JGI JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

Master of Computer Applications

23MCAC102 – Advanced Computer Networks

Dr Murugan R Professor School of CS & IT

SYLLABUS

23MCAC102 – Advanced Computer Networks

Module	Details
I (9 Hrs)	INTRODUCTION AND PHYSICAL LAYER Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Switching – Circuit-switched Networks – Packet Switching.
II (9 Hrs)	DATA-LINK LAYER & MEDIA ACCESS Introduction – Link-Layer Addressing –Media Access Control – Wired LANs: Ethernet – Wireless LANs : IEEE 802.11, Bluetooth – Connecting Devices.
III (9 Hrs)	NETWORK LAYER Network Layer Services –IPv4 Packet format –IPV4 Addresses – Network Layer Protocols: IP, ICMPv4 – Unicast Routing Protocols – IPV6 Addressing – IPV6 Protocol – Mobile IP

SYLLABUS

23MCAC102 – Advanced Computer Networks

JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

IV (9 Hrs)	TRANSPORT LAYER & APPLICATION LAYER Introduction – Transport Layer Protocols –TCP Services – Port Numbers – User Datagram Protocol. HTTP –DHCP - FTP – Email – Telnet –SSH – DNS
V (9 Hrs)	NETWORK SECURITY Security Services, Message Confidentiality, Message Integrity, Message Authentication, Digital Signature, Entity Authentication, Key Management, IP Security, SSL, Firewall types.

Text Books:	
1	"Computer Networking, A Top-Down Approach Featuring the Internet", James F. Kurose, Keith W. Ross, Pearson Education, 3rd Edition, 2006. ISBN-13: 978-0-13-285620-1 (Module 1 & 2)
2	"Computer Networks: A Systems Approach", Larry L. Peterson, Bruce S. Davie, Morgan Kaufmann Publishers Inc., 5th Edition, 2011. ISBN : 978-0123850591 (Module 1, 3 & 4)
3	William Stallings, "Data and Computer Communications", Tenth Edition, Pearson Education, 2013, ISBN-13: 978-0133506488. (Module 5)
Reference Books:	
4	"Computer and Communication Networks", Nader F. Mir, Pearson Education, First Edition, 2007, ISBN: 978-0131747999.
5	"Computer Networks: An Open Source Approach", Ying-Dar Lin, Ren-Hung Hwang and Fred Baker, McGraw Hill Publisher, First Edition, 2011. ISBN : 978-0073376240.
6	"Data communication and Networking", Behrouz A. Forouzan, Tata McGraw-Hill, 5th Edition, 2017. ISBN : 978-1259064753.

Internal Assessment (IA): 50 Marks

Internal Test (15 Marks)	Activity (30 Marks)	Class Participation (5)
Internal Test-1 (25 Marks)	MooC Course through Coursera (15 Marks)	Active Participation in Co-curricular Activities / Extra Curricular Activities (**5 Marks**)
Internal Test-2 (25 Marks)	Case Study Report (15 Marks)	
50 Marks will be reduced to **15 Marks**	Total: **30 Marks**	

End Semester Exam: 50 Marks

Section-A (20 Marks)	Section-B (18 Marks)	Section-C (12)
Answer 5 Questions out of 5 (4 x 5 = 20)	**Answer 2 Questions out of 3 (2 x 9 = 18)**	**Case Study / Long Answer Question – NO CHOICE (1 x 12=12)**

MODULE-1

INTRODUCTION AND PHYSICAL LAYER

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Switching – Circuit-switched Networks – Packet Switching.

INTRODUCTION TO NETWORKS

- A network is a set of devices (often referred to as nodes) connected by communication links.
- A node can be a computer, printer, or any other device capable of sending or receiving data generated by other nodes on the network.
- When we communicate, we are sharing information. This **sharing can be local or remote.**

CHARACTERISTICS OF A NETWORK

The effectiveness of a network depends on three characteristics.

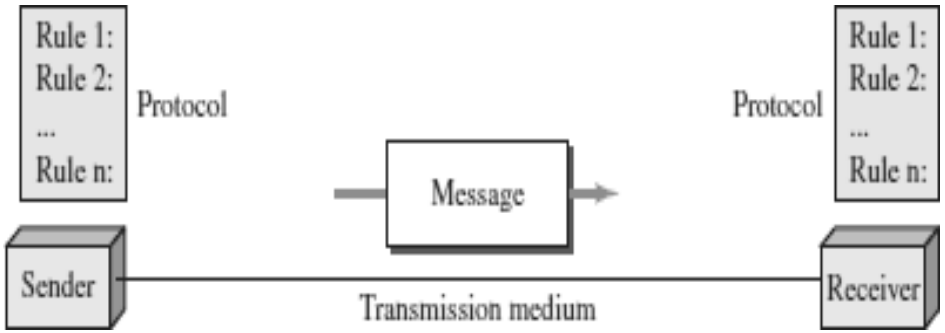
1. ***Delivery***: The system must deliver data to the correct destination.
2. ***Accuracy***: The system must deliver data accurately.
3. ***Timeliness***: The system must deliver data in a timely manner.

CRITERIA NECESSARY FOR AN EFFECTIVE AND EFFICIENT NETWORK

- A network must be able to meet a certain number of criteria. The most important of these are **Performance, Reliability, and Security.**

Factors that affect the Performance of a network:	Factors that affect the Reliability of a network:	Factors that affect the Security of a network:
1. Number of users 2. Type of transmission medium 3. Capabilities of the connected hardware	1. Efficiency of software 2. Frequency of failure 3. Recovery time of a network after a failure	Protecting data from unauthorized access and viruses.

COMPONENTS INVOLVED IN A NETWORK PROCESS



The five components are:

Message - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc.

Sender - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.

Receiver - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.

Transmission Medium - It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radiowaves etc.

Protocol - It is a **set of rules that governs the data communications**. It represents an agreement between the communicating devices. **Without a protocol, two devices may be connected but not communicating.**

KEY ELEMENTS OF PROTOCOL

Syntax: Refers to the structure or format of the data, meaning the order in which they are presented.

Semantics: Refers to the meaning of each section of bits.

Timing: Refers to two characteristics.
(1) When data should be sent **and**
(2) How fast they can be sent.

TRANSMISSION MODES

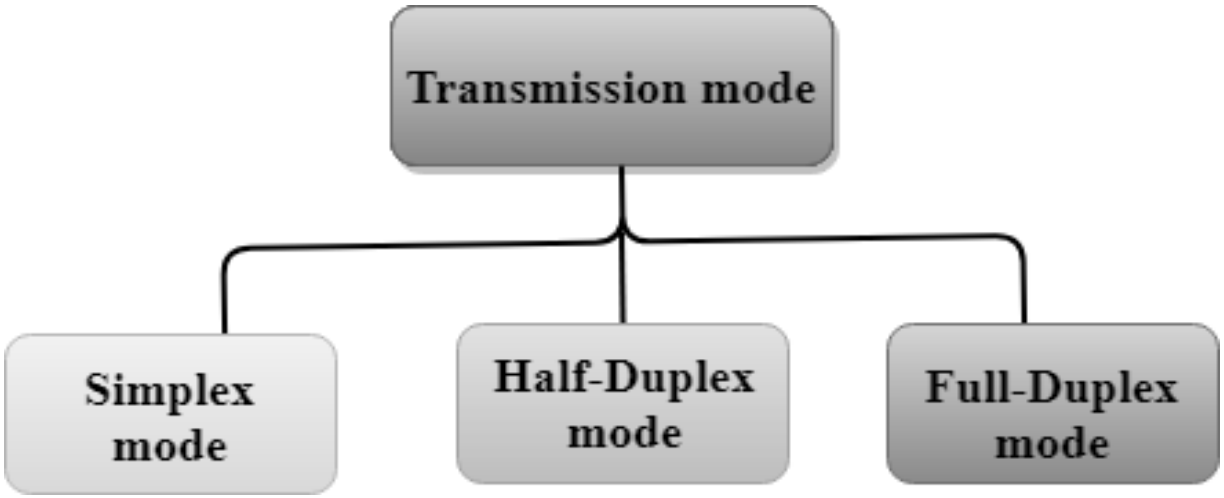
TRANSMISSION MODES

- The **way in which data is transmitted** from one device to another device is known as **transmission mode.**
- The transmission mode is also known as the communication mode.
- Each **communication channel has a direction associated** with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
- The **transmission mode is defined in the physical layer.**

Types of Transmission Mode

The Transmission mode is divided into three categories:

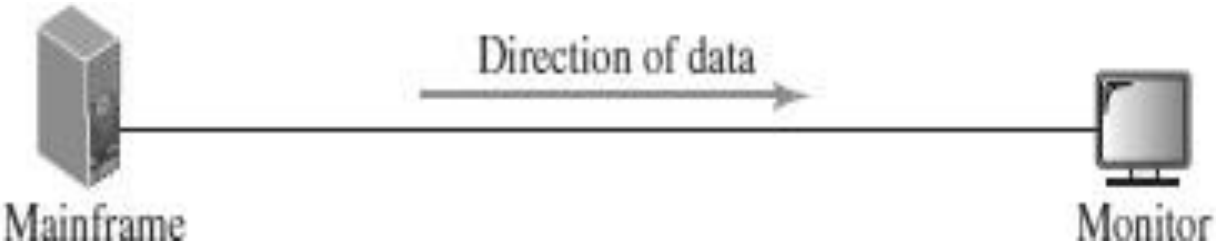
- Simplex Mode
- Half-duplex Mode
- Full-duplex mode (Duplex Mode)



SIMPLEX MODE

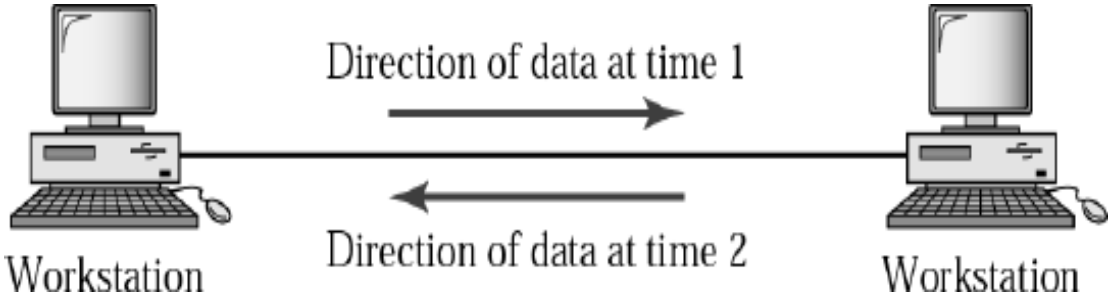
In Simplex mode, the **communication is unidirectional**, i.e., the data flow in one direction.

- A device **can only send the data but cannot receive it** or **it can receive the data but cannot send the data.**
- This transmission mode is not very popular as mainly communications require the two-way exchange of data.
- The **radio station is a simplex channel** as it transmits the signal to the listeners but never allows them to transmit back.
- **Keyboard and Monitor** are the examples of the simplex mode
- The main **advantage** of the simplex mode is that the **full capacity of the communication channel can be utilized** during transmission.
- Not possible to perform error detection.



HALF-DUPLEX MODE

- In a Half-duplex channel, direction can be reversed, i.e., the **station can transmit and receive the data as well.**
- Messages flow in both the directions, but **not at the same time**.
- The entire bandwidth of the communication channel is utilized in one direction at a time.
- In half-duplex mode, it is **possible to perform the error detection**, and **if any error occurs, then the receiver requests the sender to retransmit the data**.
- A **Walkie-talkie** is an example of the Half-duplex mode.
- In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.



***Advantage of Half-duplex mode*:**

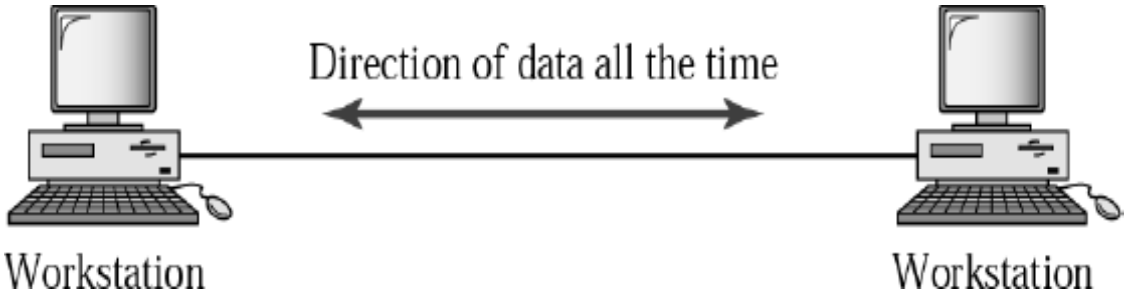
- In half-duplex mode, both the devices can send and receive the data and also **can utilize the entire bandwidth** of the communication channel during the transmission of data.

***Disadvantage of Half-Duplex mode*:**

- In half-duplex mode, **when one device is sending the data, then another has to wait**, this **causes the delay** in sending the data at the right time.

FULL-DUPLEX MODE

- In Full duplex mode, the **communication is bi-directional**, i.e., the data flow in both the directions.
- Both the stations can send and receive the message simultaneously.
- Full-duplex mode **has two simplex channels. One channel has traffic moving in one direction**, and another channel has traffic flowing in the opposite direction.
- The Full-duplex mode is the **fastest mode of communication** between devices.
- The most common example of the full-duplex mode is a **Telephone network**. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.



Advantage of Full-duplex mode:

- Both the stations can send and receive the data at the same time.

