INTRODUCTION TO COMPUTER NETWORKS

COMPUTER NETWORK

- Network is a set of computers and devices connected together for the purpose of sharing resources.
- Is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information
- The computer that provides resources to other computers on a network is known as server and the individual computer which access the shared network resources are known as nodes

Computer Network

- Networks may be classified according to:
  - (i) Medium used to transport the data
  - (ii) Communication protocol used
  - (iii) Scale
  - (iv) Topology
  - (v) Organizational scope, etc

- Computer interconnection could be through copper wire, fiber optics, microwares, satellites, etc.(communication channels)
- Network interconnections allow the use of different technologies

Network Components, Functions, and Features

- The major components of a network are end stations, applications and a network that will support traffic between the end stations.
- Computer networks all share common devices, functions, and features,
- This includes servers, clients, transmission media, shared data, shared printers and other peripherals, hardware and software resources, network interface card (NIC), local operating system (LOS) and the network operating system (NOS).

Network Components, Functions, and Features

- **Servers**: Servers are computers that hold shared files, programs and the network operating system. Servers provide access to network resources to all the users of the network and different kinds of servers are present. Examples include file servers, print servers, mail servers, communication servers etc.
- **Clients:** Clients are computers that access and use the network and access network resources. Client computers are basically the customers (users) of the network, as they request and receive service from the servers.

Network Components, Functions, and Features

- **Shared Data**: Shared data are data that file servers provide to clients, such as data files, printer access programs, and e-mail.
- **Shared Printers and other peripherals:** these are hardware resources provided to the users of the network by servers. Resources provided include network , printers, storage, software, or any other items used by the clients on the network.
- **Network interface card:** Every computer in the network has a special expansion card called network interface card (NIS), which prepares and sends data, receives data, and controls data flow between the computer and the network. While transmitting, NIC passes frames of data on to the physical layer and on the receiver side, the NIC processes bits received from the physical layer and processes the message based on its contents.

Network Components, Functions, and Features

- **Local operating system**: A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, PC-DOS, UNIX, Macintosh, OS/2, Windows 95, 98, XP and Linux.

- **Network operating system**: the NOS is a program that runs on computers and servers that allows the computers to communicate services and share over a network. The NOS provides services to clients such as log-in features, password authentication, printer access, network administration functions and data file sharing. Examples of NOS are UNIX, LINUX, MICROSOFT WINDOWS SERVER 2008, NETVELL NETWARE, etc.

BENEFIT OF NETWORK

- File sharing:- this allows files, documents, photos etc in a particular computer to be shared among other computers in a network, it rather than having the files, documents, photos, etc in all the different computer.
- Printer:- This allow all computers in a network to share a single printer.
- Internet connection sharing:- This allow multiple friendly members or officers in an organization to access internet simultaneously without having to pay an ISP for multiple accounts. Internet connection slows down when several people share it.
- Multi-player games:- Home computer games support LAN mode which family play together.
- Home entertainment:- Home entertainment products such as digital video recorder (DVRS) and video game consoles now support either wired or wireless home networking.

Benefits of Network– cont.-

- Enables access to remote networks
- Facilitate communications
- Facilitate information dissemination
- Overall cost reduction in Hardware and software.
- Facilitate Social networks

Desirable criteria for a Network

- Performance: transit time and response time. Performance depends on number of users, transmission medium, connected hardware and software.
- Reliability: accuracy of delivery, frequency of failure, time it takes a link to recover from a failure and network robustness.
- Security: unauthorised access, protecting data from damage and policies and procedures for recovery data losees

