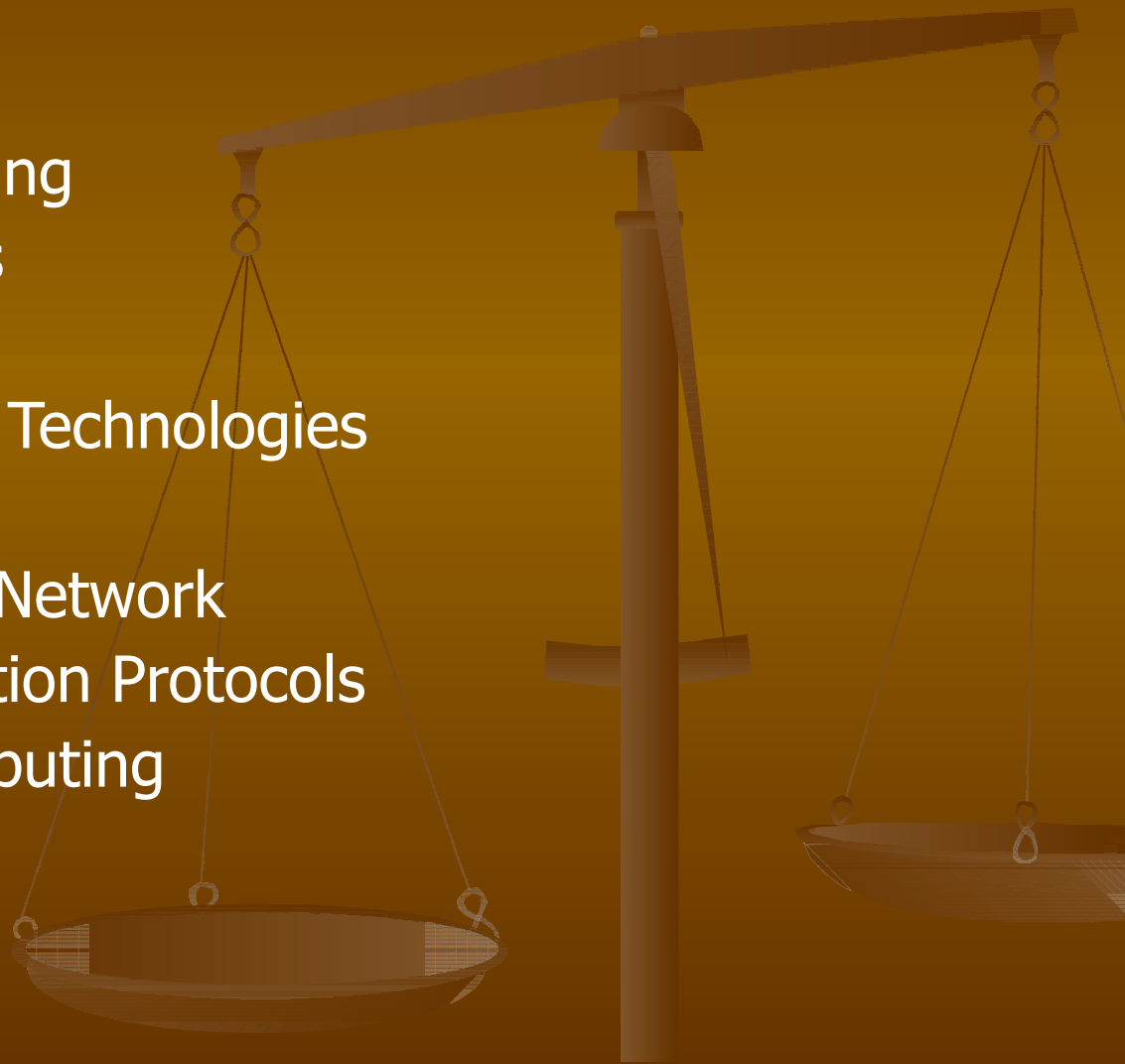
Sardar Patel College of Engineering

Computer Network : Chapter 1 Introduction to computer networks and Internet Part-1

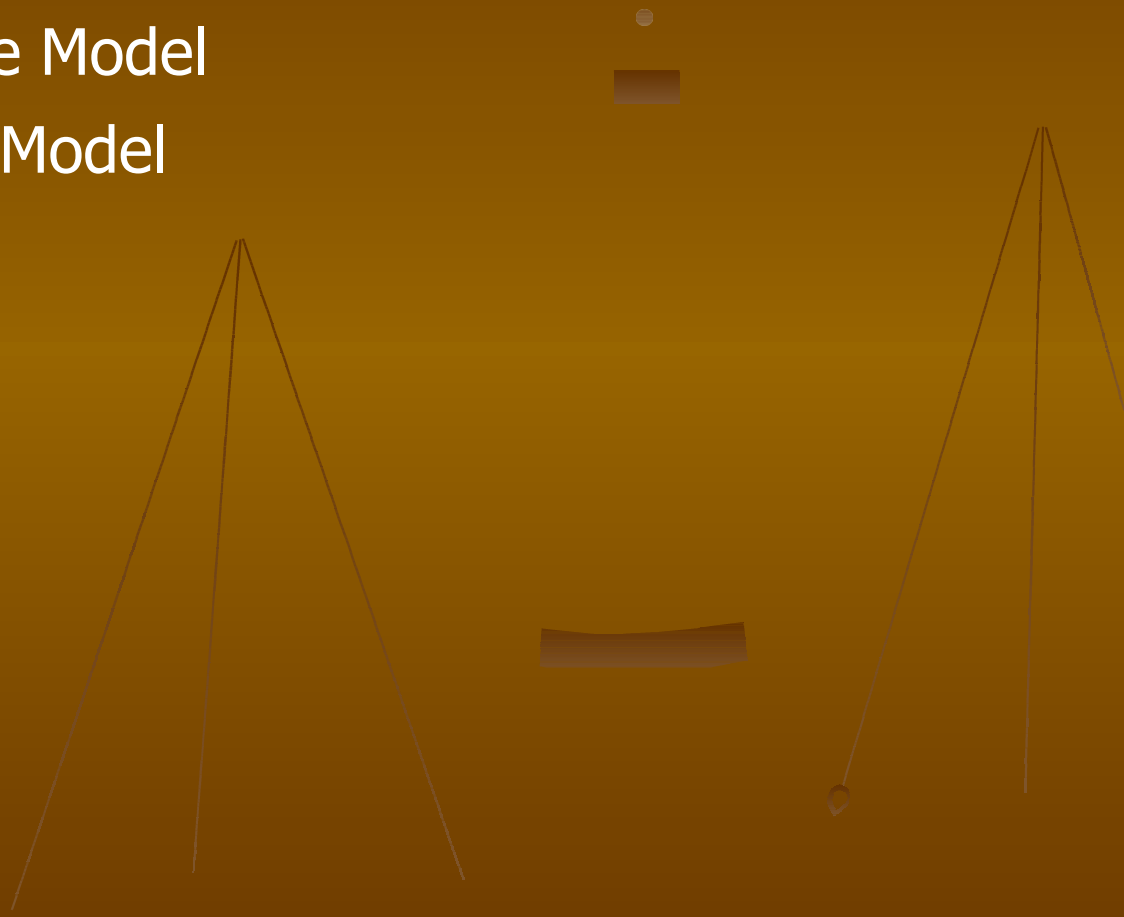
Overview

- What is a network?
- Need for networking
- Evolution of Networking
- Switching Techniques
- Transmission media
- Data Communication Technologies
- Types of Networks
- Network Topologies Network
- Devices Communication Protocols
- Wireless/Mobile Computing
-

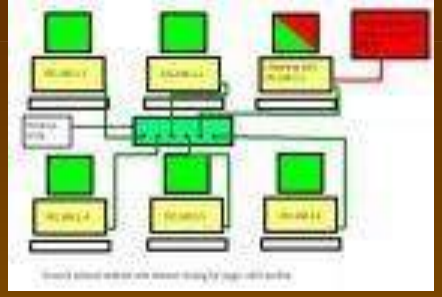


Overview

- Protocol Layers
- ISO/OSI Reference Model
- TCP/IP Reference Model



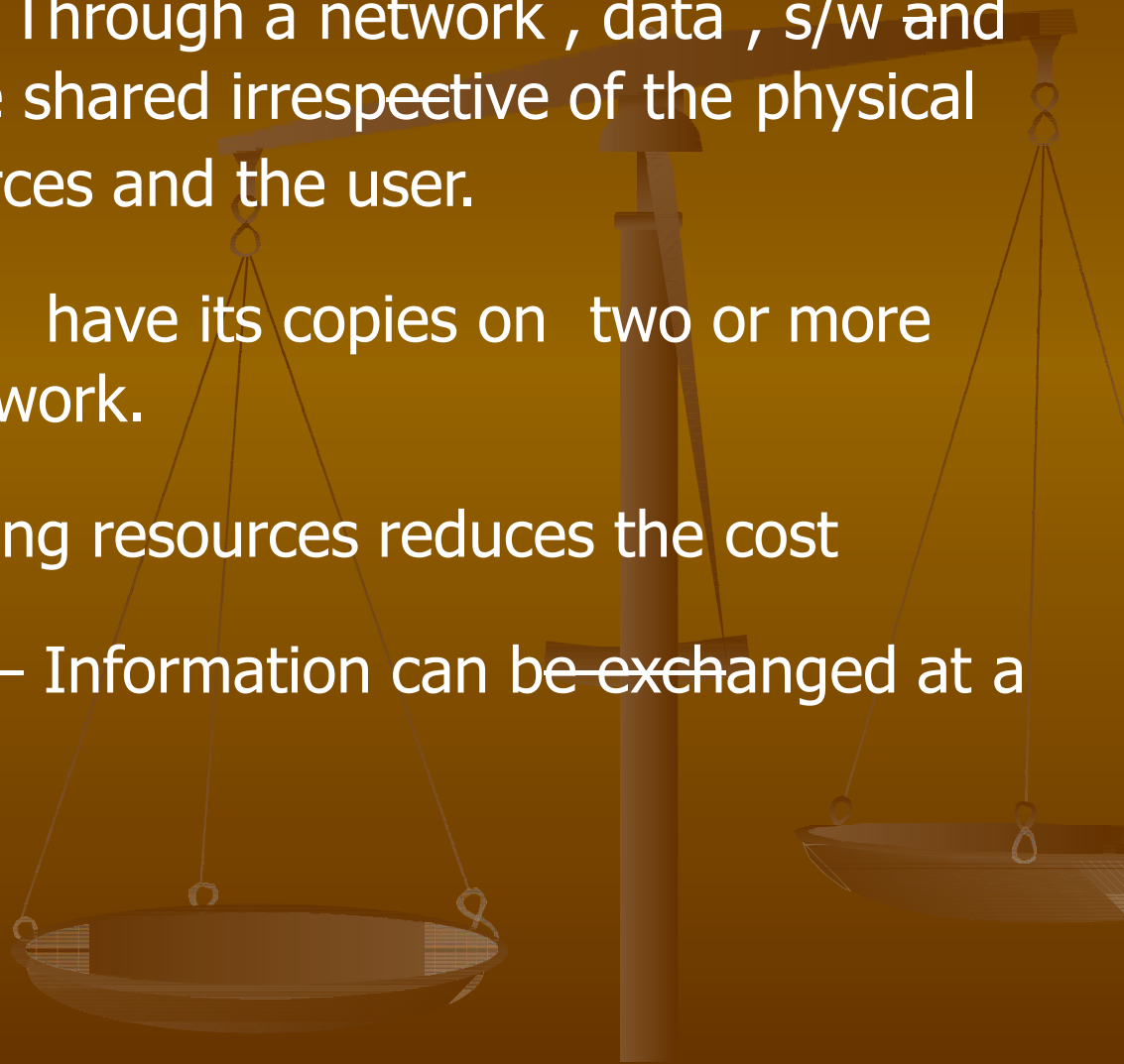
Network



- Network, in computer science, a group of computers and associated devices that are connected by communications facilities.
- Network is an inter connected collection of autonomous computers.
- When two or more computers are joined together so that they are capable of exchanging information , ~~they~~ form a network.

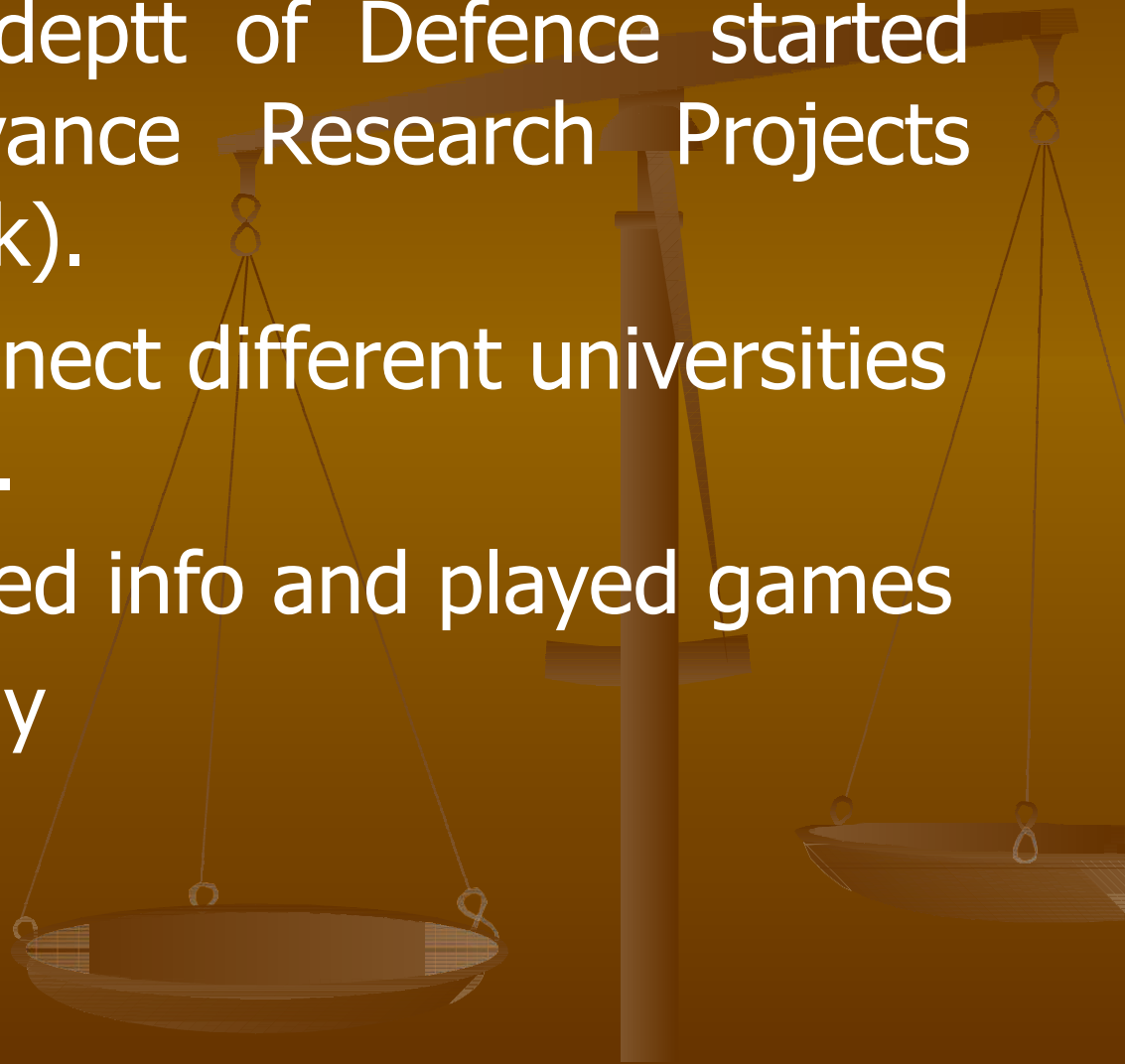
Need for Networking

- Resource sharing - Through a network , data , s/w and h/w resources can be shared irrespective of the physical location of the resources and the user.
- Reliability – A file can have its copies on two or more computers of the network.
- Reduced Cost – Sharing resources reduces the cost
- Fast Communication – Information can be exchanged at a very fast speed