Disadvantage of Full-duplex mode:

- **If there is no dedicated path exists between the devices,** then the capacity of the **communication channel is divided into two parts.**

COMPARISON - SIMPLEX, HALF-DUPLEX AND FULL-DUPLEX MODE

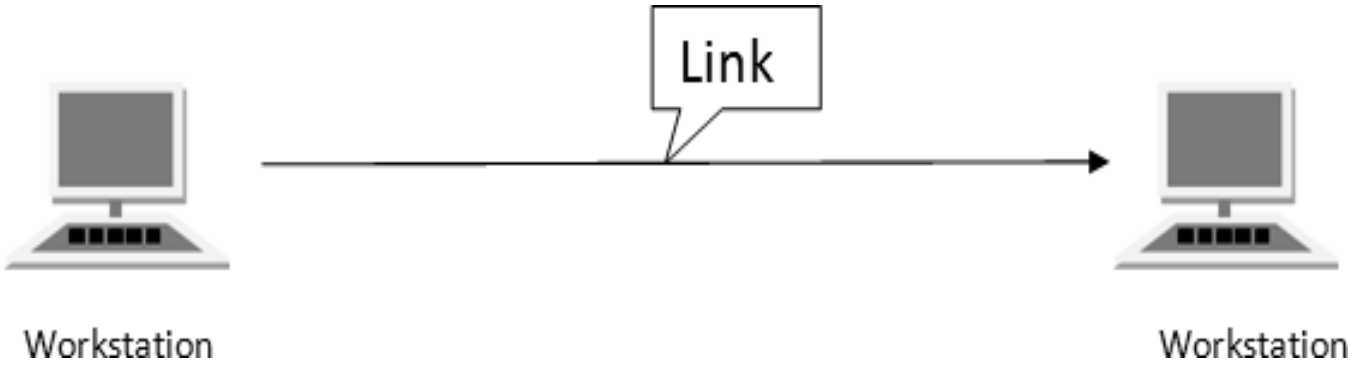
BASIS FOR COMPARISON	SIMPLEX MODE	HALF-DUPLEX MODE	FULL-DUPLEX MODE
Direction of communication	Communication is unidirectional.	Communication is bidirectional, but one at a time.	Communication is bidirectional.
Send / Receive	A device can only send the data but cannot receive it or it can only receive the data but cannot send it.	Both the devices can send and receive the data, but one at a time.	Both the devices can send and receive the data simultaneously.
Example	Radio, Keyboard, and monitor.	Walkie-Talkie	Telephone network.

LINE CONFIGURATION / LINE CONNECTIVITY

- Line configuration refers to **the way two or more communication devices attach to a link.**
- A **link is a communications pathway** that transfers data from one device to another.
- There are two possible line configurations:

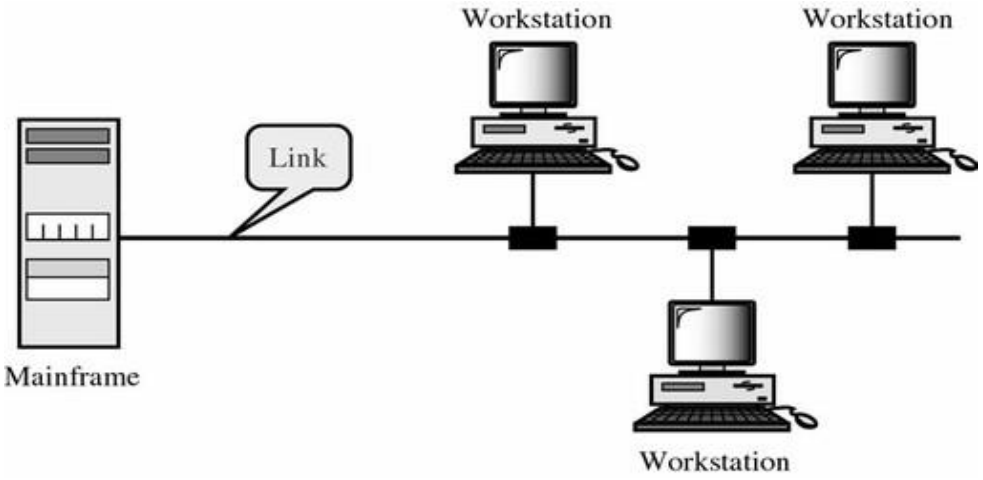
i) ***Point to Point* (PPP): Provides a dedicated Communication link between two devices.**

→ The most common example for Point-to-Point connection is a computer **connected by telephone line**. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.



ii) MultiPoint* :** It is also called ***Multidrop configuration. In this connection, **two or more devices share a single link.** **There are two kinds of Multipoint Connections.**

- **Spatial Sharing**: If **several devices can share the link simultaneously**, it is called Spatially shared line configuration.
- **Temporal (Time) Sharing**: If **users must take turns using the link** , then its called Temporally shared or Time Shared Line Configuration.



TYPES OF NETWORK TOPOLOGY

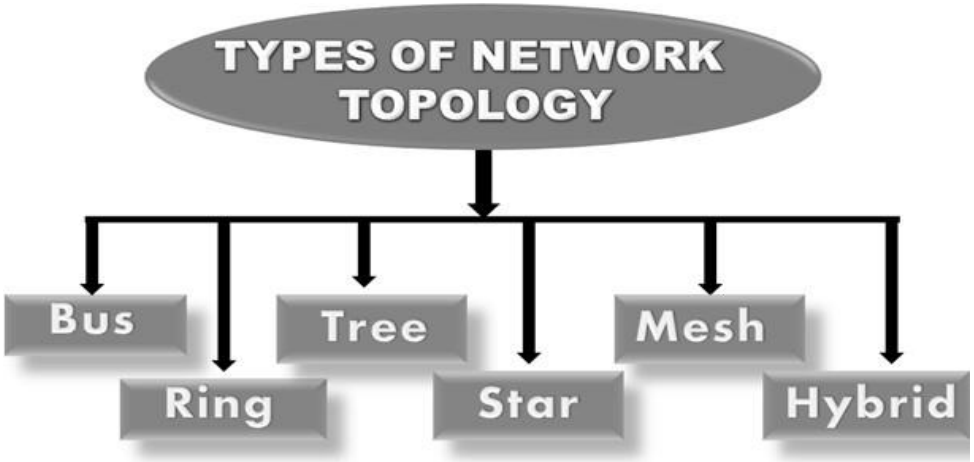
NETWORK TOPOLOGY

Two or more devices connect to a link. Two or more links form a topology.

Topology is defined as

- The **way in which a network is laid out physically.**
- The **geometric representation of the relationship of all the links and nodes** to one-another.
- The various types of topologies are :

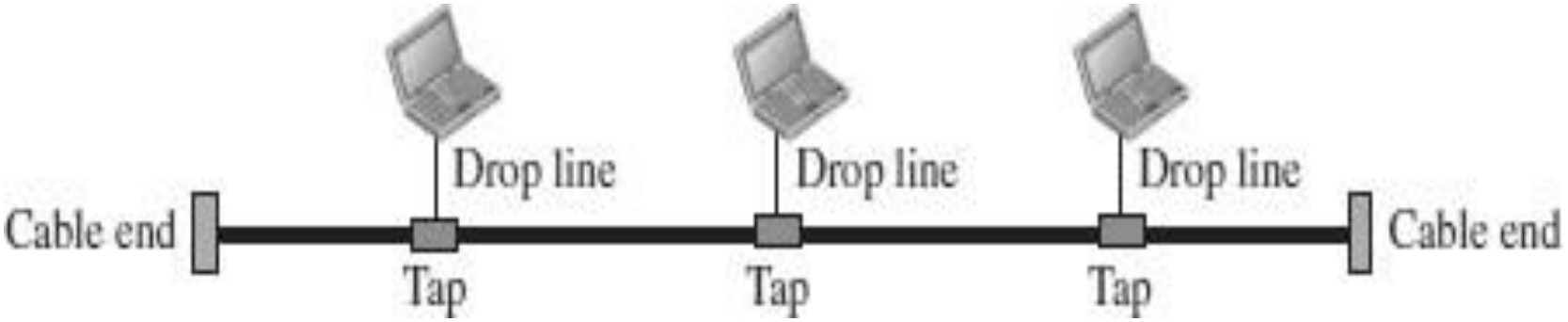
Bus, Ring, Star, Tree, Mesh and Hybrid.



BUS TOPOLOGY

Bus topology is a network type in which **every computer and network device is connected to single cable.**

- The long single cable acts as a backbone to link all the devices in a network.
- When it has exactly two endpoints, then it is called **Linear Bus topology.**
- It **transmits data only in one direction.**
- It is **useful to connect a smaller number of devices**.



Advantages of Bus Topology

1. It is cost effective.

2. Cable required is least compared to other network topology.

3. Used in small networks.

4. Easy to expand joining two cables together

Disadvantages of Bus Topology

1. Cable fails then whole network fails.

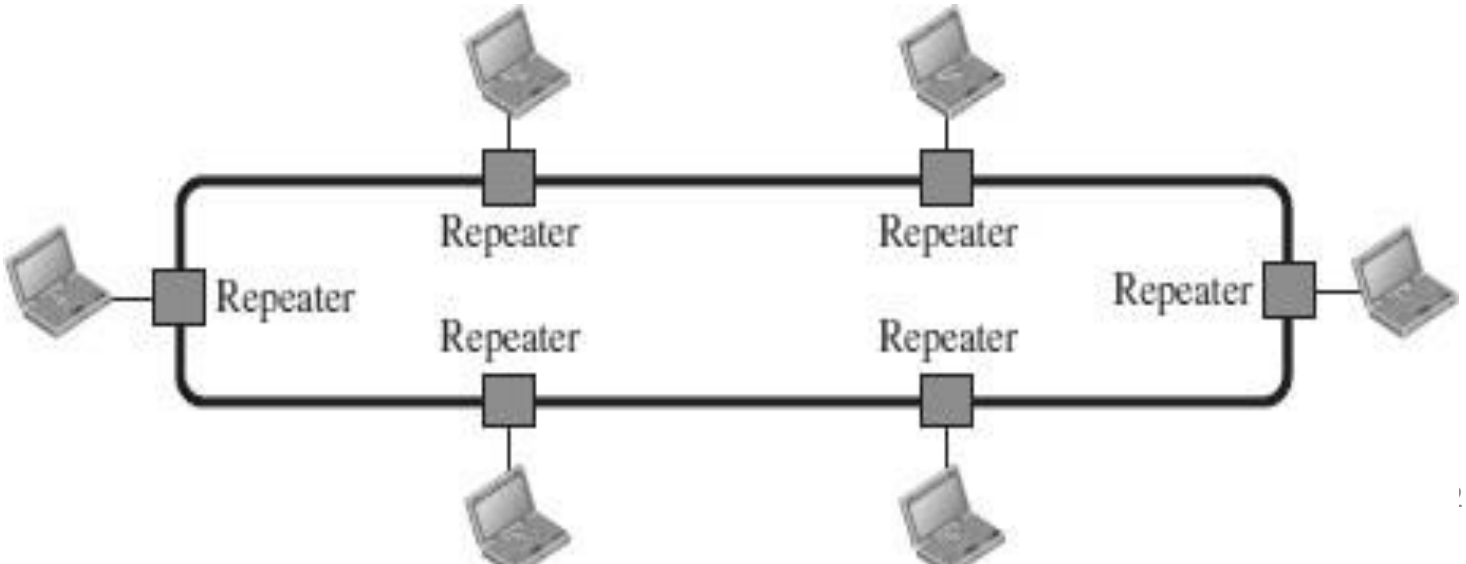
2. If network traffic is heavy or nodes are more, the performance of the network decreases.

3. Cable has a limited length.

4. It is slower than the ring topology.

RING TOPOLOGY

- In a ring topology, each device has a dedicated point-to-point connection with only two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a **repeater**.
- When a device receives a signal intended for another device, its **repeater regenerates** the bits and passes them along.
- If one of the nodes are damaged, it will **damage the whole network**
- It is used very rarely as **it is expensive and hard to install** and **manage**



Advantages of Ring Topology

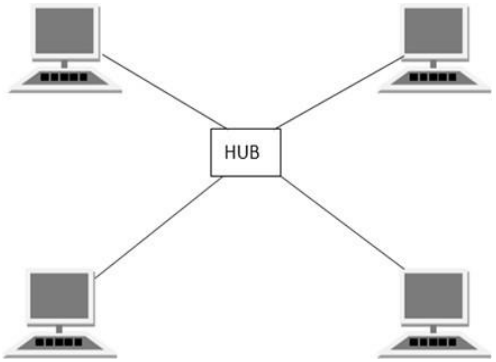
- Since data flows in one direction, the chance of a packet collision is reduced.
- A network server is not needed to control network connectivity.
- Devices can be added without impacting network performance.
- Easy to identify and isolate single point of failure.

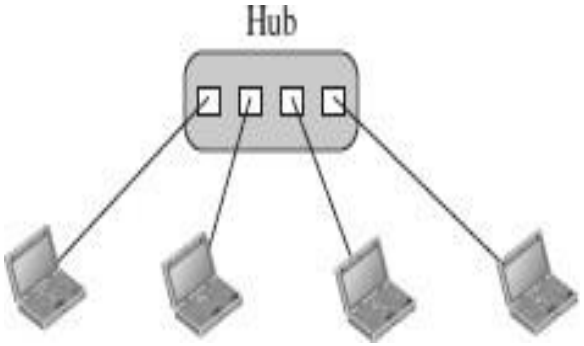
Disadvantages of Ring Topology

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network

STAR TOPOLOGY

- In a star topology, each device has a **dedicated point-to-point link** only to a **central controller, usually called a hub / switch.**
- The **devices are not directly linked to one another.**
- The controller acts as an exchange.
- If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.
- **If the central node fails the complete network is damaged**.
- Mainly used in home and office networks.





