Computer Networks
Unit I- Introduction

Note: Material for this presentations are taken from Internet and books and only being used for student reference

Outline

- **Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network**
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

Introduction of Network

- Network: A **network** is defined as a group of two or more computer systems linked together.
- Types of Networks:
  - LAN
  - MAN
  - WAN
  - PAN
  - Ad-hoc Network

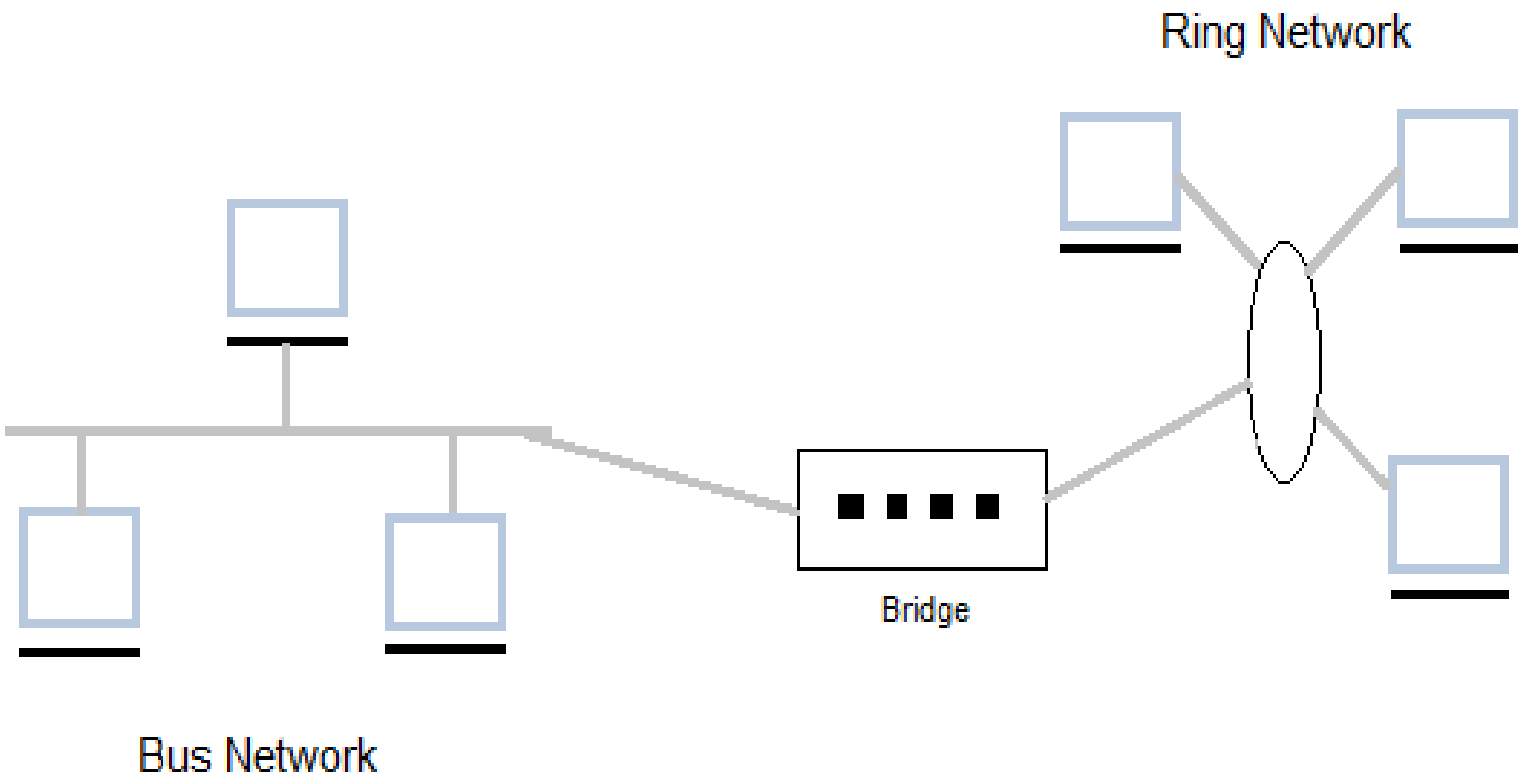
Local Area Networks (LAN)

- floor/building-wide
- single communication medium
- no routing, broadcast
- segments connected by switches or hubs
- high bandwidth, low latency
- Ethernet - 10Mbps, 100Mbps, 1Gbps
- no latency guarantees

LAN- Local Area Network

- It is designed for small physical areas such as an office, group of buildings or a factory.
- LANs are used widely as it is easy to design and to troubleshoot.
- Personal computers and workstations are connected to each other through LANs.
- We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.
- LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building
- LAN networks are also widely used to share resources like printers, shared hard-drive etc.

LAN Diagram



(Different Topologies interconnected in a Local Area Network)

LAN Advantages

- **Cost reductions** through **sharing** of **information and databases, resources and network services.**
- **Increased information exchange** between different **departments in** an **organization**, or between **individuals.**
- The trend to **automate communication and manufacturing process.**

LAN Disadvantages

- **Special security measures** are needed **to stop** users from **using programs and data that they should not have access to**;
  - **Networks** are **difficult to set up** and need to be **maintained** by **skilled technicians**.
  - **If the file server develops a serious fault, all the users are affected**, rather than just one user in the case of a stand-alone machine.

Applications

- One of the computer in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting Locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

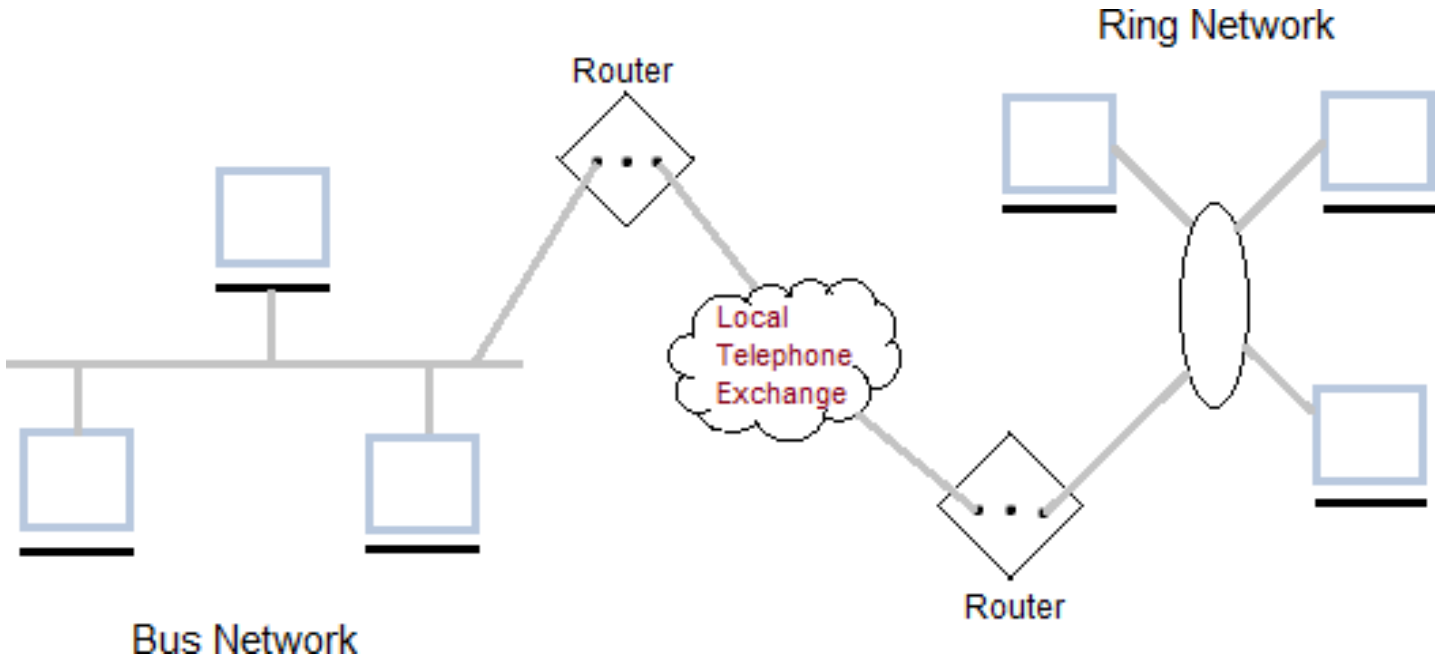
MAN- Metropolitan Area Network

- It is basically a bigger version of LAN.
- It is also called MAN and uses the similar technology as LAN.
- It is designed to extend over the entire city.
- It can be means to connecting a number of LANs into a larger network or it can be a single cable.
- It is mainly hold and operated by single private company or a public company.

MAN- Metropolitan Area Network continued….

- Metropolitan Area Networks (MAN)
  - city-wide, up to 50 km
  - Digital Subscriber Line (DSL): .25 - 8 Mbps, 5.5km from switch
    - BellSouth: .8 to 6 Mbps
  - Cable modem: 1.5 Mbps, longer range than DSL
    - Bright house w/ Road Runner: .5 to 10Mbps

MAN Diagram


Ring Network
Router
Local
Telephone
Exchange
Router
Bus Network

MAN-Advantages

- It provides a good back bone for a large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both direction simultaneously.
- A Man usually encompasses several blocks of a city or an entire city.

MAN-Disadvantages

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial espionage (spying) graphical regions.

MAN Applications

- The MAN can be used to provide services including
  - telecoms,
  - Internet access,
  - television and
  - CCTV to businesses and citizens in these metropolitan areas.