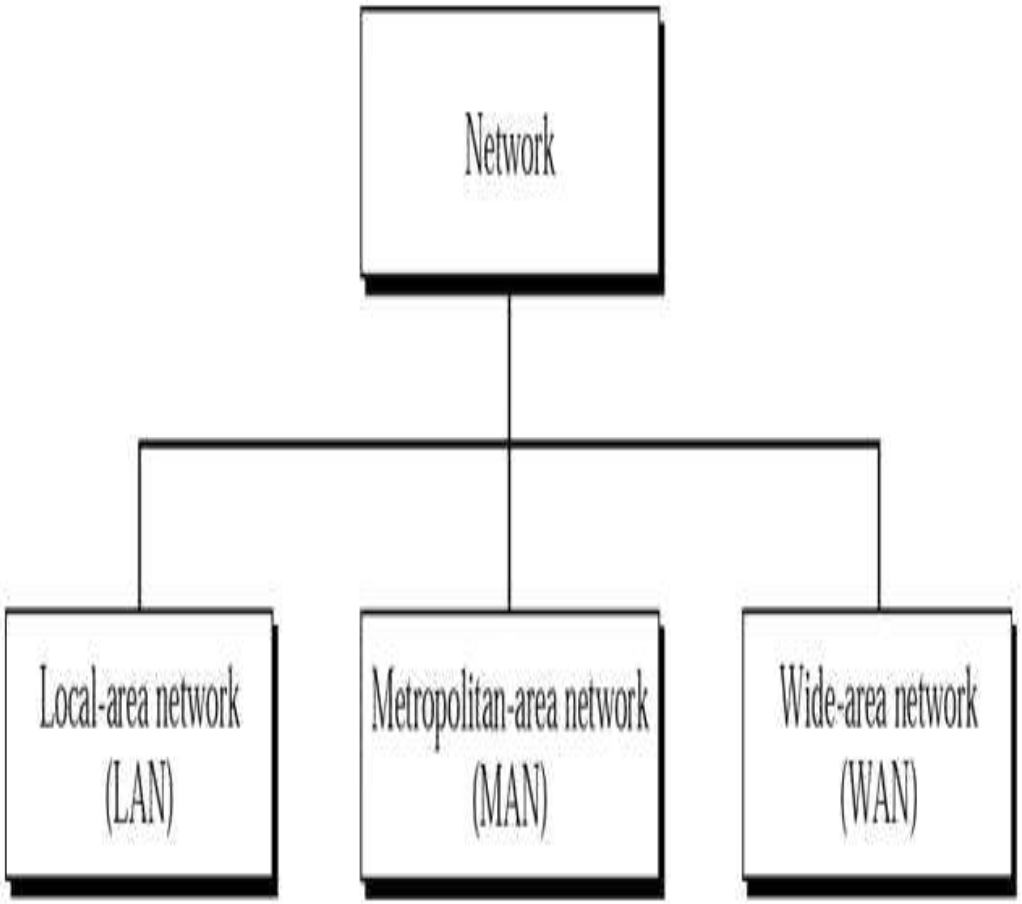
Network Models

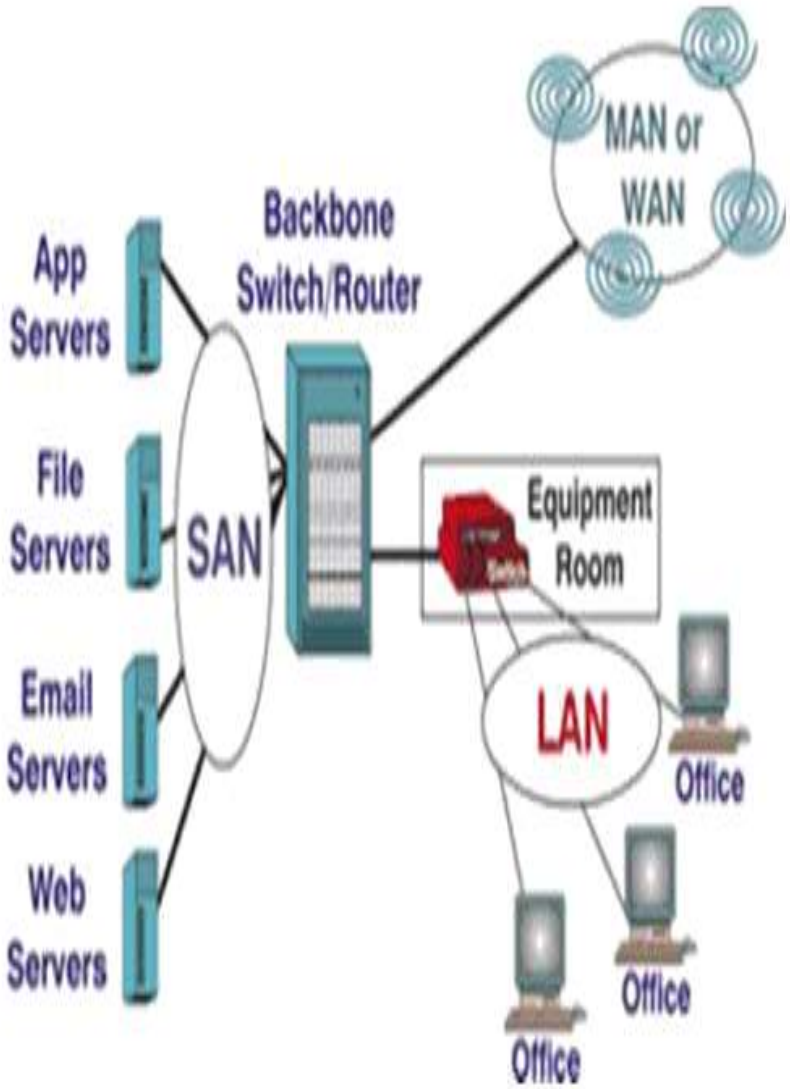
- **Peer-to-peer network:**
- Here, all the computers share their resources, such as hard drives, printers and so on with all the other computers on the network.
- Individual resources like disk drives, CD-ROM drives, and even printers are transformed into shared, collective resources that are accessible from every PC.
- The information stored across peer-to-peer networks is uniquely decentralized. Because peer-to-peer PCs have their own hard disk drives that are accessible by all computers,
- Each PC acts as both a client (information requestor) and a server (information provider).
- The peer-to-peer network is an appropriate choice when there are fewer than 10 users on the network, security is not an issue and all the users are located in the same general area

Network Models

- **Dedicated client/server network:**
- Here, one computer is designated as server and the rest of the computers are clients.
- Dedicated Server Architecture can improve the efficiency of client server systems by using one server for each application that exists within an organization.
- The designated servers store all the networks shared files and applications programs and function only as servers and are not used as a client or workstation.
- Client computers can access the servers and have shared files transferred to them over the transmission medium. In some client/server networks, client computers submit jobs to one of the servers and once they process the jobs, the results are sent back to the client computer.
- In general, the dedicated client/server model is preferable to the peer-to-peer client/server model for general purpose data networks.

Typical Network architecture





Classification of Computer Network

- There is no generally accepted criteria for classification of computer network.
- However, two dimensions stand out:
  - - Transmission technology
  - - Scale of network

Transmission technology

- Broadcast Links – A communication channel that is shared by all machines in the network

- Point-to-Point links- A communication channel that is dedicated to individual pairs of machines.

Scale of network

- GAN - Global Area Network
- WAN - Wide Area Network
- MAN - Metropolitan Area Network
- LAN - Local Area Network
- WLAN - Wireless Local Area Network
- CAN - Campus Area Network,
- PAN - Personal Area Network

Local area network:

- A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings.
- LANs use a network operating system to provide two-way communications at bit rates in the range of 10 Mbps to 100 Mbps.
- LANs are also typically owned, controlled, and managed by a single person or organization.
- They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.

Advantages of LAN

- Share resources efficiently
- □
- Individual workstation might survive network failure if it doesn't rely upon others
- □
- Component evolution independent of system evolution
- □
- Support heterogeneous hardware/software
- □
- Access to other LANs and WANs
- □
- High transfer rates with low error rates

Metropolitan area network

- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- Its geographic scope falls between a WAN and LAN.
- A MAN might be a single network like the cable television network or it usually interconnects a number of local area networks (LANs) using a high_x0002_capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks and the Internet.
- MANs typically operate at speeds of 1.5 Mbps to 10 Mbps and range from five miles to a few hundred miles in length. Examples of MANs are FDDI (fiber distributed data interface) and ATM (asynchronous transfer mode).

Wide area network

- Wide area networks are the oldest type of data communications network that provide relatively slow-speed, long-distance transmission of data, voice and video information over relatively large and widely dispersed geographical areas, such as country or entire continent.
- WANs interconnect routers in different locations.
- Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management.
- WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

Global area network

- A GAN provides connections between countries around the entire globe.
- Internet is a good example and is essentially a network comprised of other networks that interconnect virtually every country in the world.
- GANs operate from 1.5 Mbps to 100 Gbps and cover thousands of miles.

Campus Area Network

- CAN is a network spanning multiple LANs but smaller than a MAN, such as on auniversity or local business campus.

IMPORTANT NETWORK DEVICES

All network traffic requires devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator

1) HUB

Hubs are simple devices that direct data packets to all devices connected to the hub, regardless of whether that data package is destine for the devices and can create a performance bottleneck on busy networks.

A hub does nothing except provide a pathway for the electrical signals to travel along such a device is called a passive hub. However when a hub provide a path for the data signals and regenerates the signals before forwarding it to all the connected devices is called active hub.

Hubs are used in networks that use twisted pair cable.

Important Network Devices Cont…….

2) SWITCHES

Switches does essentially what a hub does but more efficiently. It forwards package only to the port that connects to the destination devices.

It does this by learning the MAC address of the devices attached to it and then by matching the destination MAC address in the data is receives.

It forward data / package only to the connection that should receive it , the switch can improve network performance.

There are basically two ways switches improve network performance

- By creating a direct path between two devices and controlling their communications, this greatly reduce the number of collisions on the network.
- Due to reduction of collision, switches can communicate with devices in full duplex mode. That is, devices can send and receive data from the switch of the same time.

Important Network Devices Cont…….

5 Router

- Routers are used to create larger networks by joining two network segments.
- A router can be a dedicated hardware device or a computer system with more than one network interface and the appropriate routing software
- A router derives its name from the fact that it can route data if receives from one network onto another. Where a router receives a packet to determine the destination address.
- A router books in its routing table to determine the destination of a data or forward the data to the next hub on the route. It uses the routing table to makes routing decisions.

Important Network Devices Cont.……

- A routing table need to be up-to-date and it must be complete. This is achieve through:
  - Static Routing: Route information are entered into the routing tables manually. This is time-consuming task and also common to error, static routing is suited to only for small network
  - Dynamic Routing : it uses routing protocols to enable routers to pass on information about themselves to others routers so that other routers can build routing tables. The routing protocols can be ; distance vector routing or link state routing.

Read – DVR and LSR

A router functions at the network and data link layers of the OSI network model.

Important Network Devices Cont…….

6. GATEWAY

- A gateway is a device that can translate information between different network data formats or network architectures. It can translate TCP / IP to Apple Talk, so computers supporting TCP / IP can communicate with apple brand computers
- Most gateways operates at the application layer, but can also operate at the network or session layer of the OSI model.
- The key point about a gateway is that only the data format is translated; not the data itself.

Important Network Devices Cont…….

3. **REPEATER**

- A repeater connects two segment of a network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments
- Repeaters requires a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Repeaters work only at the physical layer of the OSI network model.