Advantages of Star Topology

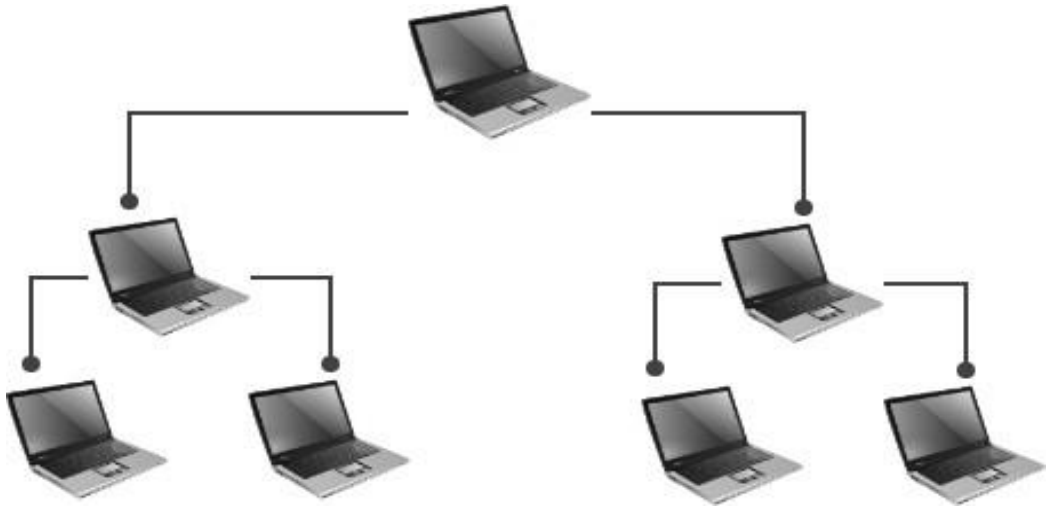
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly

Disadvantages of Star Topology

- Cost of installation is high.
- Expensive to use.
- If the hub fails, then the whole network is stopped.
- Performance is based on the hub that is it depends on its capacity

TREE TOPOLOGY

- It has a **root node** and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should **at least have three levels to the hierarchy**.
- Tree topology is **ideal if workstations are located in groups**. They are **used in Wide Area Network.**
- If the main bus fails, the **whole network is damaged.**



Advantages of Tree Topology

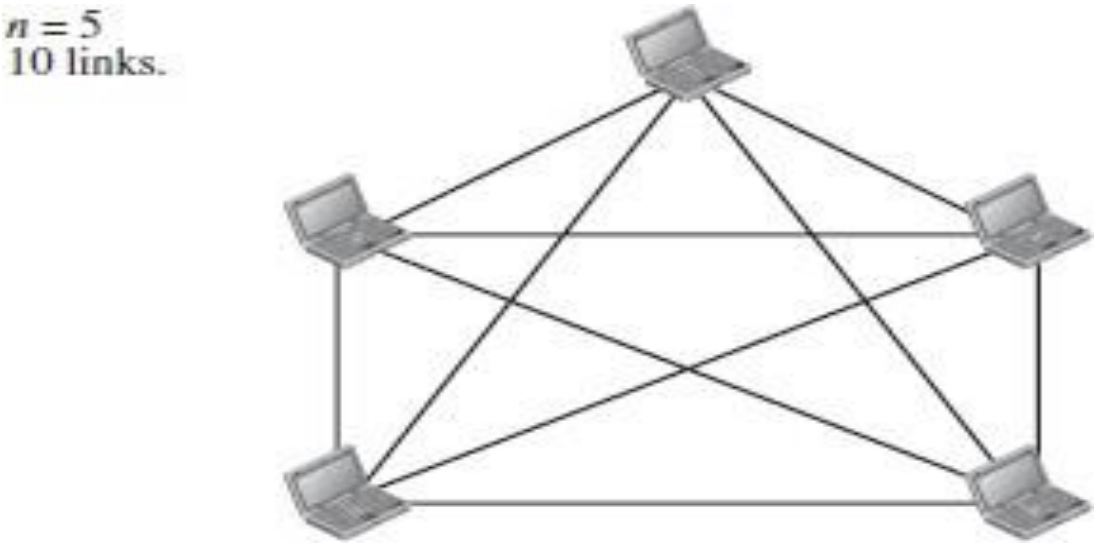
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

MESH TOPOLOGY

- In a mesh topology, every device has a **dedicated point-to-point link to every other device.**
- The term dedicated means that the link carries traffic only between the two devices it connects.
- The number of physical links in a fully connected mesh network with *n* nodes is given by ***n* (*n* – 1) / 2.**
- It is **robust** as failure in one link only disconnects that node.
- It is rarely used and installation and management are difficult.
- **Cabling cost is high** as it requires bulk wiring.



Advantages of Mesh Topology

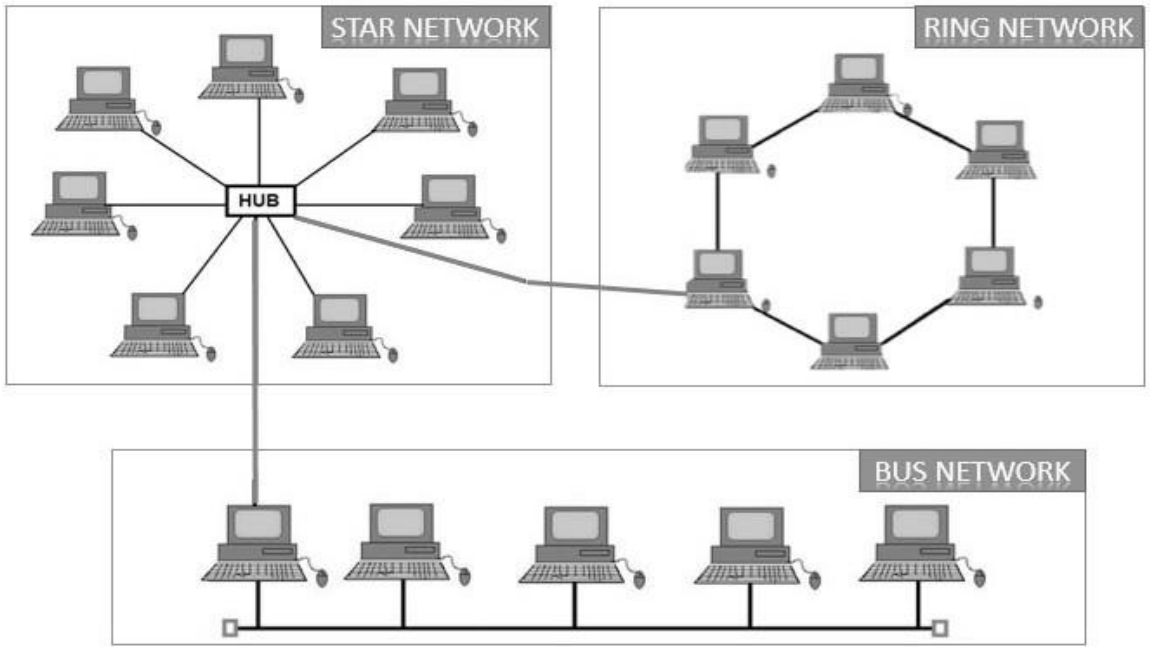
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

HYBRID TOPOLOGY

- Hybrid Topology is a combination of one or more basic topologies.
- For example if one department in an office uses ring topology, the other departments uses star and bus topology, then connecting these topologies will result in Hybrid Topology.
- Hybrid Topology **inherits the advantages and disadvantages of the topologies included.**



Advantages of Hybrid Topology

- Reliable as Error detecting and trouble shooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.
- Used for a vast network

Disadvantages of Hybrid Topology

- Complex in design
- Difficult to install
- Costly
- Hardware requirements are more
- Cable failures

NETWORK TYPES

NETWORK TYPES

- 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.**

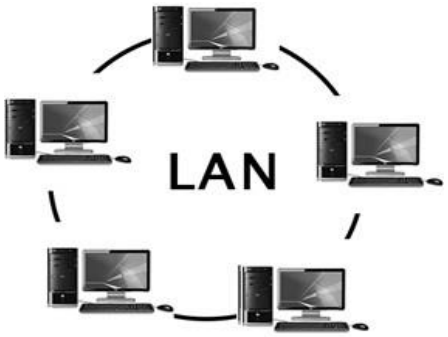
- A computer network can be **categorized by their size.**

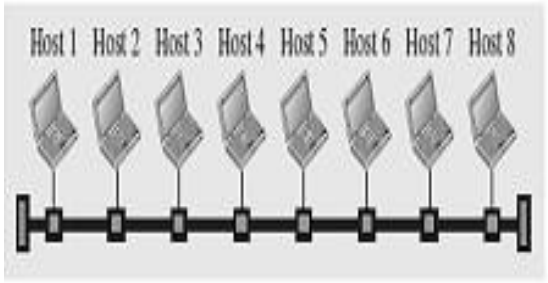
- A computer network is mainly of **three types:**
  - Local Area Network (**LAN**)
  - Wide Area Network (**WAN**)
  - Metropolitan Area Network (**MAN**)

LOCAL AREA NETWORK (LAN)

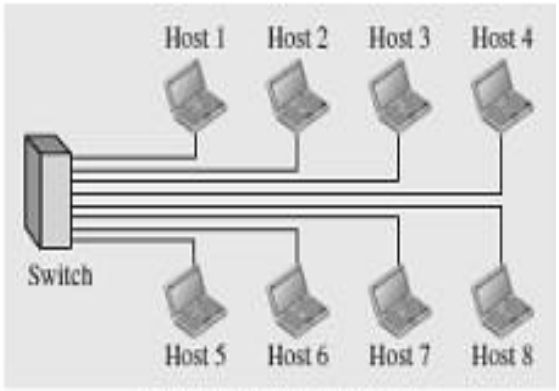
JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

- LAN 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 an extremely faster rate** in Local Area Network.
- **LAN can be connected using a common cable or a Switch**.





a. LAN with a common cable (past)



b. LAN with a switch (today)

LAN – Advantages & Disadvantages

Advantages of LAN

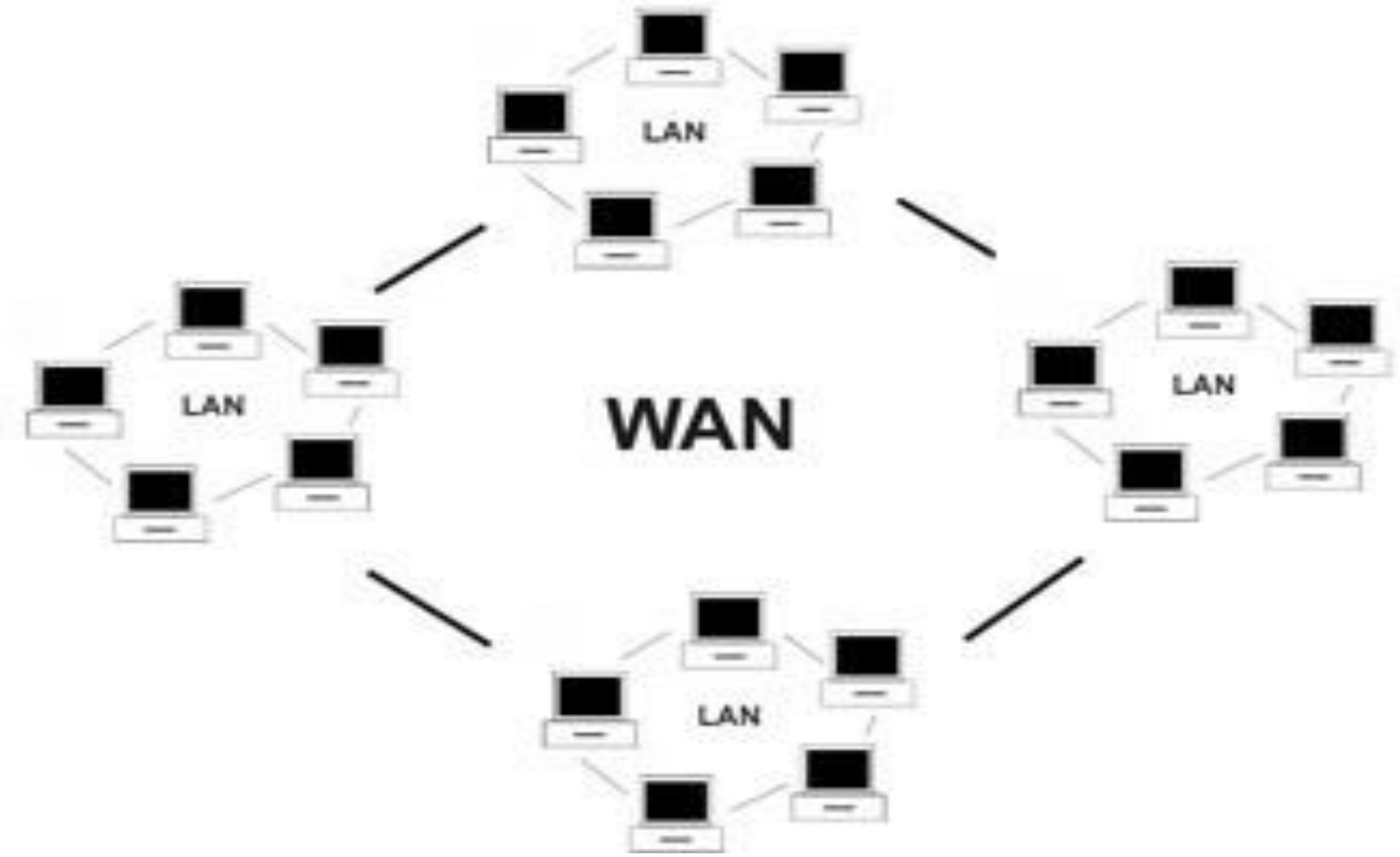
- Resource Sharing
- Software Applications Sharing.
- Easy and Cheap Communication
- Data Security
- Internet Sharing

Disadvantages of LAN

- LAN Maintenance
- Covers Limited Area

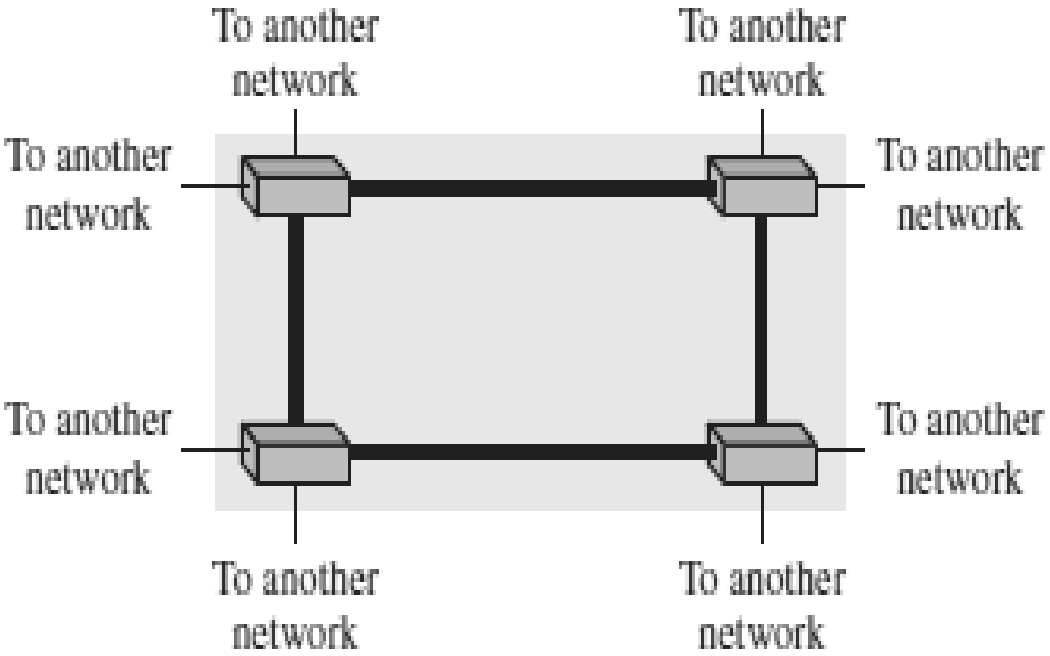
WIDE AREA NETWORK (WAN)

- A Wide Area Network is a network that **extends over a large geographical area** such as states or countries.
- A Wide Area Network 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, fibre 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**.
- WAN can be either a point-to-point WAN or Switched WAN.


