Unit- Four

OVERVIEW OF DATA COMMUNICATION NETWORKING AND PROTOCOLS

- ❖ Network Types, Topology
- ❖ OSI layers and Functions, TCP/IP layer, Local Area Networks (LAN) Architecture,
- ❖ LLC/MAC & Routing
- ❖ IEEE Standards, Ethernet (Aloha, CSMA), Wide Area Networks (WAN): X.25, Frame
- ❖Relay, ATM

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Overview

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

Types of Networks

A computer network can be categorized as:

Personal Area Network (PAN):

PAN is a network arranged within an individual person, typically within a range of 10 meters. PAN is used for connecting the computer devices of personal use is known as Personal Area Network. PAN covers an area of 30 feet. Personal devices that are used to develop the personal area network are the laptop, mobiles phones, medial player and play stations.

Types of Networks

Local Area Network (LAN):

Local area network is a group of computers connected to each other in a small area such as building, office. LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable etc. It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables. The data is transferred at extremely faster rate in Local Area Network.

Types of Networks

Local Area Network (LAN):

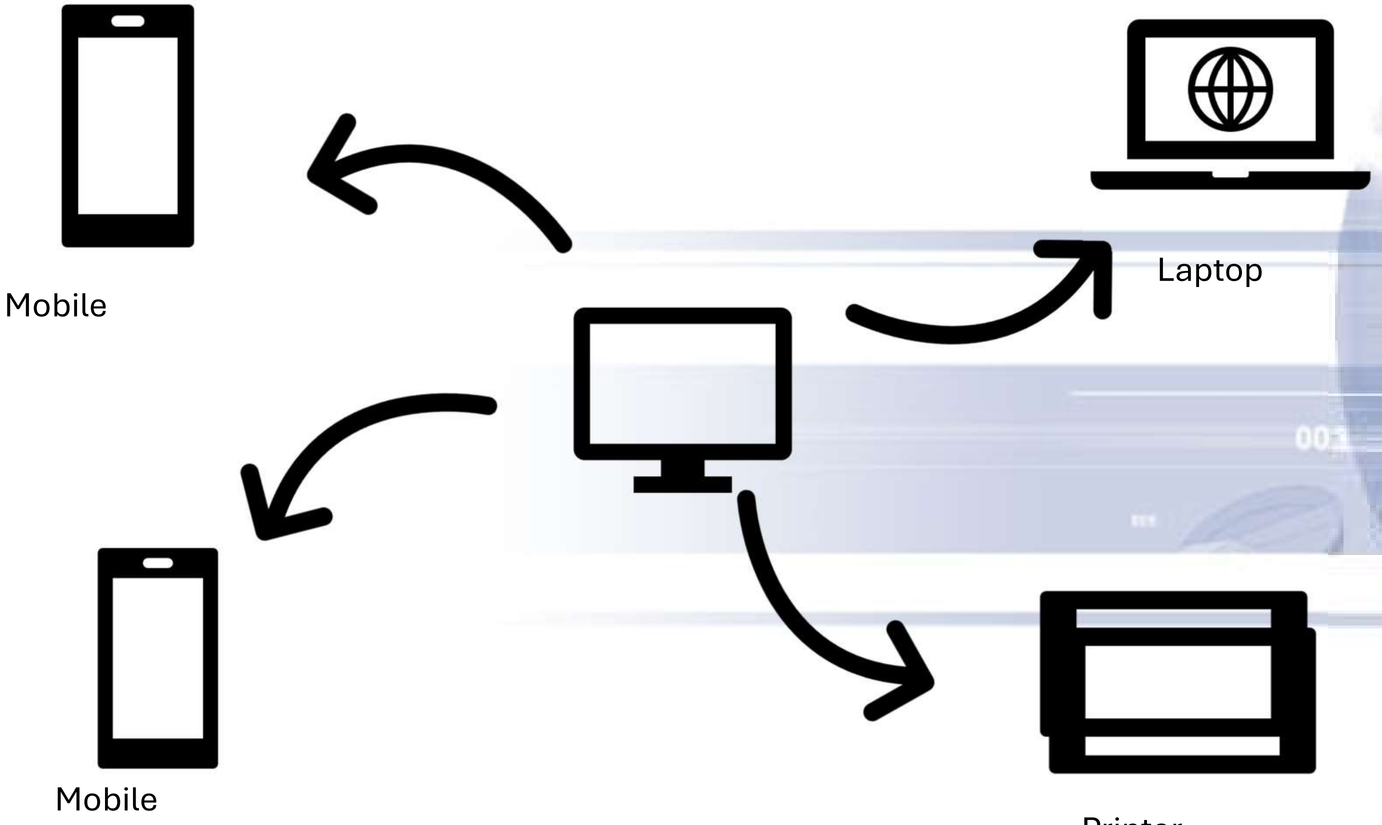


Fig: Personal Area Network

Types of Networks

Metropolitan Area Network (MAN):

Metropolitan Area Network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network. Government agencies use MAN to connect to the citizens and private industries. In MAN, various LANs are connected to each other through a telephone exchange line. The most widely used protocols in MAN are RS-232, Frame Relay, ATM etc. It has higher range than LAN.