Evolution of Network

- In 1969 , US deptt of Defence started ARPANET(Advance Research Projects Agency NETwork).
- Goal was to connect different universities and US defence.
- People exchanged info and played games
- Expanded rapidly



Evolution of Network

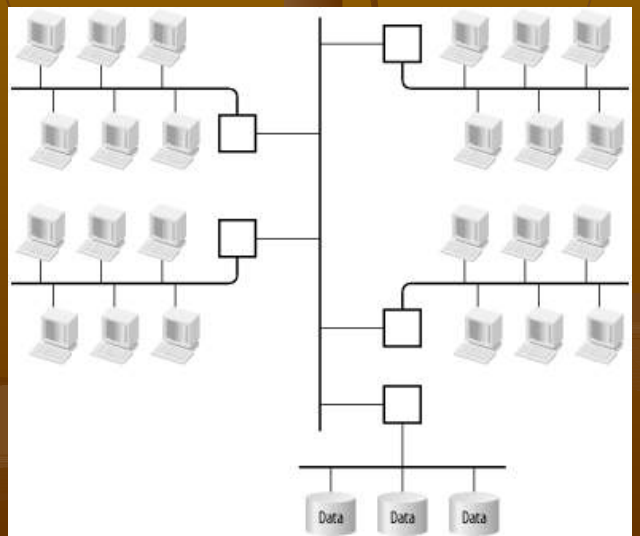
- In mid 80's National Science Foundation created a high capacity network called NSFnet.
- Allowed Academic use and private business
- Many private companies built their own networks which were later interconnected along with ARPANET and NSFnet to form Internet.
- Arpanet was shut down in 1990 .
- Govt funding for NSFnet discontinued in 1995.
- But commercial services can into the scenario which are still running the internet.

Internet

Internet is worldwide network of computer networks.

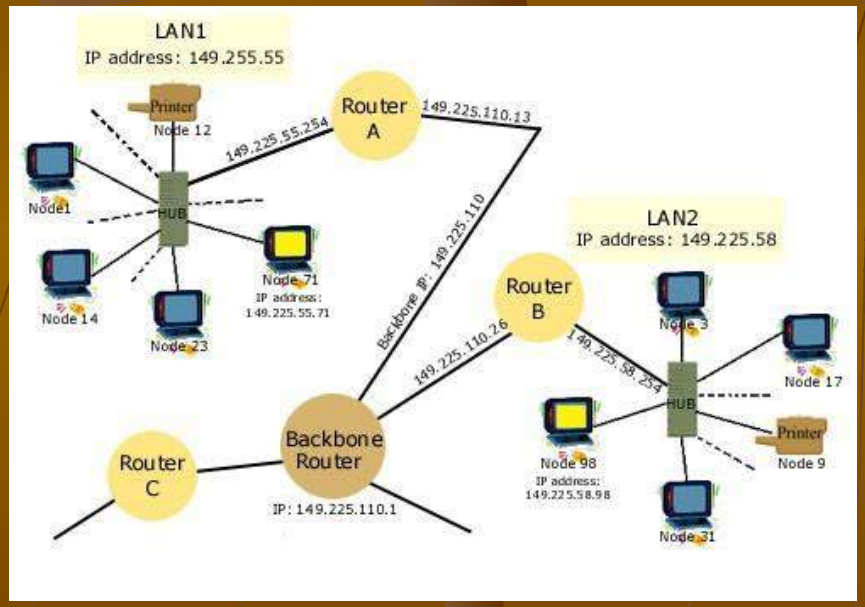
How does it work?

- Most computers are not connected directly to the internet.
- They are connected to smaller networks
- Which are connected through gateways to the internet backbone



Gateway

- Gateway is a device that connects dissimilar networks.
- A backbone is a central interconnecting structure that connects one or more networks just like the trunk of a tree.



How does internet work?

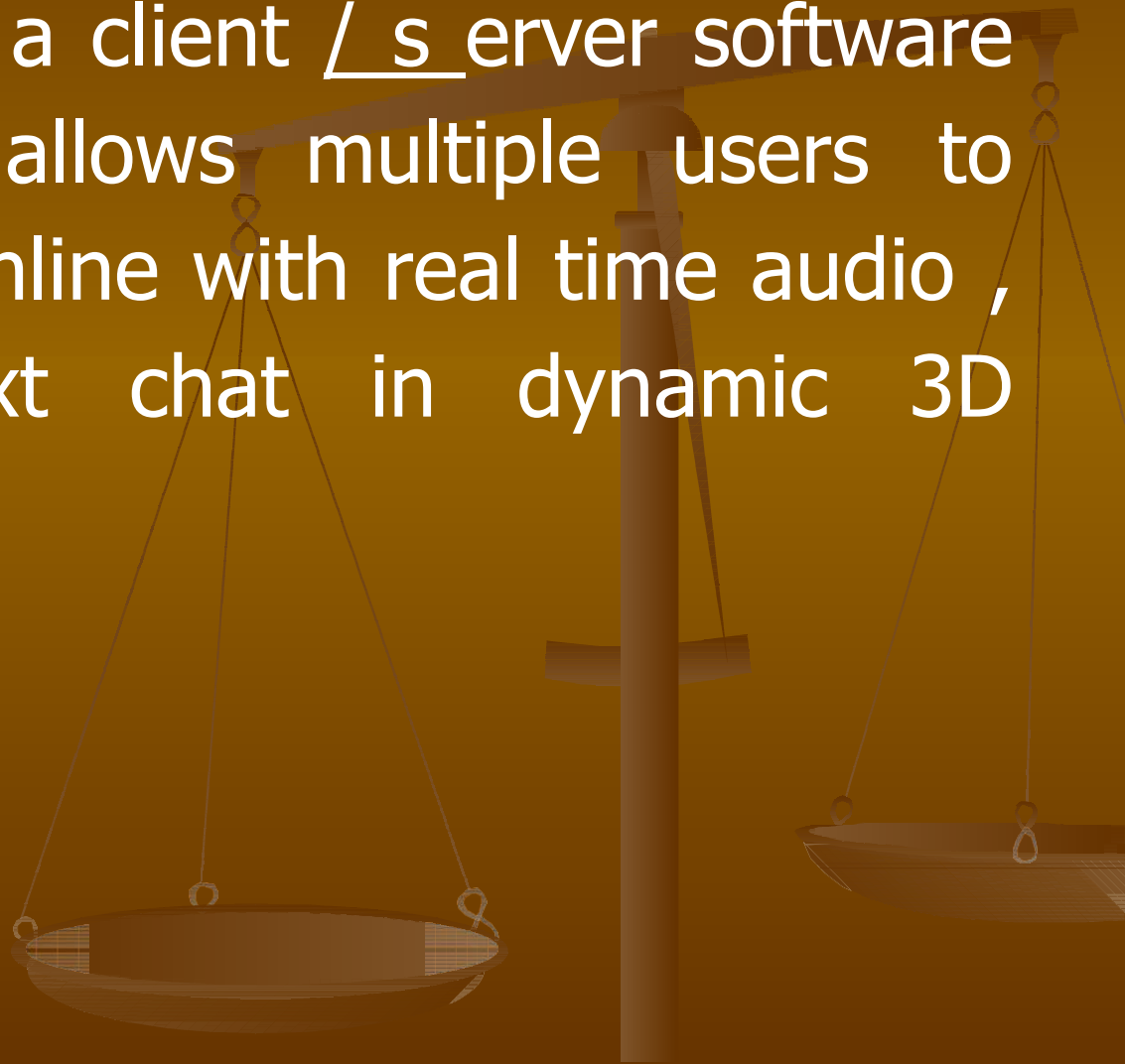
- At the source comp the message to be sent is broken down into small parts called packets.
- Each packet is given a serial no e.g. 1,2,3
- All these packet are sent to the destination computer
- The destination comp receives the packets in random order(10 may come before 1)
- The packets are reassembled in the order of their no and message is restored.

How it functions smoothly?

- Every computer connected to the internet uses same set of rules for communication.
- Set of rules is called protocol
- Communication protocol used by internet is TCP/IP
- The TCP (Transmission control protocol) part is responsible for dividing the message into packets on the source comp and reassembling them at the destination comp.
- The IP (Internet Protocol) is responsible ~~for ha~~ndling the address of the destination comp so that the packet is sent to its proper destination.

Future of Internet- InterSpace

InterSpace is a client / server software program that allows multiple users to communicate online with real time audio , video and text chat in dynamic 3D environments.



Few terms related to Network

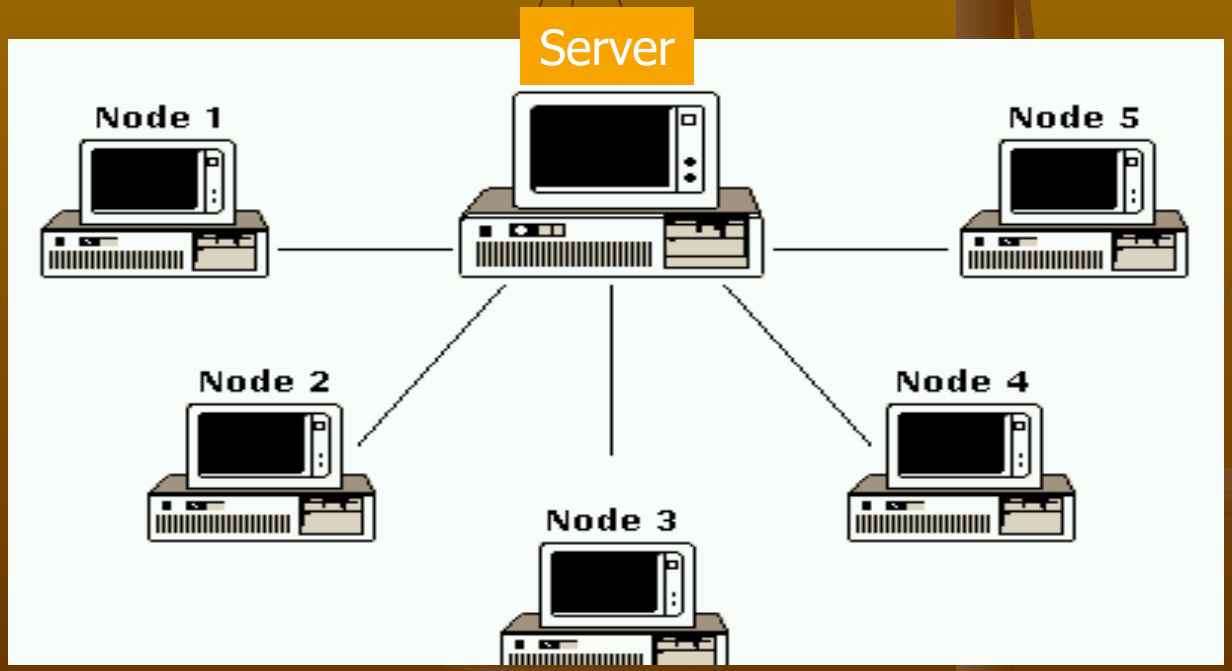
- Workstation or Nodes

  refers to a computer that are attached to a network

- Server

  The master comp is called server.

  Facilitates the sharing of data, s/w and h/w concepts.



Network Interface Unit (NIU)

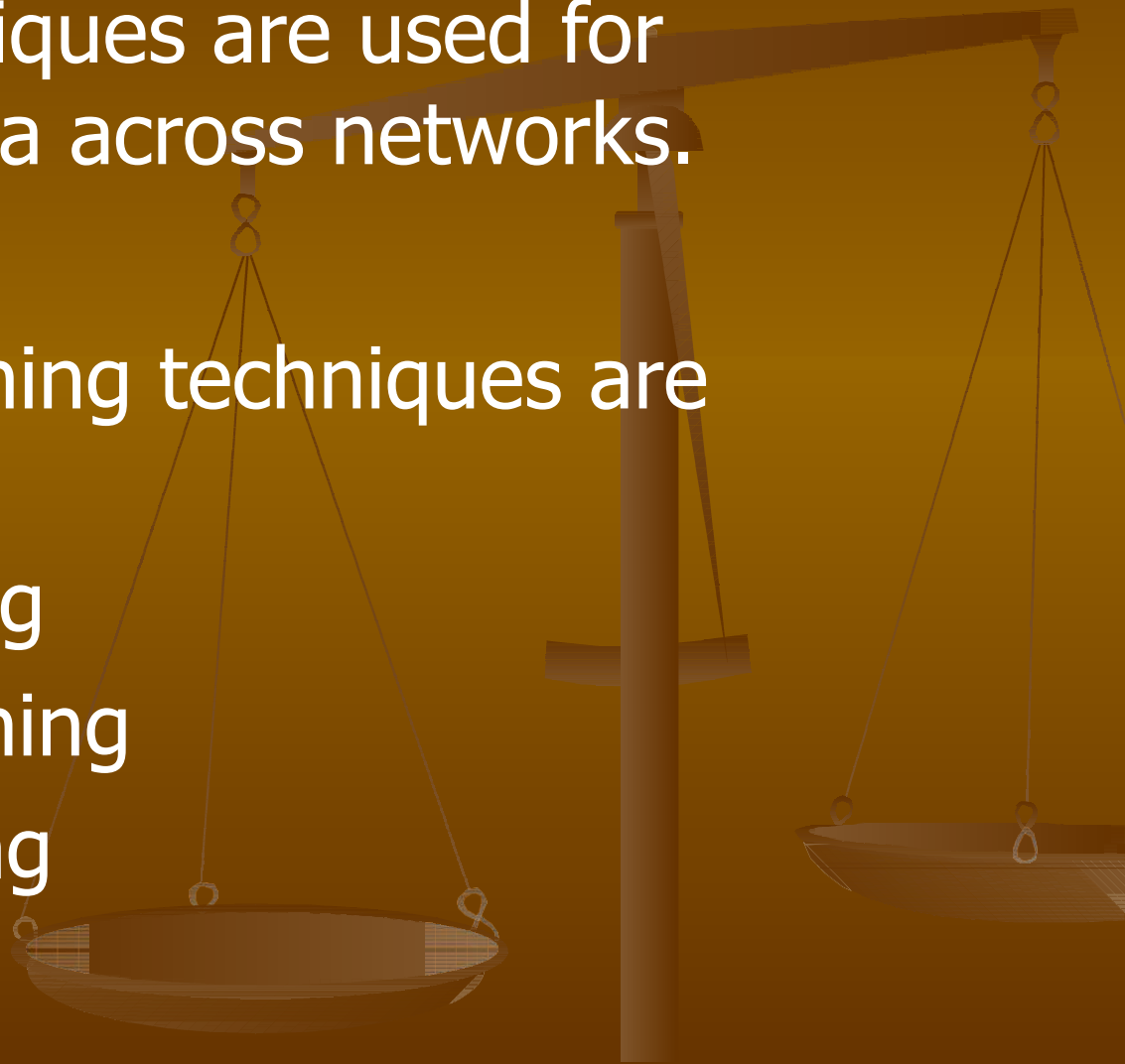
- It is a device attached to each workstation and server.
- Helps to make connections within the network.
- Each NIU has a unique no identifying it called node address.
- NIU is also called terminal access point (TAP).
- Also called Network Interface Card (NIC)
- Each NIC is given a unique physical address called MAC address.