LAN
LAN
WAN
LAN
LAN

Point-to-point WAN

Switched WAN



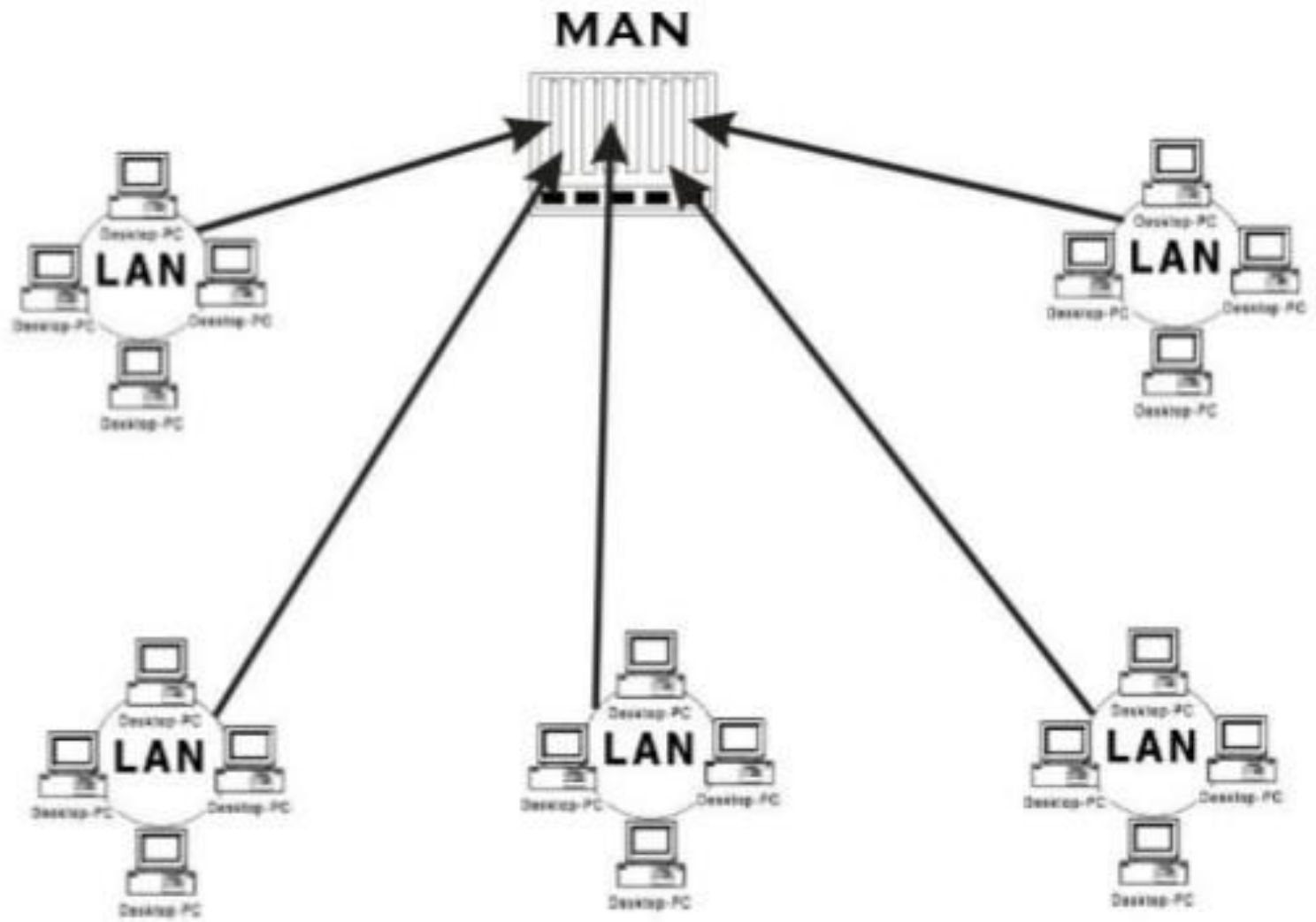
- **A router in growing network, creating an internetwork and breaking up broadcast domains**

WAN – Advantages & Disadvantages

Advantages of Wide Area Network:	*Disadvantages of Wide Area Network:*
• Large Geographical area • Centralized data • Exchange messages • Sharing of software and resources • High bandwidth	• Security issue • Needs Firewall & antivirus software • High Setup cost • Troubleshooting problems

METROPOLITAN AREA NETWORK (MAN)

- A metropolitan area network is a network that **covers a larger geographic area by interconnecting a different LAN** to form a larger network.
- It generally **covers towns and cities (50 km)**
- In MAN, various LANs are connected to each other through a telephone exchange line.
- **Communication medium** used for MAN are **optical fibers, cables etc.**
- It has a **higher range than Local Area Network**(LAN).
- It is adequate for distributed computing applications.


MAN
LAN
LAN
LAN
LAN
LAN

- **PAN (Personal Area Network)**: Its **range limit is up to 10 meters**. It is created for personal use. Generally, **personal devices are connected** to this network. For example computers, telephones, fax, printers, etc.

- **HAN (House Area Network)**: It is actually a **LAN that is used within a house** and used to connect homely devices like personal computers, phones, printers, etc.

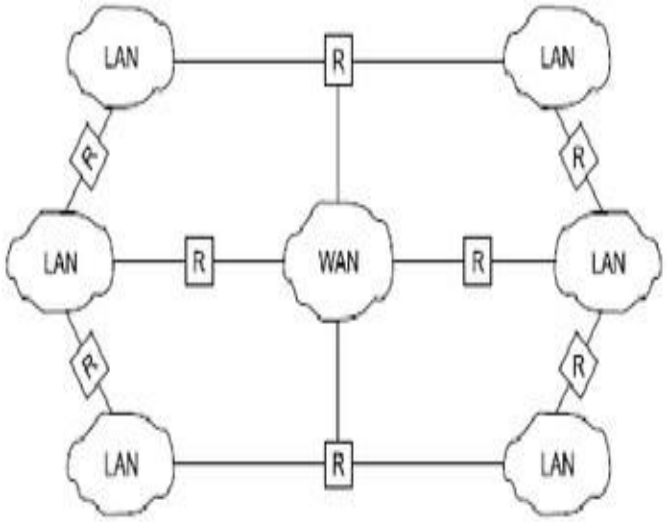
- **CAN (Campus Area Network)**: It is a **connection of devices within a campus area** which links to other departments of the organization within the same campus.

- **GAN (Global Area Network)**: It **uses satellites to connect devices over global area**

INTERNETWORK

An internetwork is defined as two or more computer network LANs or WAN.

- An Internetwork can be formed by **joining two or more individual networks by means of various devices such as routers, gateways and bridges.**
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.



Intranet & Extranet

Intranet

- An **intranet is a private network** used by employees to **communicate and collaborate**.
- They can also use the company intranet **to create content, complete their work, and engage in the company culture**.

Extranet

- An **extranet is a private network**. It works similarly to a company intranet;
- however an extranet **allows access to authorized users from outside the company.**
- These external users may include **suppliers and partners**.

Extranet Vs. Intranet

- An extranet is used for information sharing.
- The access to the extranet is restricted to only those users who have login credentials.
- It can be categorized as MAN, WAN or other computer networks.
- An extranet cannot have a single LAN, atleast it must have one connection to the external network.

- An intranet belongs to an organization which is only accessible by the organization's employee or members.
- The main aim of the intranet is to share the information and resources among the organization employees.
- An intranet provides the facility to work in groups and for teleconferences.

PROTOCOL LAYERING

PROTOCOL LAYERING

- In networking, a protocol **defines the rules** that both the sender and receiver and all intermediate devices need to follow to be able **to communicate effectively**.
- When the communication is complex, we may **need to divide the task between different layers**, in which case we need a protocol at each layer, or **protocol layering.**
- Protocol layering is that it allows us to separate the services from the implementation.
- A layer needs to be able **to receive a set of services from the lower layer** and to give the services to the upper layer.
- Any **modification in one layer will not affect** the other layers.

Basic Elements of Layered Architecture

- **Service:** It is a set of actions that a layer provides to the higher layer.
- **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity.
  ➔ These rules mainly concern about both the contents and order of the messages used.
- **Interface:** It is a way through which the message is transferred from one layer to another layer.

Features of Protocol Layering

- **It decomposes the problem of building a network** into more manageable components.
- **It provides a more modular design.**

Principles of Protocol Layering

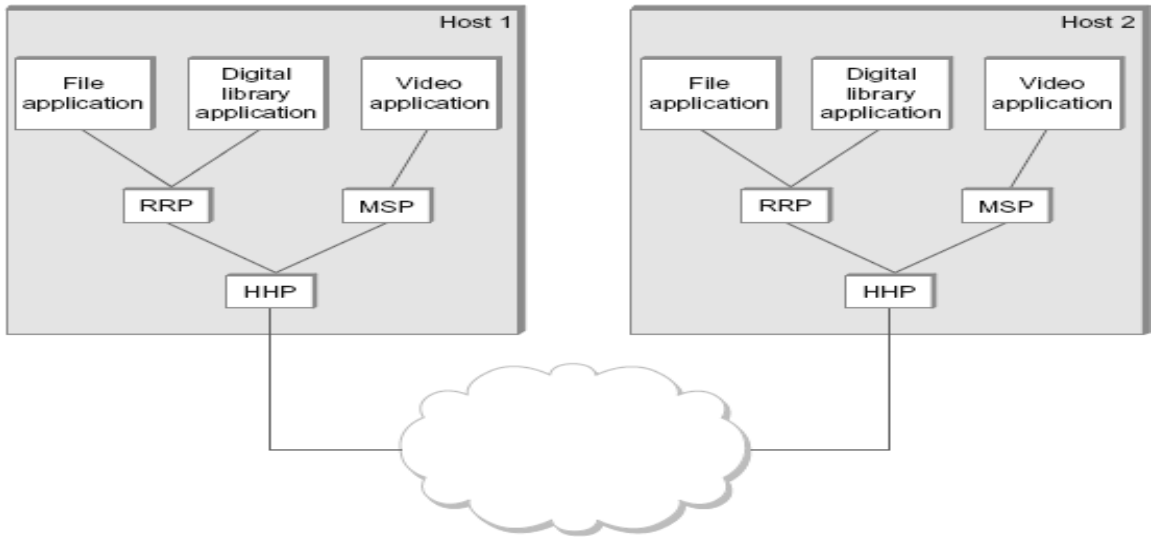
1st Principle: If we want **bidirectional communication**, we need to make each layer so that it is able **to perform two opposite tasks, one in each direction.**

2nd Principle: We need to follow in protocol layering is that the **two objects under each layer at both sites should be identical.**

Protocol Graph

- The set of protocols that make up a network system is called a **protocol graph**.
- The nodes of the graph correspond to protocols, and the edges represent a dependence relation.

Protocol graph consists of protocols ***RRP (Request/Reply Protocol)*** and ***MSP (Message Stream Protocol)***



OSI MODEL

- OSI stands for **Open System Interconnection.**
- It is a reference model that describes **how information from a software application in one computer moves** through a physical medium **to the software application in another computer.**
- OSI consists of **seven layers**, and **each layer performs a particular network function.**
- **OSI model** was developed by the ISO in 1984, and it is now considered as **an architectural model for the inter-computer communications**.
- OSI model **divides the whole task into seven smaller and manageable tasks**. Each layer is assigned a particular task.
- **Each layer is self-contained**, so that **task assigned to each layer can be performed independently.**

ORGANIZATION OF THE OSI LAYERS

The OSI model is divided into two layers: **upper layers and lower layers**.