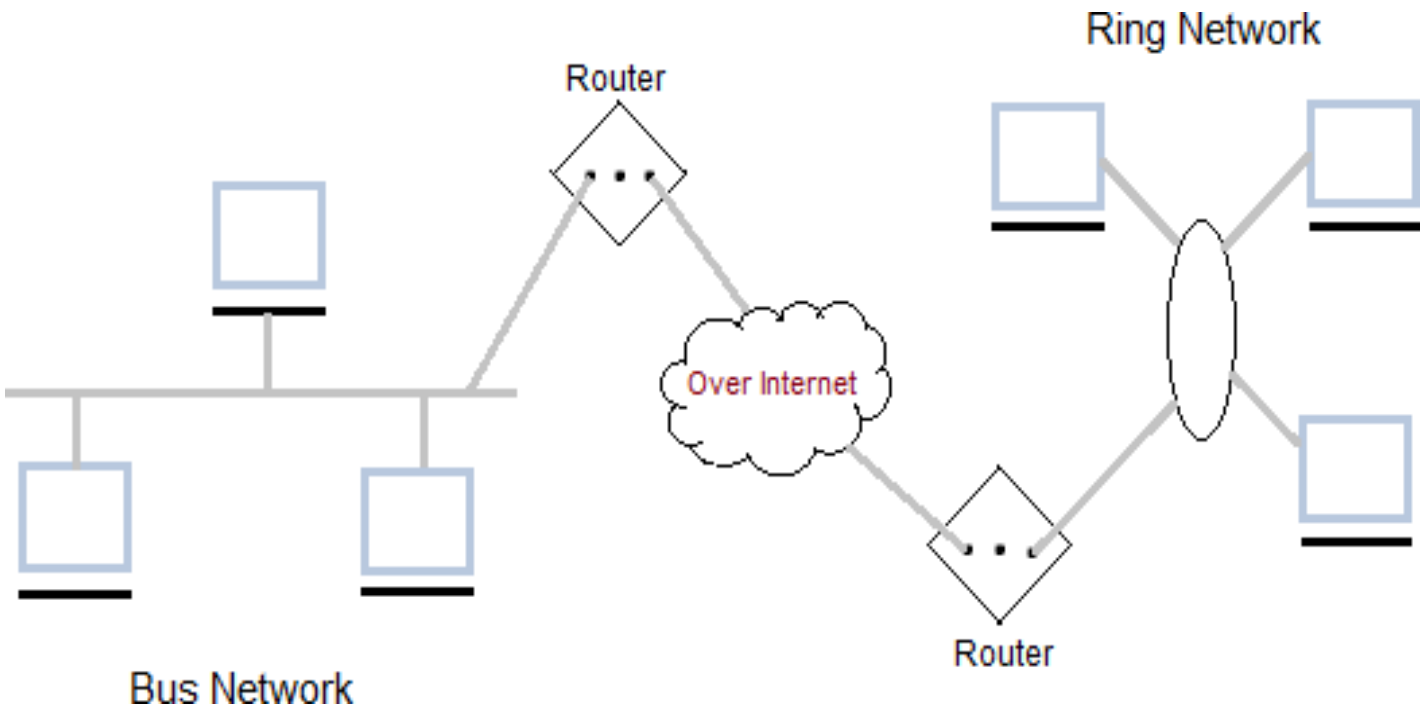
WAN-Wide Area Network

- **Wide Area Network (WAN)**
- It is also called WAN.WAN can be private or it can be public leased network.
- It is used for the network that covers large distance such as cover states of a country.
- It is not easy to design and maintain.
- Communication medium used by WAN are PSTN or Satellite links.
- WAN operates on low data rates.

WAN-Wide Area Network...continued

- Wide Area Networks (WAN)
  - world-wide
  - Different organizations
  - Large distances
  - routed, latency .1 - .5 seconds

WAN Diagram



WAN Advantages

- Covers a **large geographical area** so long distance businesses can connect on the one network.
- Shares software and resources with connecting workstations.
- Messages can be sent very quickly to anyone else on the network
- Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

WAN Disadvantages

- **Need a good firewall to restrict outsiders** from entering and disrupting the network Setting up a **network** can be an **expensive, slow andcomplicated.**
- The **bigger the network** the **more expensive** it is.
- Once set up, **maintaining a network** is a **full-time job** which **requires network supervisors** and **technicians** to be employed.
- **Security** is a real **issue** when many different **people have the ability to use information from other computers.**
- **Protection** against **hackers and viruses** adds **more complexity** and **expense.**

PAN-Personal Area Network

- PAN stands for personal area network, a network covering a very small area, usually a small room. PAN's can be wired or wireless.
- The best known wireless PAN network technology is Bluetooth, and the most popular wired PAN is USB.
- Wi-Fi also serves as a PAN technology, since Wi-Fi is also used over a small area.

PAN- Diagram

PAN-Advantages

- The pan is a personal network of one or two person so there is no risk of any leak of data.

PAN-Disadvantages

- The network it can only travel straight up to 10 (Mbps) and if in different rooms then only 2 (Mbps).
- In the case of infrared the infra red sensor bust be in a straight line otherwise it won't communicate.
- Transmission speed is slow to moderate.

Ad-hoc Networks

- A wireless **ad hoc network** (WANET) or MANET is a decentralized type of wireless **network**.
- The **network** is **ad hoc** because it does not rely on a pre- existing infrastructure, such as routers in wired **networks** or access points in managed (infrastructure) wireless **networks**.
- **Ad-hoc means without base station or Access point** (means without infrastructure)

Ad-hoc Network Diagram

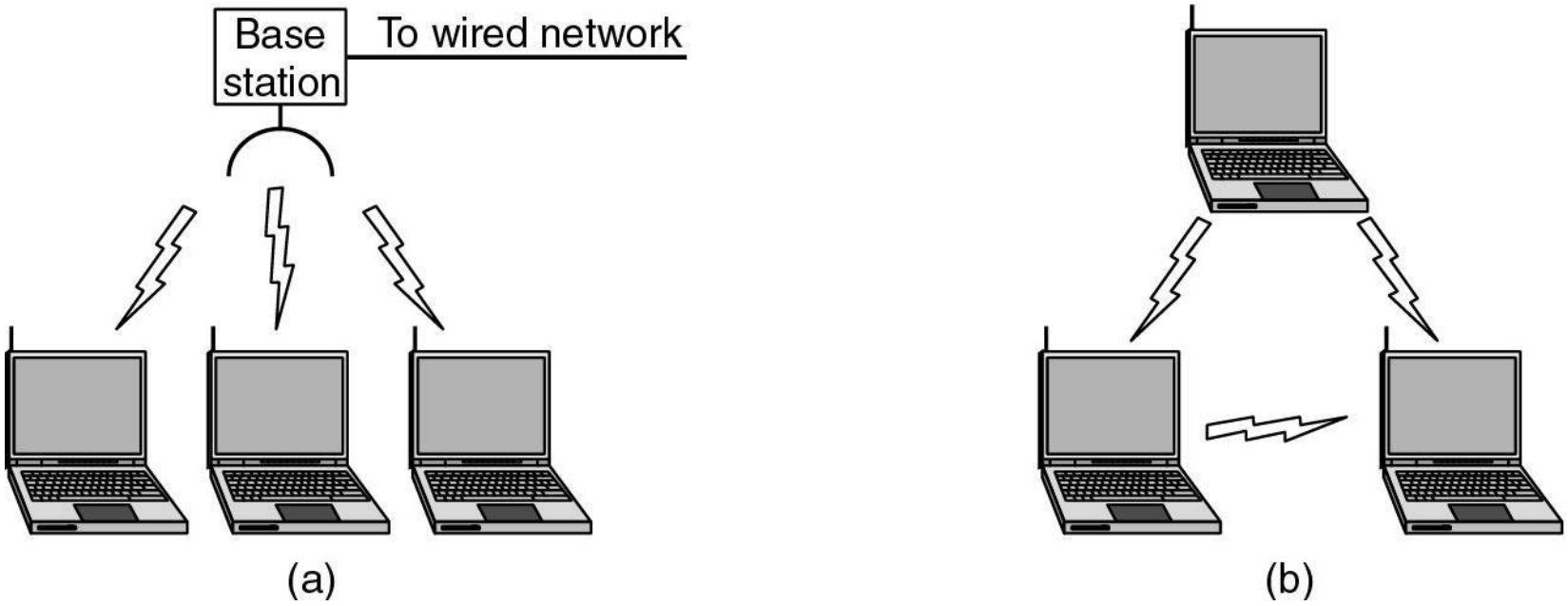
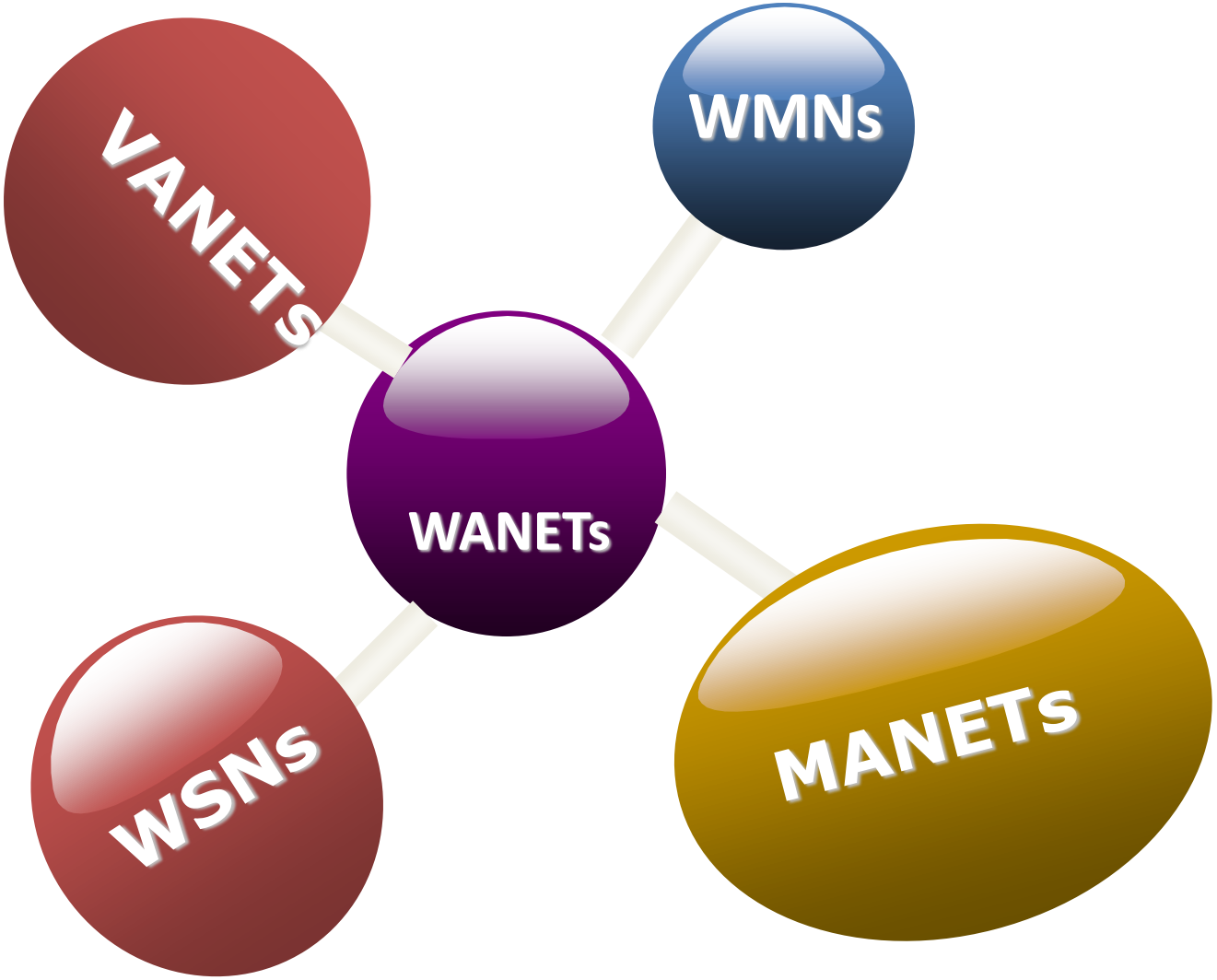