4. **BRIDGES**

- Bridges are used to divide/jion larger networks into smaller sections. They sits between two physical network segments and manage the flow of data
- Bridges uses the MAC address of the devices connected to each segment, to forward the data to another segment or block it from crossing.
- Bridging occurs of the data link layer of the OSI model, so it can only read the MAC address and not the IP address of the package.
- Bridges do not normally allow connection of networks with different architecture.

Network LAN Technologies

1. ETHERNET

- Ethernet is a widely deployed LAN technology, and the most common networks.
- It was standardized in IEEE 802.3 in 1980.
- Ethernet uses share media
- Network which uses shared media has high probability of data collision.
- Ethernet uses Carries Sense Multi Access / Collision Detection (CSMA / CD) technology to detect collisions.
- On the occurrence of collision in Ethernet, all its host roll back, wait for some random amount of time and then re-transmit the data.
- Each Ethernet network interface card is equipped with 48 – bits MAC address. This helps other Ethernet devices to identify and communicate.
- Traditional Ethernet uses 10BASE T. specifications the number 10 depicts the speed – 10mbps, Base stands for base band and T stands for thick Ethernet. It uses coaxial cable or Cat-5 twisted pair cable with RJ-5 connector.
- Ethernet follows star topology with segment length up to 100 meters.
- All devices are collected to a hub / switch in a star fashion.

Network LAN Technologies Cont…

2. **Fast – Ethernet.**

- Fast Ethernet was inverted to meet the need of fast emerging software and hardware technology.
- Fast Ethernet can run on UTP, optical fiber and wireless technology.
- It can provide a speed up to 100mbps
- This standard is named as 100BASE – T in IEEE 803.2
- It uses CSMA/CD technique for wired media and CSMA/CA (CA stands for collision Avoidance). Technique for wireless media.
- Fast Ethernet over fiber can be extended up to 100 meters in half – duplex mode and can reach maximum of 2000 meters in full – duplex over multimode fibers.

Network LAN Technologies Cont…

3. GIGA – ETHERNET

- Giga – Ethernet was invented in 1995.
- Giga – Ethernet provides speed up to 1000mbps.
- It was standardized in IEEE 2.3ab over UTP.
- It uses Cat-5, Cat-5e, Cat-6 cables
- IEEE 802.3ah defines Giga Ethernet over fiber.

Classical Vs. Distributed Networking

- In classical network, the user explicitly logs into one machine and performs each task on the machine by giving an explicit command to the machine

- A distributed computer network is a collection of independent computers that appears to its users as a single coherent system. If the user types a command to run a program, the system assigns the best processor to run the program and assign the communication path between the processor an the user. These are done by the operating system without the user's input.

- The distributed network have task scheduling system built on top of the network, and it also have multiple processors in the system.

Classical Vs. Distributed Networking

- One of the advantage of distributed network is that it offers a good system reliability because of the processors redundancy in the system. If one processor fails, the system can still be up and running.

- Also it may be cheaper and easy to deploy a distributed network (microcomputer) than a mainframe system of a classical network.

- Difference between the two type of networks lies in who gives the command, the user for classical network while the operating system for distributed network.

- NETWORK SECURITY

COMPUTER NETWORK SECURITY

Introduction

- During initial days of internet, its usage was limited to military and universities for research and development purpose.
- Later all networks are merged together to form internet, data used to travel through public network.
- These data sent, could include highly sensitive data such as personal credentials, username and passwords, personal document, online shopping details confidential documents etc.
- All these data and information are expose to security threats.

What Is Network Security

- Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft.
- It involves creating a secure infrastructure for devices, applications, users, and applications to work in a secure manner.
- Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.
- Network security combines multiple layers of defenses at the edge and in the network.
- Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

Types of network security

- Firewalls
  - A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Intrusion prevention systems
  - An intrusion prevention system (IPS) scans network traffic to actively block attacks. Secure IPS appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.
- Workload security
  - Workload security protects workloads moving across different cloud and hybrid environments. These distributed workloads have larger attack surfaces, which must be secured without affecting the agility of the business.

Types of network security

- Network segmentation
  - Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.
- Web security
  - A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.
- Wireless security
  - Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

Types of network security

- VPN
  - A virtual private network encrypts the connection from an endpoint to a network, often over the internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.
- Access control
  - Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).
- Anti-virus and anti-malware software
  - "Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.
- Application security
  - Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes

Types of network security

- Behavioral analytics
  - To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.
- Cloud security
  - This is a broad set of technologies, policies, and applications applied to defend online IP, services, applications, and other imperative data. It helps you better manage your security by shielding users against threats anywhere they access

Types of network security

- Data loss prevention
  - Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.
- Email security
  - Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.
- Mobile device security
  - Cybercriminals are increasingly targeting mobile devices and apps. Within the next three years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.
- Security information and event management
  - SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.

Types of Cyber Attacks

- Malware Attack
- Phishing Attack
- Password Attack
- Man-in-the-Middle Attack
- SQL Injection Attack
- Denial-of-Service Attack
- Insider Threat
- Cryptojacking

How to secure Network

- Use strong passwords.
- Keep everything updated.
- Turn on encryption.
- Use a VPN.
- Use multiple firewalls.
- Rename routers and networks.
- Turn off the WPS setting.

Who are hackers

- Hackers are digital safecrackers who use their computer skills to **break into restricted digital spaces**, such as networks, servers, personal devices, online accounts, and cloud infrastructure.
- Since hackers use non-standard methods to gain entry into computer systems, their motivation is often malicious, but some actually work for the greater good.
- Many hackers who break into computers hope to steal money, access information, or hold files for ransom.
- Others work above board and are paid to probe and test the security of digital systems.

Types of hackers

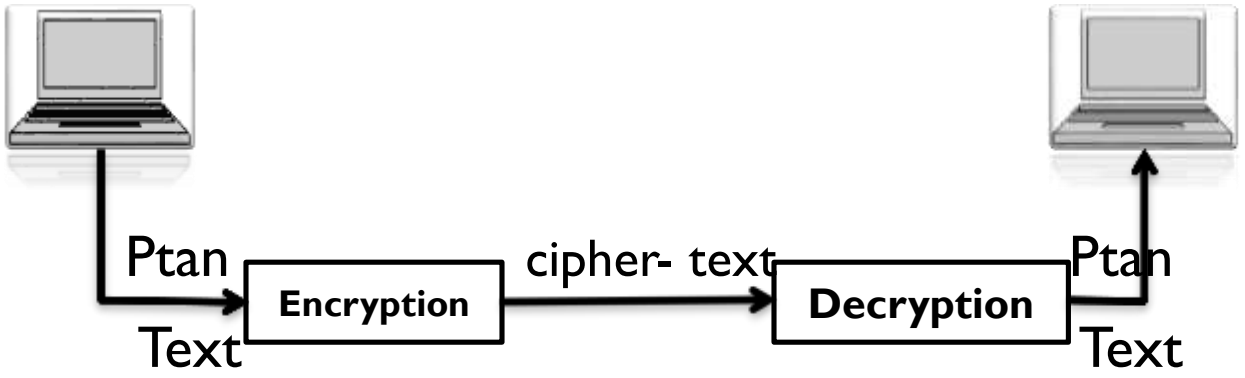
- White hat hackers
  - White hat hackers engage in **legal hacking to improve digital security** for those who contract them. They are paid to infiltrate digital systems to identify potential security vulnerabilities and report their findings to their clients.
- Black hat hackers
  - Black hat hackers are **cybercriminals who orchestrate scams and exploit vulnerabilities** with the intent to cause harm. The aim of black hat hackers is usually to make money.
- Gray hat hackers
  - Gray hats exist in an ambiguous ethical hacking area between white and black. These hackers **infiltrate systems without their targets' consent, but they don't exploit vulnerabilities** to cause harm. Instead, they inform the victims of the hack in order to help them improve their security.
- Red hat hackers
  - Red hat hackers see themselves as the "superheroes" of the hacking world. They typically **target black hat hackers to disrupt their attacks** or retaliate against them.