How data is transmitted across networks?

Switching Techniques are used for transmitting data across networks.

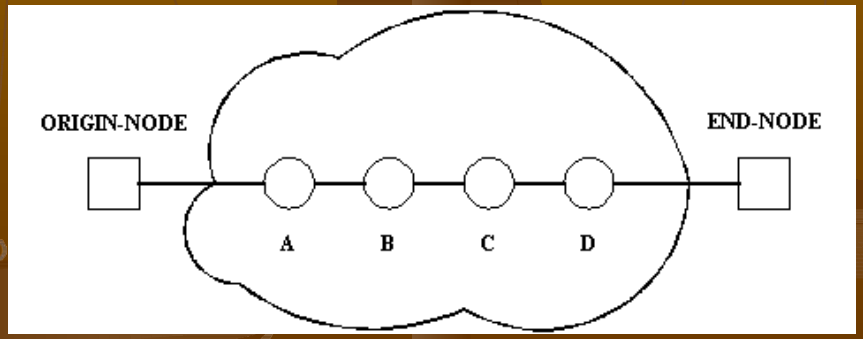
3 types of switching techniques are there.

- Circuit Switching
- Message Switching
- Packet Switching



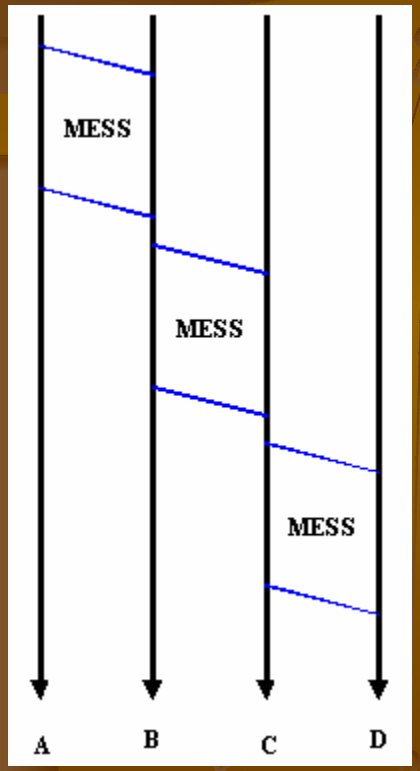
Circuit Switching

- Physical connection between the two computers is established and then data is transmitted from source to destination computer.
- When a computer places a telephone call , the switching equipment within the telephone system seeks out a physical copper path from sender's to receiver's telephone.
- It sets up end-to-end connection between computers before any data can be sent.



Message Switching

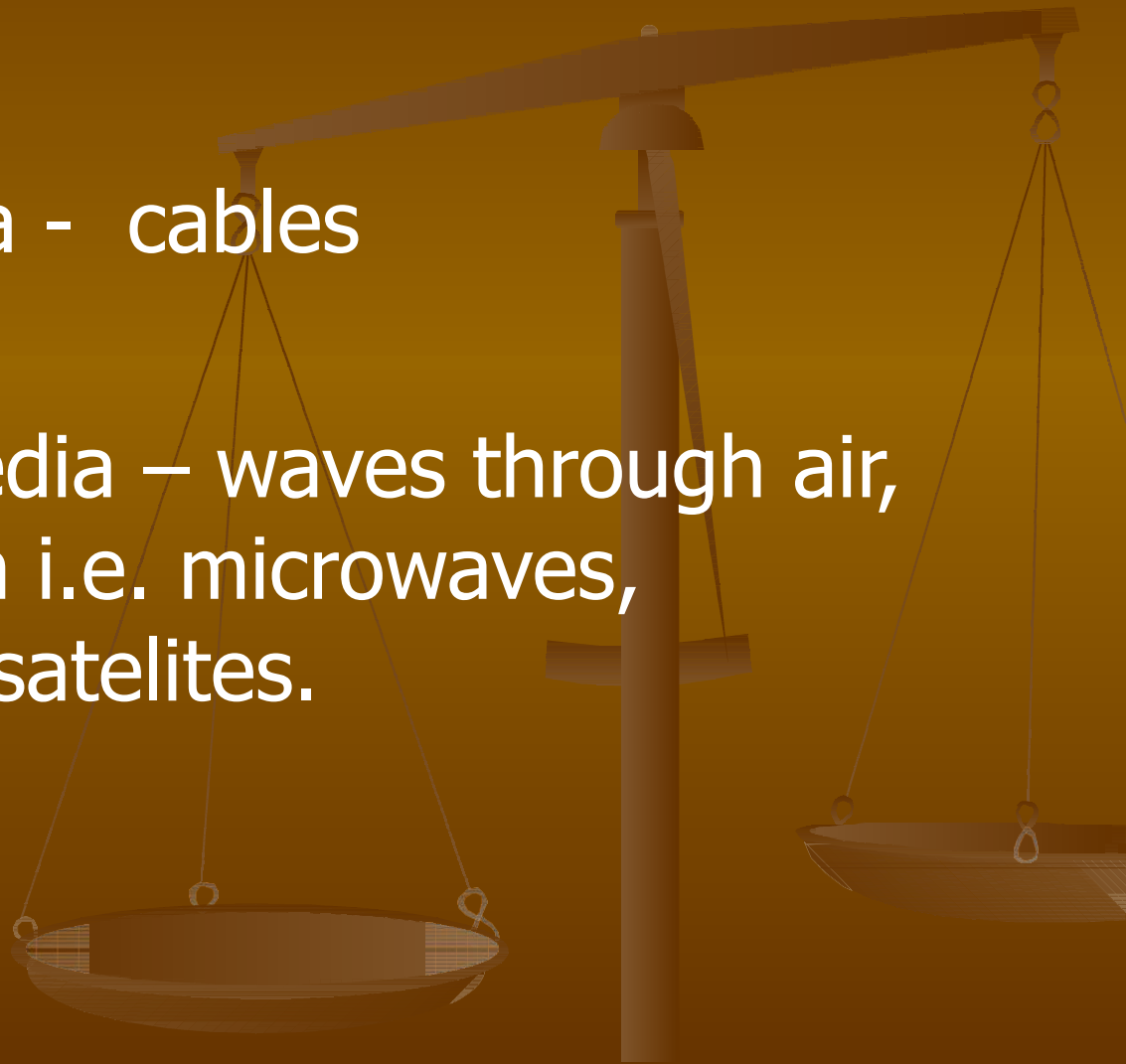
- The source comp sends the data to the switching office first which stores the data in its buffer.
- It then looks for a free link to another switching office and then sends the data to this office.
- Process is continued till the data is delivered to the destination computer.
- It is also known as store and forward technique.



Packet Switching

- There is a tight upper limit on the block size. In message switching there was no upper limit.
- A fixed size of packet is specified.
- All the packets are stored in main memory in switching office. In message switching packets are stored on disk.
- This increases the performance as access time is reduced.

Transmission media or communication Channel



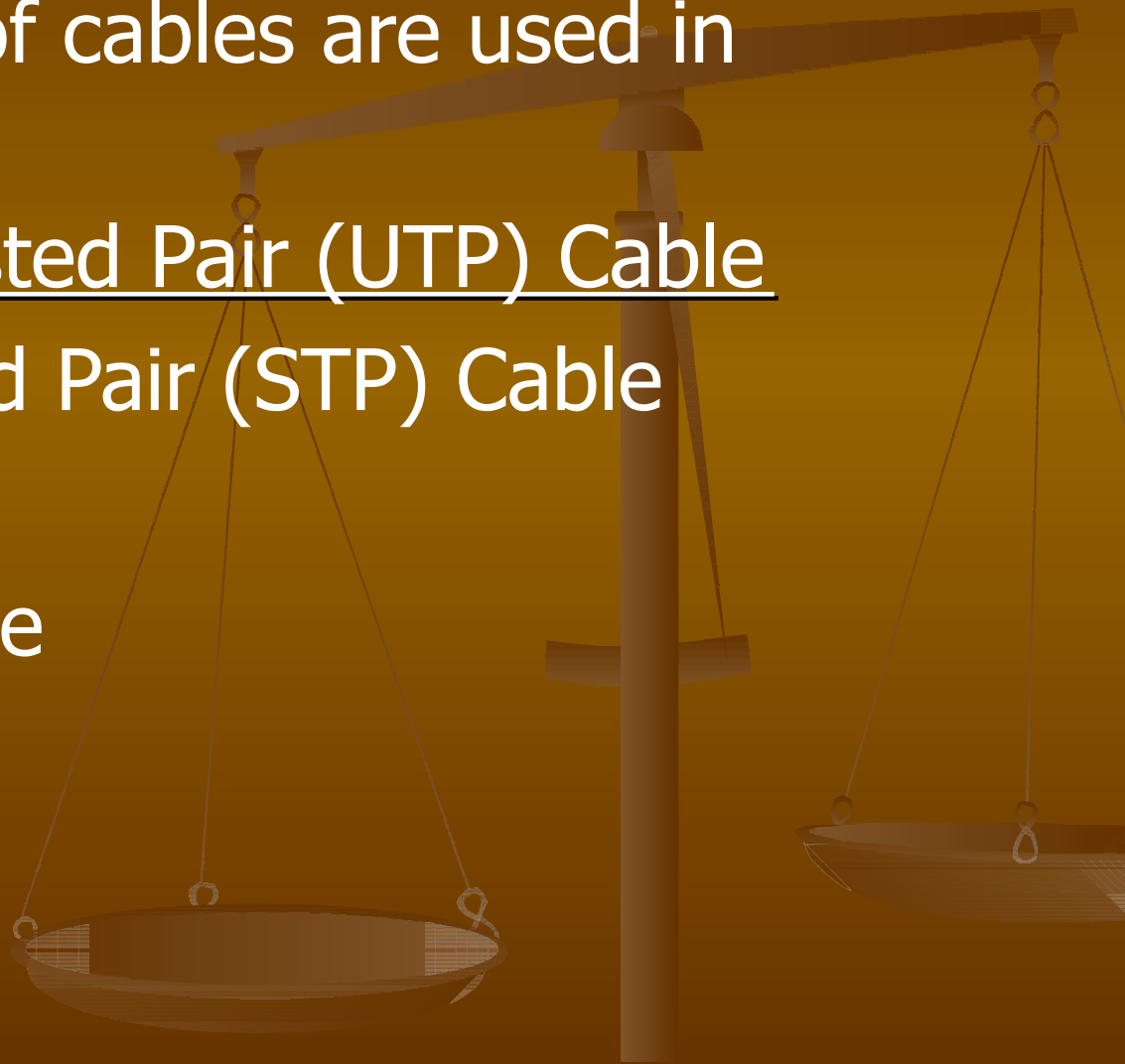
(1) Guided Media - cables

(3) Unguided media – waves through air, water or vacuum i.e. microwaves, radiowaves and satelites.

Cables

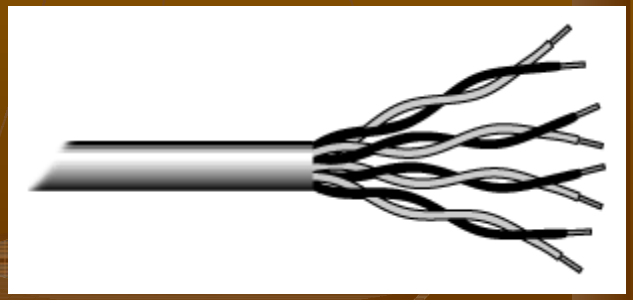
Following types of cables are used in networks

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Wireless LANs



Unshielded Twisted Pair (UTP) Cable

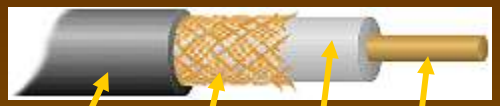
Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks .



Shielded Twisted Pair (STP) Cable

- A disadvantage of UTP is that it may be susceptible to radio and ~~elec~~trical frequency interference.
- Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky.
- Shielded twisted pair is often u~~sed~~ on networks using Token Ring topology.

Coaxial Cable

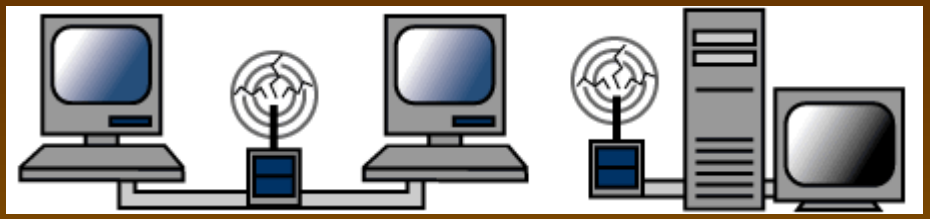


- Coaxial cabling has a single copper conductor at its center.
- A plastic layer provides insulation between the center conductor and a braided metal shield .
- The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.
- Outer shield provides the ground.

Optical Fibers

- Fiber optic cabling consists of ~~a~~ center glass core surrounded by several layers of protective materials.
- It transmits light rather than electronic signals eliminating the problem of electrical interference.
- This makes it ideal for certain ~~environments~~ that contain large amount of electrical interference.
- It has also made it the standard ~~for~~ connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Wireless LANs



- Not all networks are connected with cabling; some networks are wireless.

- Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs.