Figure (a) Wireless networking with a base station.
(b) Ad hoc networking

INTRODUCTION



- **Wireless Ad Hoc Networks (WANETs):** "A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner."

- **Mobile Ad Hoc Networks (MANETs):** " A MANETs is a self-configuring network of mobile routers (and associated hosts) connected by wireless links- the union of which form an arbitrary topology. Owing to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves ."

- **Wireless Sensor Networks (WSNETs):** "A wireless sensor networks (WSNs) are spatially distributed autonomous sensors to monitor physical conditions such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location. "

A wireless sensor networks (WSNs) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions.

Wireless Mesh Networks (WMNs): "A WMNs are multi-hop wireless networks, but with a wireless infrastructure/backbone provided by mesh routers. Mesh routers are used to direct data traffic from one place, or node, to another. WMNs support ad hoc networking, and have the capability of self-forming, self-healing, and self-organization."

Vehicular Ad Hoc Networks (VANETs): " Vehicular ad hoc networks (VANETs) are an envision of the intelligent transportation system (ITS). Vehicles communicate with each other in two way: inter-vehicle communication and vehicle to roadside infrastructure communication. VANETs are based on short-range wireless communication between vehicles." The optimal goal of VANETs is to provide safer and more efficient roads in future by communicating timely information to drivers and concerned authorities.

Ad-hoc Network Advantages

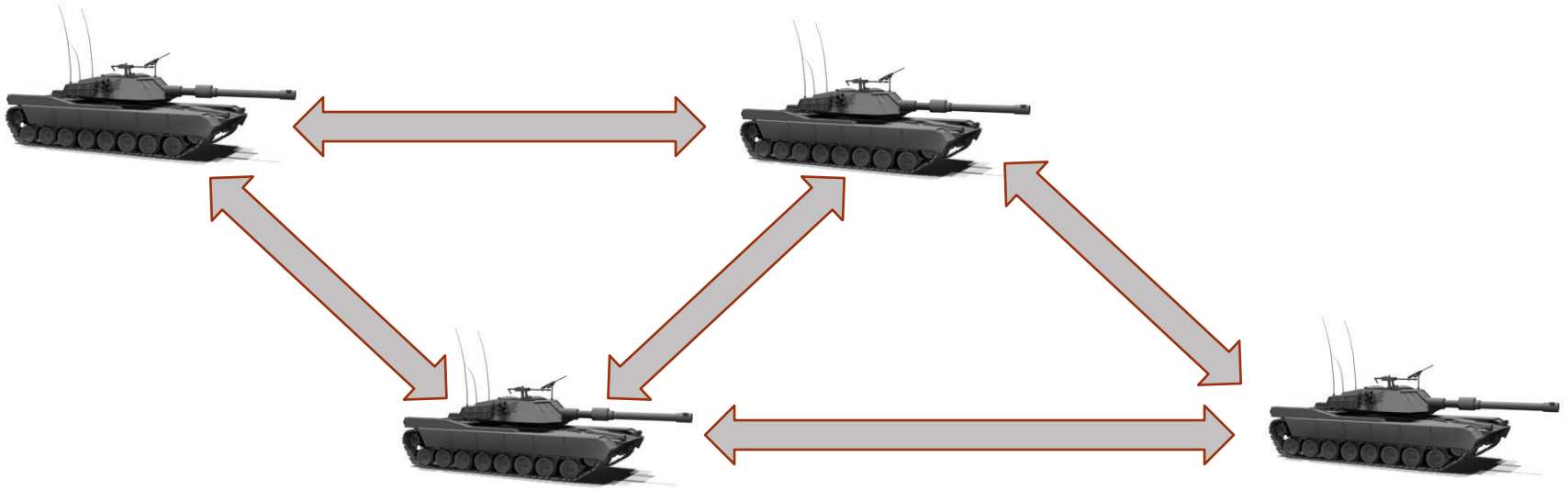
- Ad-hoc networks can have more flexibility.
- It is better in mobility.
- It can be turn up and turn down in a very short time.
- It can be more economical.
- It considered a robust network because of its non-hierarchical distributed control and management mechanisms

Ad-hoc Network Disadvantages

- Hostile environment and irregular connectivity.
- There are no known boundaries for the maximum range that nodes will be able to receive network frames.
- The wireless channel is weak, unreliable, and unprotected from outside interferences.
- Limited wireless range.
- Hidden terminals.
- Packet losses.
- Routes changes.
- Devices heterogeneity.
- Battery power constraints.

Ad-hoc Network Applications

- Group of people with laptops and they want to exchange files and data without having an access point.
- Incase if we need to exchange information and the network's infrastructure has been destroyed.
- It is suitable for military communications at battlefield where there is no network infrastructure.



Other Wireless Networks

- Wireless local area networks (WLAN)
  - IEEE 802.11 (WiFi)
  - 10-100 Mbps, 1.5km
    - 802.11 (1997): upto 2 Mbps, 2.4 GHz
    - 802.11a (1999): upto 54 Mbps, 5 GHz, ~75 feet outdoor
    - 802.11b (1999): upto 11 Mbps, 2.4 GHz, ~150 feet [most popular]
    - 802.11g (2003): upto 54 Mbps, 2.4 GHz, ~150 feet [backward compatible with 802.11b, becoming more popular]
- Wireless metropolitan area networks (WMAN)
  - IEEE 802.16 (WiMax)
  - 1.5-20 Mbps, 5-50km

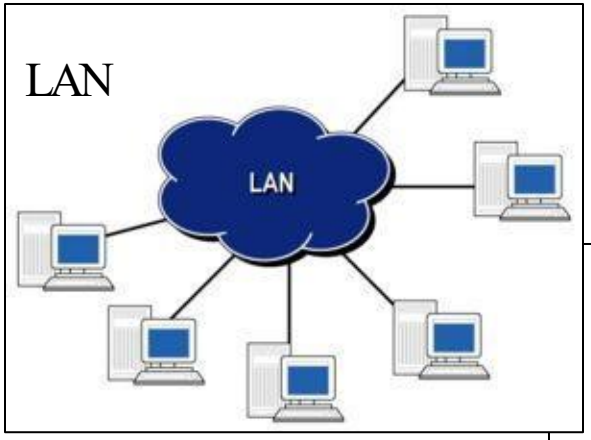
Other Wireless Networks

- Wireless wide area networks (WWAN)
  - worldwide
  - GSM (Global System for Mobile communications)
  - 9.6 – 33 kbps
  - 3G ("third generation"): 128-384 kbps to 2Mbps