Types of hackers

- **Malicious insider (whistleblower)**
  - A malicious insider also known as a whistleblower is someone who works for an organization and decides to **expose wrongdoing from within**
- Blue hat hackers
  - Blue hat hackers are white hat hackers who are employed by an organization. Their job is to maintain the cybersecurity of the organization and prevent attacks.
- Script kiddies and green hat hackers
  - These are **inexperienced hackers**, they use existing malware and scripts created by other hackers to launch their attacks.
- Hacktivists
  - Hacktivists are people who hack into systems to **fight back against perceived political or social injustice.**
- State/nation-sponsored hackers
  - State-sponsored hackers work for governments. Some are white hat hackers who work to improve national cybersecurity, but others use black hat tactics to harm other countries.

SOME SOLUTIONS TO SECURITY THREATS

- The most used technique to security threat is cryptography.



- Cryptography is a technique use to encrypt the main text which makes it difficult to understand and interpret by unauthorized user. There are several cryptographic algorithms available such as secret key, public key, message digest e.t.c

SOME SOLUTIONS TO SECURITY THREATS Cont…

1. **Secrete Key Encryption**

In secrete key encryption, both the sender and receiver have one secrete key. The secrete key is used to encrypt the plain text from the user's end to cypher text and the same secrete key at receiver end will decrypt the data to plain text. Example of the secrete key encryption is data encryption standard (EDS) -sms

2. **Public Key Encryption**

In this encryption system, every user has its own secrete key, the secrete key is not revealed on public domain. The senders use this key to encrypt the plaintext and every users uses his own secrete key to decrypt the cypher text to plain text. email

Example of public key encryption is Rivest - Shamir-Adlemain (RSA)

3. **Message Digest**

In this encryption system, actual data is not send, instead a hash value is calculated and send. The other end user computes its own hash value and compares with the one just received if both hash value are matched, then it is accepted, otherwise rejected. Example of message Digest is MDS hashing.

- NETWORK TOPOLOGY

Network Topology

- Topology refers to the layout of connected devices on a network.
- The way in which different systems and nodes are connected and communicate with each other is determined by topology of the network
- Physical topology is the physical layout of nodes, workstation and cables in the network
- Logical topology is the way information flows between different components.

Network Topologies

LAN topologies

WAN topologies

LAN topologies

- A LAN is an inter-connection of microprocessors/microcomputers, minicomputer in a star, ring or bus topology with a routing algorithm embedded in a central controller.

- A LAN is composed of transmission medium, transmission control mechanism, network interface card, server, clients machines and transmission protocol controller, applications, network and system software

- Physical
  - Describes the geometric arrangement of components that make up the LAN
- Logical
  - Describes the possible connections between pairs of networked end-points that communicate

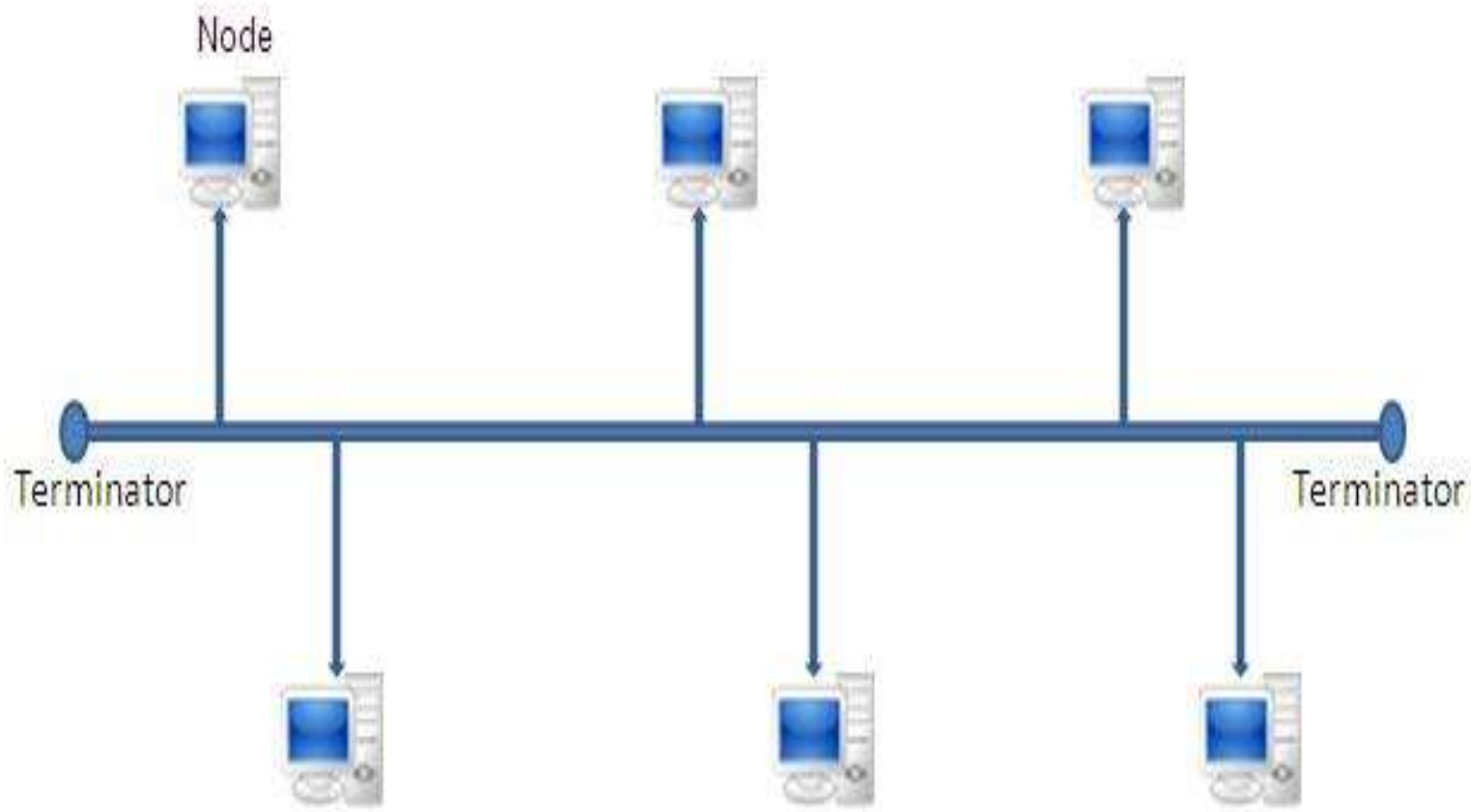
LAN Topologies(Physical)

1) Bus
2) Star
3) Ring
4) Daisy chains
5) Hierarchical

Bus topology

- Bus networks use a common backbone to connect all devices. A single cable, (the backbone) functions as a shared communication medium that devices attach or tap into with an interface connector.
- A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.
- The bus topology is the simplest and most common method of interconnecting computers.
- The two ends of the transmission line never touch to form a complete loop. A bus topology is also known as multidrop or linear bus or a horizontal bus
- Both ends of the bus must be terminated with a terminating resistor to prevent signal bounce

Bus topology



Advantages of Bus topology

1) Easy to implement and extend
2) Well suited for temporary networks that must be set up in a hurry
3) Typically the least cheapest topology to implement
4) Failure of one station does not affect others
5) Require less cable

