept of Open standard

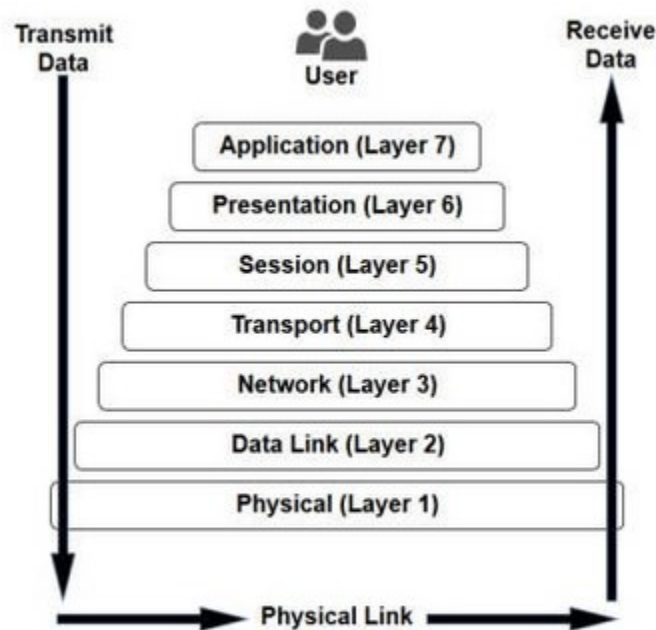
OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network. This model focuses on providing a visual design of how each communications layer is built on top of the other, starting with the physical cabling, all the way to the application that's trying to communicate with other devices on a network.

A reference model is a conceptual framework for understanding relationships. The motivation of creating the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system that's in use.

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

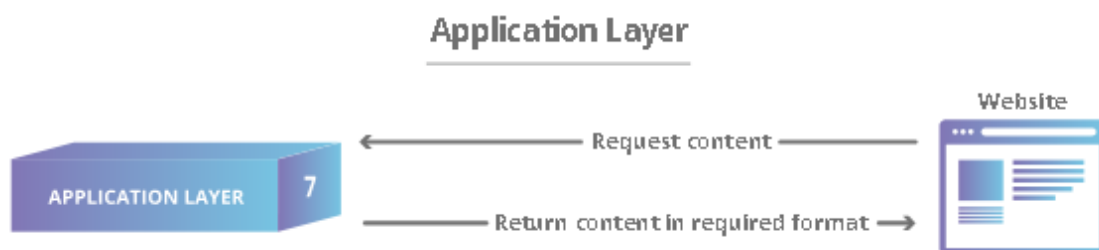
Figure 15 Summary of OSI Model functionality

OSI layer used to encapsulate and decapsulate data as it moves from source to destination vice versa. Below is the picture that explain how the data moves from sender to receiver.



2.1 Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).



2.2 Presentation Layer

This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer. Layer 6 Presentation examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.

Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.

If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.

Finally, the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.



2.3 Session Layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100-megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 57 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 45 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.



2.4 Transport Layer

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.



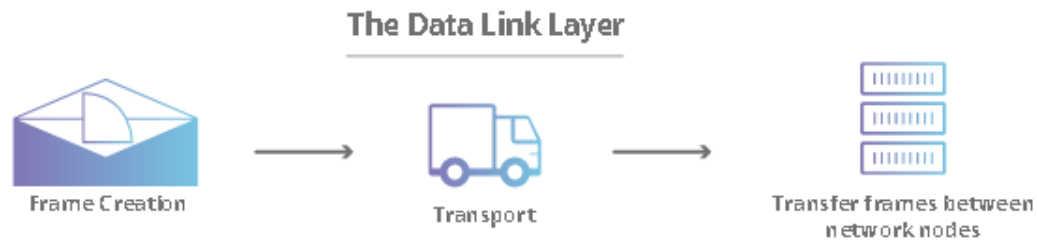
2.5 Network Layer

The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.



2.6 Data Link Layer

The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the SAME network (basically on the same switch). The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).



2.7 Physical Layer

This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.



2.8 Advantages of OSI Model

The OSI model helps users and operators of computer networks:

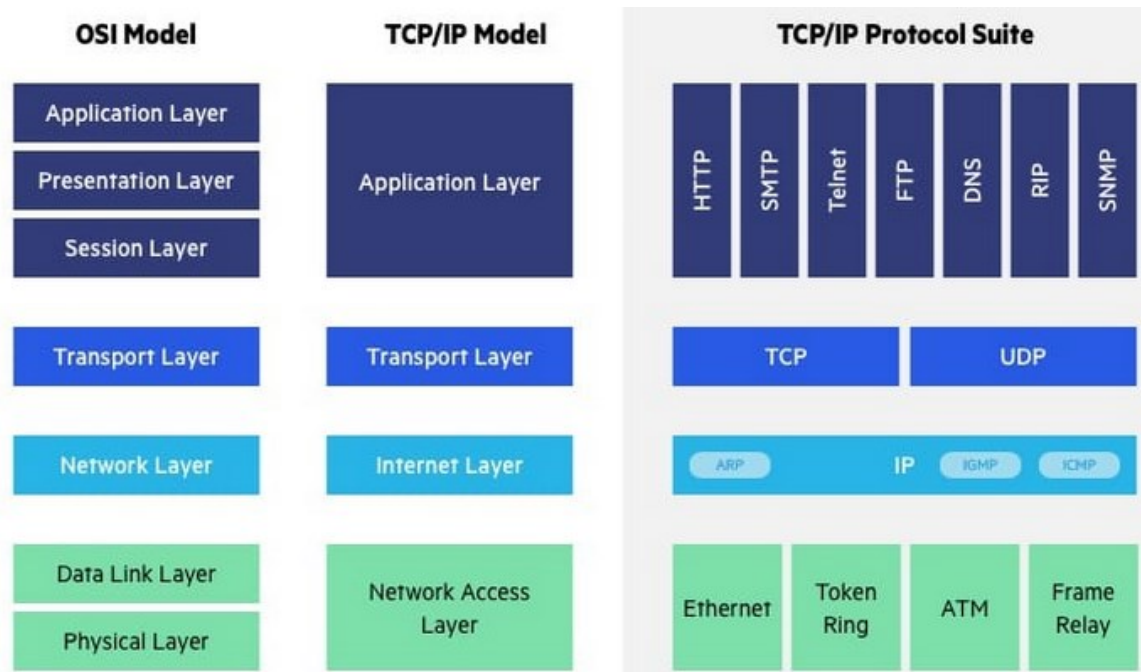
- ✓ Determine the required hardware and software to build their network.
- ✓ Understand and communicate the process followed by components communicating across a network.
- ✓ Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer.

The OSI model helps network device manufacturers and networking software vendors:

- ✓ Create devices and software that can communicate with products from any other vendor, allowing open interoperability
- ✓ Define which parts of the network their products should work with.
- ✓ Communicate to users at which network layers their product operates – for example, only at the application layer, or across the stack.

2.2 OSI vs. TCP/IP Model

Below is the comparison between OSI and TCP/IP model



The Transfer Control Protocol/Internet Protocol (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:

- ✓ OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP
- ✓ OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP – however TCP/IP does not take responsibility for sequencing and acknowledgement functions, leaving these to the underlying transport layer.

Other important differences:

- ✓ TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.
- ✓ In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.

Chapter Three

3. Network Layer