Types of Networks

Metropolitan Area Network (MAN):

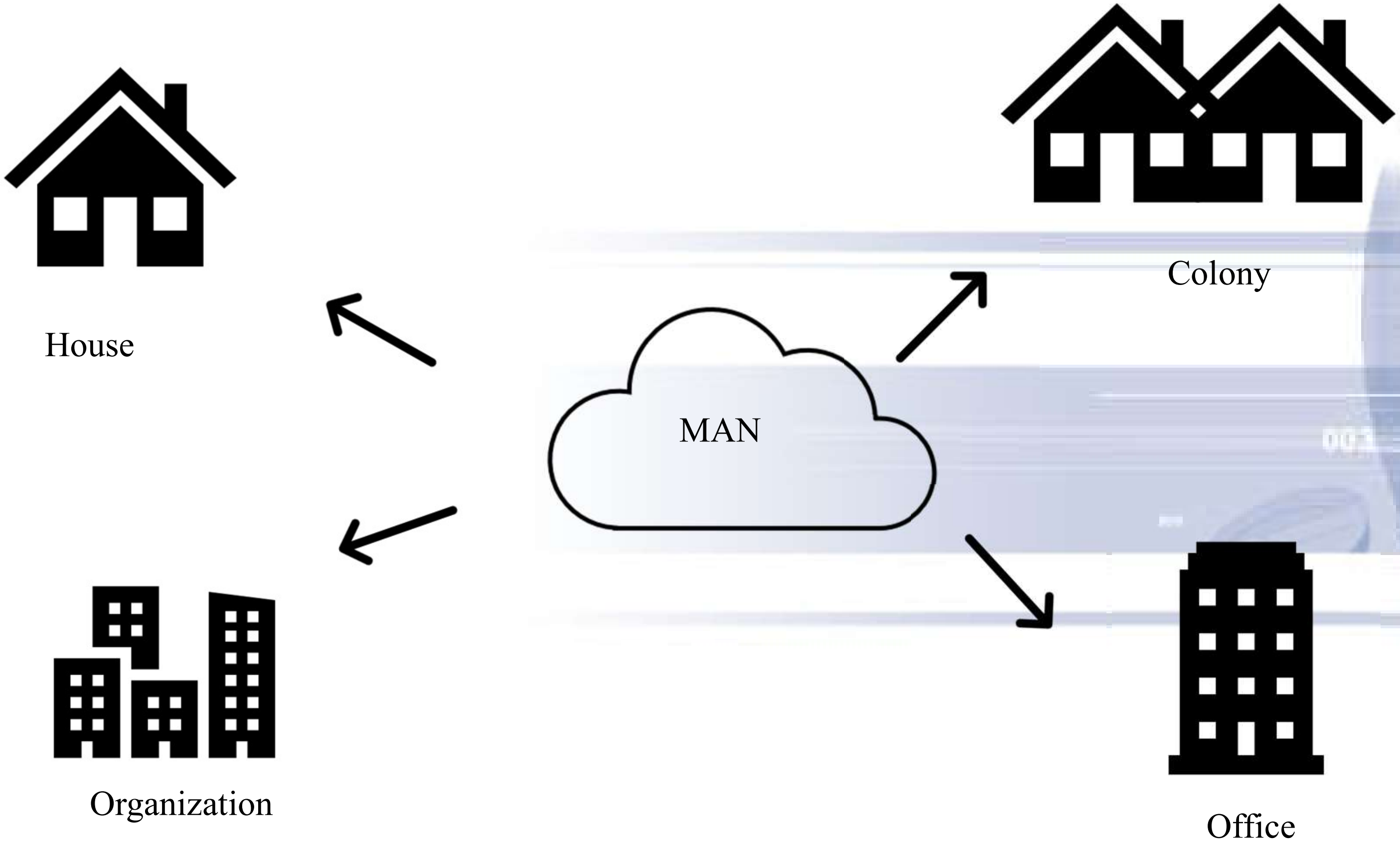


Fig: Metropolitan Area network

Types of Networks

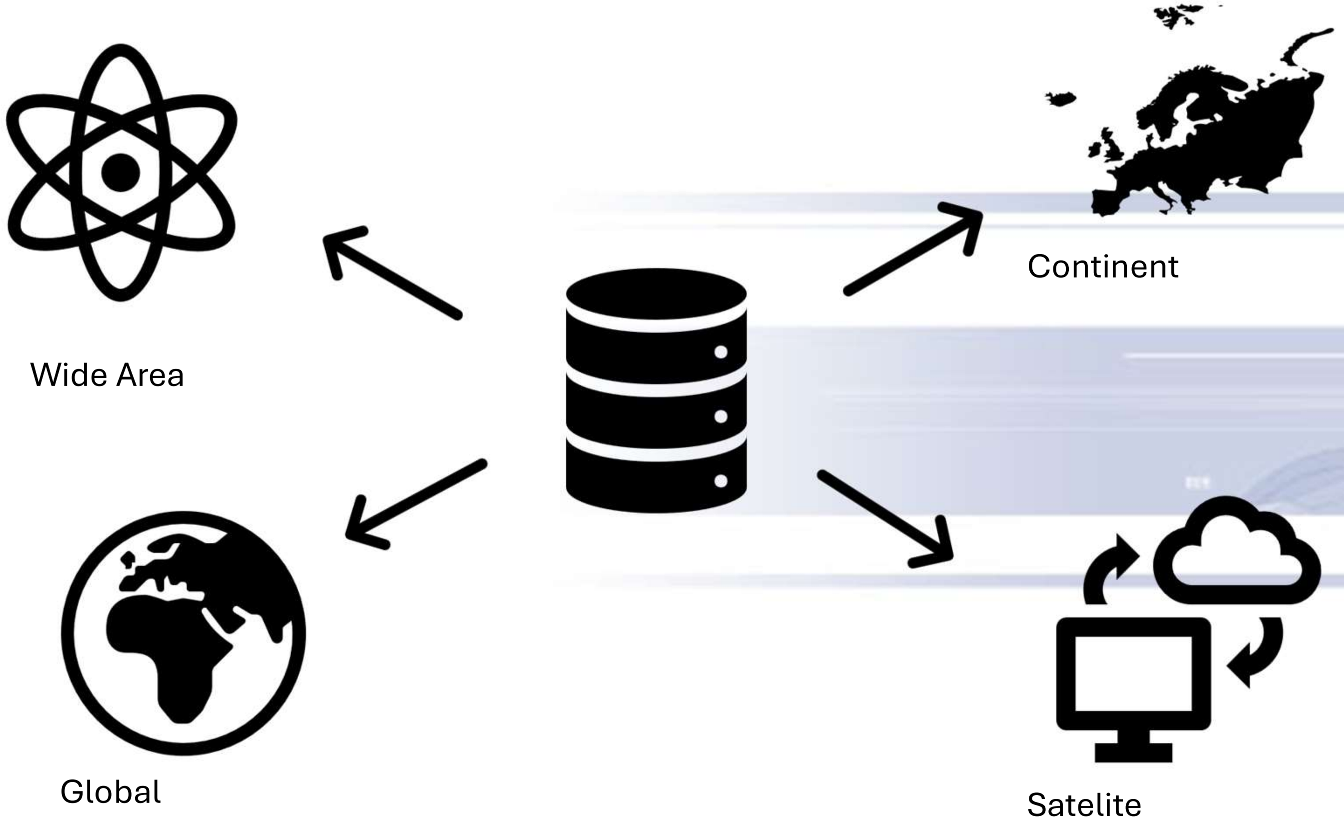
Wide Area Network (WAN):

A Wide Area Network is a network that extends over a large geographical area such as states or countries. WAN is quite bigger network than the LAN. A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links. The internet is one of the biggest WAN in the world. A Wide Area Network is widely used in the field of business, government and education.