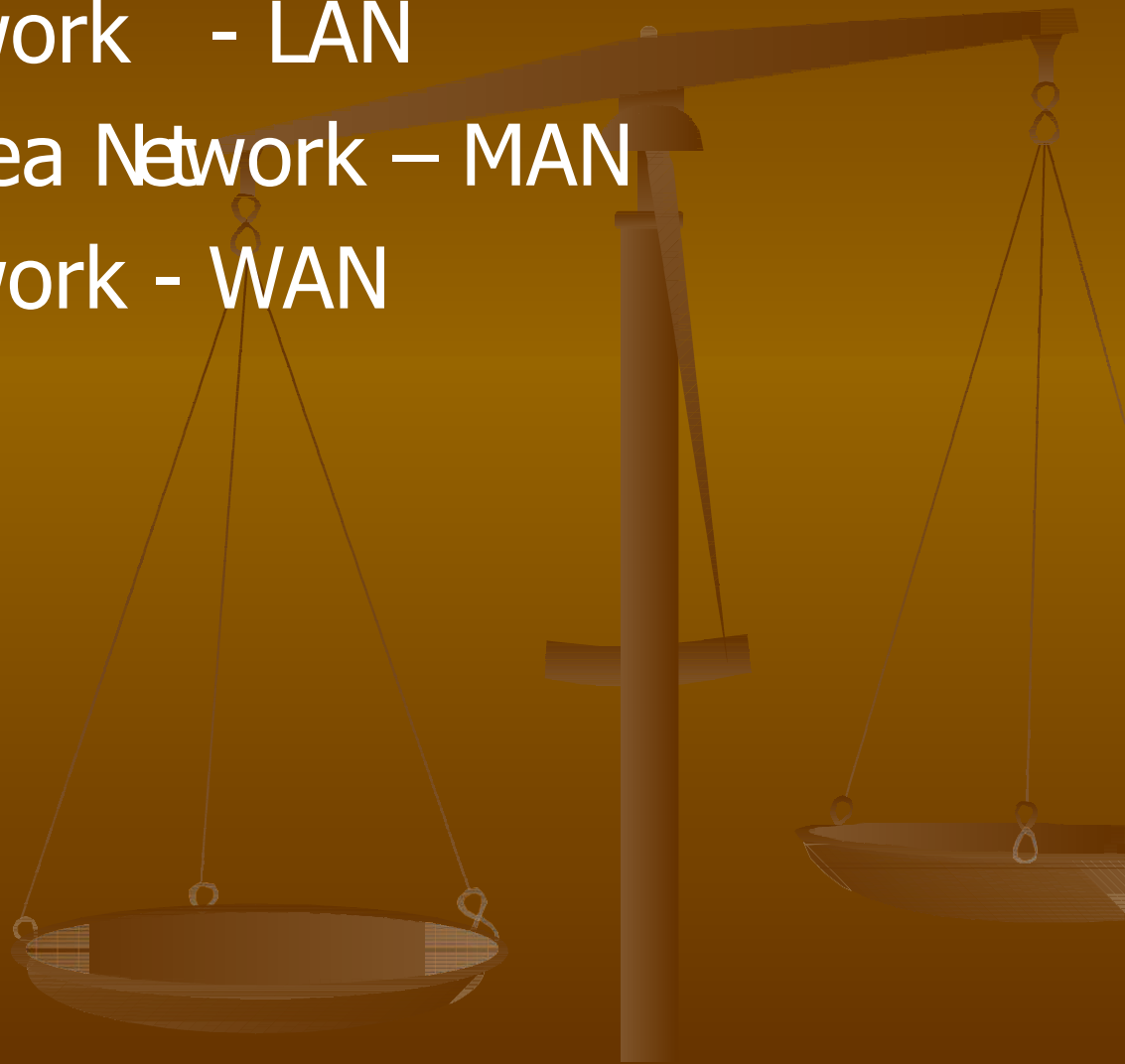
- Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data.

Wireless LAN contd.

- For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.
- Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN.
- Wireless networks are also beneficial in older
- buildings where it may be difficult or impossible to install cables.

Types of Networks

- Local Area Network - LAN
- Metropolitan Area Network – MAN
- Wide Area Network - WAN

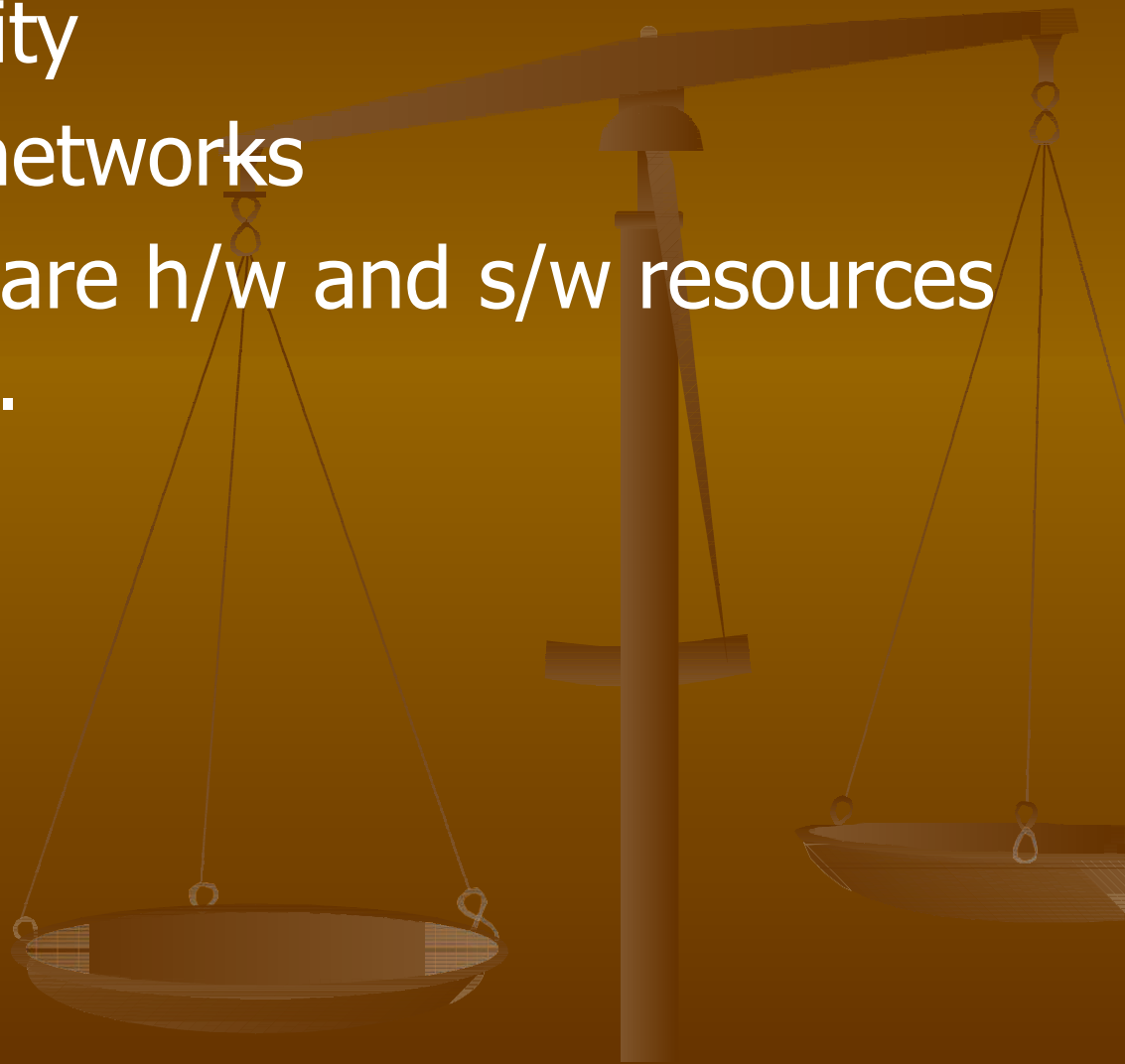


Local Area Network

- A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a writing lab, school, or building. Rarely are LAN computers more than a mile apart.
- In a typical LAN configuration, one computer is designated as the file server. It stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network.
- Computers connected to the file server are called workstations.
- On most LANs, cables are used to connect the network interface cards in each computer.

MAN

- Spread over a city
- E.g. Cable T.V. networks
- Purpose is to share h/w and s/w resources among its users.



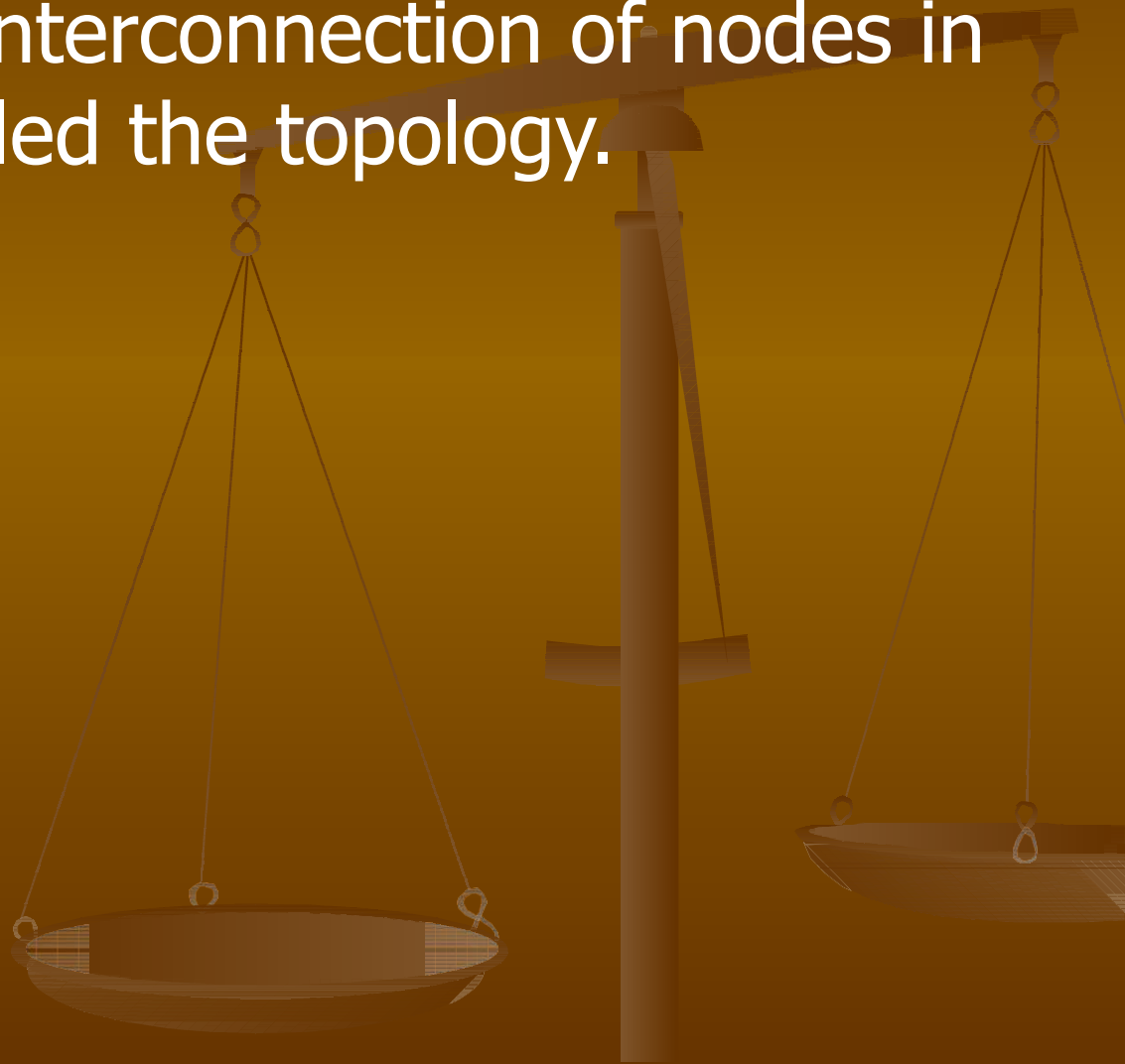
WAN

- Wide Area Networks (WANs) connect larger geographic areas, ~~su~~ch as India, the United States, or the world.
- Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of network.
- Connected thru public networks such as telephone lines , leased lines ~~or sat~~ellites.
- Largest WAN is Internet.

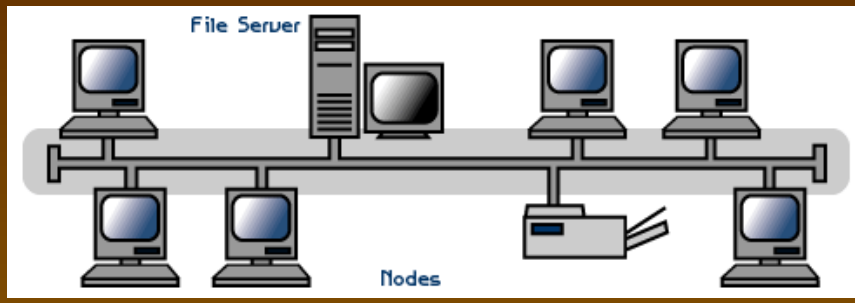
LAN	WAN
(1) Diameter of not more than few km	Span entire countries
(2) Operate at data transfer rate of several MBPS (1 to 10 MBPS)	<= 1 MBPS
(3) Complete ownership by a single organization	Owned by multiple organizations
(4) Very low error rates	Comparative~~ly h~~igher error rates

Topologies

- The pattern of interconnection of nodes in a network is called the topology.

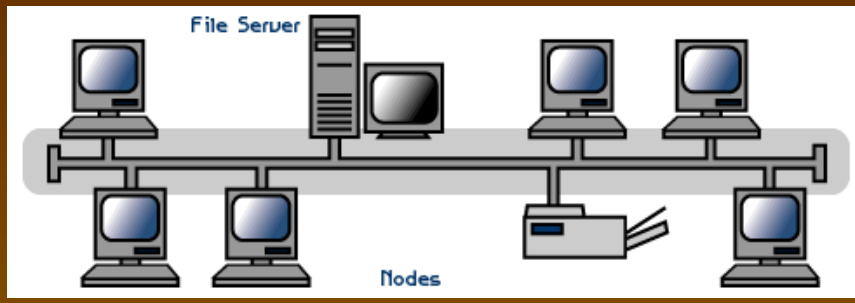


Bus topology



- A linear bus topology consists of a main run of cable with a terminator at each end .
- All nodes (file server, workstations, and peripherals) are connected to the linear cable.

Bus topology



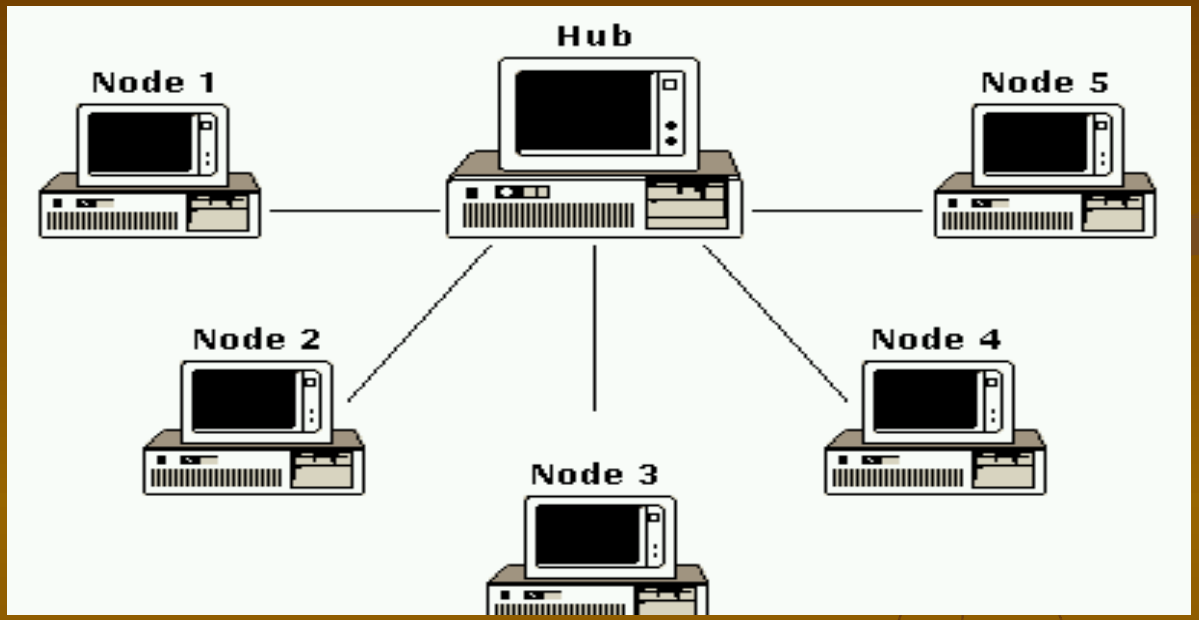
Advantages of a Linear Bus Topology

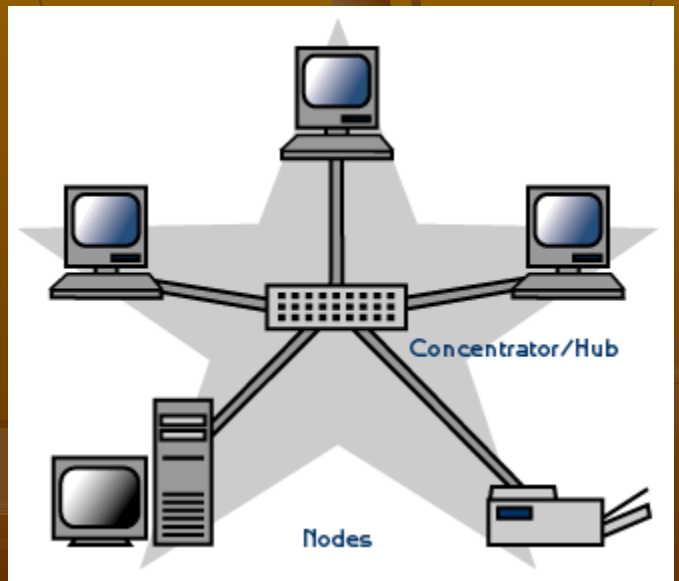
- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