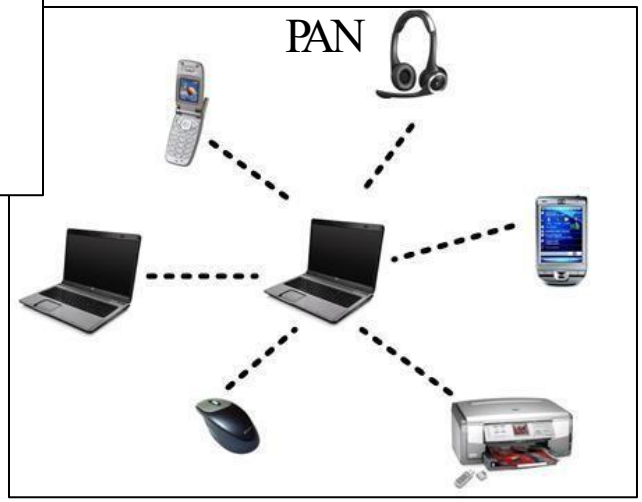
Other Networks

- Internetworks
  - connecting different kinds of networks
  - routers, gateways

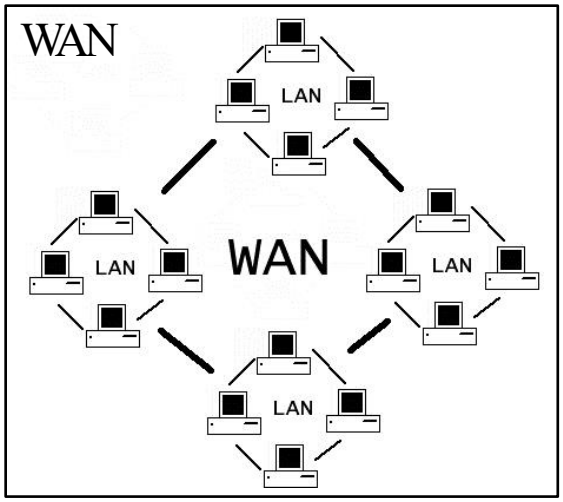
LAN



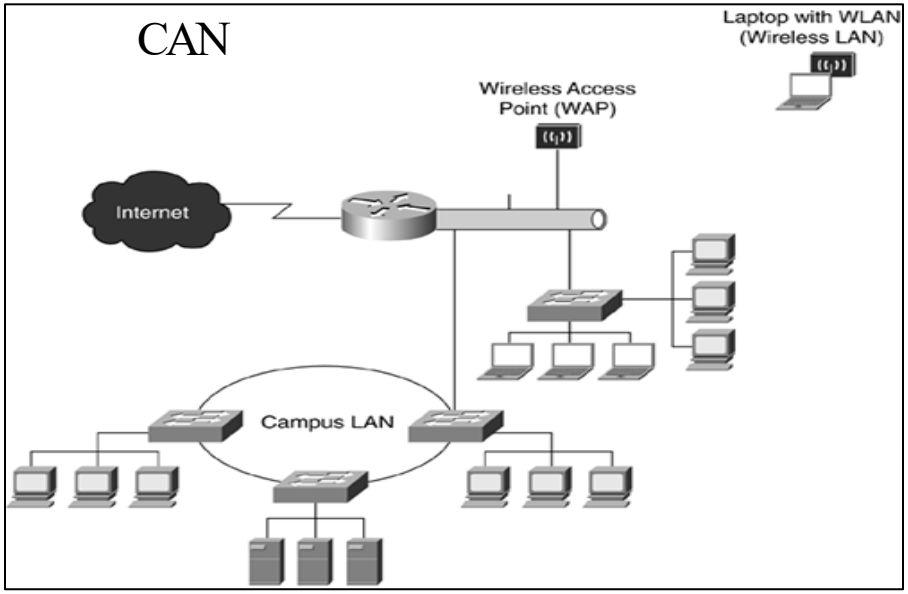
PAN



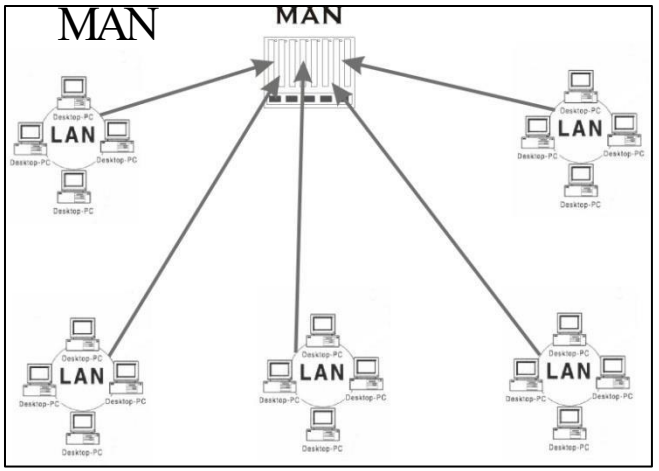
WAN



CAN



MAN



DISTINGUISH BETWEEN LAN,WAN,MAN

PARAMETERS	LAN	WAN	MAN
Ownership of network	Private	Private or public	Private or public
Geographical area covered	Small	Very large	Moderate
Design and maintenance	Easy	Not easy	Not easy
Communication medium	Twisted Pair cable (UTP)	PSTN or satellite links	Coaxial cables, PSTN, optical fibre, cables, wireless
Bandwidth	Low	High	moderate
Data rates(speed)	High	Low	moderate

Network performance

	Example	*Range*	*Bandwidth (Mbps)*	*Latency (ms)*
Wired:				
LAN	Ethernet	1-2 km	10-1000	1-10
MAN	ATM	250 km	1-150	10
WAN	IP routing	worldwide	.01-600	100-500
Internetwork	Internet	worldwide	0.5-600	100-500
Wireless:				
WPAN	Bluetooth (802.15.1)	10 - 30m	0.5-2	5-20
WLAN	WiFi (IEEE 802.11)	0.15-1.5 km	2-54	5-20
WMAN	WiMAX (802.16)	550 km	1.5-20	5-20
WWAN	GSM, 3G phone nets	worldwide	0.01-2	100-500

Outline

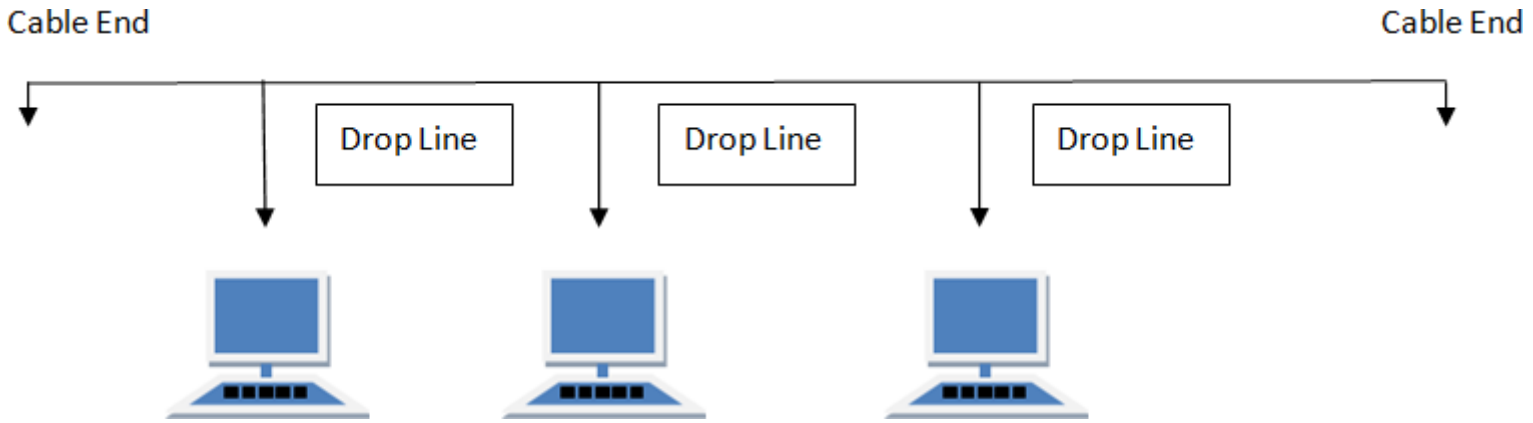
- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- **Topologies**
- Network Architectures
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

Topologies-Types of Network Topology

- BUS
- RING
- STAR
- MESH
- TREE
- HYBRID

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable.When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

It transmits data only in one direction.

Every device is connected to a single cable

BUS Topology

Advantages of Bus Topology

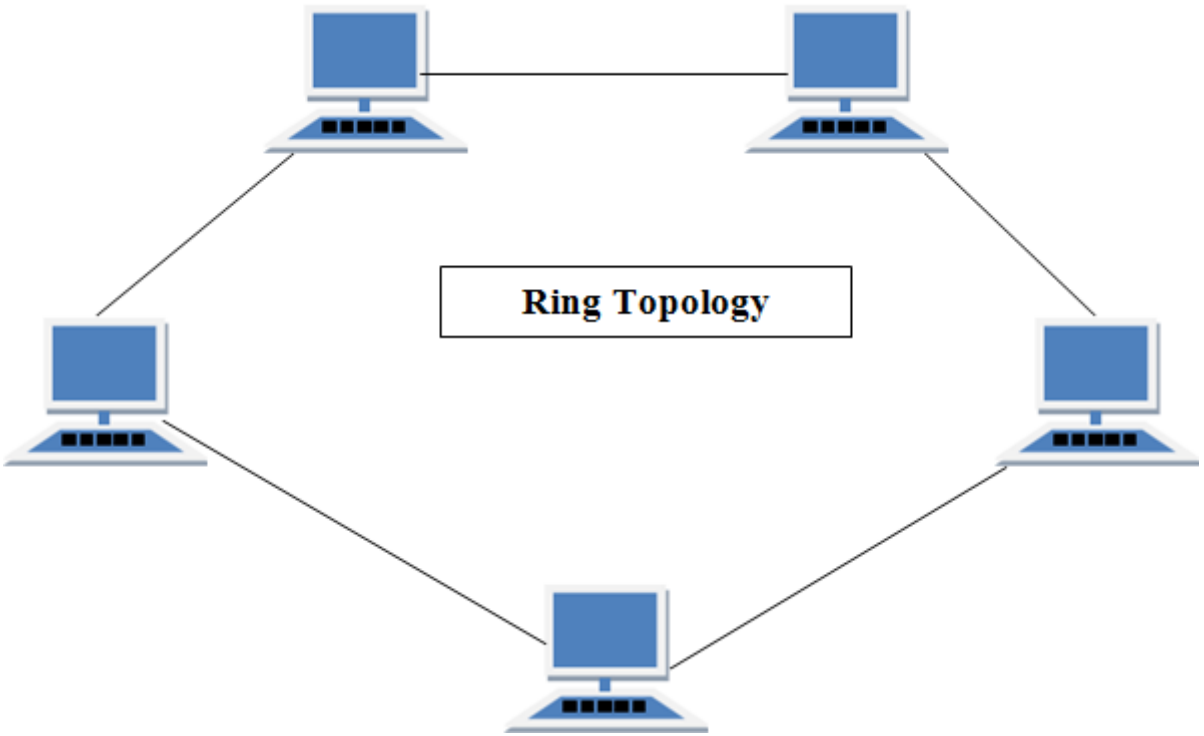
- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

- A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Ring Topology

Advantages of Ring Topology

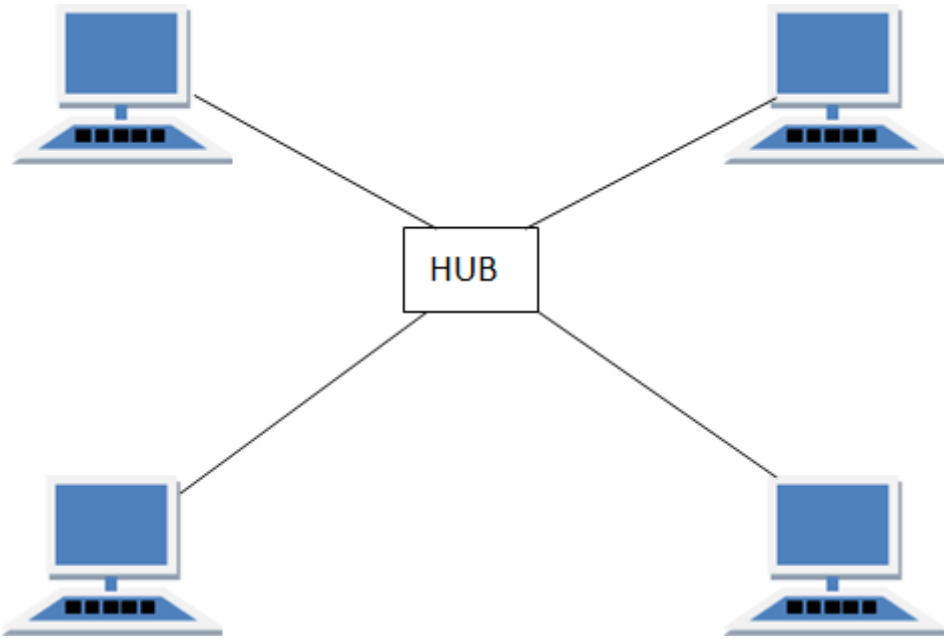
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data. Cheap to install and expand.