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Types of Networks

Wide Area Network (WAN):



Wide Area

Continent

Global

Satelite

Fig: Wide Area Network

Network Topology

Network topology is the physical layouts of computer on the network. In other words, it can be defined as the pattern of interconnection of computers on the network. There are five major network topologies, they are:

Network Topology

i) Bus Topology

In bus topology, a single cable serves as the backbone of the network. The nodes or computers are connected to this single cable backbone. The broadcast message is seen by all the nodes but only the intended node will accept the message. For example: Ethernet that uses coaxial cable

Network Topology

i) Bus Topology

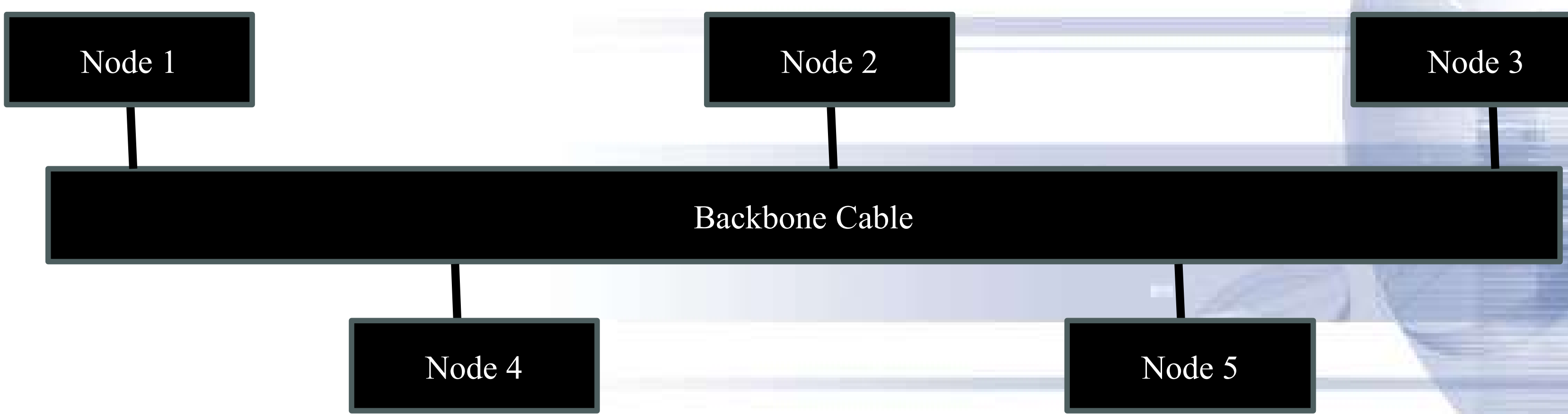


Fig: Bus Topology

Network Topology

i) Bus Topology

Advantages:

- Easy to install and extend the network.
- It is scalable
- Failure of one node does not affect entire network.

Disadvantages:

- It is difficult to troubleshoot when any problem arises.
- If the backbone fails, entire network is unusable.

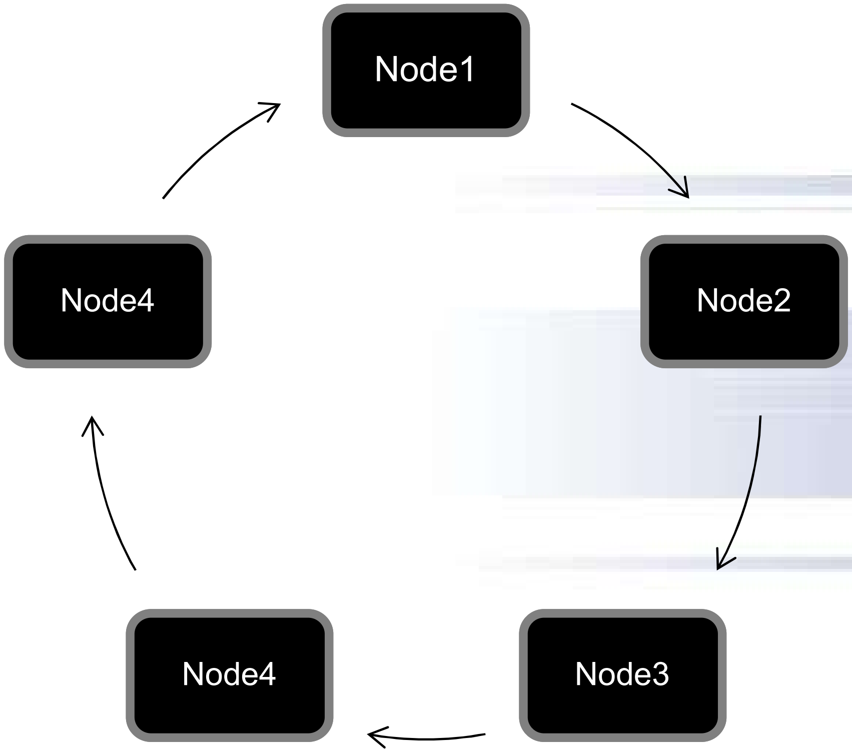
Network Topology

ii) Ring Topology

In ring topology, each node is connected to other two nodes in either side forming a circular structure. In this topology, message passes from node to node to reach the destination node.