UPPER LAYERS

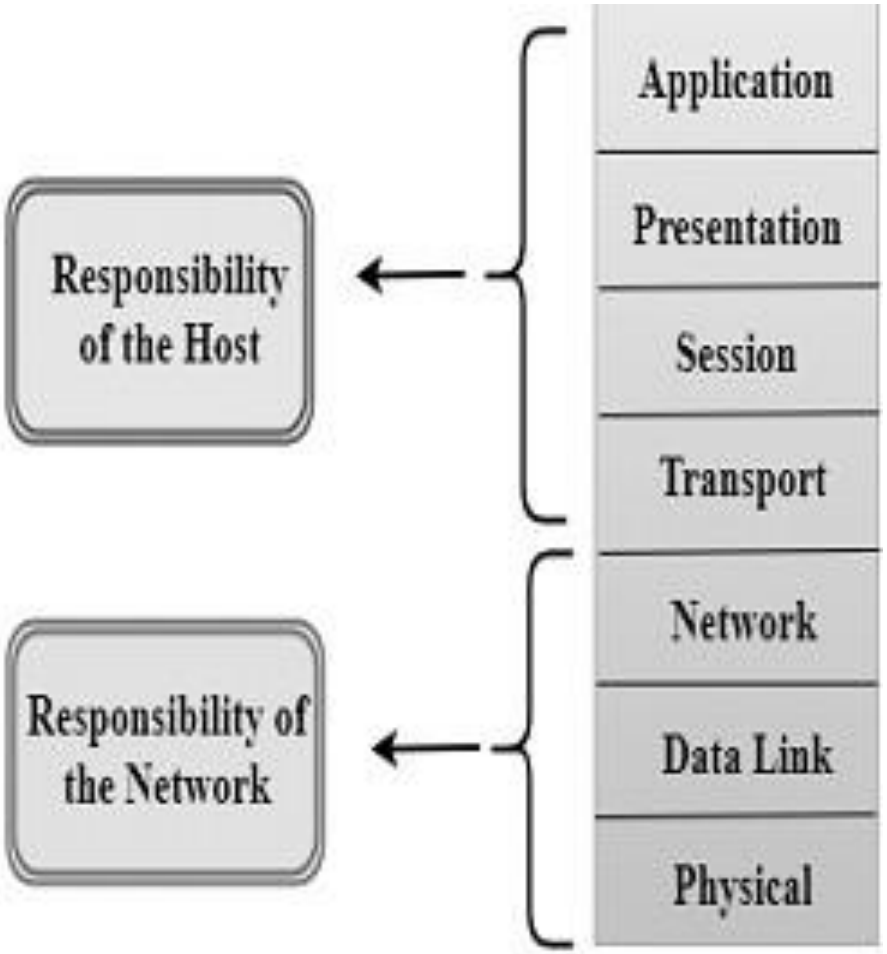
(Responsibility of the Host)

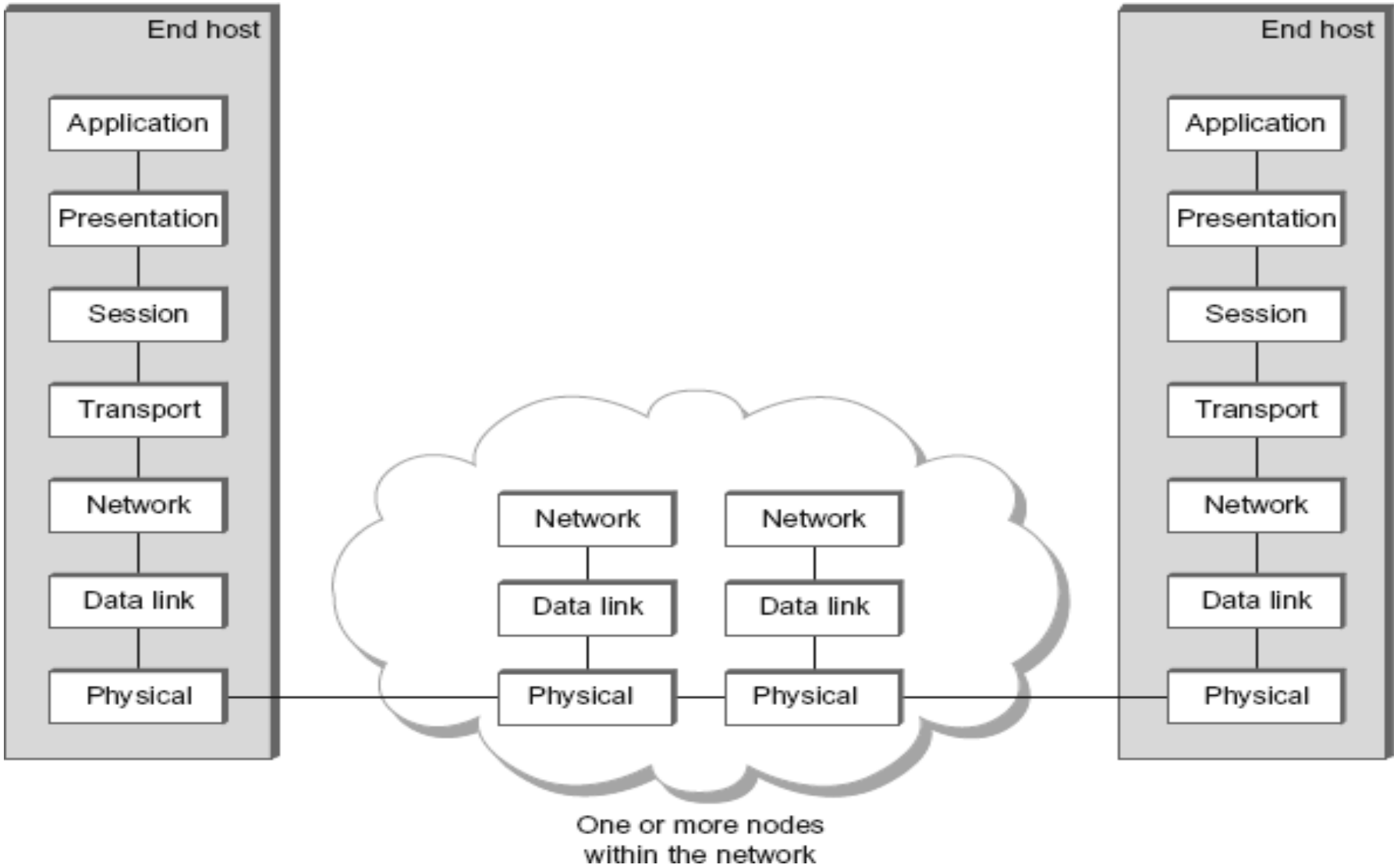
The upper layers of the OSI model mainly deals with the application related issues. They are implemented only in the software.

LOWER LAYERS

(Responsibility of the Network)

The lower layers of the OSI model deals with the data transport issues. They are implemented in hardware and software.




End host
Application
Presentation
Session
Transport
Network
Data link
Physical
Network
Data link
Physical
Network
Data link
Physical
End host
Application
Presentation
Session
Transport
Network
Data link
Physical
One or more nodes
within the network

FUNCTIONS OF THE OSI LAYERS

PHYSICAL LAYER

The physical layer coordinates the functions required to **transmit a bit stream over a physical medium.**

The physical layer is concerned with the following functions:

Physical characteristics of interfaces and media - The physical layer defines the characteristics of the interface between the devices and the medium.

Representation of bits - To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.

Signals: It determines the type of the signal used for transmitting the data

Data Rate or Transmission rate - The number of bits sent each second –is also defined by the physical layer.

Synchronization of bits - The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.

Line Configuration - In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.

Physical Topology - The physical topology defines how devices are connected to make a network. Eg.: mesh, bus, star or ring topology.

Transmission Mode - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex or full-duplex.

DATA LINK LAYER

It is responsible for **transmitting frames from one node to the next node**. The other **responsibilities of this layer are**

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the network, data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the **rate at which the data are absorbed** by the receiver is less than **the rate produced in the sender,** the Data link layer imposes a flow control mechanism.
- **Error control**- Used for **detecting and retransmitting damaged or lost frames** and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Medium Access control** -Used to determine which device has control over the link at any given time.

NETWORK LAYER

This layer is responsible for the **delivery of packets from source to destination**.

- It **determines the best path to move data from source to the destination** based on the network conditions, the priority of service, and other factors.

The other responsibilities of this layer are

- **Logical addressing** - **If a packet passes the network boundary**, we need another addressing system for source and destination called logical address. This addressing is used to identify the device on the internet.
- **Routing** – Routing is the major component of the network layer, and it **determines the best optimal path** out of the multiple paths from source to the destination.

TRANSPORT LAYER

It is responsible for **Process to Process** delivery. That is **responsible for source-to-destination (end-to-end) delivery** of the entire message, It **also ensures whether the message arrives in order or not.**

The other responsibilities of this layer are

- **Port addressing / Service Point addressing** - The header includes an address called port address / service point address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be **connectionless or connection oriented.**

  → The connectionless treats each segment as an individual packet and delivers to the destination.

  → The connection-oriented makes connection on the destination side before the delivery. After the delivery the connection will be terminated.
- **Flow control** - The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error Control -** Error control is performed end-to-end rather than across the single link..

SESSION LAYER

This layer establishes, manages and terminates connections between applications.

- The other responsibilities of this layer are
  - → **Dialog control** - Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
  - → **Synchronization**- Session layer adds some checkpoints when transmitting the data in a sequence.
  - → If some error occurs in the middle of the transmission of data, **then the transmission will take place again from the checkpoint.** This process is known as Synchronization and recovery.

PRESENTATION LAYER

It is concerned with the **syntax and semantics of information exchanged between two systems.**

The other responsibilities of this layer are

- **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.
- **Encryption and decryption** - It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.
- **Compression and expansion** - Compression reduces the number of bits contained in the information particularly in text, audio and video.

APPLICATION LAYER

This layer **enables the user to access the network**. It handles issues such as **network transparency, resource allocation**, etc.

- This **allows the user to log on to remote user.**

The other responsibilities of this layer are

→ **FTAM (File Transfer, Access, Management)** - Allows user to access files in a remote host.

→ **Mail services** - Provides email forwarding and storage.

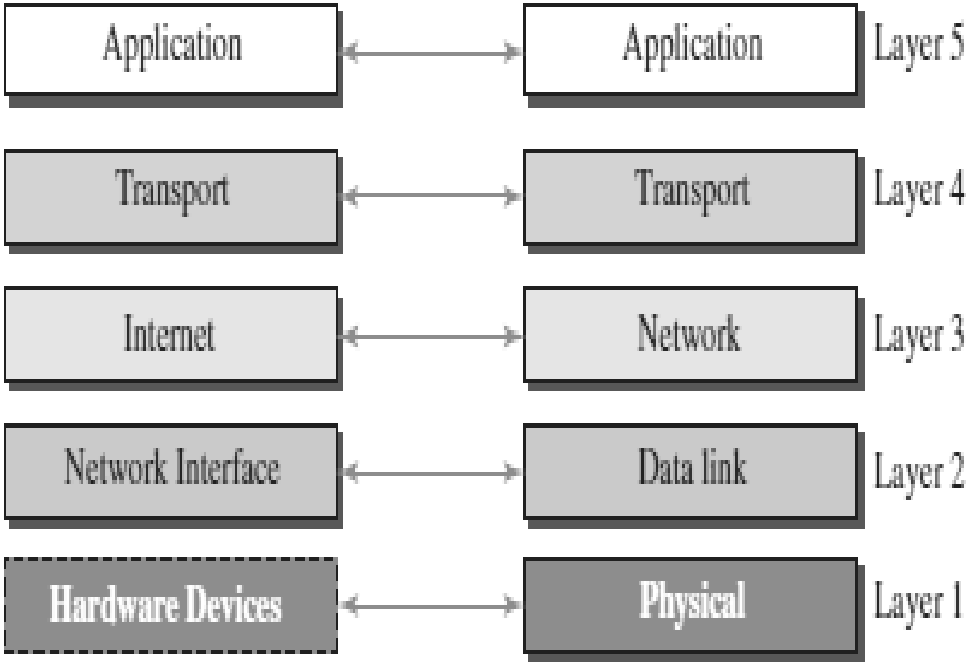
- **Directory services** - Provides database sources to access information about various sources and objects

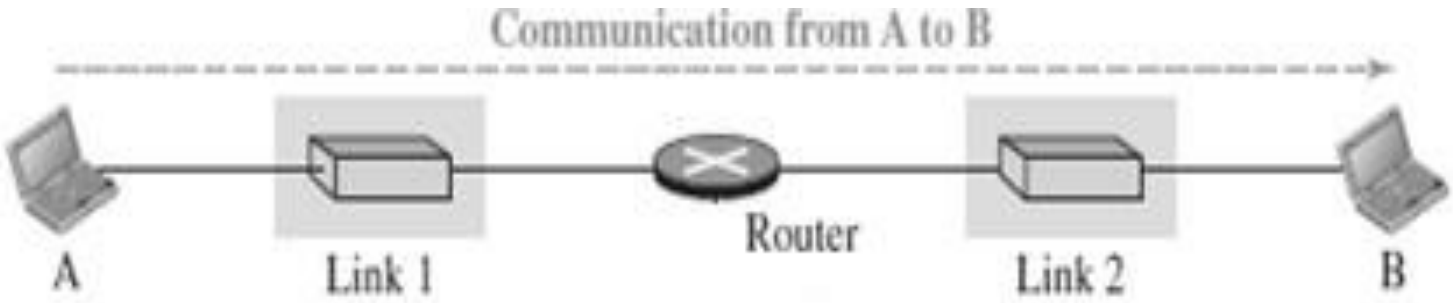
TCP / IP PROTOCOL SUITE

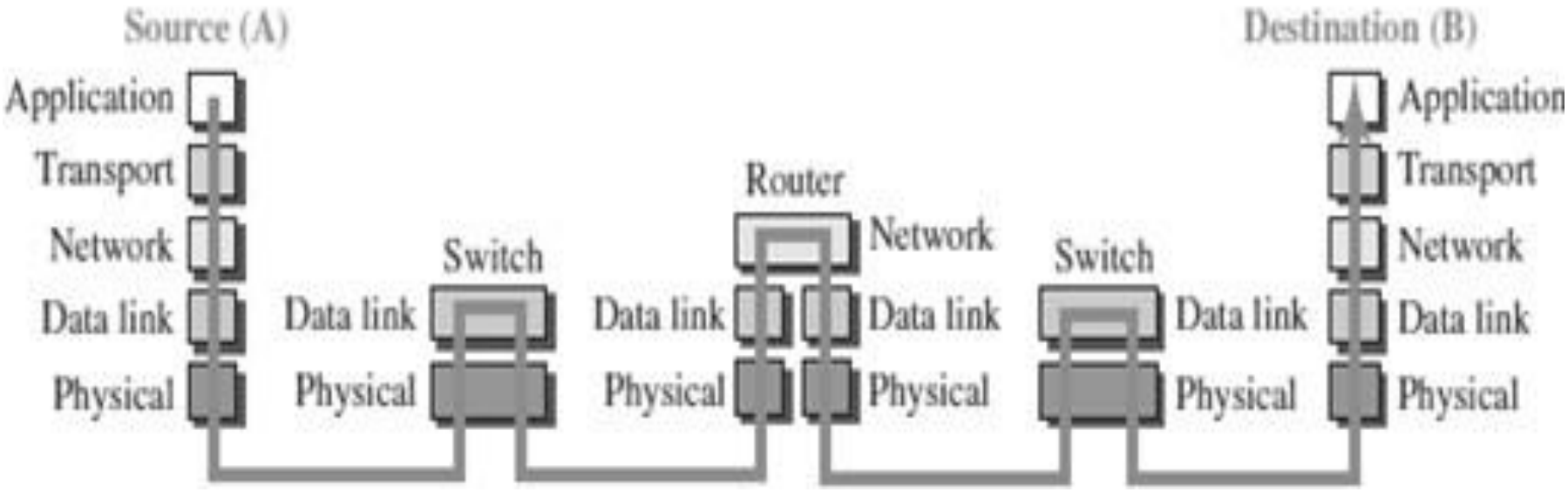
TCP / IP PROTOCOL SUITE

- The TCP/IP architecture is also called as **Internet architecture.**
- TCP/IP is a protocol suite used in the Internet today.