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 this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

Every node has its own dedicated connection to the hub.

Hub acts as a repeater for data flow.

Can be used with twisted pair, Optical Fibre or coaxial cable.

STAR Topology

Advantages of Star Topology

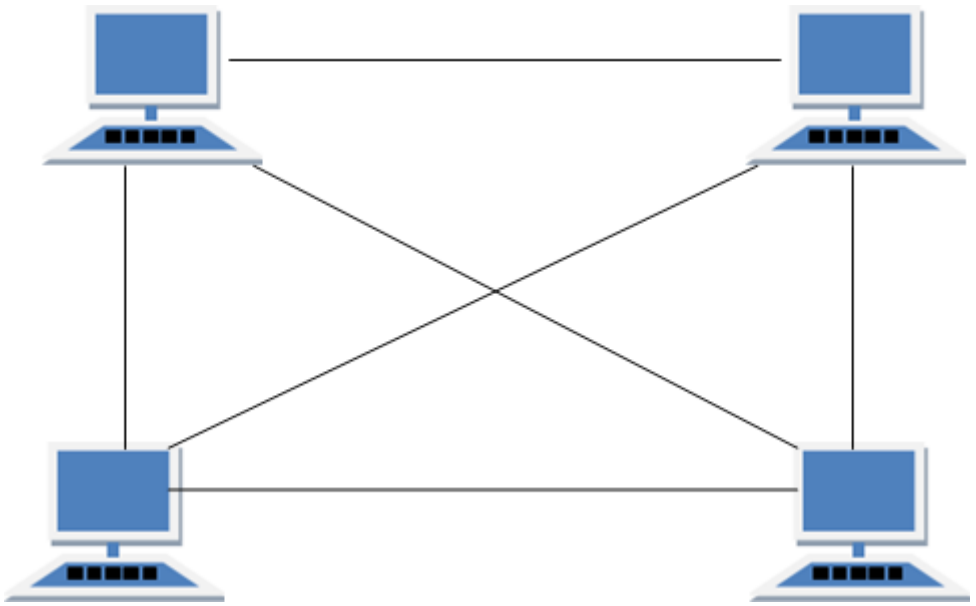
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

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

MESH Topology

It is a point-to-point connection to other nodes or devices.All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.



Features of Mesh Topology

Fully connected.

Robust.

Not flexible.

MESH Topology

Advantages of Mesh Topology

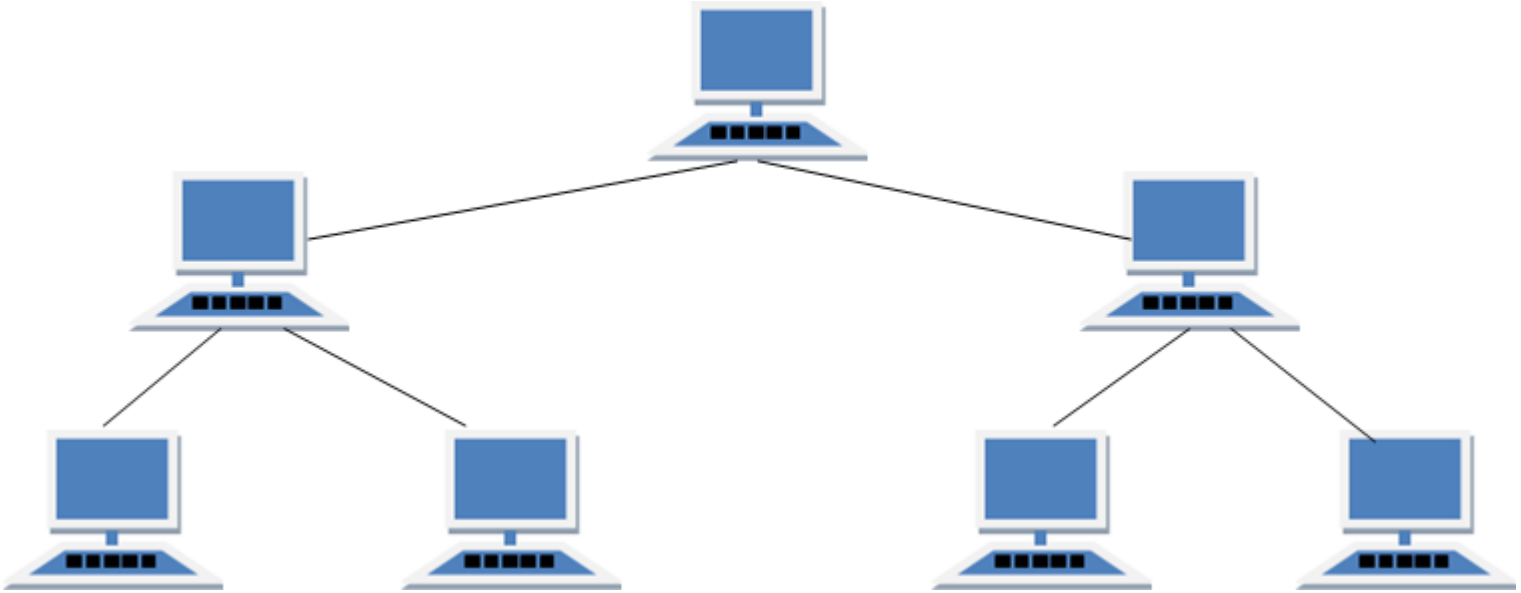
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

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

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.



Features of Tree Topology

Ideal if workstations are located in groups.

Used in Wide Area Network.

TREE Topology

Advantages of Tree Topology

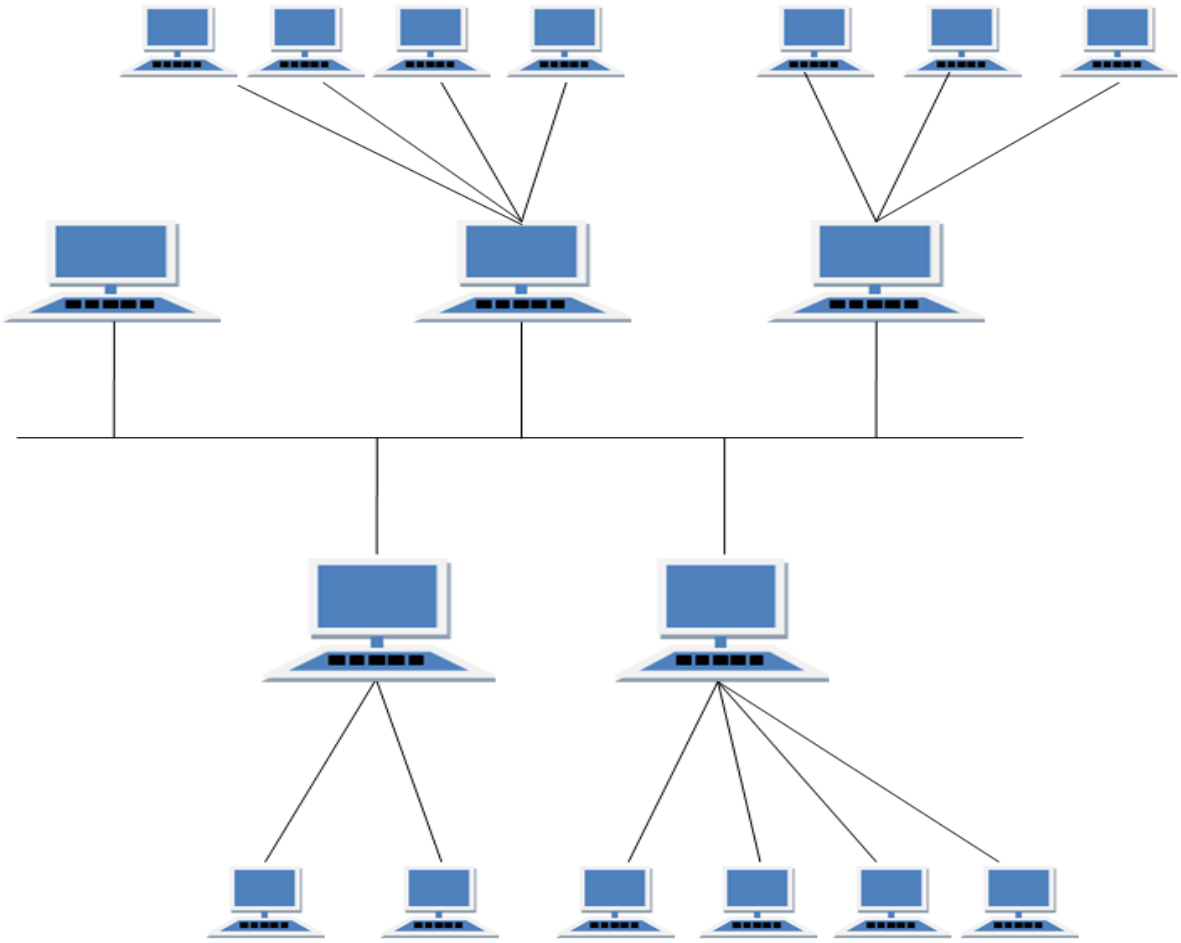
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages of Tree Topology

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

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in HybridTopology (ring topology and star topology).