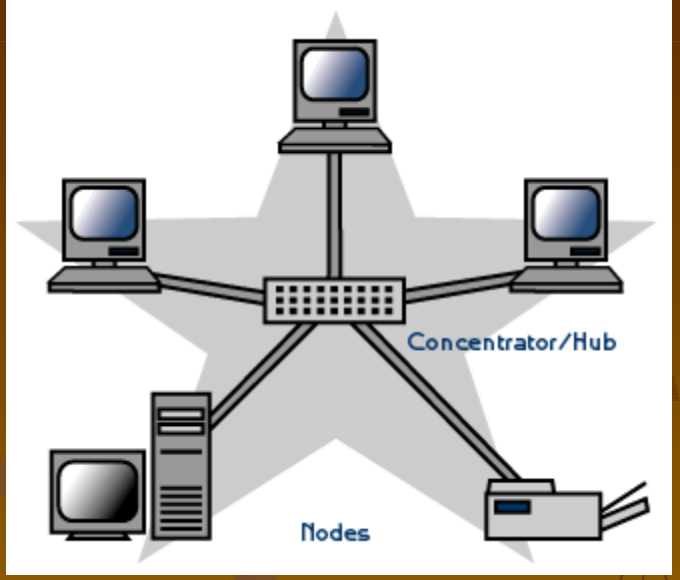
- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Nodes must be intelligent .Each node is directly connected to the central bus.

Star Topology





Star topology



A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub or concentrator

Data on a star network passes through the hub or concentrator before continuing to its destination.

The hub or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow.

Star topology

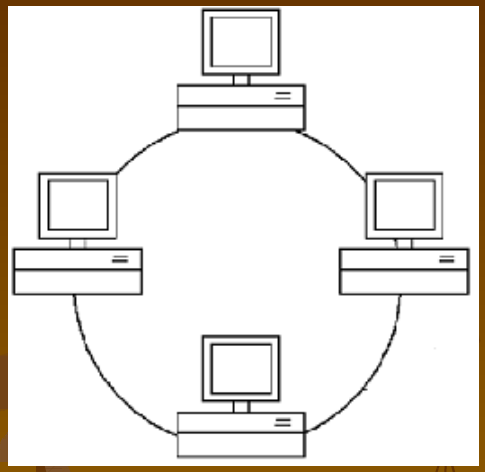
Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the concentrators.

Ring Topology



- Ring Network, a local area network formed in a ring (closed loop) topology that uses token passing as a means of regulating traffic on the line.

•On a token ring network, a token governing the right to transmit is passed from one station to the next in a physical circle.

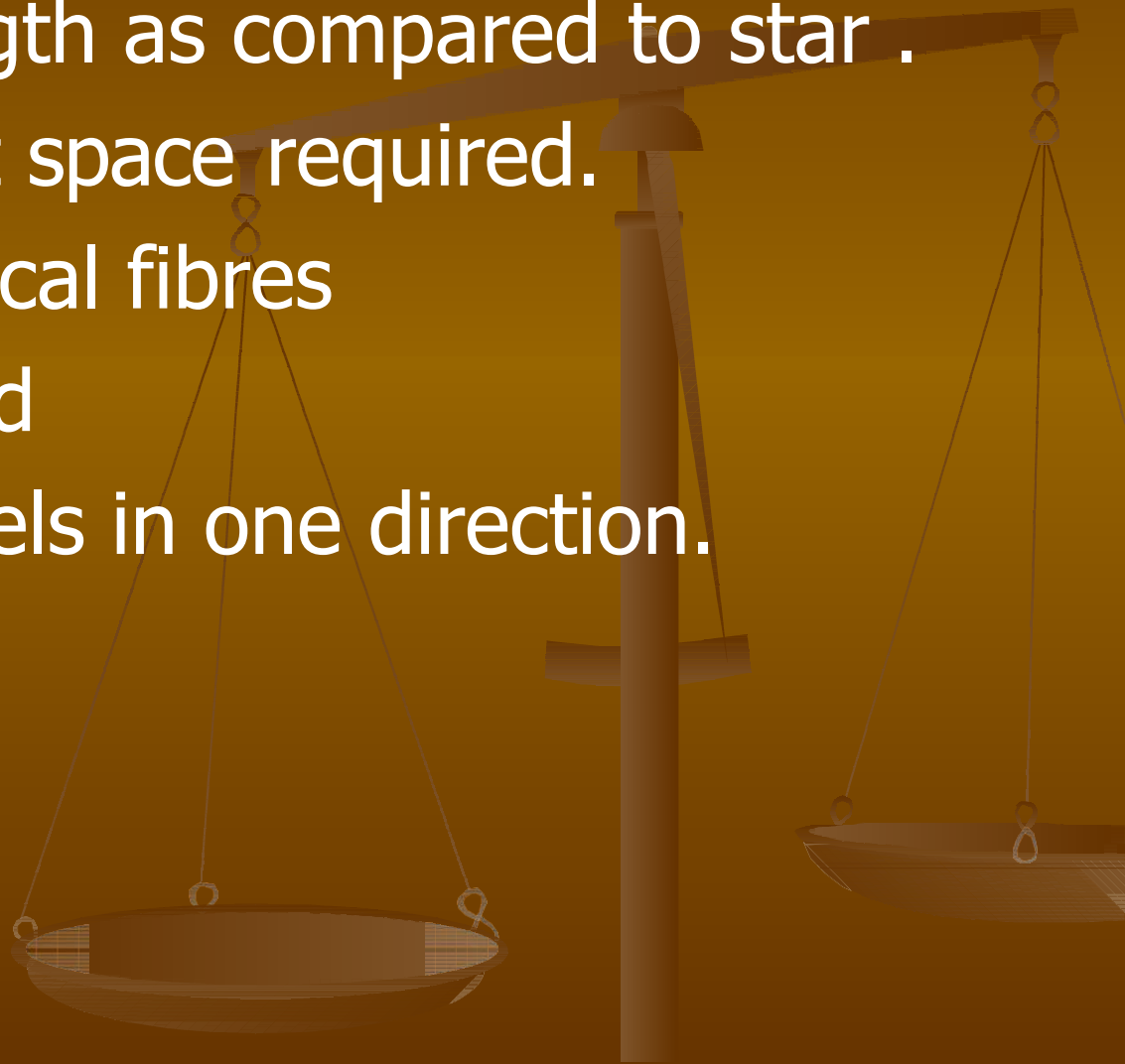
•If a station has information to transmit, it "seizes" the token, marks it as being in use, and inserts the information

•. The "busy" token, plus message, is then passed around the circle, copied when it arrives at its destination, and eventually returned to the sender.

•The sender removes the attached message and then passes the freed token to the next station in line.

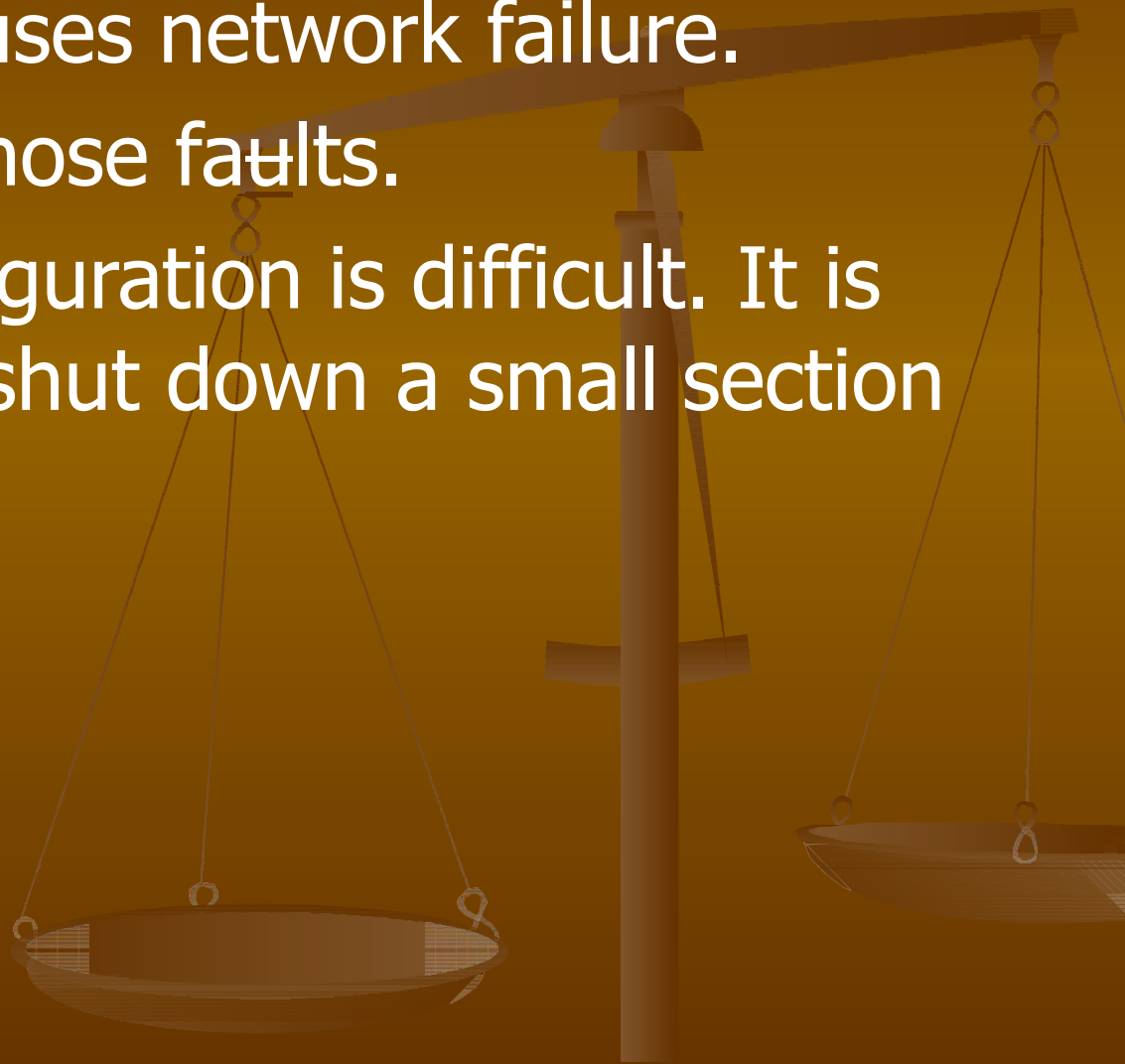
Advantages of Ring Topology

- Short Cable length as compared to star .
- No wiring closet space required.
- Suitable for optical fibres
  - high speed
  - traffic travels in one direction.



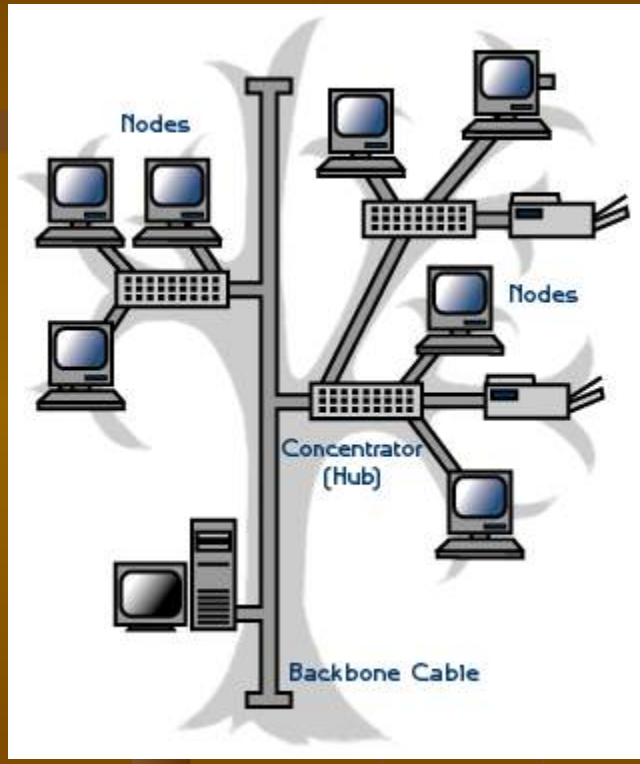
Disadvantages of Ring Topology

- Node failure causes network failure.
- Difficult to diagnose faults.
- Network reconfiguration is difficult. It is not possible to shut down a small section of the ring.



Tree Topology

- A tree topology combines characteristics of linear bus an d star topologies.
- It consists of groups of star-configured workstations connected to a linear bus backbone cable.
- Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs



Tree Topology

Advantages of a Tree Topology

- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Considerations When Choosing a Topology:

- **Money.** A linear bus network may be the least expensive way to install a network; you do not have to purchase concentrators.
- **Length of cable needed**. The linear bus network uses shorter lengths of cable.
- **Future growth**. With a star topology, expanding a network is easily done by adding another concentrator.
- **Cable type**. The most common cable in schools is unshielded twisted pair, which is most often used with star topologies.

Network Device

Modem

- Modems are most frequently used to enable computers to communicate with each other across telephone lines.
- Stands for Modulation – demodulation.
- Converts digital signal to analog signal and vice

RJ 45 Connector

- Register Jack 45 is an 8 wire connector which is commonly used to connect computers on LAN.
- Looks like RJ-11 telephone connector

Ethernet Card

- Ethernet, is a LAN architecture developed by the Xerox corporation in 1976, originally for linking minicomputers at the Palo Alto Research Center.
- Computers that uses Ethernet architecture have to install ethernet card .
- Now computers are coming fitted with ethernet card.

Hub

- A common connection point for devices in a network.
- Hubs are commonly used to connect segments of a LAN.
- A hub contains multiple ports.
- A ***passive hub*** serves simply as a conduit for the data, enabling it to go from one device (or segment) to another.
- Active hub electrically amplify the signal as ~~it mo~~ves from one connected device to another.
- Support 8, 12 or 24 RJ-45 ports
- Used in star or ring topo~~logy.~~

Switch

- A switch (**switch**ing hub) in the context of networking refers to a device which filters and forwards data packets across a network.

  Unlike a standard hub which simply replicates what it receives on one port onto all the other ports, a switching hub keeps a record of the MAC addresses of the devices attached to it.