Disadvantages of Bus topology

1) Difficult to administer/troubleshoot
2) Limited cable length and number of stations
3) A cable break can disable the entire network; no redundancy
4) Maintenance costs may be higher in the long run
5) Performance degrades as additional computers are added

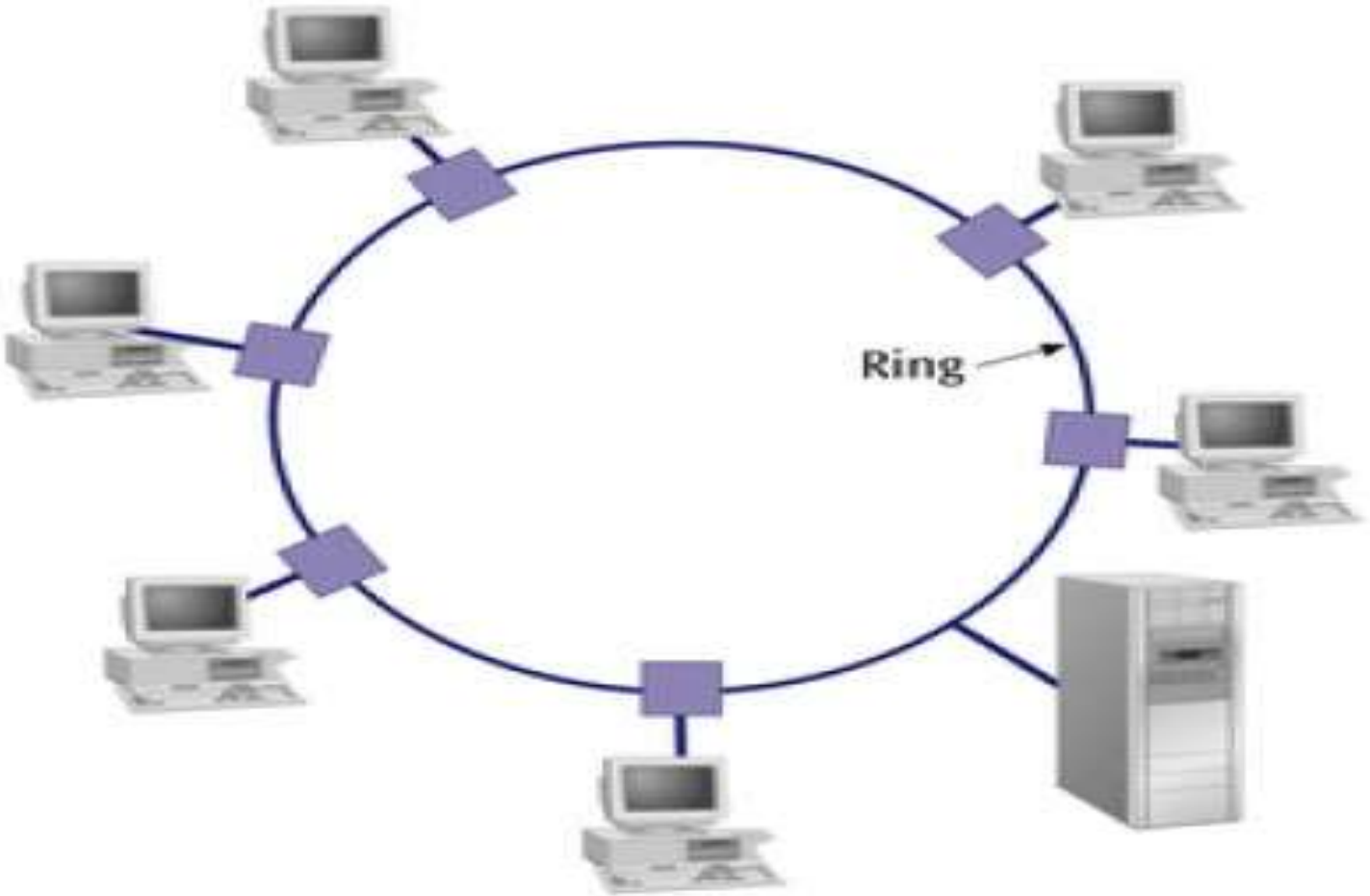
Ring topology

- Every device has exactly two neighbours for communication purposes.
- All messages travel through a ring in the same direction (either "clockwise" or "counter clockwise").
- All the stations are interconnected in tandem (series) to form a closed loop or circle.
- Transmissions are unidirectional and must propagate through all the stations in the loop
- Each computer acts like a repeater
- Sending and receiving of data takes place by the help of TOKEN

Token Passing

- Token contains a piece of information which along with data is sent by the source computer
- This token then passes to next node, which checks if the signal is intended to it
  - If yes, it receives it and passes the empty token into the network
  - otherwise passes token along with the data to next node

Ring topology



Advantages of Ring topology

1) This type of network topology is very organized
2) Performance is better than that of Bus topology
3) No need for network server to control the connectivity between workstations
4) Additional components do not affect the performance of network
5) Each computer has equal access to resources