HYBRID Topology

Features of Hybrid Topology

- It is a combination of two or topologies
- 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.

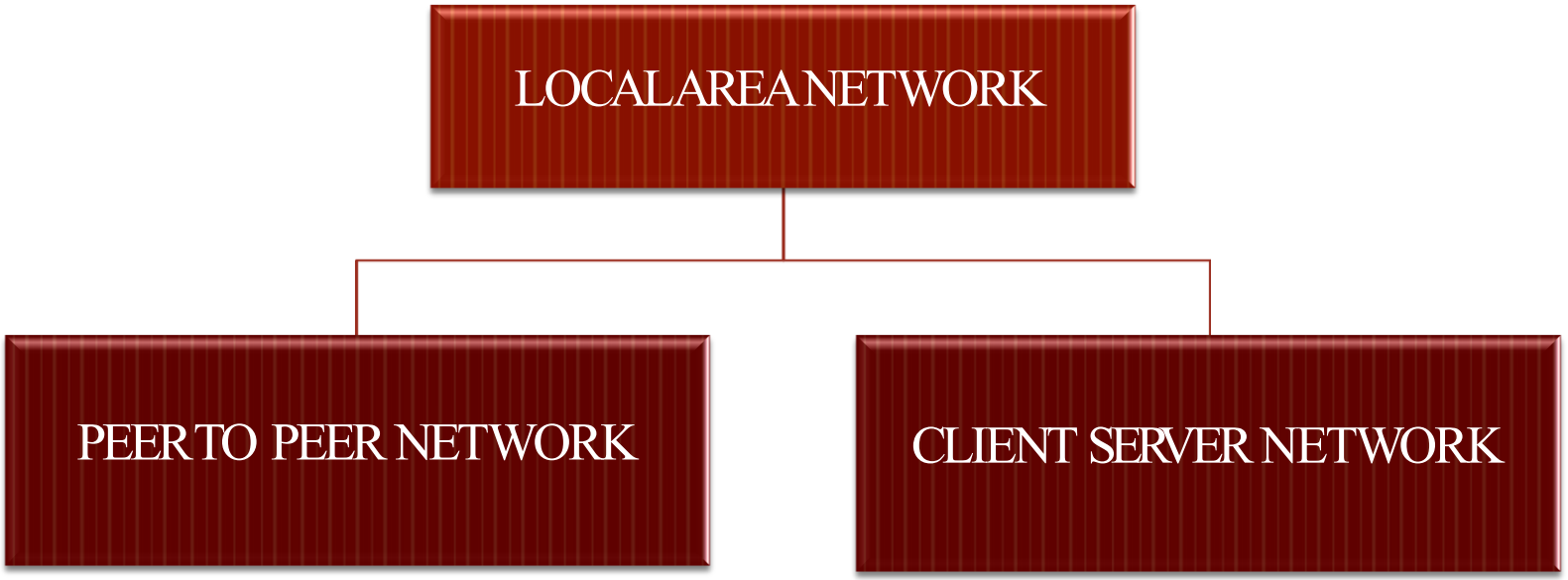
Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- **Network Architectures**
- OSI Model
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

NETWORK CLASSIFICATION BY THEIR COMPONENT ROLE



PEER TO PEER NETWORK

- A peer-to-peer network is a distributed network architecture composed of participants that make a portion of their resources, such as processing power, disk storage or network bandwidth directly to network participants without the need for central coordination instances.
- Used largely for sharing of content files such as audio, video, data or anything in a digital format.
- There are many p2p protocols such as Ares, Bittorrent, or eDonkey.
- Can be very large
- Can also be used for business solutions for relatively small companies that may not have resources available to implement a server solution.
- Peer to peer network is useful for a small network containing less than 10 computers on a single LAN .
- In peer to peer network each computer can function as both client and server.
- Peer to peer networks do not have a central control system. There are no servers in peer networks.
- Peer networks are amplified into home group.

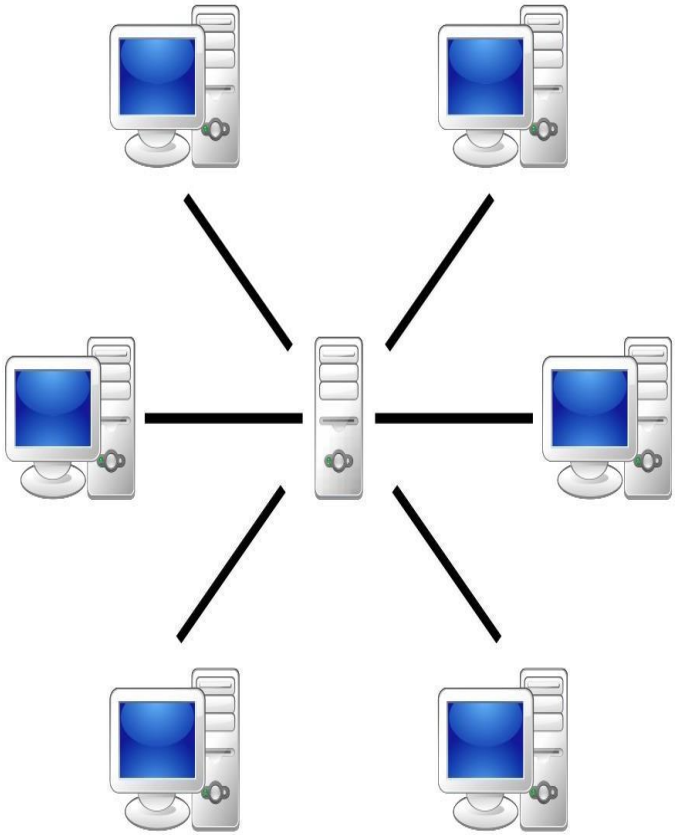
ADVANTAGES & DISADVANTAGES OF PEER TO PEER NETWORK

Advantages:

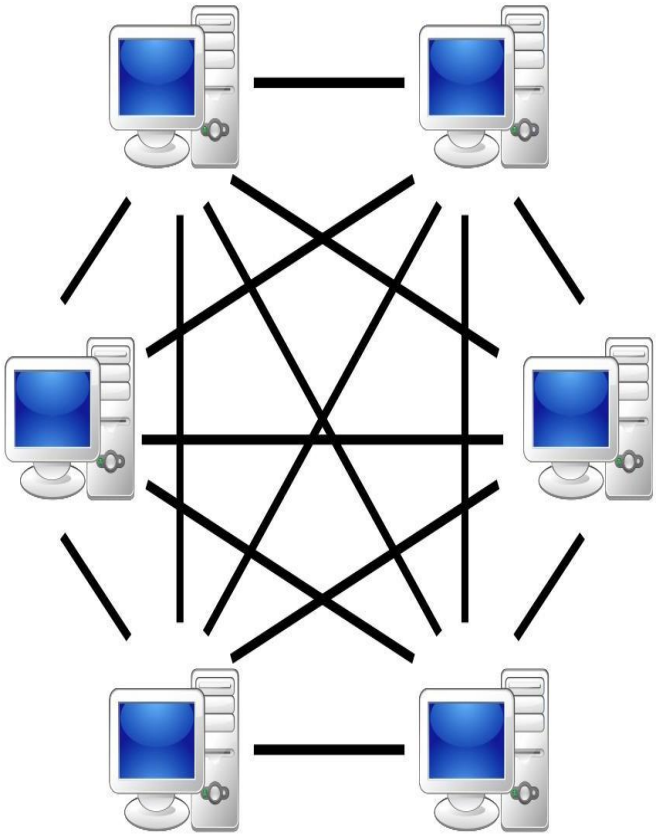
- Use less expensive computer hardware
- Easy to administer
- No NOS required
- More built in redundancy
- Easy setup & low cost

Disadvantages:

- Not very secure
- No central point of storage or file archiving
- Additional load on computer because of resource sharing
- Hard to maintain version control



Server-based



P2P-network

CLIENT/SERVER NETWORK

- In client-server network relationships, certain computers act as server and other act as clients. A server is simply a computer, that available the network resources and provides service to other computers when they request it. A client is the computer running a program that requests the service from a server.
- Local area network(LAN) is based on client server network relationship.
- A client-server network is one n which all available network resources such as files, directories, applications and shared devices, are centrally managed and hosted and then are accessed by client.
- Client serve network are defined by the presence of servers on a network that provide security and administration of the network.