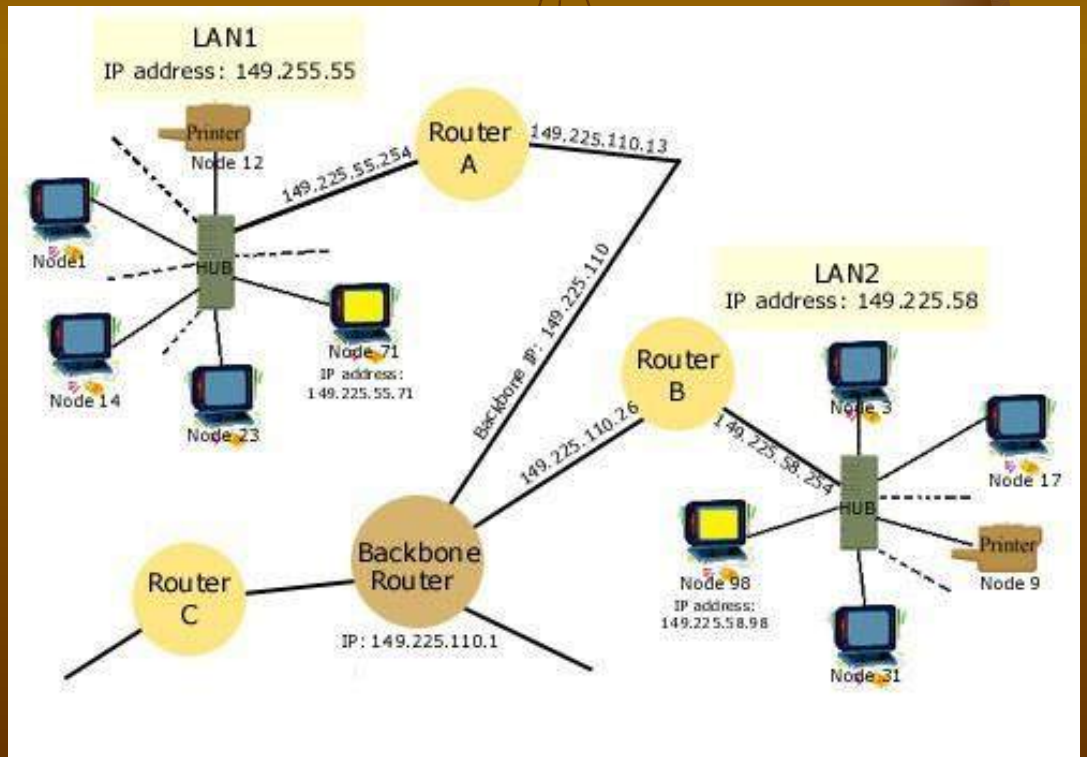
  When the switch receives a data packet, it forwards the packet directly to the recipient device by looking up the MAC address.

  A network switch can utilise the full throughput potential of a networks connection for each device making it a natural choice over a standard hub.

  In other words, say for instance you had a network of 5 PCs and a server all connected with 10Mbps UTP cable, with a hub the throughput (10Mbps) would be shared between each device, with a switch each device could utilise the full 10Mbps connection.

Repeater

- A **repeater** is an electronic device that receives a weak or low-level signal and retransmits it at a higher level or higher power, so that the signal can cover longer distances without degradation.



Bridge – connects two LANS having the same protocol – (e.g. Ethernet or Token ring)

LAN A

Bridge

Data not destined for other network is prevented from passing over the bridge.

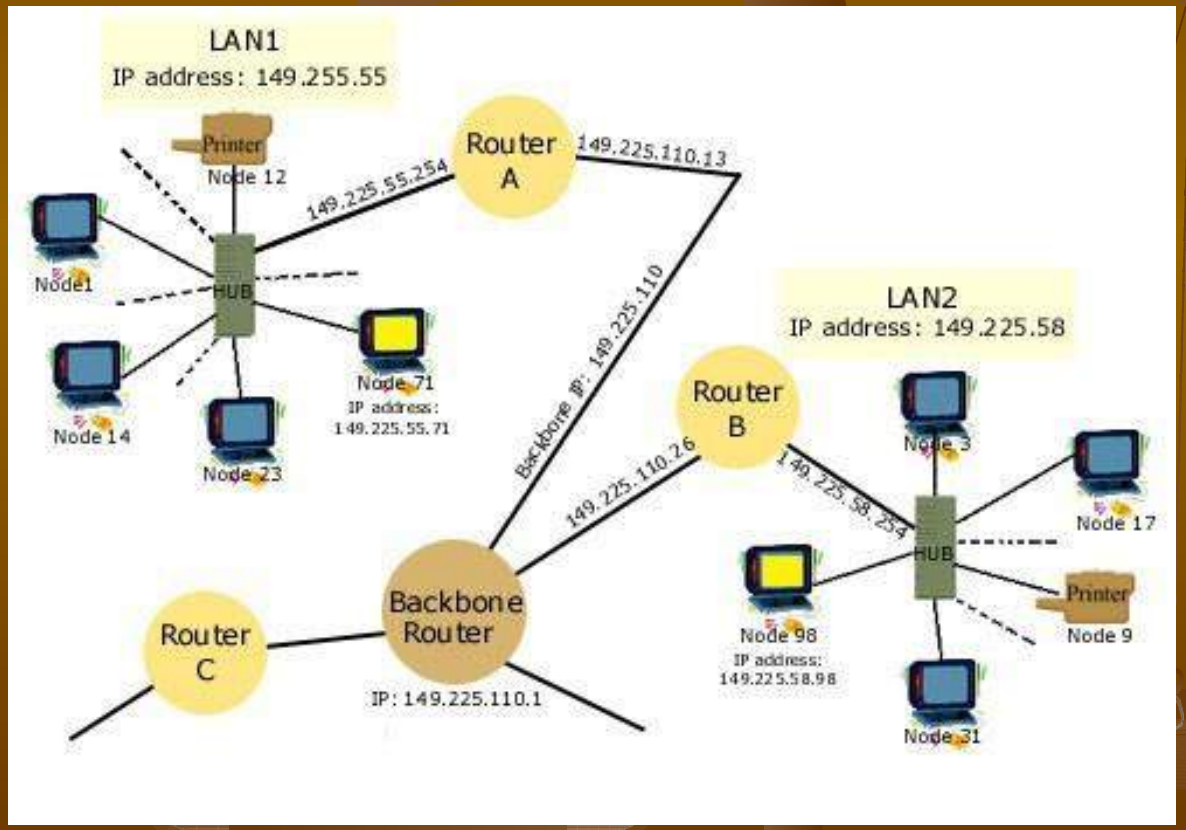
LAN B

Bridge

- In telecommunication networks, a bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or Token Ring).
- You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street.
- A bridge examines each message on a LAN, "passing" those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

Router

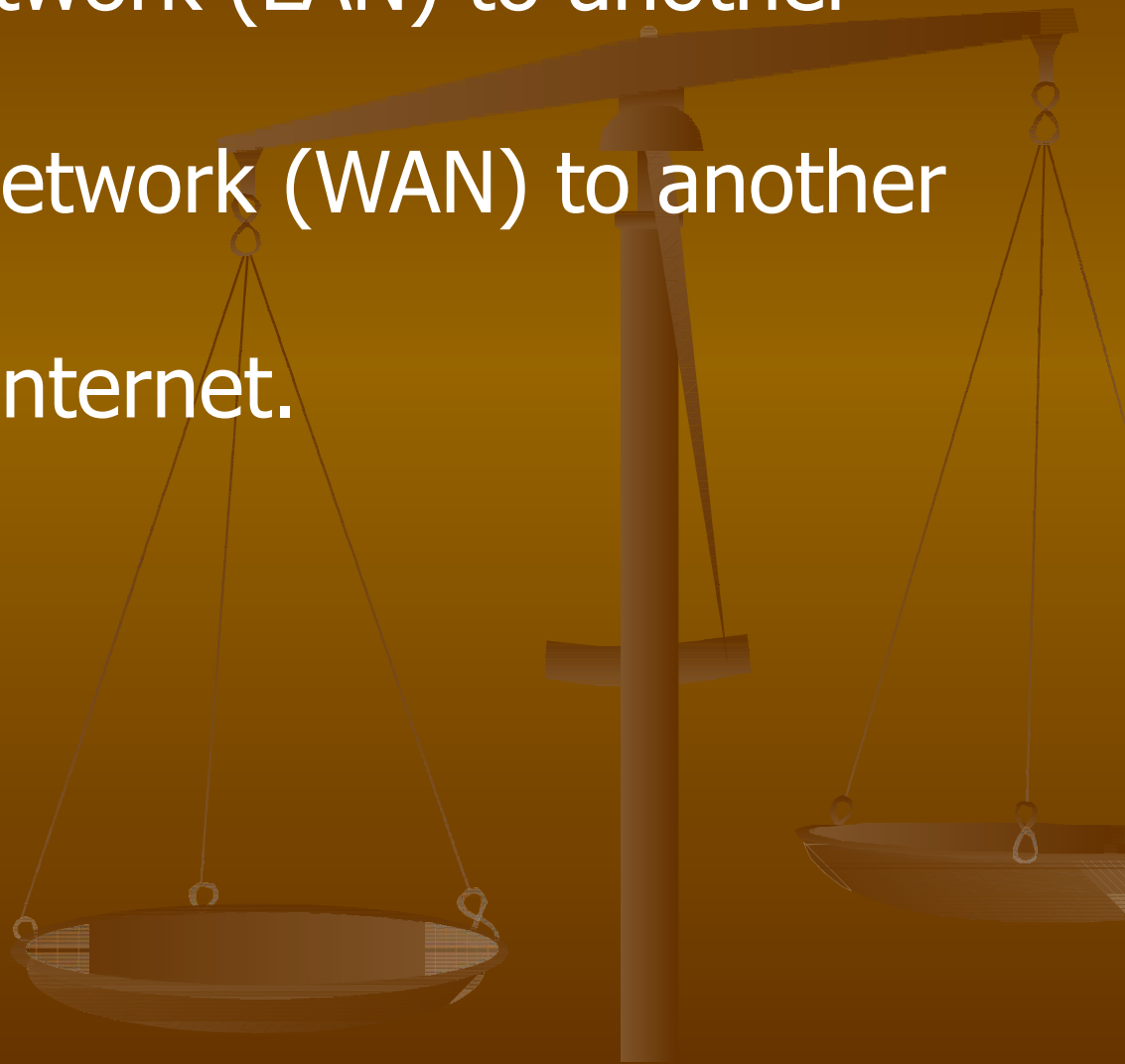
- Router is a specialized network device used to interconnect different types of computer network that uses different protocols e.g. Ethernet to a mainframe.



Uses of Router

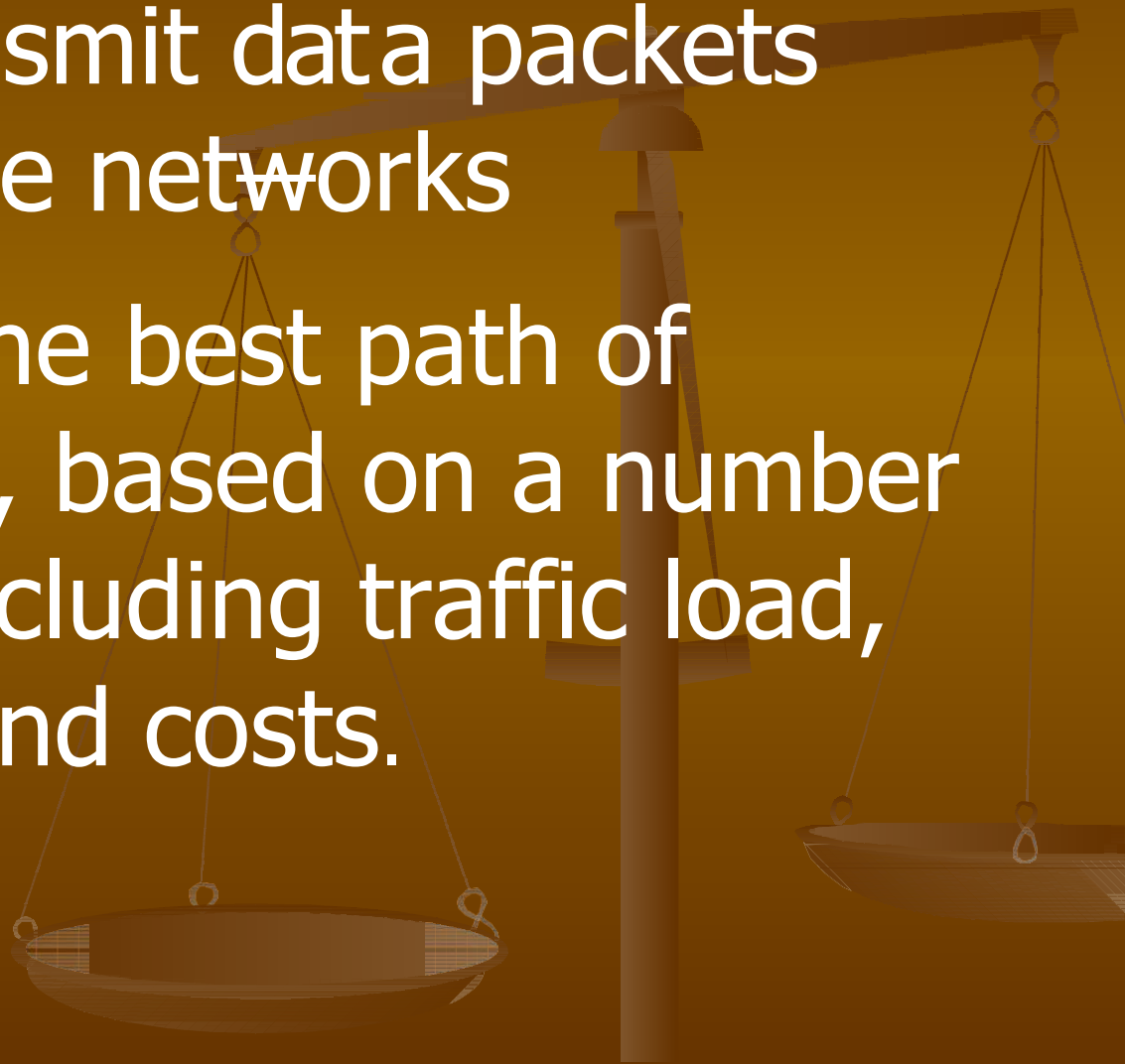
A router can be used to connect

- a Local Area Network (LAN) to another LAN,
- a Wide Area Network (WAN) to another WAN,
  - a LAN to the Internet.