Network Topology

ii) Ring Topology



Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Network Topology

ii) Ring Topology

Advantages:

- Every node act as receiver
- Performs better than bus topology
- Doesn't need network services.

Disadvantages:

- Failure of one node affects entire network
- Network is not flexible.

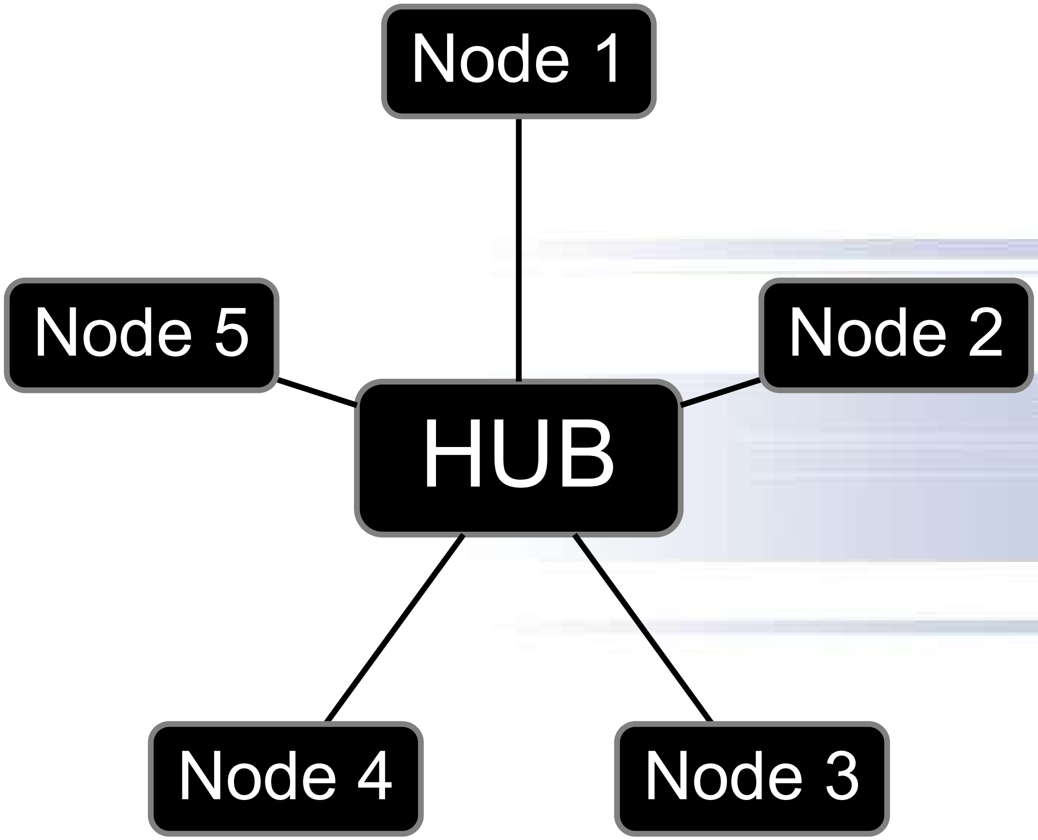
Network Topology

iii) Star Topology

In Star topology, all the nodes are connected to a central unit which is known as switch or hub. To transmit a message from one node to another, the message must pass through hub.

Network Topology

iii) Star Topology



Network Topology

iii) Star Topology

Advantages:

- Easy to install
- Flexible in adding nodes or reducing nodes
- Failure of one node does not affect entire network.

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Network Topology

iii) Star Topology

Disadvantages:

- A fault in central unit causes the whole network to fail.
- A lot of cable is required, so cost of cabling is high
- Performance of hub limits the performance of whole network.

iv) Mesh Topology

It is a type of topology where each node is directly connected to multiple nodes.