ADVANTAGES AND DISADVANTAGES OF CLIENT-SERVER NETWORK

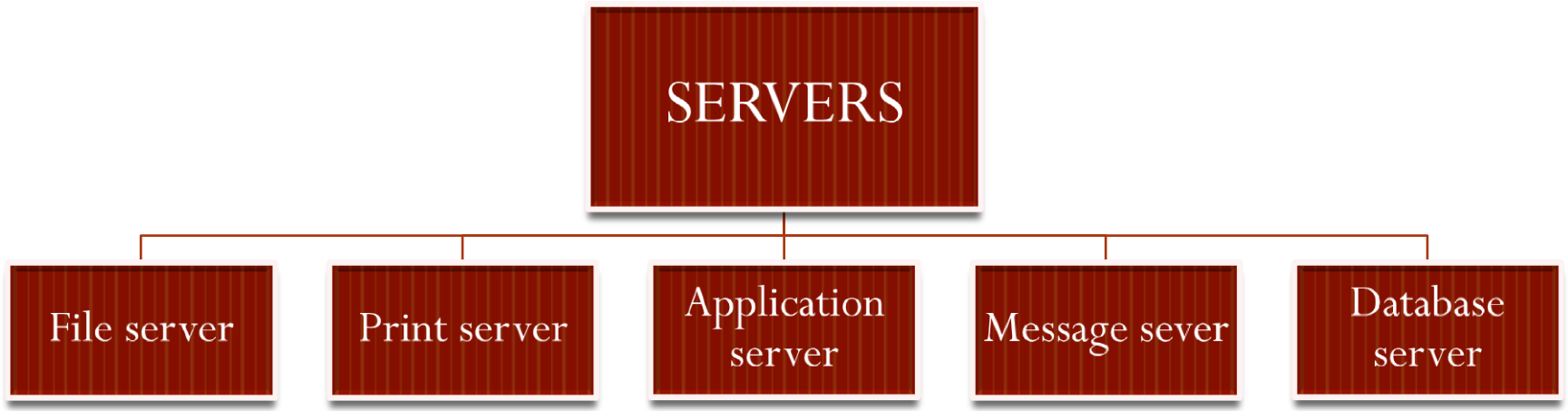
Advantages:

- Very secure
- Better performance
- Centralized backup
- very reliable

Disadvantages:

- requires professional administration
- More hardware-intensive
- More software intensive
- Expensive dedicated software

TYPES OF SERVERS



TYPES OF SERVERS

- **File server**: These servers provide the services for storing, retrieving and moving the data. A user can read, write, exchange and manage the files with the help of file servers.
- **Printer server**: The printer server is used for controlling and managing printing on the network. It also offers the fax service to the network users.
- **Application server**: The expensive software and additional computing power can be shared by the computers in a network with he help of application servers.
- **Message server**: It is used to co-ordinate the interaction between users, documents and applications. The data can be used in the for of audio, video, binary, text or graphics.
- **Database server**: It is a type of application server. It allows the uses to access the centralised strong database.

Distributed Networks

- Arrangement of networked computers in which several processors (the CPUs) are located on scattered machines, but are capable of working both independently and jointly as required.
- The key elements of Distributed Network Architecture are, as the name implies, the distribution of decision-making and control out to each site, while simultaneously, networking and synchronizing the various sites together via a central hub.
- **Distributed networking** is a distributed computing network system, said to be distributed when the computer programming and the data to be worked on are spread out across more than one computer. Usually, this is implemented over a computer network.

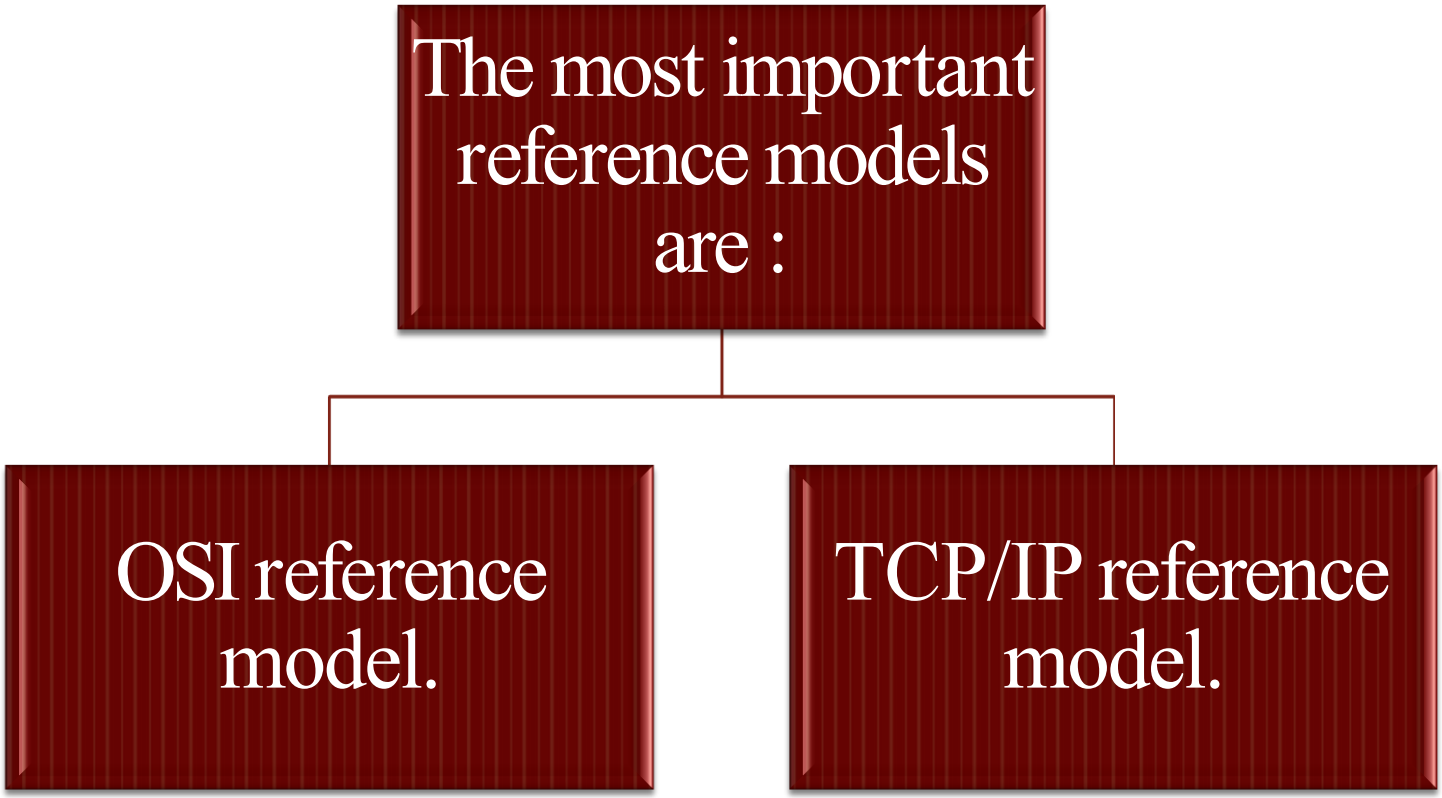
Benefits of Distributed Network Architecture

- **Scalability:** Enterprise solutions that rely on a single Enterprise server inevitably suffer from performance issues as the Enterprise grows and the server is overwhelmed. Moreover, single server solutions are highly susceptible to network failures.
- **Cost:** Servers and software at each local site can be appropriately sized to meet the specific needs of each site, without requiring installing an expensive server at even the smallest sites.
- **Reliability:** Distributed Network Architecture is much more tolerant of network and hardware failures than a single server approach.

Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- **OSI Model**
- TCP/IP Model
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

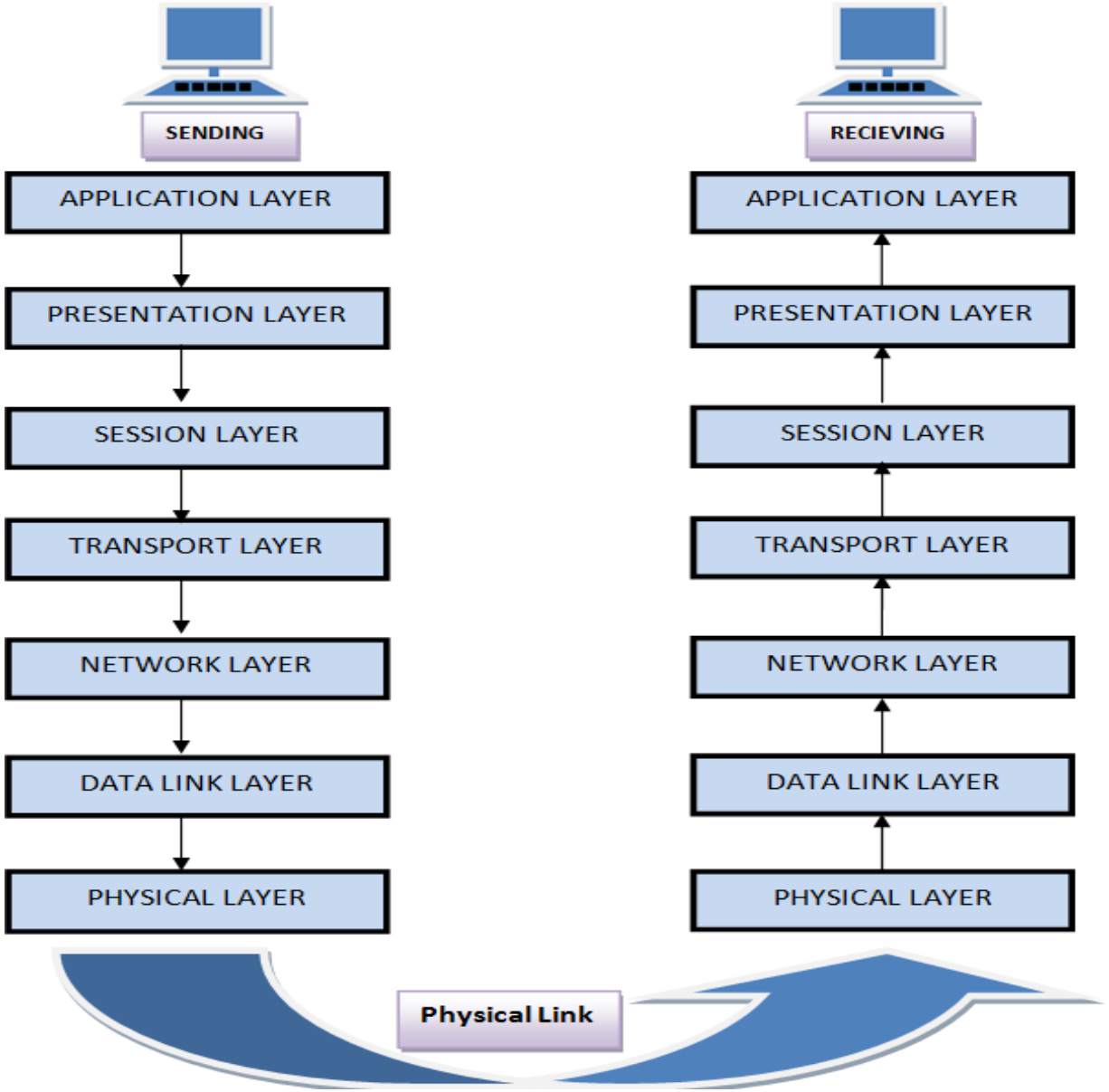
Reference Models in Communication Networks



OSI

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

OSI Model


SENDING
APPLICATION LAYER
PRESENTATION LAYER
SESSION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHYSICAL LAYER
RECIEVING
APPLICATION LAYER
PRESENTATION LAYER
SESSION LAYER
TRANSPORT LAYER
NETWORK LAYER
DATA LINK LAYER
PHYSICAL LAYER
Physical Link

Feature of OSI Model :

- Big picture of communication over network is understandable through this OSI model.
- We see how hardware and software work together.
- We can understand new technologies as they are developed.
- Troubleshooting is easier by separate networks.
- Can be used to compare basic functional relationships on different networks.