- It is a **4-layer model**. The layers of TCP/IP are
  - **i) Application layer**
  - **ii) Transport Layer (TCP/UDP)**
  - **iii) Internet Layer**
  - **iv) Network Interface Layer**




Communication from A to B
A
Link 1
Router
Link 2
B


Source (A)
Destination (B)
Application
Transport
Network
Data link
Physical
Switch
Router
Switch

APPLICATION LAYER

- An application layer **incorporates the function of top three OSI layers.** An application layer is the topmost layer in the TCP/IP model.
- It is responsible **for handling high-level protocols**, **issues of representation.**
- This layer **allows the user to interact with the application.**
- When one application layer protocol wants to communicate with another application layer, it **forwards its data to the transport layer.**
- Protocols such as **FTP, HTTP, SMTP, POP3,** etc running in the application layer provides service to other program running on top of application layer

TRANSPORT LAYER

- **The transport layer is responsible for the reliability, flow control, and correction of data** which is being sent over the network.
- The two protocols used in the transport layer are **User Datagram Protocol (UDP) and Transmission Control Protocol (TCP)**.

  - **UDP** – UDP provides connectionless service and end-to-end delivery of transmission. It is an **unreliable protocol** as **it discovers the errors but not specify the error.**

  - **TCP** – TCP provides a full transport layer services to applications. TCP is a **reliable protocol** as **it detects the error and retransmits the damaged frames.**

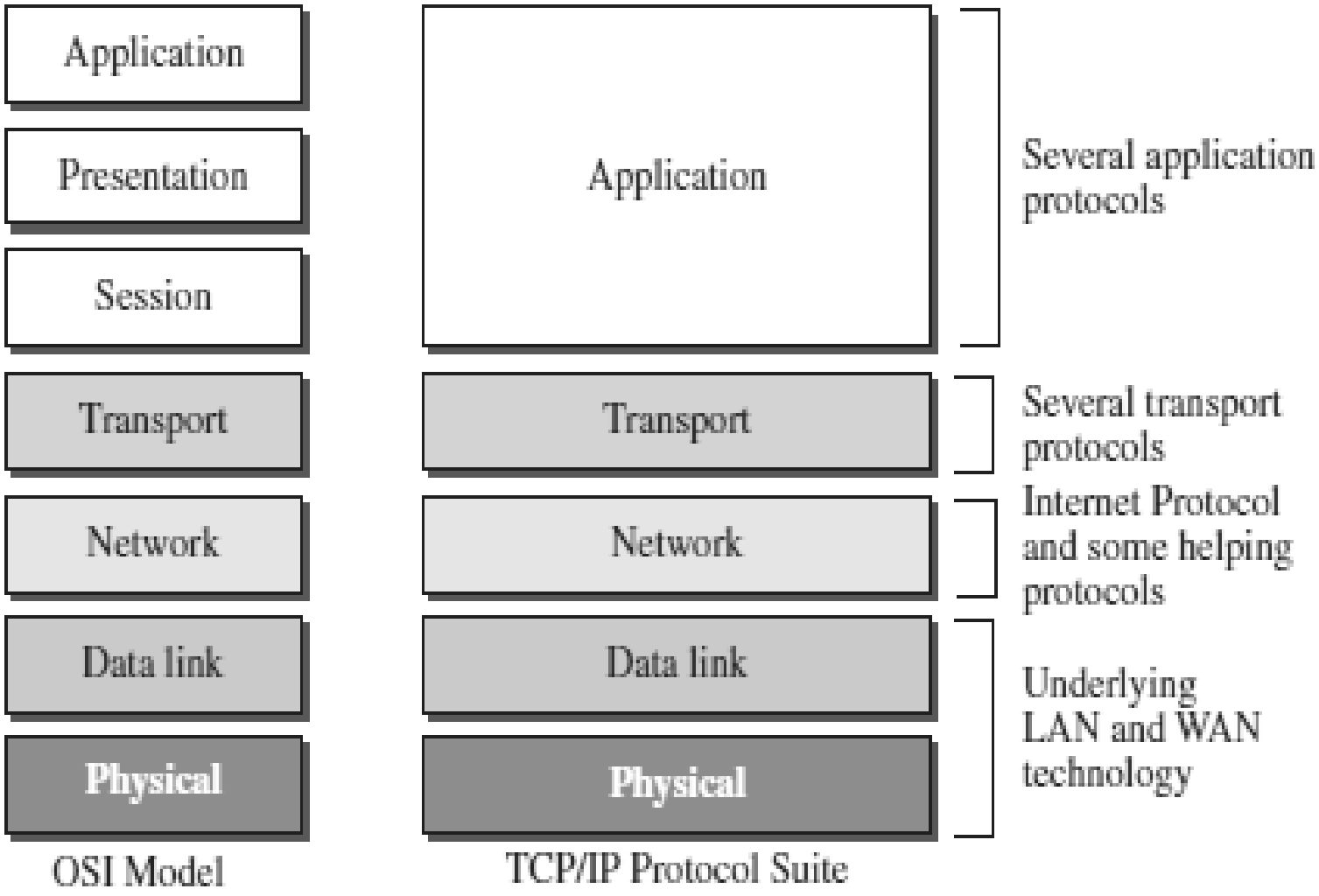
INTERNET LAYER

- The internet layer is the second layer of the TCP/IP model.
- An internet layer is also **known as the network layer.**
- The main responsibility of the internet layer is **to send the packets from any network**, and they **arrive at the destination irrespective of the route they take.**
- Internet layer handle the **transfer of information across multiple networks through router and gateway** .
- **IP protocol is used in this layer**, and it is the most significant part of the entire TCP/IP suite

NETWORK INTERFACE LAYER

- The network interface layer is the lowest layer of the TCP/IP model.
- This layer is the **combination of the Physical layer and Data Link layer** defined in the OSI reference model.
- It defines **how the data should be sent physically** through the network.
- This layer is mainly **responsible for** the **transmission of the data between two devices on the same network.**
- The **functions carried out** by this layer are **encapsulating the IP datagram into frames** transmitted by the network and **mapping of IP addresses into physical addresses.**
- The protocols used by this layer are **Ethernet, token ring, FDDI, X.25, frame relay.**

COMPARISON - OSI MODEL AND TCP/IP MODEL



SWITCHING

SWITCHING

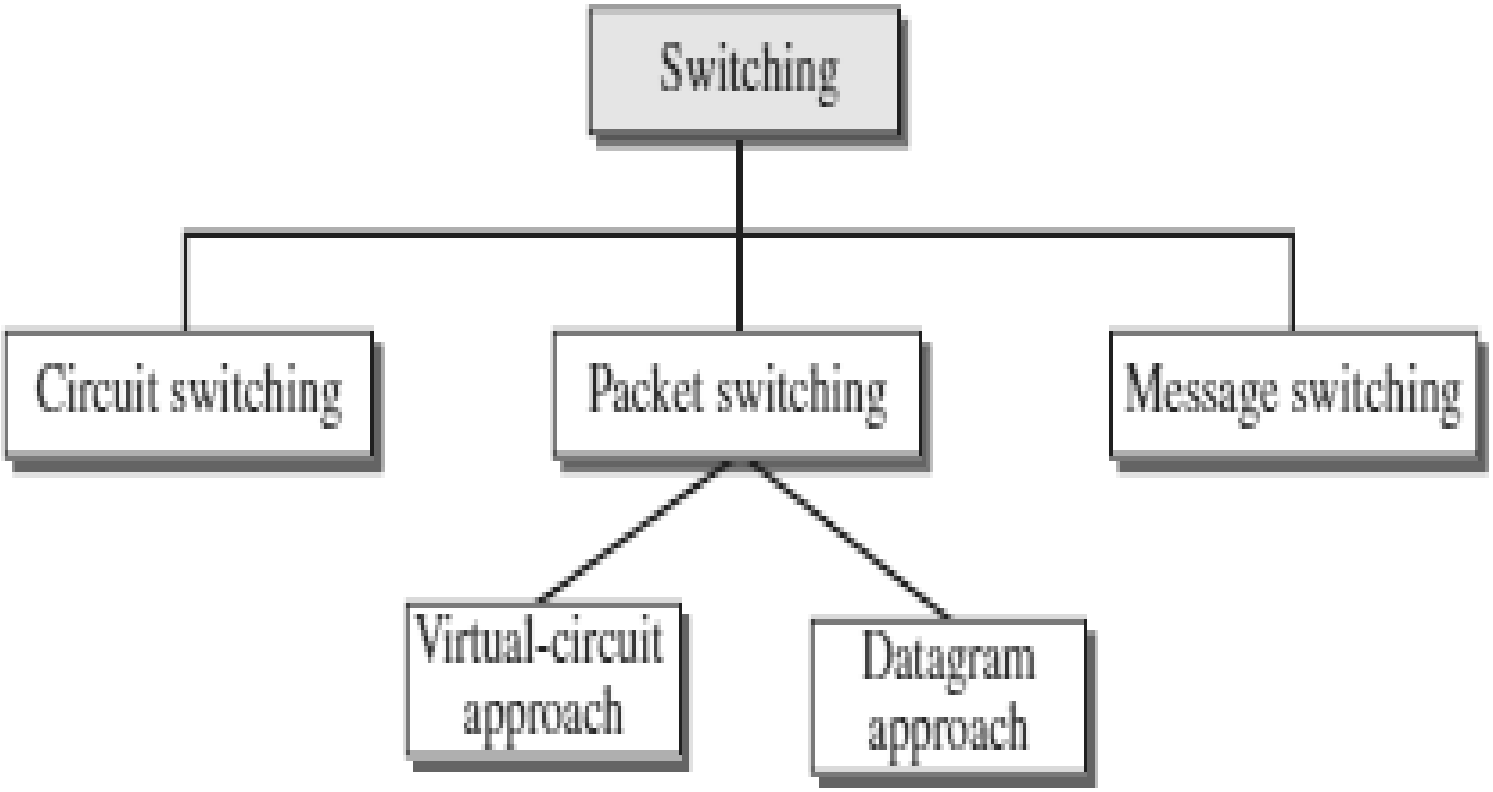
- The technique of **transferring the information from one computer network to another network** is known as **switching**.
- Switching in a computer network is **achieved by using switches.**
- A **switch is a small hardware device** which is **used to join multiple computers together** with one local area network (LAN).
- Switches are devices **capable of creating temporary connections** between two or more devices linked to the switch.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed.
- It verifies the destination address to route the packet appropriately.
- It is **operated in full duplex mode.**
- It **does not broadcast the message** as it works with limited bandwidth.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to **only that device which has been addressed.**
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch **cannot determine the network connectivity issues** easily.
- Proper designing and configuration of the switch are required to handle multicast packets.