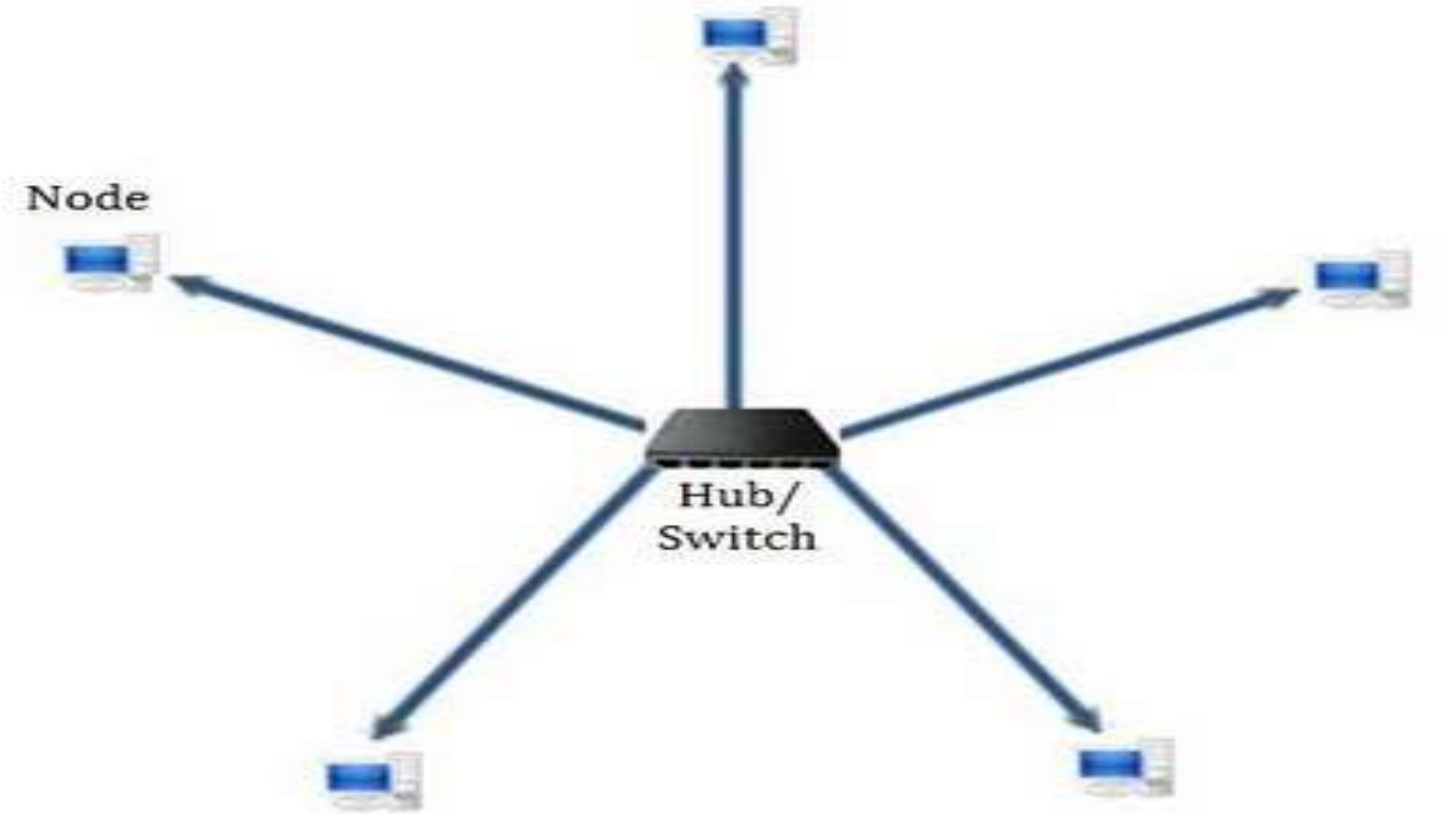
Disadvantages of Ring topology

1) Each packet of data must pass through all the computers between source and destination, slower than star topology
2) If one workstation or port goes down, the entire network gets affected
3) Network is highly dependent on the wire which connects different components

Star topology

- A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator.
- Data on a star network passes through the hub, switch, or concentrator before continuing to its destination.
- Each networked device in star topology can access the media independently
- Have become the dominant topology type in contemporary LANs
- The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow

Star topology



Advantages of star topology

1) Compared to Bus topology it gives far much better performance
2) Easy to connect new nodes or devices
3) Centralized management. It helps in monitoring the network
4) Failure of one node or link doesn't affect the rest of network

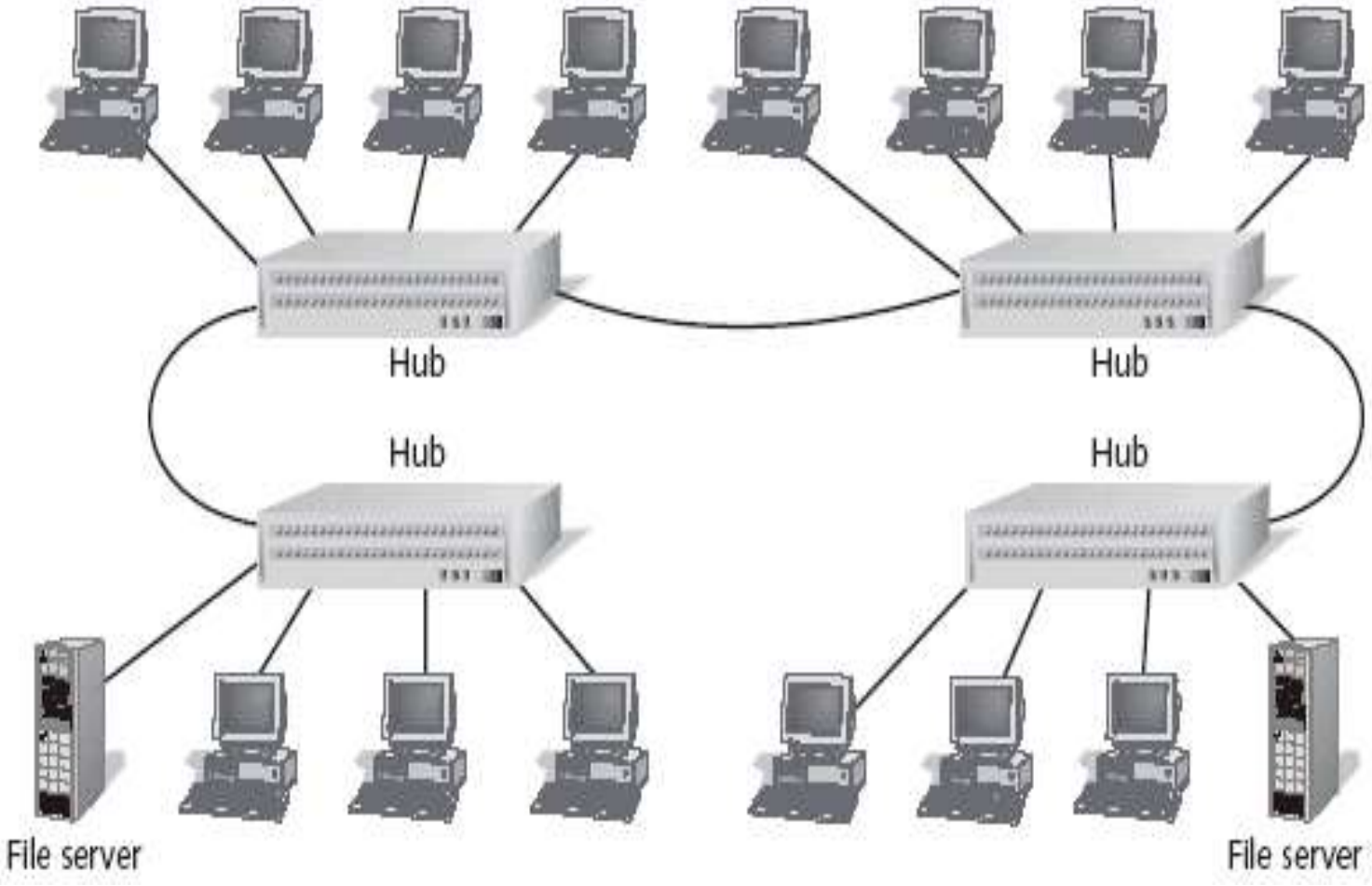
Disadvantages of star topology

1) If central device fails whole network goes down
2) The use of hub, a router or a switch as central device increases the overall cost of the network
3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

Daisy chains

- Developed by serially interconnecting all the hubs of a network
- This simple approach uses ports on existing hubs for interconnecting the hubs
- Daisy chains are easily built and don't require any special administrative skills
- Daisy chains were, historically, the interconnection method of choice for emerging, first-generation LANs

Daisy chains



Disadvantage of Daisy chain

- Increases the number of connections, and therefore the number of devices, on a LAN. Too many devices competing for the same amount of bandwidth can create collisions and quickly incapacitate a LAN