Layer 1 : The Physical Layer :

- It is the lowest layer of the OSI Model.
- It activates, maintains and deactivates the physical connection.
- It is responsible for transmission and reception of the unstructured raw data over network.
- Voltages and data rates needed for transmission is defined in the physical layer.
- It converts the digital/analog bits into electrical signal or optical signals.
- Data encoding is also done in this layer.

Layer 2: Data Link Layer :

- Data link layer synchronizes the information which is to be transmitted over the physical layer.
- The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
- Transmitting and receiving data frames sequentially is managed by this layer.
- This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
- This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer :

- It routes the signal through different channels from one node to other.
- It acts as a network controller. It manages the Subnet traffic.
- It decides by which route data should take.
- It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer :

- It decides if data transmission should be on parallel path or single path.
- Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
- It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
- Transport layer can be very complex, depending upon the network requirements.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer :

- Session layer manages and synchronize the conversation between two different applications.
- Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer :

- Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
- While receiving the data, presentation layer transforms the data to be ready for the application layer.
- Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
- It perfroms Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer :

- It is the topmost layer.
- Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
- This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model:

- OSI model distinguishes well between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- Protocols can be replaced by new protocols as technology changes.
- Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.
- It is just used as a reference model.

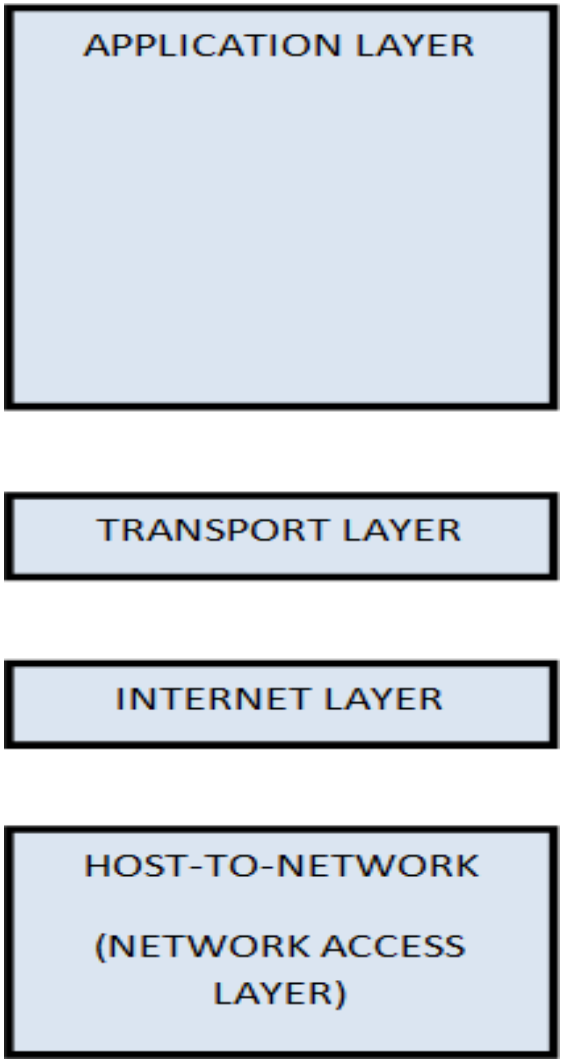
Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- **TCP/IP Model**
- Design issues for Layers
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

TCP/IP model overview

- TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.
- The features of TCP/IP reference model were:
  - Support for a flexible architecture. Adding more machines to a network was easy.
  - The network was robust, and connections remained intact untill the source and destination machines were functioning
  - The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

TCP/IP reference model diagram



Layer 1 : Host-to-network Layer

- Lowest layer of the all.
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.

Layer 2: Internet layer

- Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

- TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
- FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
- SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
- DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports a number of routing protocols.
- Can be used to establish a connection between two computers.

Demerits of TCP/IP

- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

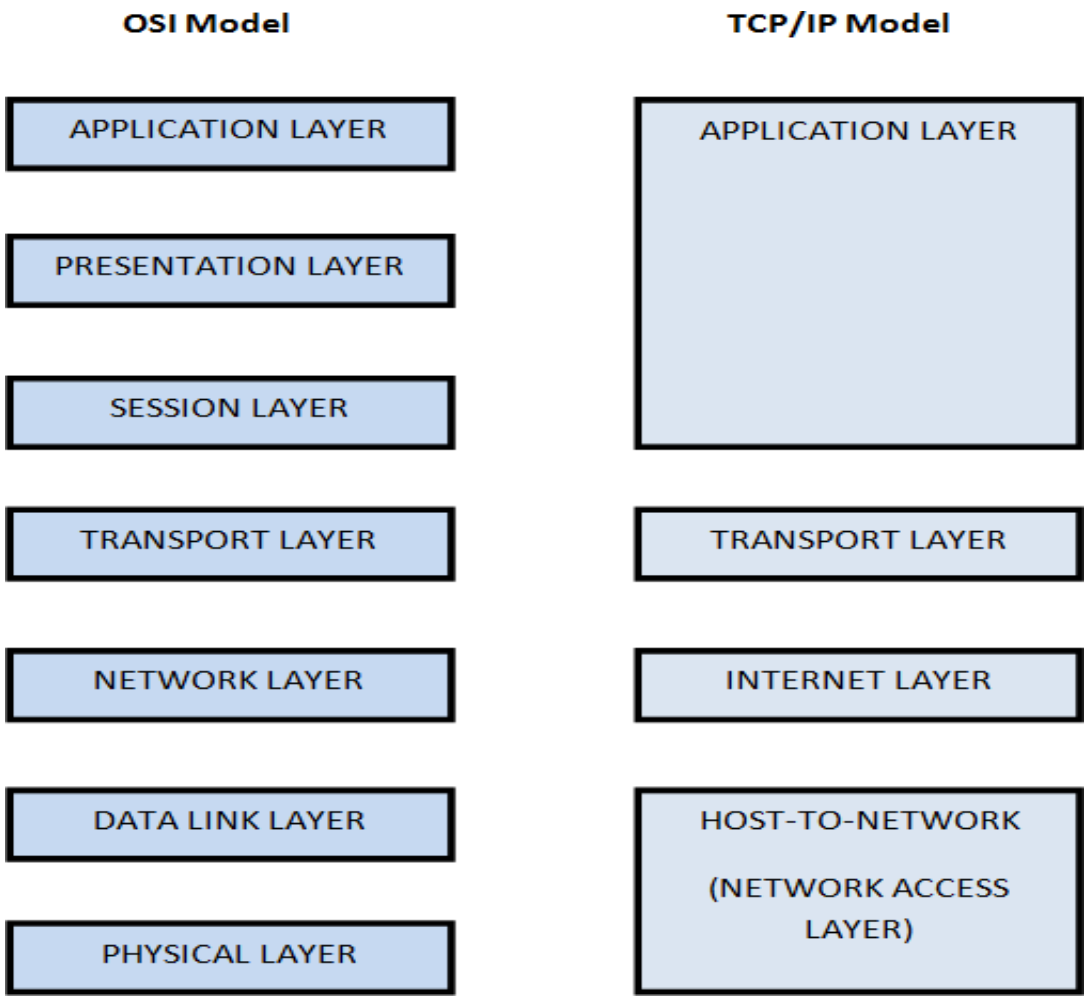
Comparison of OSI Reference Model and TCP/IP Reference Model

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.

Comparison of OSI Reference Model and TCP/IP Reference Model

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model



Outline

- Introduction of LAN; MAN;WAN; PAN,Ad-hoc Network
- Topologies
- Network Architectures
- OSI Model
- TCP/IP Model
- **Design issues for Layers**
- Transmission Mediums
- Network Devices
- Manchester and Differential Manchester Encodings;
- IEEE802.11: Frequency Hopping (FHSS) and Direct Sequence (DSSS)

Design issues for Layers

- Addressing
- Error Control
- Flow Control
- Multiplexing
- Routing

Addressing

- Addressing Level

• Unique address for each end system (computer) and each intermediate system(router)

•Network level address-IP or internet address (TCP/IP)
Network service access point or NSAP (OSI)

• Process within the system-Port number (TCP/IP)
Service access point or SAP

- Addressing Scope

•Global nonambiguity-Global address identifies unique system,There is only one system with address X

• Global applicability-It is possible at any system (any address) to identify any other system (address) by the global address of the other system
Address X identifies that system from anywhere on the network

• e.g MAC address on IEEE 802 networks

Error Control

- Observation against loss or damage of data and control information
  Error control is implemented as two separate functions:

  Error detection

  Sender inserts error detecting bits Receiver checks these bits

  If OK, acknowledge

  If error, discard packet

  Retransmission

  If no acknowledge in given time, re-transmit

  Performed at various layers of protocol

Flow Control

- Done by receiving entity
  Function to limit amount or rate of data sent by a transmitting entity
  Simplest form: stop-and-wait procedure
  More efficient protocols: Credit systems Sliding window
  Needed at application as well as network layers

Multiplexing

- Supporting multiple connections on one machine

  -Mapping of multiple connections at one level to a single connection at another

  -Carrying a number of connections on one fiber optic cable

  -Aggregating or bonding ISDN (Integrated Services Digital Network) lines to gain bandwidth

Routing

- Determine path or route that packets will follow. Use routing protocol based on a routing algorithm "Good" path should be least cost path

  Cost : depends on the following factors. Average queuing delay

  Propagation delay

  Bandwidth, mean queue length, etc.

  End systems and routers maintain routing tables Dynamic or static