Switching
Circuit switching
Packet switching
Message switching
Virtual-circuit approach
Datagram approach

CIRCUIT SWITCHING

Circuit switching is a switching technique that **establishes a dedicated path between sender and receiver.**

- In the Circuit Switching Technique, once the connection is established then the **dedicated path will remain to exist until the connection is terminated**. Ie., similar to telephone.
- A complete **end-to-end path must exist** before the communication takes place.
- In case of circuit switching technique, **when any user wants to send the data, voice, video,**

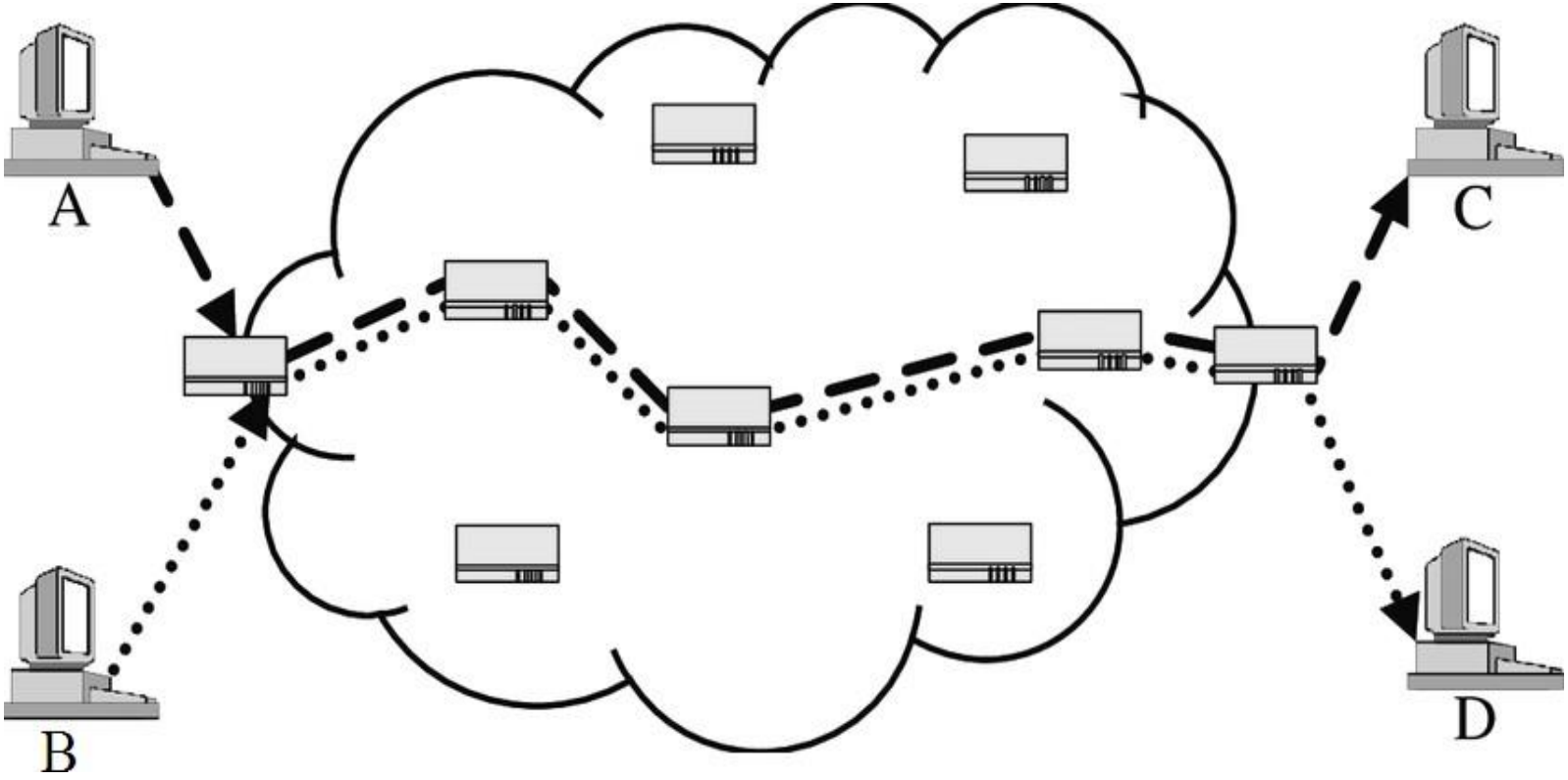
  ➔ a **request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path**.

  → After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Phases in Circuit Switching

Communication through circuit switching has **3 phases:**

- ***Connection Setup / Establishment*** - In this phase, a **dedicated circuit is established from the source to the destination** through a number of intermediate switching centres. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.
- ***Data transfer*** - Once the circuit has been established, **data and voice are transferred from the source to the destination**. The dedicated connection remains as long as the end parties communicate.
- ***Connection teardown / Termination*** - When data transfer is complete, the connection is relinquished. The **disconnection is initiated by any one of the user**. Disconnection involves **removal of all intermediate links from the sender to the receiver.**


A
B
C
D

Advantages

- It is suitable for long continuous transmission, since a continuous transmission route is established, that remains throughout the conversation.
- The **dedicated path** ensures a steady data rate of communication.
- No intermediate delays are found once the circuit is established. So, they are suitable for real time communication of both voice and data transmission.

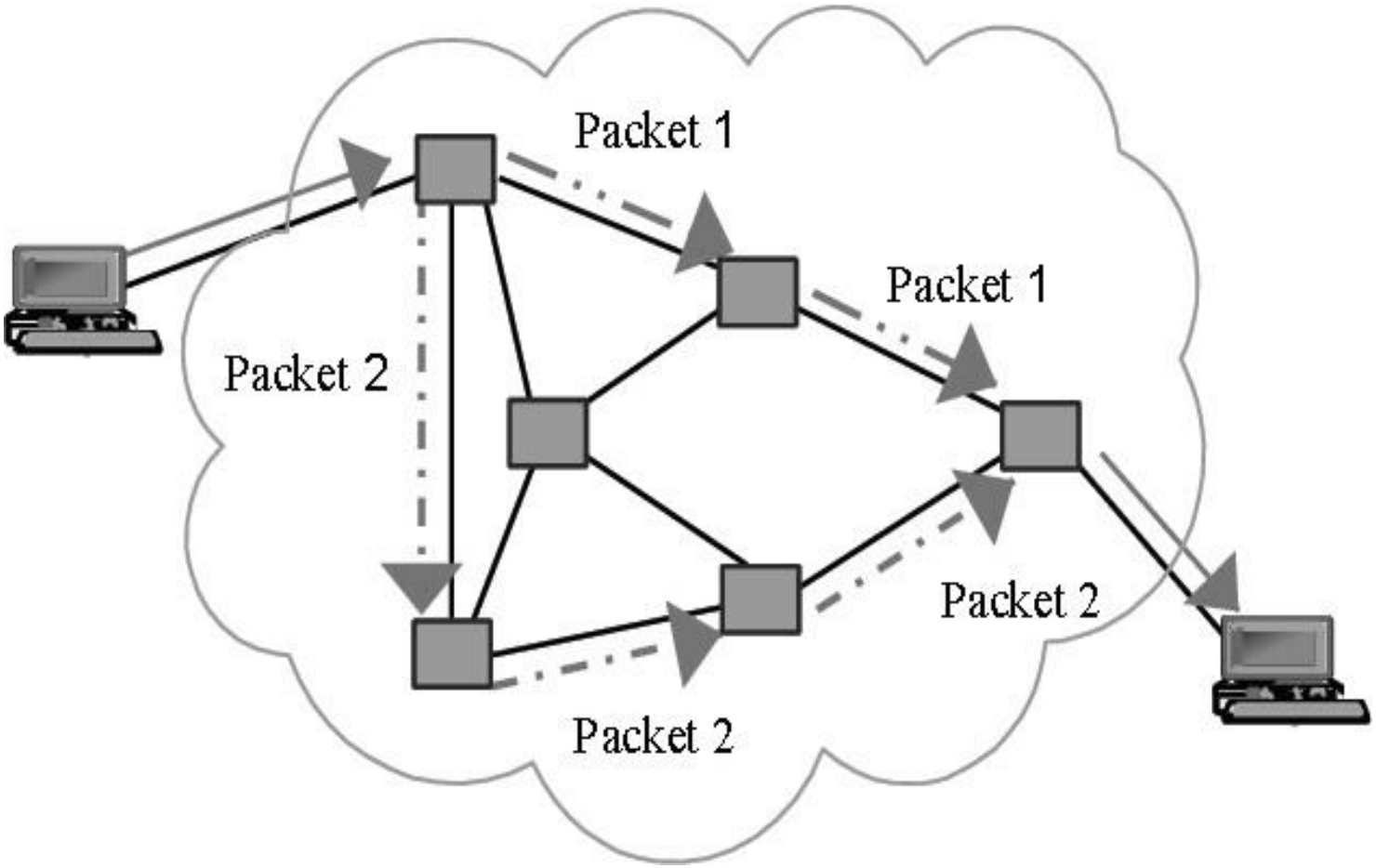
Disadvantages

- Circuit switching establishes a dedicated connection between the end parties. This dedicated connection cannot be used for transmitting any other data, **even if the data load is very low.**
- Bandwidth requirement is high even **in cases of low data** volume.
- There is **underutilization of system resources.** Once resources are allocated to a particular connection, they cannot be used for other connections.
- Time required to establish connection may be high.
- It is **more expensive than other switching techniques** as a dedicated path is required for each connection.

PACKET SWITCHING

The packet switching is a switching technique in which the message is sent in one go, but it is **divided into smaller pieces, and they are sent individually**.

- The message is divided into smaller pieces known as packets and packets are given a **unique number to identify their order** at the receiving end.
- Every **packet contains some information in its headers such as** source address, destination address and sequence number.
- Packets will **travel across the network,** taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any **packet is missing or corrupted**, then the message will be sent to resend the message.
- If the **correct order of the packets is reached,** then the acknowledgment message will be sent.


Packet 1
Packet 1
Packet 2
Packet 2
Packet 2

Advantages of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** It does not require any established path prior to the transmission, and **many users can use the same communication channel simultaneously**, hence **makes use of available bandwidth very efficiently.**

Disadvantages of Packet Switching:

- Packet Switching technique cannot be implemented in those applications **that require low delay and high-quality services.**
- The **protocols** used in a packet switching technique **are very complex and requires high implementation cost.**
- If the network is overloaded or corrupted, then **it requires retransmission of lost packets.** It can also lead to the loss of critical information if errors are not recovered.

APPROACHES OF PACKET SWITCHING

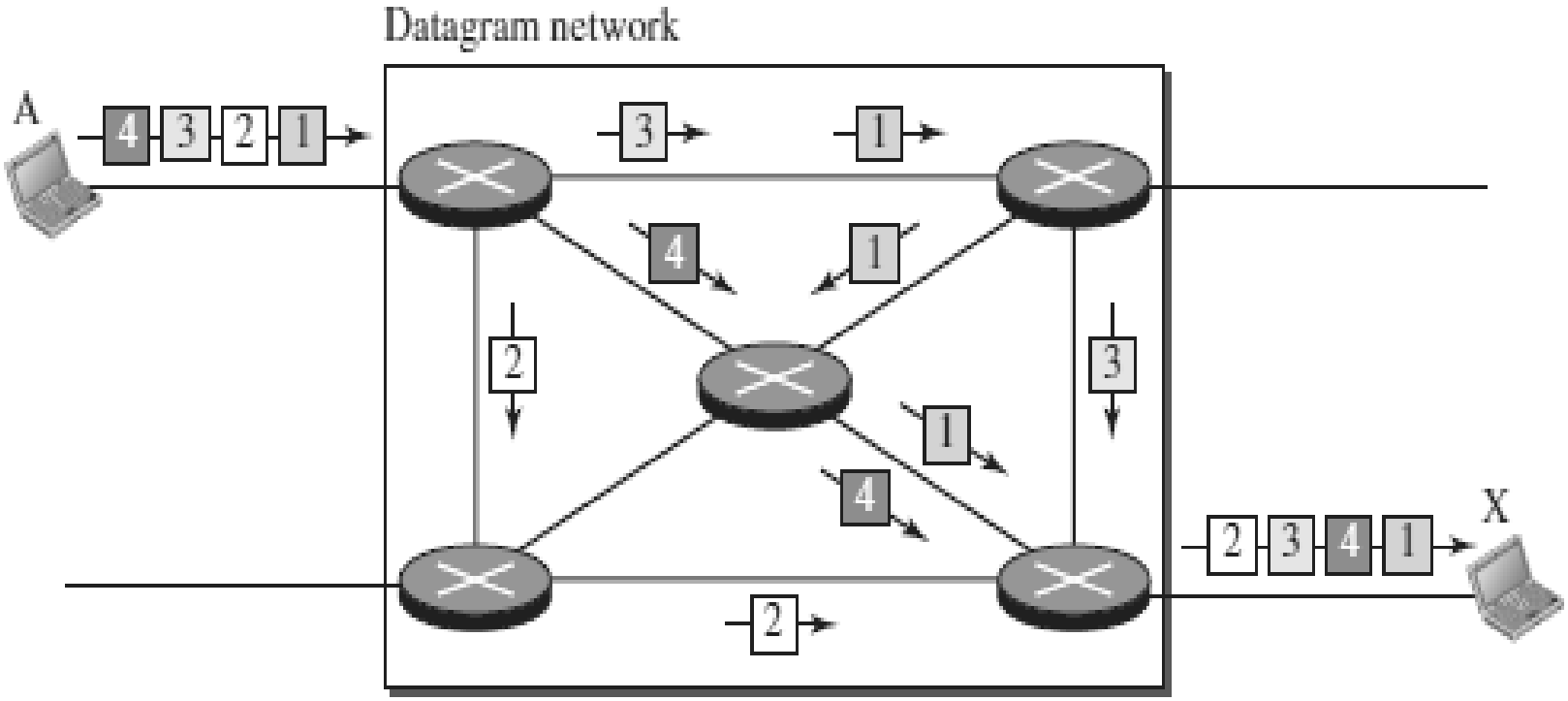
There are **two approaches to Packet Switching:**

i) Datagram Packet switching

ii) Virtual Circuit Switching

i) Datagram Packet Switching

- It is a packet switching technology in which packet is known as a datagram, is considered as an **independent entity.**
- Each **packet contains the information about the destination** and **switch uses this information** to forward the packet to the correct destination.
- The **packets are reassembled at the receiving end** in correct order.
- In Datagram Packet Switching technique, **the path is not fixed.**
- **Intermediate nodes take the routing decisions** to forward the packets.
- Datagram Packet Switching is also known as **connectionless switching.**
- There are **no setup or teardown phases.**
- Each packet is treated as the same by a switch regardless of its source or destination.