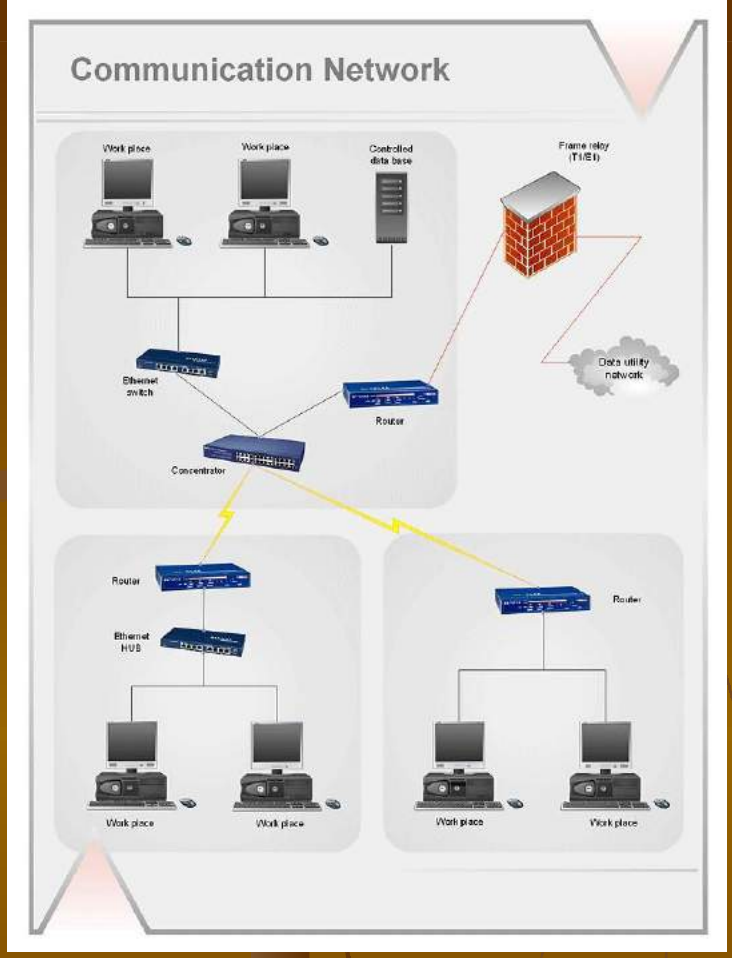
Working of Router

- Routers transmit data packets through these networks
- determine the best path of transmission, based on a number of factors, including traffic load, line speed, and costs.



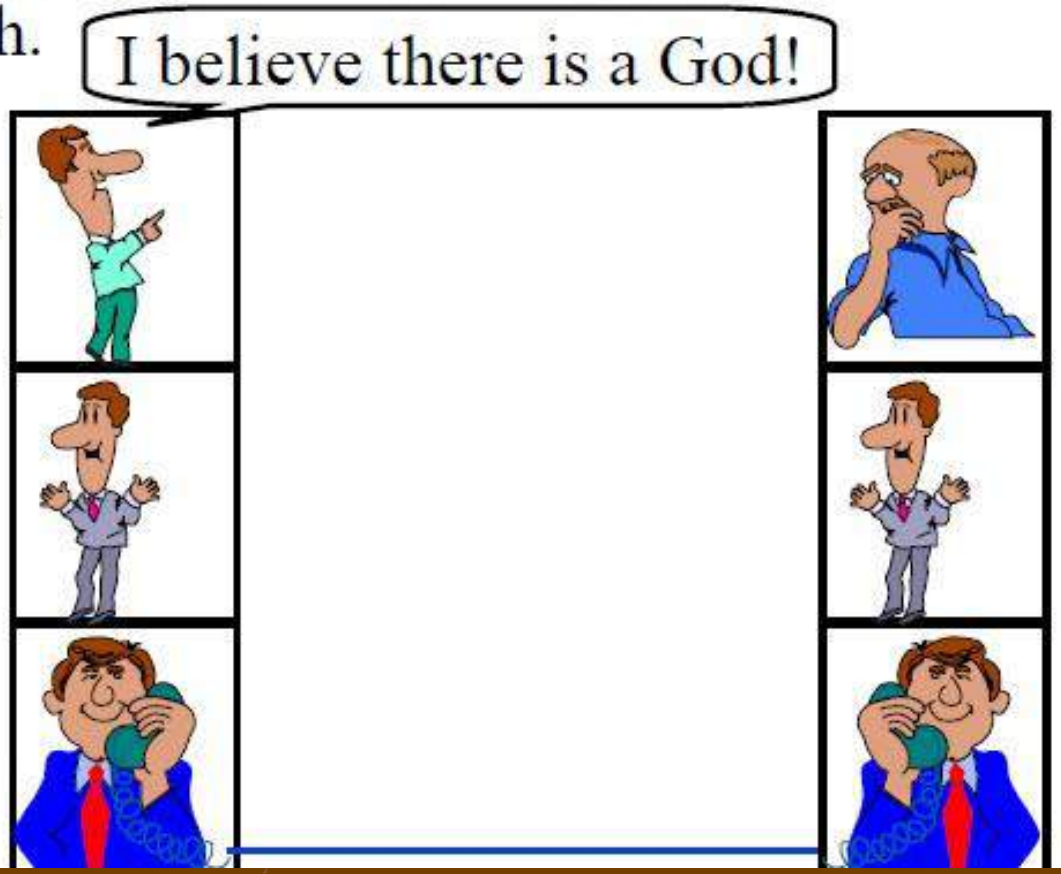
Gateway

- Gateway is a device that connects dissimilar networks.
- Establishes intelligent connection between a local network and external networks with completely different structures.
- Gateway is the ISP that connects the user to the internet.



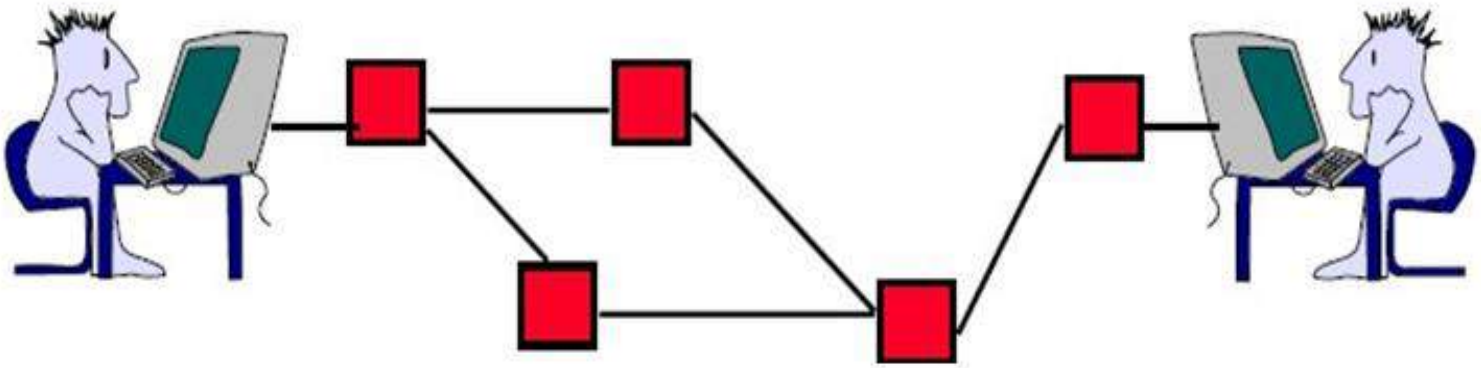
Protocol Layers

- Problem: Philosophers in different countries speak different languages. The Telex system works only with English.

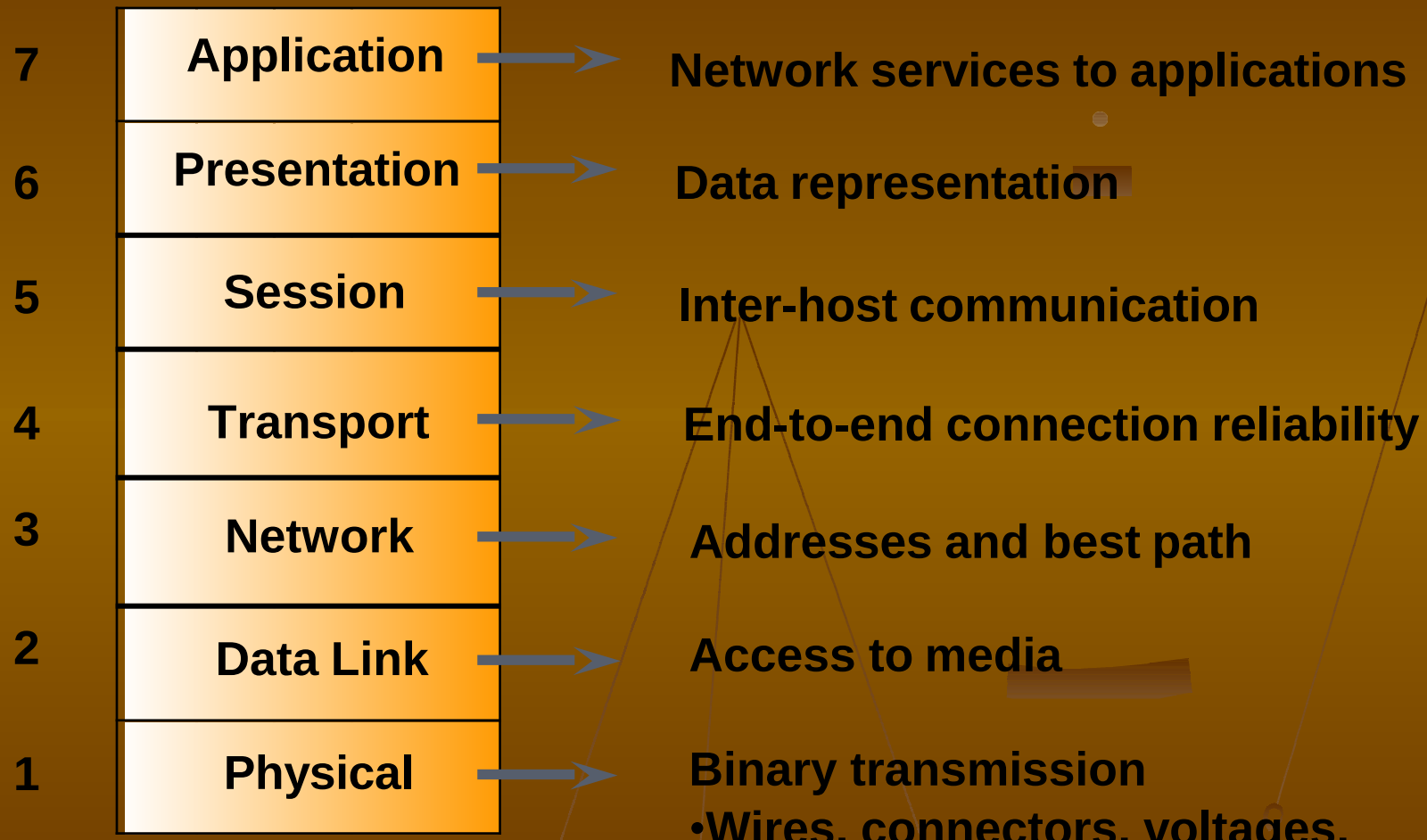


ISO/OSI Reference Model

Application	File transfer, Email, Remote Login
Presentation	ASCII Text, Sound
Session	Establish/manage connection
Transport	End-to-end communication: TCP
Network	Routing, Addressing: IP
Datalink	Two party communication: Ethernet
Physical	How to transmit signal: Coding



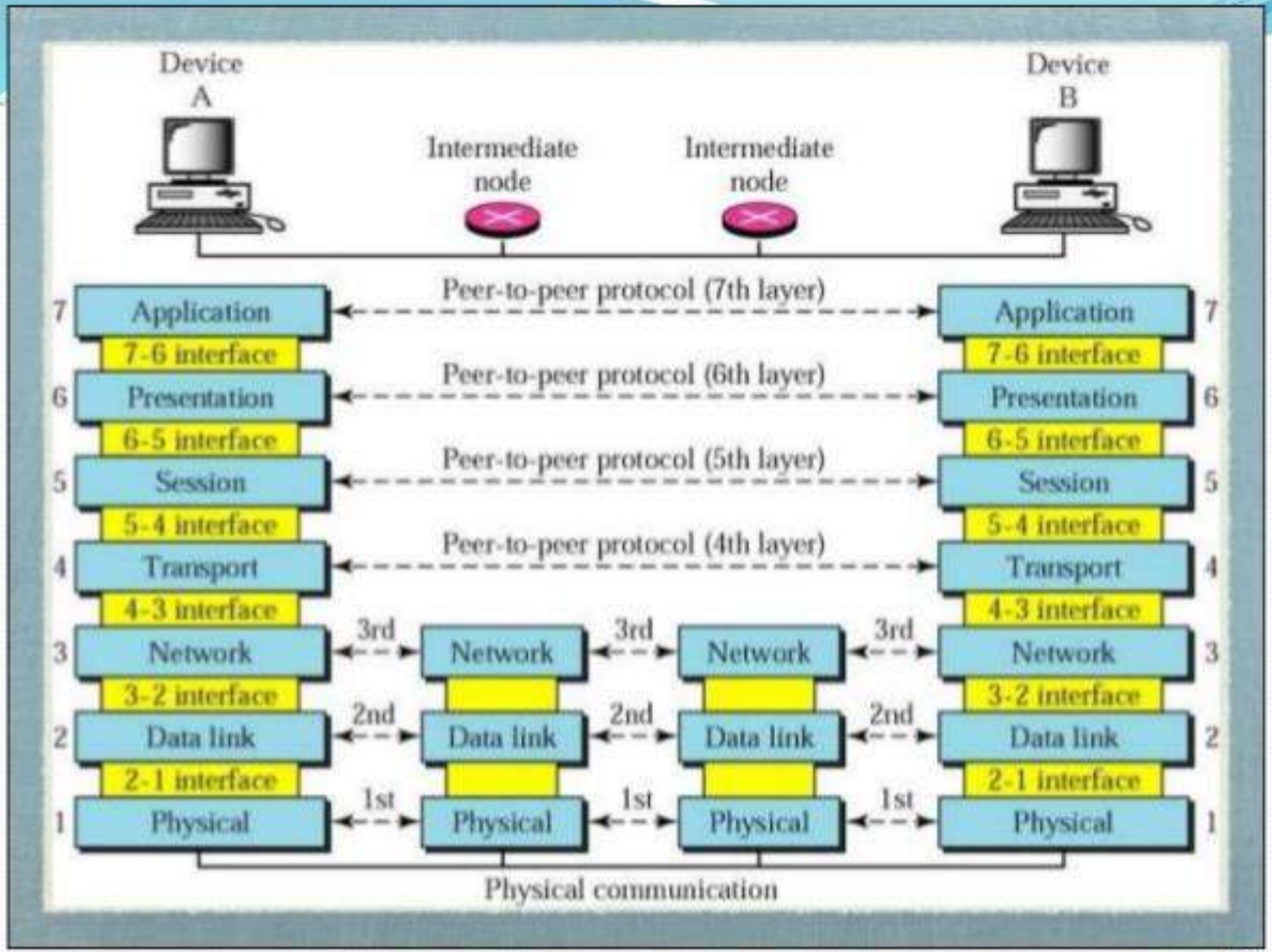
Layer Functions



OSI Reference model

- The Open Systems Interconnection Reference Model, the OSI model was developed by the ISO (International Standards Organization) and released in 1984.

- The OSI model, as it is called for short, defines the rules, mechanisms, formats, and protocols used to guide how data flows from one device to another.