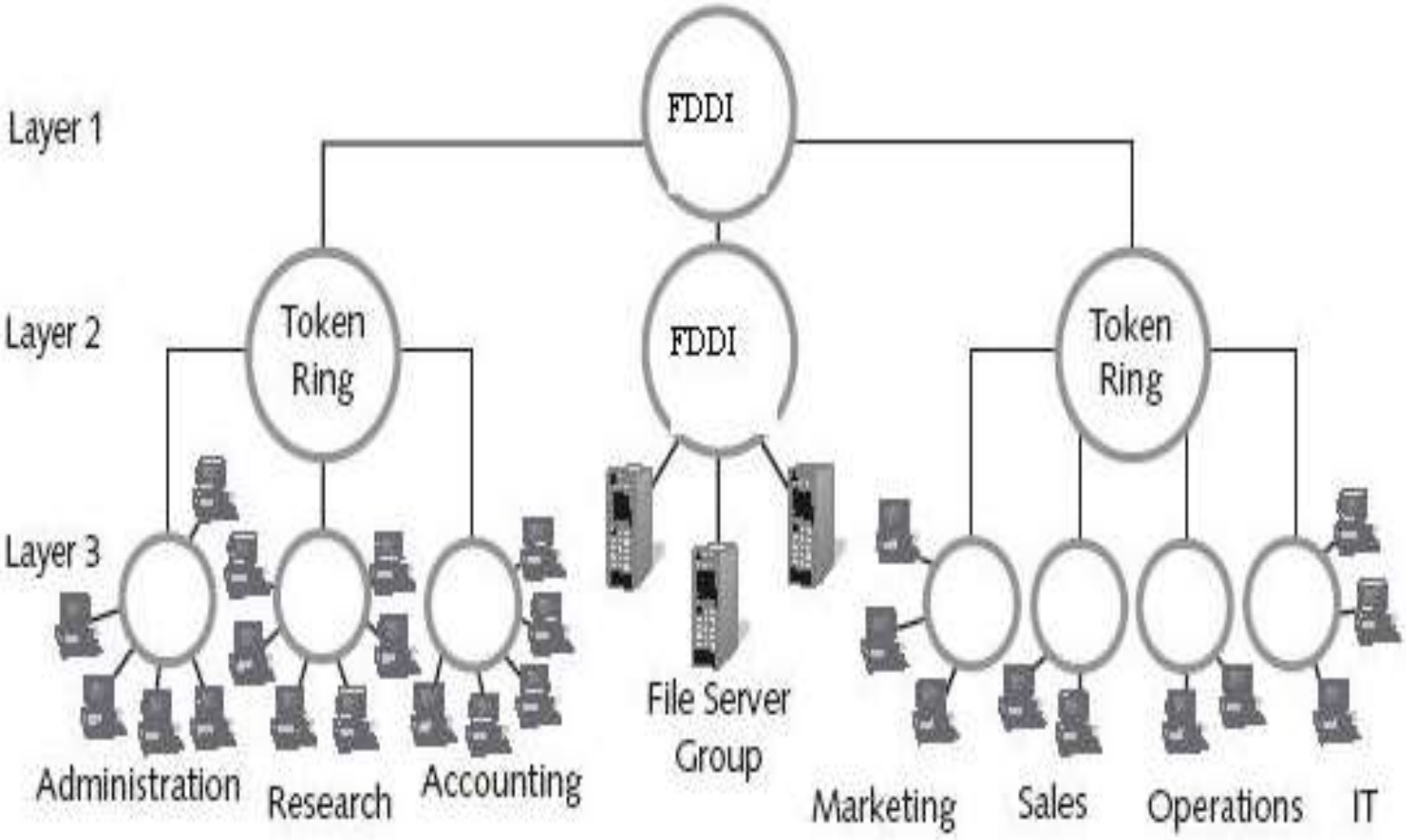
Hierarchical topology

- Hierarchical topologies consist of more than one layer of hubs. Each layer serves a different network function
- The bottom tier is reserved for user station and server connectivity. Higher-level tiers provide aggregation of the user-level tier
- A hierarchical arrangement is best suited for medium-to-large-sized LANs that must be concerned with scalability of the network and with traffic aggregation

Hierarchical rings

- Ring networks can be scaled up by interconnecting multiple rings in a hierarchical fashion
- User station and server connectivity can be provided by as many limited size rings as are necessary to provide the required level of performance
- A second-tier ring, either Token Ring or FDDI, can be used to interconnect all the user level rings and to provide aggregated access to the Wide Area Network (WAN)

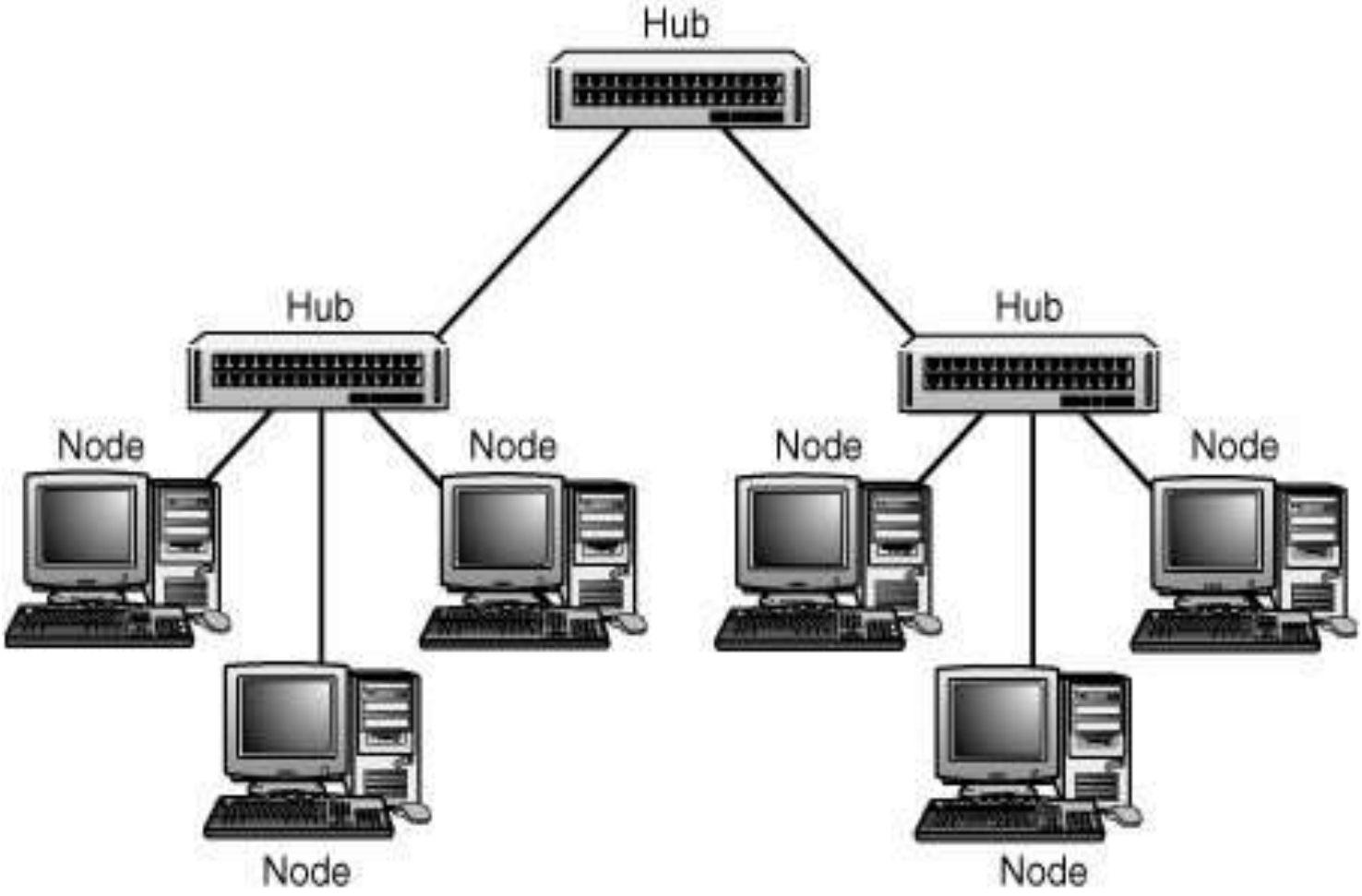
Hierarchical rings



Hierarchical stars

- Star topologies, can be implemented in hierarchical arrangements of multiple stars
- Hierarchical stars can be implemented as a single collision domain or segmented into multiple collision domains using switches, routers or bridges