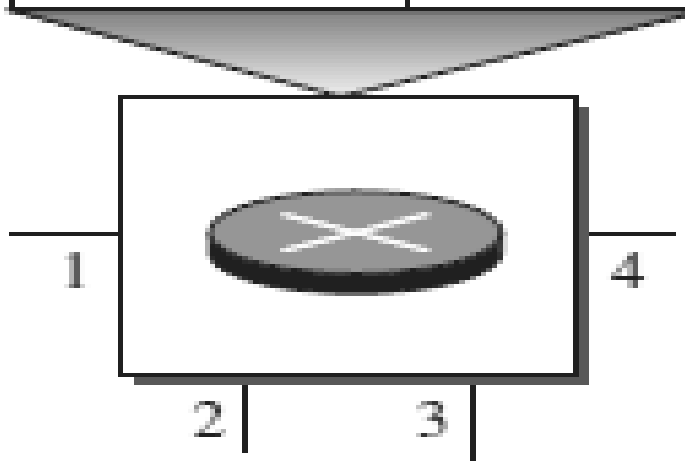
In this example, **all four packets** (or datagrams) belong to the same message, but **may travel different paths to reach their destination.**

Routing Table

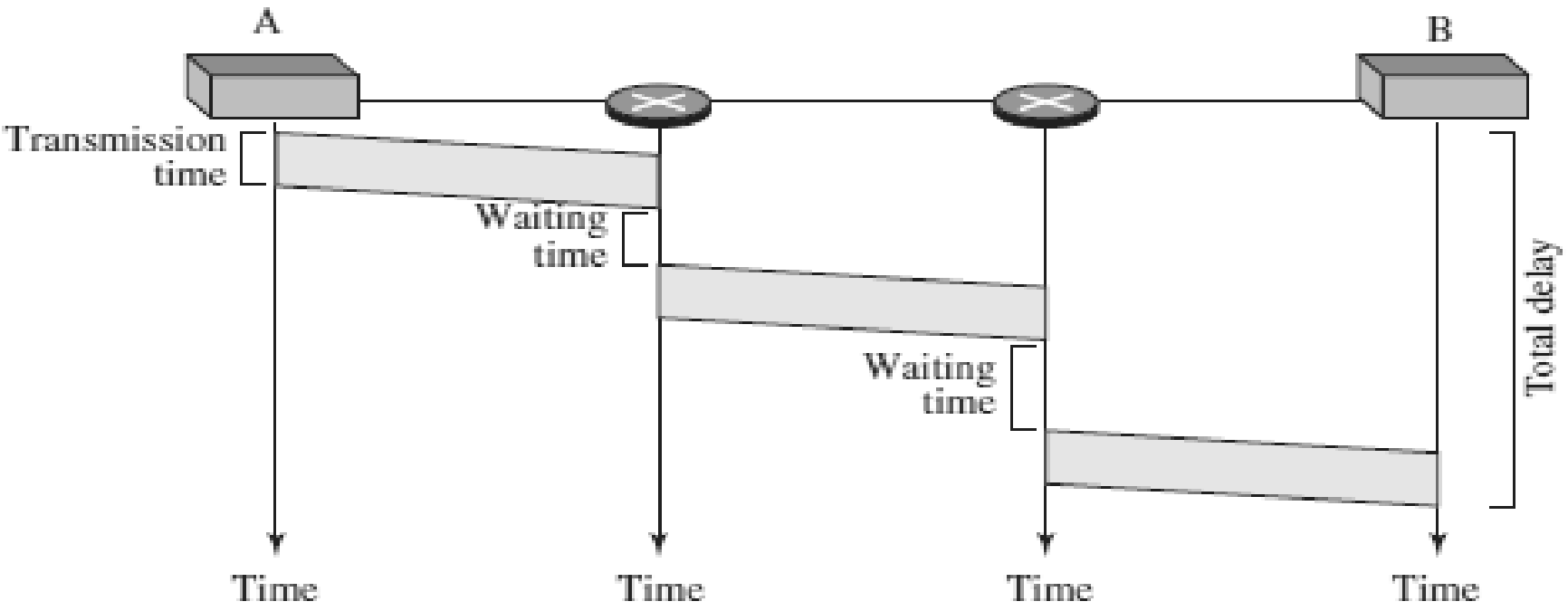
- In this type of network, **each switch (or packet switch) has a routing table which is based on the destination address.**
- The routing tables are dynamic and are updated periodically.

- The destination addresses and the corresponding forwarding output ports are recorded in the tables.

Destination address	Output port
1232	1
4150	2
⋮	⋮
9130	3



Delay in a datagram network



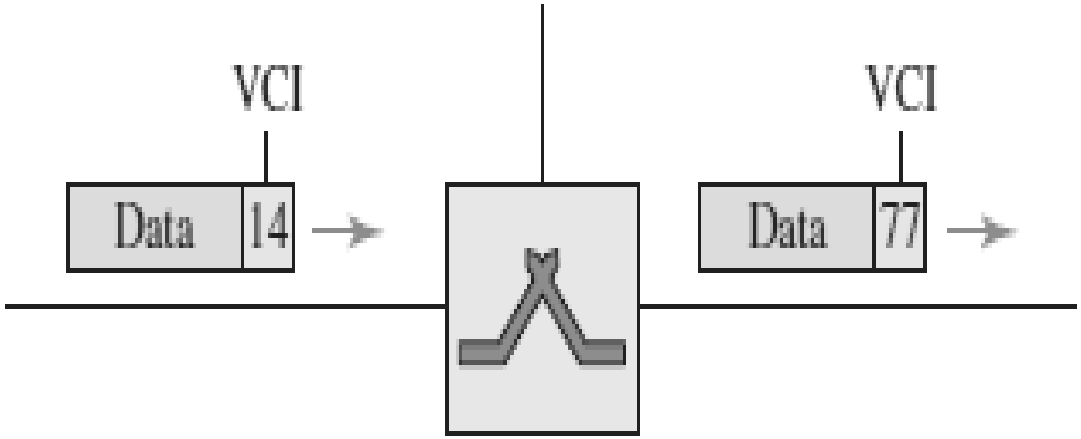
- The packet travels through two switches.
- There are three transmission times (3*T*), three propagation delays (slopes 3t of the lines), and two waiting times (*w*1 + *w*2).
- We ignore the processing time in each switch.
- **Total delay = 3*T* + 3t + *w*1 + *w*2**

ii) Virtual Circuit Switching

- Virtual Circuit Switching is also known as **connection-oriented switching.**
- In the case of Virtual circuit switching, a **virtual connection is established before the messages are sent.**
- **Call request and call accept packets are used to establish the connection** between sender and receiver.
- In this case, the **path is fixed for the duration of a logical connection.**

Virtual Circuit Identifier (VCI)

- A virtual circuit identifier (**VCI**) that **uniquely identifies the connection at this switch.**
- A VCI, unlike a global address, is a small number that has only switch scope; **it is used by a frame between two switches**.
- **When a frame arrives at a switch, it has a VCI**; **when it leaves, it has a different VCI.**



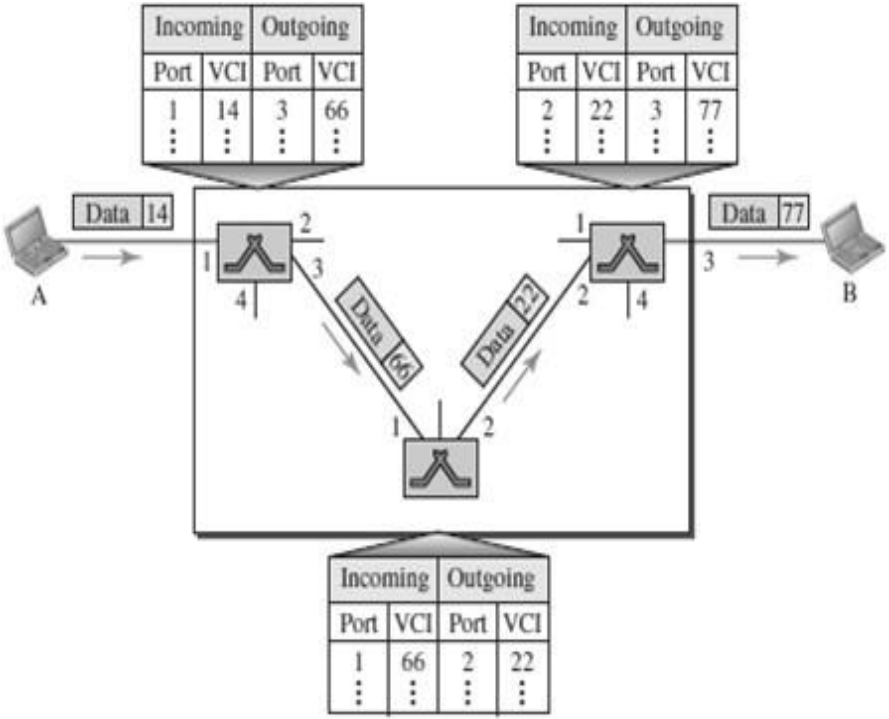
Virtual Circuit Table

Every Virtual Circuit (VC) **maintains a table called Virtual Circuit table**. One **entry in the VC table on a single switch contains the following:**

- An **incoming interface on which packets for this VC arrive** at the switch
- An **outgoing interface in which packets for this VC leave** the switch
- A **outgoing VCI that will be used for outgoing packets**

Example :

Source A sends a frame to Source B through Switch 1, Switch 2 and Switch 3.



Types of Virtual Circuits

There are two broad classes of Virtual Circuits. They are

PVC – Permanent Virtual Circuit

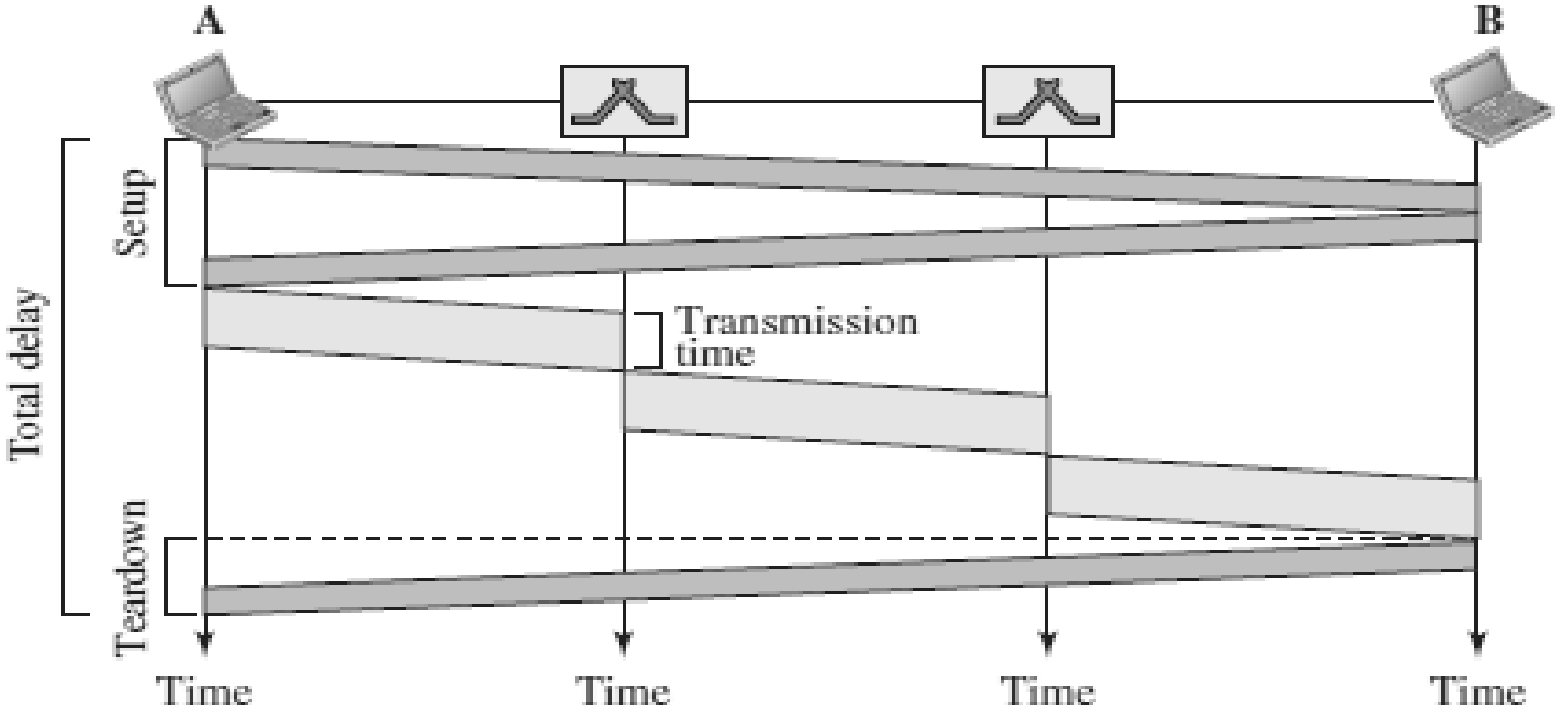
- Network Administrator will configure the state
- The virtual circuit is permanent (PVC)

SVC – Switched Virtual Circuit

- A host can send messages into the network to cause the state to be established. This is referred as signaling.

- A host may set up and delete such a VC dynamically without the involvement of a network administrator

Delay in Virtual-Circuit Networks



- The packet is traveling through two switches (routers).
- There are three transmission times (3*T*), **three propagation times (3t)**, data transfer depicted by the sloping lines, a setup delay (which includes transmission and propagation in two directions), and a **teardown delay** (which includes transmission and propagation in one direction).

Total delay = 3*T* + 3t + Setup delay + Teardown delay

CIRCUIT SWITCHING	PACKET SWITCHING	
	Virtual Circuit Switching	Datagram Switching
Connection oriented	Connection oriented	Connection less
Ensures in order delivery	Ensures in order delivery	Packets may be delivered outof order
No reordering is required	No reordering is required	Reordering is required
A dedicated path existsfor data transfer	A dedicated path exists fordata transfer	No dedicated path exists fordata transfer
All the packets take thesame path	All the packets take thesame path	All the packets may not takethe same path
Resources are allocatedbefore data transfer	Resources are allocated ondemand using 1st packet	No resources are allocated
Stream oriented	Packet oriented	Packet oriented
Fixed bandwidth	Dynamic Bandwidth	Dynamic bandwidth
Reliable	Reliable	Unreliable
No overheads	Less overheads	Higher overheads
Implemented at physicallayer	Implemented at data linklayer	Implemented at networklayer
Inefficient in terms ofresource utilization	Provides better efficiencythan circuit switched systems	Provides better efficiencythan message switched systems
Example- Telephonesystems	Examples- X.25, Framerelay	Example- Internet