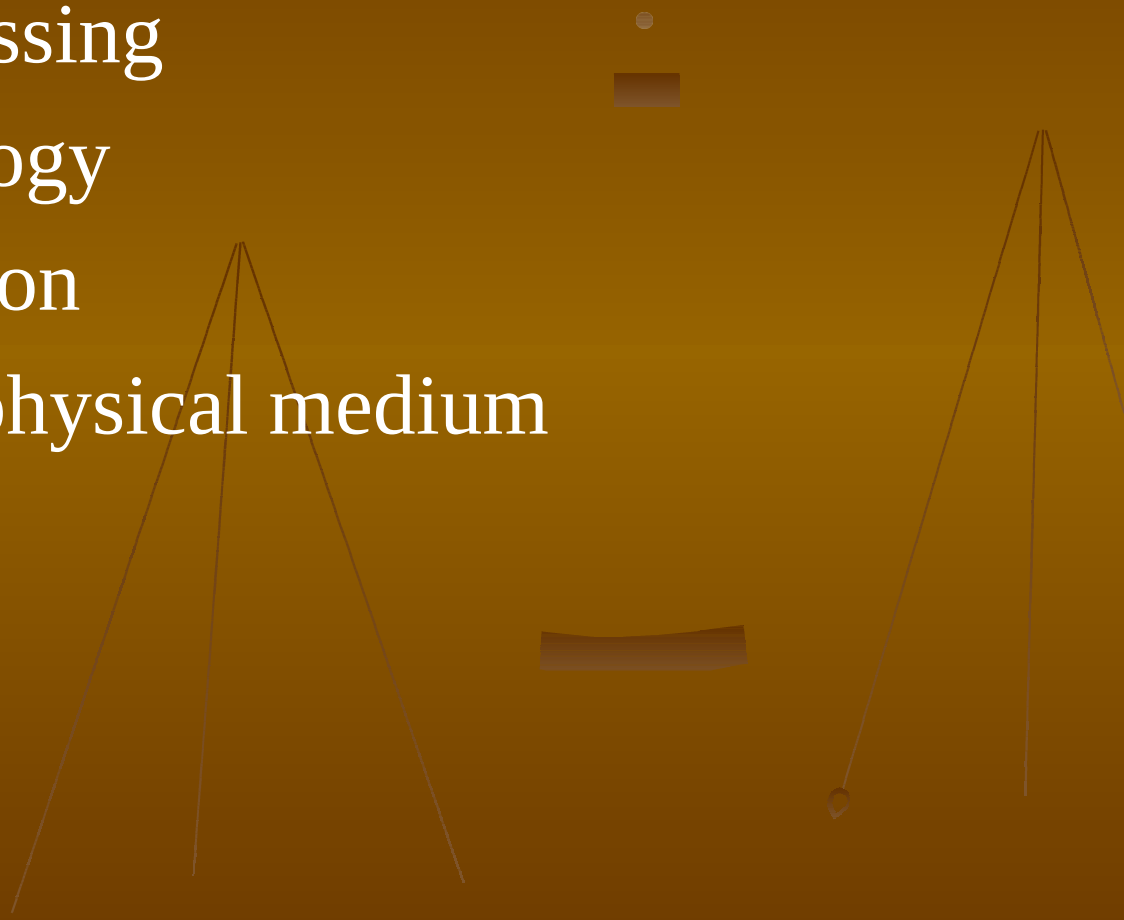

Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7
Application
7-6 interface
6
Presentation
6-5 interface
5
Session
5-4 interface
4
Transport
4-3 interface
3
Network
3-2 interface
2
Data link
2-1 interface
1
Physical
3rd
2nd
1st
Physical communication

Physical Layers

- The Physical layer of the OSI model defines the electrical and mechanical specifications used in networking, including transmission distances, the various types of media available, and electrical issues.

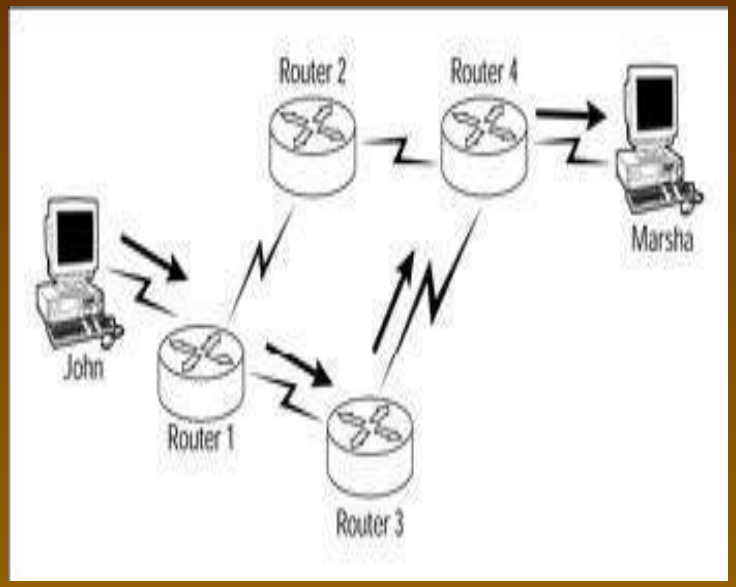
The Data Link Layer

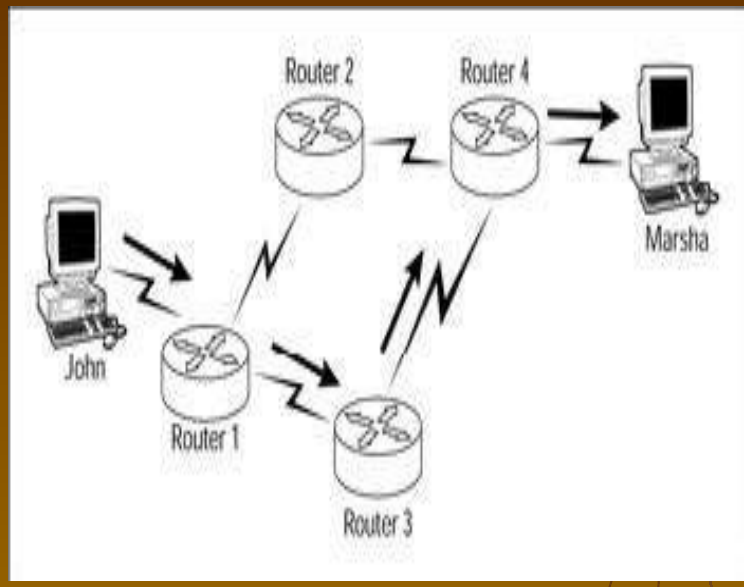
- Physical addressing
- Network topology
- Error notification
- Access to the physical medium
- Flow control



The Network Layer

- Message addressing
- Path determination between source and destination nodes on different networks
- Routing messages between networks
- Controlling congestion on the subnet
- Translating logical addresses into physical addresses





- When the message (which moves down through the seven OSI layers on Johns computer before its sent out on the local network in binary form) arrives at Router 1, it moves up from the Physical layer to the Data Link layer to the Network layer. At Layer 3, its determined that the message is not on a network attached to Router 1 and the message is sent down $_{07}t_{/1}h_{1/}r_{17}$ough the Data Link layer to the Physical layer and on to Router 3.

The Transport Layer

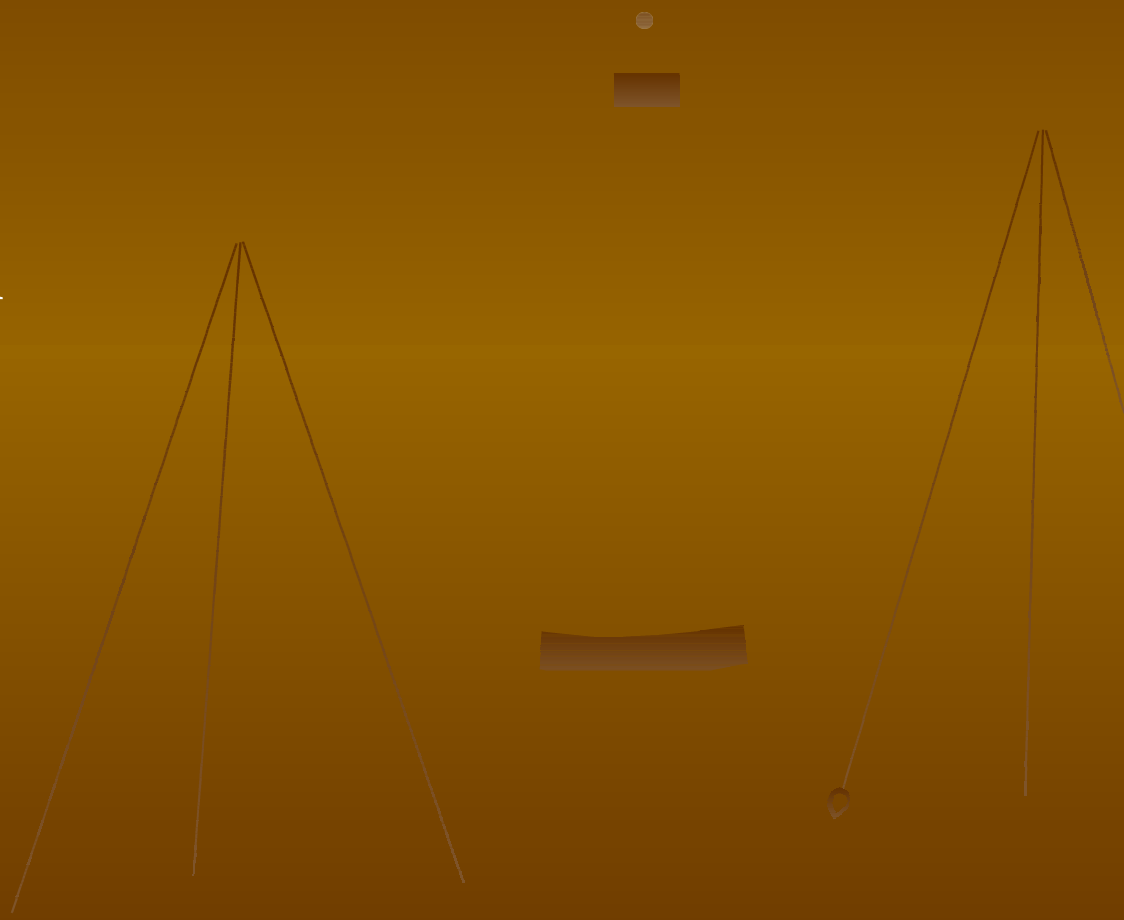
- Segment and assemble upper−layer applications
- Transport segments from one host to another host
- Establish and manage end−to−end operations
- Error recovery

The Session Layer

- A *session* is a series of related connection−oriented transmissions between network nodes.
- Session Layer, establishes, manages, and terminates sessions between applications.
- The *session* layer provides a name space that is used to tie together the potentially different transport streams that are part of a single application.
- Session layer is its role in deciding whether a communications session uses a simplex, half−duplex, or full−duplex transmission mode.

Presentation Layers

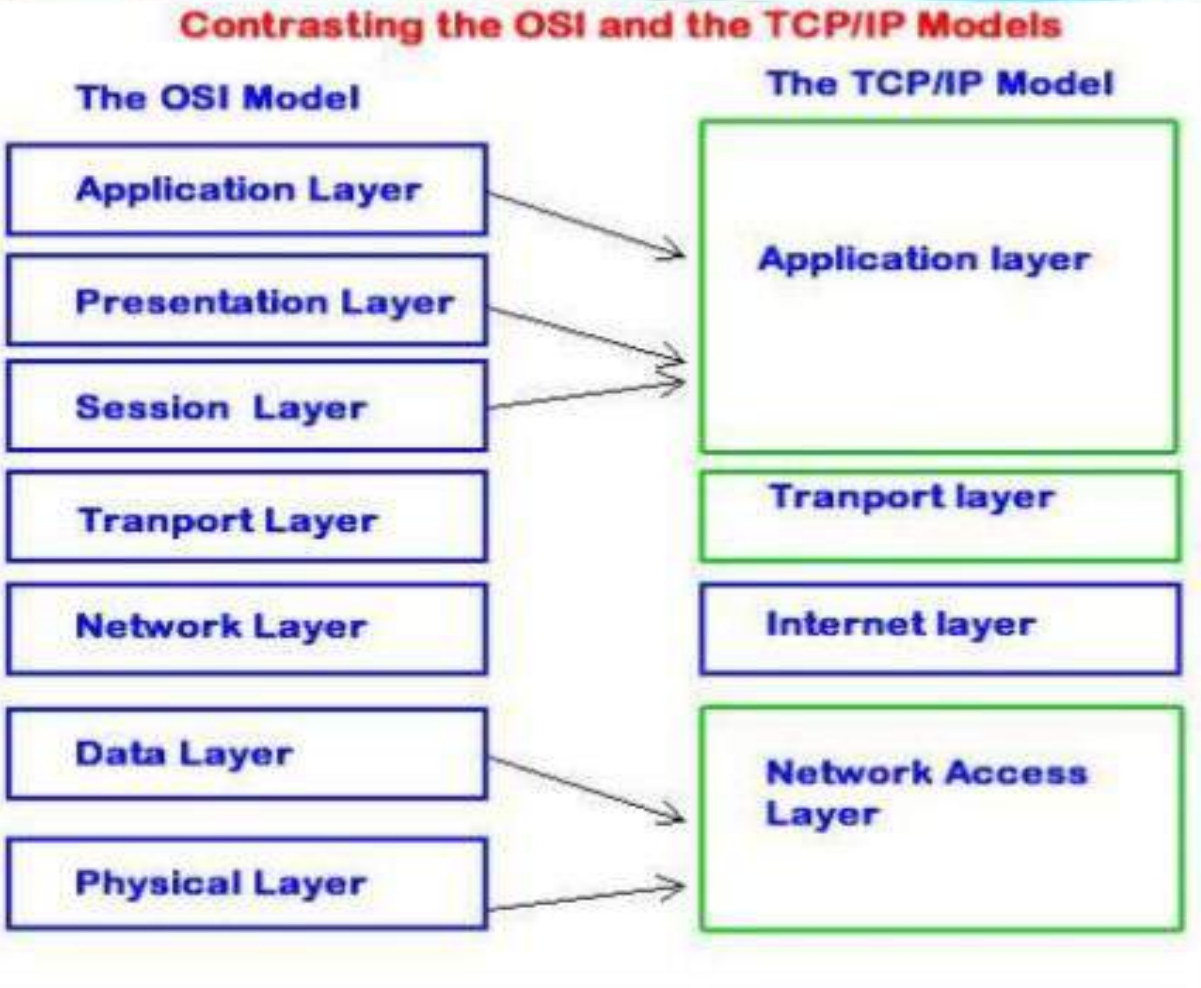
- Data encryption
- Data compression
- Data formatting
- Data conversion



The Application Layer

- Application layer defines the communication services used by the users applications to transmit data over the network.
- FTP (File Transfer Protocol)
- E–mail clients
- Web browsers
- Telnet
- SNMP (Simple Network Management Protocol)
- BBS (bulletin board system) servers
- EDI(Electronic Data Interchange) and other transaction services

OSI vs TCP/IP


Contrasting the OSI and the TCP/IP Models
The OSI Model
The TCP/IP Model
Application Layer
Presentation Layer
Session Layer
Tranport Layer
Network Layer
Data Layer
Physical Layer
Application layer
Tranport layer
Internet layer
Network Access Layer

OSI vs TCP Reference Models

- OSI introduced concept of services, interface, protocols. These were force-fitted to TCP later
  - ⇒ It is not easy to replace protocols in TCP.
- In OSI, reference model was done before protocols. In TCP, protocols were done before the model
- OSI: Standardize first, build later TCP: Build first, standardize later
- OSI took too long to standardize.

TCP/IP was already in wide use by the time.

- OSI became too complex.
- TCP/IP is not general. Ad hoc.

Thank you