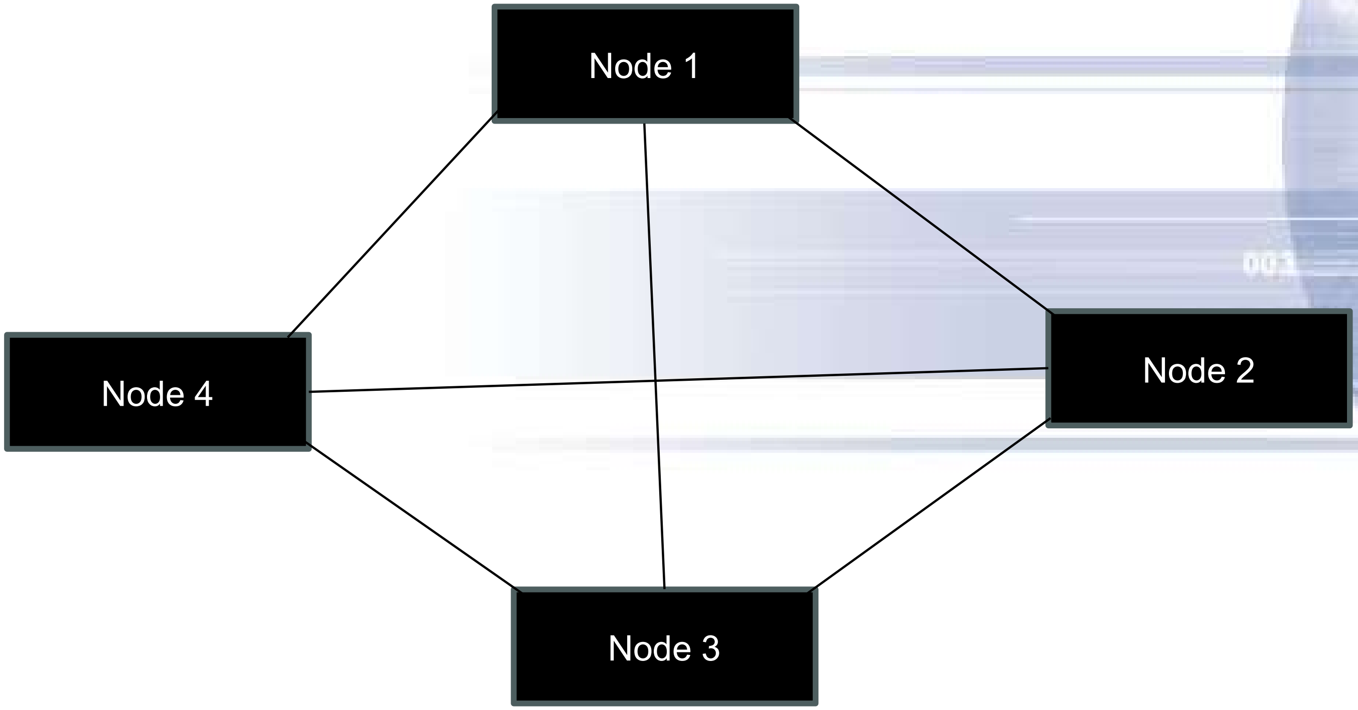


Fig: Hybrid Topology

Network Topology

iv) Mesh Topology

Advantages:

- Because of multiple paths to reach the nodes, failure of any node will not affect other nodes.
- There is no traffic problem as it has multiple paths.

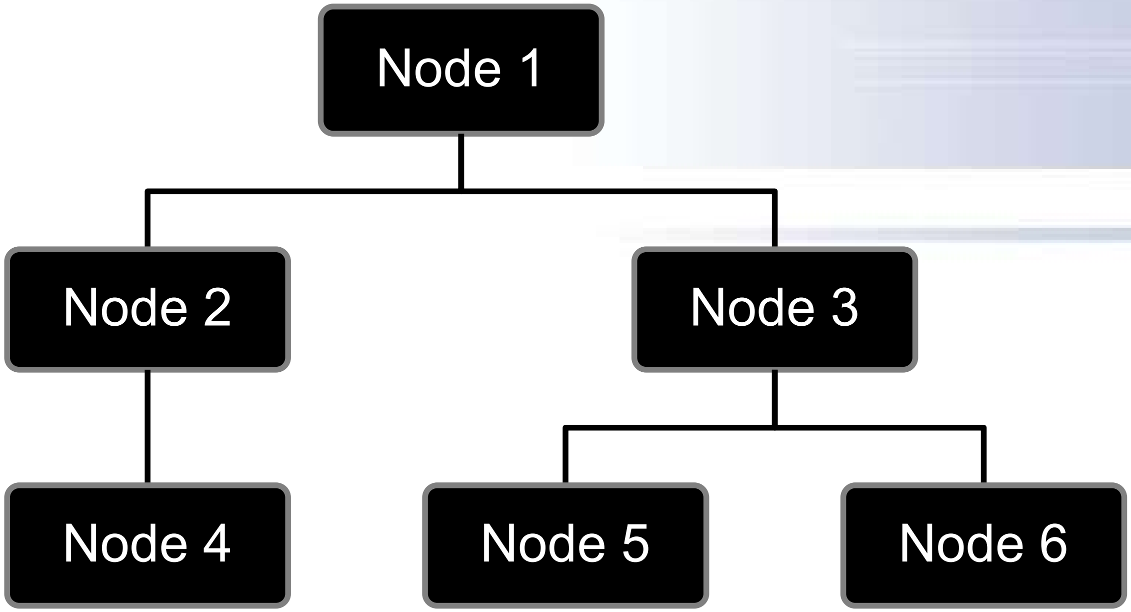
Disadvantages:

- It is complex & difficult to find the faults.
- A lot of network cable is needed, so it is costly.
- It is difficult to install & extended the network.

Network Topology

v) Tree Topology

In tree topology, the central root node is connected to one or more nodes in second level of hierarchy. The second level nodes can again be connected to third level root nodes or leaf nodes.



Node 1

Node 2

Node 3

Node 4

Node 5

Node 6

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Network Topology

v) Tree Topology

Advantages:

- It is flexible to extend & reduce
- Failure of leaf nodes does not affect the whole network.

Disadvantages:

- Failure of any hierarchical nodes may cause failure of network of that node.
- It is not easy to install.

OSI layer

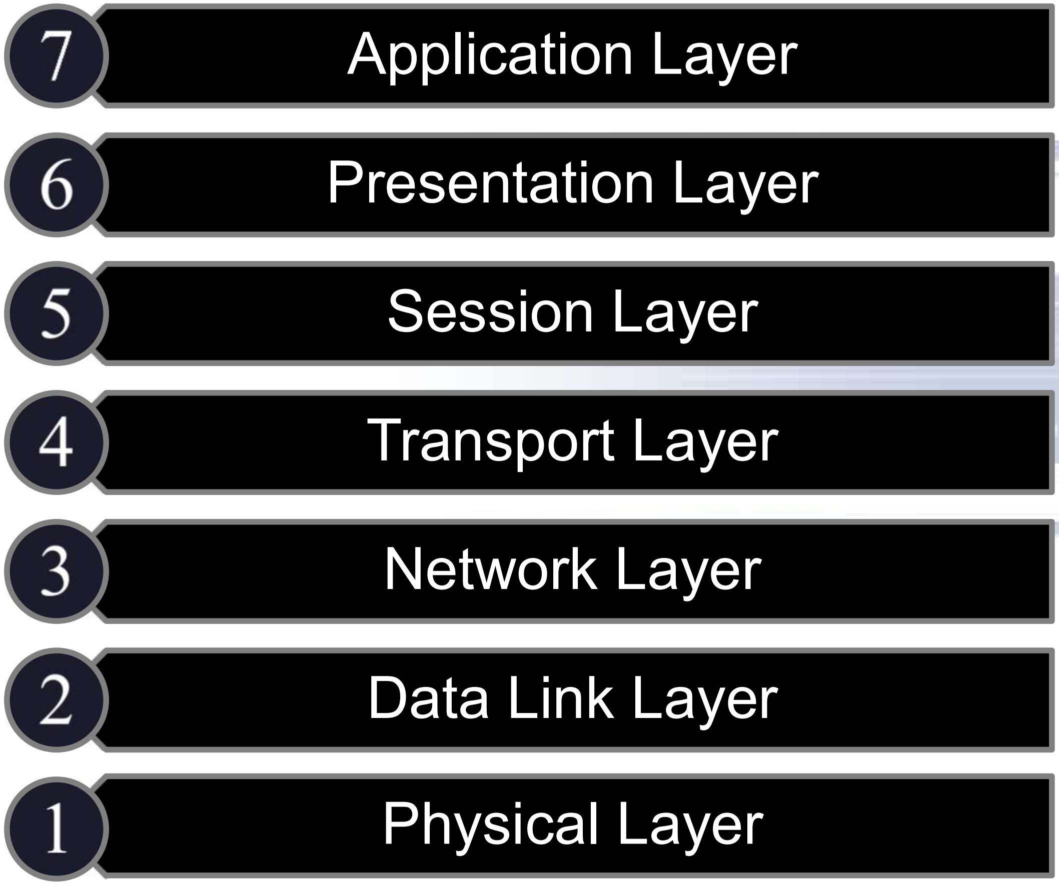
To place the distinct function in distinct place OSI is divided into several layers so that the interconnection of these layers becomes a whole system. The function of each layer is distinct so that no overhead to another layer from one layer. OSI layer consists of 7 layers but related to each other given as:

OSI layer

→ All Process Seems To Need Data Processing or

→ Please Do Not Touch Suresh’s Pet Animals or

→ Please Do Not Through Suresh’s Pizza Away



7 Application Layer

6 Presentation Layer

5 Session Layer

4 Transport Layer

3 Network Layer

2 Data Link Layer

1 Physical Layer

OSI layer

Physical Layer

This layer co-ordinates the functions required to carry a bit stream over a physical medium. It deals with the electrical and mechanical specifications of the interface and transmission medium. The main responsibility of this layer is:

- Bit Signal Representation
- Bit Synchronization
- Multiplexing
- Switching

OSI layer

Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packages into frames and sends them from source to destination. This layer is composed of two layers; i) Logical Link Layer (LLC) which identifies network protocols, performs error checking and synchronizes frames, and ii) Media Access Control (MAC) which uses MAC addresses to connect devices and defines permissions to transmit and receive data.

OSI layer

Network Layer

This layer is responsible for for the source to destination delivery of packets across multiple networks. The main functions of this layer is:

- Logical Addressing: It adds the header to the packet coming from the upper layer that includes logical address of sender and receiver.
- Routing: It chooses the best path from different alternatives. It helps to control congestion of packets.

OSI layer

Transport Layer

The transport layer takes data transferred in the session layer and breaks it into "segments" on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

OSI layer

Transport Layer

The main functions of transport layer are:

- Adds the port address to the data so that the message goes to correct receiving computers.
- It segments and reassemble the message into transmittable segments so that sequence number, destination number and data bit
- It also helps error control and flow control.

OSI layer

Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer-if the session is interrupted, devices can resume data transfer from the last checkpoint.

OSI layer

Session Layer

Its major functionalities are:

- ➢ Dialog Control: It allows the communication between two processes to take place either in half-duplex or full-duplex mode.
- ➢ Session layer allows a process to add a check-points into stream of data due to which data is error free.

OSI layer

1. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

OSI layer

1. Presentation Layer

The main duties of presentation layers are:

- Translation: This layer at the sender changes the information from its sender dependent format into a common format.
- Encryption: This layer encrypts the data at the sender and decrypts them at the receiver.

OSI layer

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).

TCP/IP Layer

Protocols are sets of rules for message formats and procedures that allow machines and application programs to exchange information. The TCP/IP suite of protocols can be understood in terms of layers (or levels). TCP/IP carefully defines how information moves from sender to receiver.

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

TCP/IP Layer

First, application programs send messages or streams of data to one of the Internet Transport Layer Protocols, either the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP). These protocols receive the data from the application, divide it into smaller pieces called packets, add a destination address, and then pass the packets along to the next protocol layer, the Internet Network layer.

TCP/IP Layer

4 Application Layer

3 Transport Layer

2 Internet Layer

1 Network Access Layer

TCP/IP Layer

The Internet Network layer encloses the packet in an Internet Protocol (IP) datagram, puts in the datagram header and trailer, decides where to send the datagram (either directly to a destination or else to a gateway), and passes the datagram on to the Network Interface layer. The Network Interface layer accepts IP datagrams and transmits them as frames over a specific network hardware, such as Ethernet or Token-Ring networks.

TCP/IP Layer

Application Layer

This is the topmost layer which indicates the applications and programs that utilize the TCP/IP model for communication. Some of the protocols used in this layer are:

- HTTP: Hypertext transfer protocol is used for accessing the information available on the internet.
- SMTP: Simple mail transfer protocol, assigned the task of handling e-mail-related steps and issues.
- FTP: This is the standard protocol that oversees the transfer of files over the network channel.

TCP/IP Layer

Transport Layer

This layer is responsible for establishing the connection between the sender and the receiver device and performs the task of dividing the data from the application layer into packets, which are then used to create sequences. It also performs the task of maintaining the data, i.e., to be transmitted without error, and controls the data flow rate over the communication channel for smooth transmission of data.

TCP/IP Layer

Transport Layer

The protocols used in this layer are:

- TCP: Transmission Control Protocol is responsible for the proper transmission of segments over the communication channel. It also establishes a network connection between the source and destination system.

UDP: User Datagram Protocol is responsible for identifying errors, and other tasks during the transmission of information.

TCP/IP Layer

Internet Layer

The Internet layer performs the task of controlling the transmission of the data over the network modes and enacts protocols related to the various steps related to the transmission of data over the channel, which is in the form of packets sent by the previous layer. The protocol applied in this layer is:

- IP: This protocol assigns your device with a unique address; the IP address is also responsible for routing the data over the communication channel.

TCP/IP Layer

Network Access Layer

This layer is the combination of data-link and physical layer, where it is responsible for maintaining the task of sending and receiving data in raw bits, i.e., in binary format over the physical communication modes in the network channel. It uses the physical address of the system for mapping the path of transmission over the network channel. Till this point in this tutorial on what is TCP/IP model, you understood the basic idea behind the model and details about its layers, now compare the model with another network model

Local Area Networks (LAN) Architecture

A Local Area Network (LAN) is a type of network that covers a small geographic area, like a home, office, or building. A LAN can be as small as two computers or as large as several hundred computers. They are usually connected using Ethernet cables, hubs, or switches. A network architecture is a blueprint that defines the structure, behavior, and protocols of a computer network

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Local Area Networks (LAN) Architecture

This architecture will determine how the LAN is designed and structured, as well as its performance. A good LAN architecture will ensure that the LAN is secure, reliable, and efficient. It will also help prevent network congestion and avoid the need for expensive upgrades or repairs. Good network architecture can also help reduce the cost of ownership by allowing for easy expansion and scalability.

Local Area Networks (LAN) Architecture

The architecture of a LAN also affects the cost of ownership, as it will determine how much hardware needs to be purchased and how much maintenance needs to be done.

Local Area Networks (LAN) Architecture

There are several different types of LAN architectures:

- **2-Tier LAN Architecture:** 2-Tier LANs are the simplest and most common type of LAN architecture. It consists of two parts: a client part, consisting of computers and other end-user devices, and a server part, consisting of servers and other networking equipment.

Logical Link Control (LLC)/Medial Access Control (MAC)

IEEE-802 standard divide OSI data link layer into two parts; LLC and MAC. These are the sublayers of the data link layer in the OSI reference model.

Network	Network Layer
Data Link	LLC Sublayer
	MAC Sublayer
Physical	Physical Layer

Logical Link Control (LLC)/Medial Access Control (MAC)

The upper sublayer of the data link layer is known as LLC sublayer. It determines with upper layers of the OSI model. It gets the network protocol data, which is usually an IPv4 packet. LLC sublayer also adds control information to help deliver the packet to the destination. The LLC sublayer communicates with the upper layers of the application and transmission the packet to the lower layers for delivery.

Logical Link Control (LLC)/Medial Access Control (MAC)

The main functionality of the LLC layer is that it multiplexes the protocols over the MAC layer while sending and de-multiplex the protocols while receiving. This layer controls the flow control. The error-checking of the data link layer is performed by LLC. It can also track the acknowledgements.

Logical Link Control (LLC)/Medial Access Control (MAC)

The Media Access Control sublayer is responsible for controlling access to the media. It is also responsible for the placement of frames on the media and the removal of frames from the media. It communicates directly with the physical layer.

It is a unique address that is allocated to the NIC of the device. It is used as an address to transmit data within ethernet. It identifies and verifies the address of source stations and destinations.

Routing

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes and paths or links that connect those nodes. Routing creates efficiency in network communication. Network communication failure results in long wait times for website pages to load for users.

A router is an internetworking device that can intelligently use network address information to decide the best path for data to take to it destination.

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

IEEE Standards

IEEE is the abbreviation of Institute of Electrical and Electronic Engineers. The IEEE computer society started a project in 1985 called Project-802 to enable standard communication between various devices.

The 802 committee of the IEEE has developed a series of standards for LANs and WANs. The 802 standards according to the OSI model.

- IEEE 802.2: Logical Link Control
- IEEE 802.3: Ethernet
- IEEE 802.4: Token Bus
- IEEE 802.5: Token Ring
- IEEE 802.11: Wireless

Compiled by: Er. Ganesh Datt Joshi, Lecturer at NAST

Contention

Contention: System in which multiple users share a common channel in a way that led to conflict is known as contention. There are three different types of contention methods:

- Aloha
- CSMA

Aloha

a. Pure Aloha

It is developed at University of Hawaii in 1970. It can transfer data with rate 9600 bps (bit per second). Whenever data is available for sending over a channel at stations we use pure aloha. The time of transmission is continuous.

Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it. Its maximum channel utilization is 18%.

Aloha

b. Slotted Aloha

It is an improvement of Aloha. It is efficient on which time on channel based on uniform slots equal to frame transmission time. It requires central clock to synchronize all stations where transmission is permitted to begin only at slot boundary. It reduces number of collisions and doubles the capacity of pure Aloha. Its maximum channel utilization is 37%.

Carrier Sense Multiple Access (CSMA)

To minimize the chances of collision and in return to increase the performance, the method name CSMA was developed. If a station senses the medium before trying to use it leads to a reduction in the chances of the collision. The carrier sense multiple access mainly requires that each station first listens to the medium before sending the data.

Carrier Sense Multiple Access (CSMA)

In simple word, CSMA method is based on the principle "Sense before transmit" or "listen before talking". It cannot eliminate the collision but it can reduce it. It is effective for networks in which the average frame transmission time is much longer than the propagation time.

Carrier Sense Multiple Access (CSMA)

CSMA/CD

The collision detection protocol known as Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is utilized to identify collisions within the media access control (MAC) layer. Upon detecting a collision CSMA/CD promptly ceases transmission y transmitting a signal, thereby preventing the sender from wasting time on sending the data packet/ If collisions occur from multiple stations while broadcasting packets, CSMA/CD rapidly transmits a jam signal to halt transmission and enters a random time delay before attending to transmit another data packet.

Carrier Sense Multiple Access (CSMA)

CSMA/CD

One the channel is found to be free; it promptly sends the data and waits a response.

The algorithm of CSMA/CD is:

- When frame is ready, checks channel is busy?
  - If busy, channel becomes idle
  - Else, start transmitting & continually monitor the channel to detect collision.
- If Collision occurred, station start collision resolution.
- Station resets the transmission counters & completes frame transmission.

Carrier Sense Multiple Access (CSMA)

CSMA/CA

This protocol is modification of pure CSMA. It improves the performance of CSMA by attempting to be less "greedy" on the channel. This protocol does not listen and detect collisions, instead it does not avoid collisions before they happen.

All devices before they transmit, must wait an amount of time called an intra-frame space (IFS). If two applications want to transmit at the same time, the applications with the shorter IFS will go first.

Carrier Sense Multiple Access (CSMA)

CSMA/CA

A station wishing to transmit must first listen to the channel for a predetermined amount of time to check for any activity on the channel. Once the channel is clear a station sends a signal telling all other stations not to transmit and then sends its packet.

CSMA/CD is used in 802.11 based wireless LANs. One of the problems of wireless LANs is that it is not possible to listen while sending; therefore, collision detection is not possible.

Wide Area Networks (WAN)

X.25

It is a network protocol developed in 1976 and it specifies an interface between a host system and packet switching network. It allows computer on different public network to communicate through an intermediatory computers at the network layer level.

Wide Area Networks (WAN)

X.25

X.25 describes the procedure, which are related for establishing, maintaining and terminating connections. The functionality of X.25 is specified on three levels.

i) Physical Level

ii) Link Level

iii) Packet Level

Wide Area Networks (WAN)

X.25

Network Layer	Packet-level
Data link layer	Link level
Physical layer	Physical level

Wide Area Networks (WAN)

X.25

The features of X.25 are as follows:

- ✓ Both layers ii) and iii) include flow control and error control mechanism.
- ✓ Physical layer is called X.21 interface, interface exists between DTE and X.25 network.
- ✓ X.25 provides data-link control using a link-access protocol and transmit data as a sequence of frames.

Wide Area Networks (WAN)

X.25

The features of X.25 are as follows:

- ✓ X.25 provides virtual circuit service this enables any subscriber to network setup, logical connection to another subscriber.

Wide Area Networks (WAN)

X.25

The drawbacks of X.25 are:

- ✓ X.25 has low data rate i.e. 64 kbps.
- ✓ It has extensive flow and error control at both data-link layer and network layer which create a large overhead and slowdown transmission.

Wide Area Networks (WAN)

Frame Relay

Frame relay is a virtual circuit wide area network that was designed in response to demands for a new type of WAN in late 1980s and early 1990s. Frame relay provides permanent virtual circuits. The frame relay WAN is used as one link in the global internet.

Frame Relay

Frame relay has physical and data link layer:

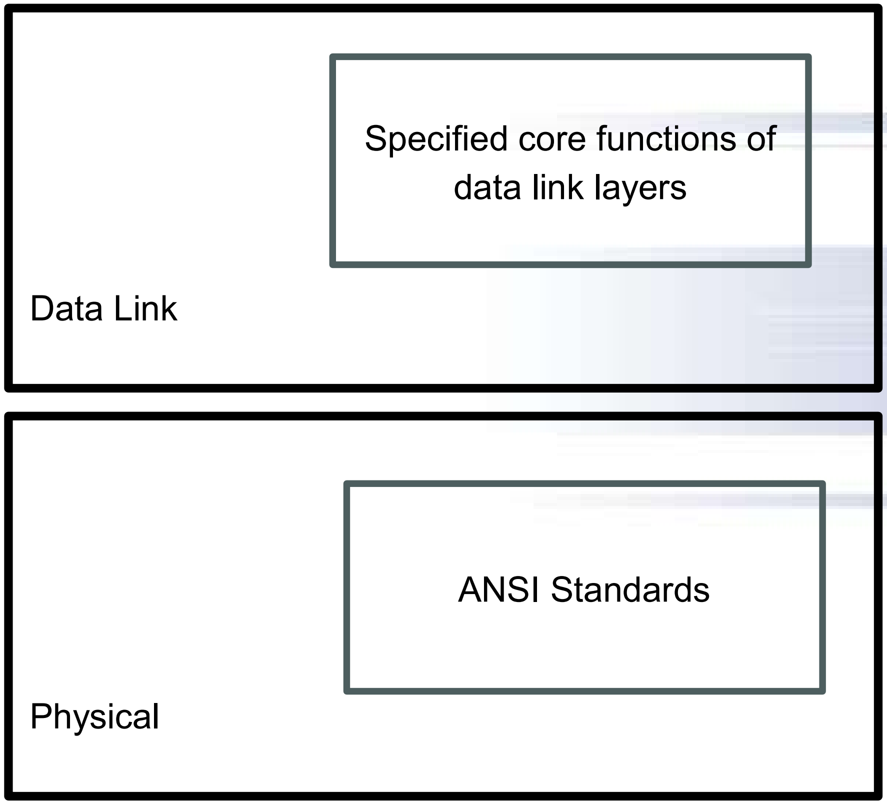


Fig: Frame Relay Layers

Wide Area Networks (WAN)

Frame Relay

i) Physical Layer:

No specific protocol is defined for the physical layer in frame relay. Instead, it is left to the implementer to use whatever is available. Frame relay supports any of the protocols recognized by ANSI.

Wide Area Networks (WAN)

Frame Relay

ii) Data Link Layer:

At the data link layer, frame relay uses a simple protocol that does not support flow or error control. It only an error detection mechanism.

Wide Area Networks (WAN)

Frame Relay

The features of frame relay are as follows:

- ✓ It operates at higher speed (1.544 Mbps and recently 44.375 Mbps)
- ✓ It allows bursty data.
- ✓ Frame relay is less expensive than other traditional WANs.
- ✓ Frame relay has error detection at the data link layer only.
- ✓ Frame relay allows a frame size of 9000 bytes, which can accommodate at local area network frame sizes.

Asynchronous Transfer Mode (ATM)

It is the cell relay protocol designed by the ATM forum and adopted by the ITU-T. ATM uses asynchronous time division multiplexing to multiplex cells coming from different channels.

In ATM, connection between two endpoints is accomplished through transmission path, virtual paths and virtual circuits. In ATM, a combination of virtual path identifier identifies a virtual connection.

Wide Area Networks (WAN)

Asynchronous Transfer Mode (ATM)

The ATM standard defines three layers.

i) Application Adaption Layer
ii) ATM Layer
iii) Physical Layer

The application adaptation layer (AAL) accepts transmissions from upper-layer services and maps them to ATM cells.

ATM layer provides routing, traffic management, switching and multiplexing services.