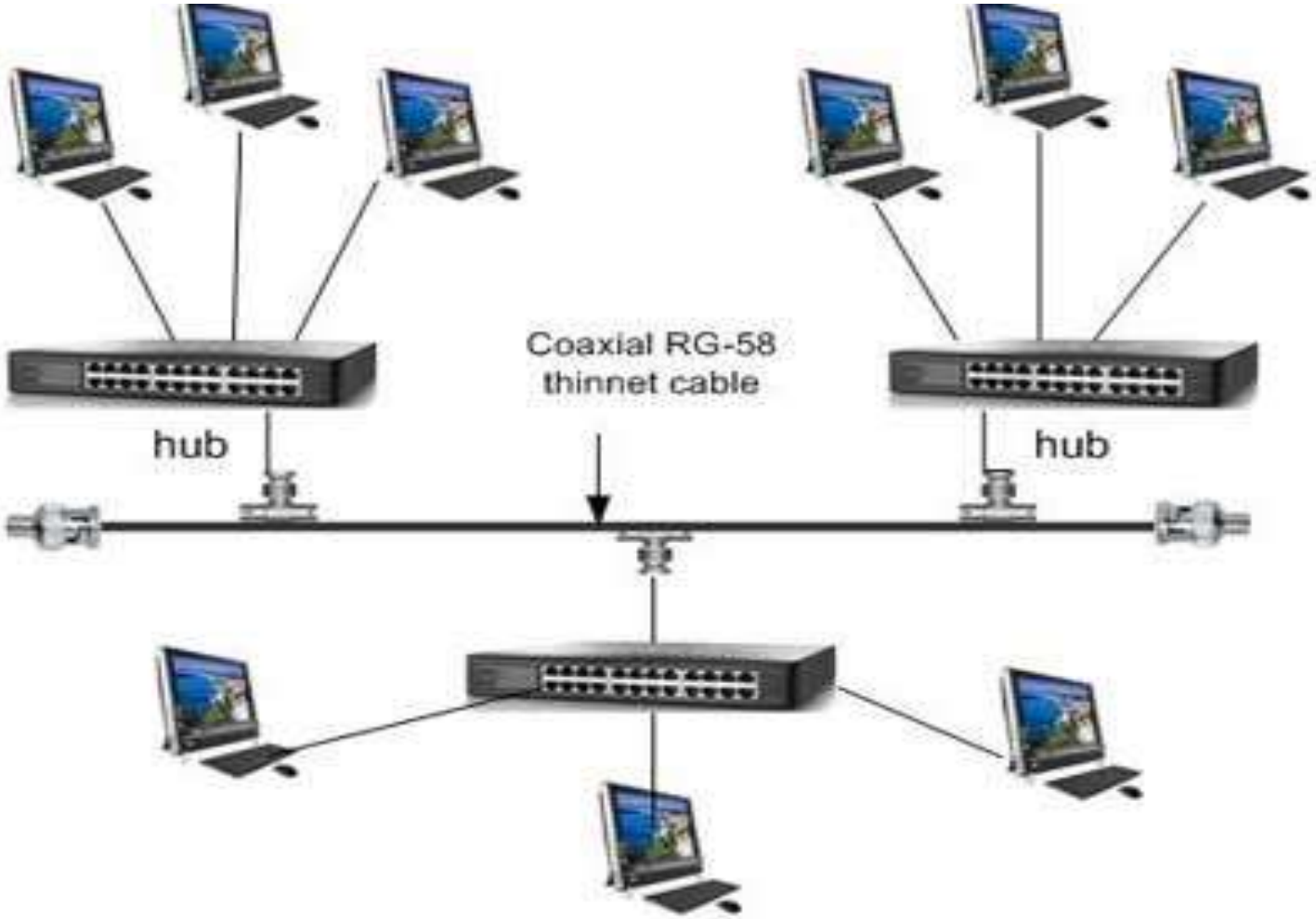
Hierarchical stars



Hierarchical combinations

- Overall network performance can be enhanced by not force-fitting all the functional requirements of the LAN into a single solution
- Today's high-end switching hubs enable you to mix multiple technologies

Hierarchical combinations



WAN Topologies

- The topology of a WAN describes the way the transmission facilities are arranged relative to the locations that they interconnect
- Numerous topologies are possible, each one offering a different mix of cost, performance and scalability

WAN Topologies

1) Peer-to-peer WANs
2) Ring WANs
3) Star WANs
4) Full-mesh WANs
5) Partial-mesh WANs
6) Two-tiered
7) Three-tiered
8) Hybrids

Peer-to-peer topology

- A peer-to-peer WAN can be developed using leased private lines or any other transmission facility
- This WAN topology is a relatively simple way of interconnecting a small number of sites
- Represents the least-cost solution for WANs that contain a small number of internetworked locations

Advantage/Disadvantage of Peer-to-peer

- Advantage:
  - It is inexpensive relative to other options
- Disadvantages:
  - They don't scale very well. As additional locations are introduced to the WAN, the number of hops between any given pair of locations remains highly inconsistent and has an upward trend
  - An equipment or facility failure anywhere in a peer-to-peer WAN can split the WAN

Ring topology

- Can be developed fairly easily from a peer-to-peer network by adding one transmission facility and an extra port on two routers
- A ring-shaped WAN constructed with point-to-point transmission facilities can be used to interconnect a small number of sites and provide route redundancy at a potentially minimal incremental cost
- Can use dynamic routing protocols

Advantages/Disadvantages of Ring topology

- Advantages:
  - It provides alternative routes
  - It is less expensive than all but the peer-to-peer WAN
- Disadvantages:
  - Depending on the geographic dispersion of the locations, adding an extra transmission facility to complete the ring may be cost prohibitive
  - Rings are not very scalable

Full-mesh topology

- This topology features the ultimate reliability and fault tolerance
- Every networked node is directly connected to every other networked node
- Redundant routes to each location are plentiful, hence static routing impractical.
- Use dynamic routing protocols
- One application would be to provide interconnectivity for a limited number of routers that require high network availability
- Another potential application is to fully mesh just parts of the WAN, such as the backbone of a multitiered WAN or tightly coupled work centers

Advantages/Disadvantages of full-mesh

- Advantages:
  - Minimizes the number of hops between any two network-connected machines
  - Can be built with virtually any transmission technology
- Disadvantages:
  - These WANs can be fairly expensive to build
  - A finite (although substantial) limit on the scalability of the network

Partial-mesh topology

- Partial meshes are highly flexible topologies that can take a variety of very different configurations
- The routers are much more tightly coupled than any of the basic topologies but are not fully interconnected, as would be the case in a fully meshed network
- A partially meshed WAN topology is readily identified by the almost complete interconnection of every node with every other node in the network

Advantages of partial-mesh

- Partial meshes offer the capability to minimize hops for the bulk of the WAN's users
- Unlike fully meshed networks, a partial mesh can reduce the startup and operational expenses by not interconnecting low-traffic segments of the WAN, hence more affordable and scalable

Two-tiered topology

- A two-tiered topology is a modified version of the basic star topology. Rather than single concentrator routers, two or more routers are used
- A two-tiered WAN constructed with dedicated facilities offers improved fault tolerance over the simple star topology without compromising scalability

Three-tiered topology

- WANs that need to interconnect a very large number of sites, or are built using smaller routers that can support only a few serial connections, may find the two-tiered architecture insufficiently scalable.
- Therefore, adding a third tier may well provide the additional scalability they require

Advantage/Disadvantage of three-tiered

- Advantage:
  - A three-tiered WAN constructed with dedicated facilities offers even greater fault tolerance and scalability than the two-tiered topology
- Disadvantage:
  - Three-tiered networks are expensive to build, operate and maintain

Hybrid topologies

- Hybridization of multiple topologies is useful in larger, more complex networks
- Multitiered networks, in particular, lend themselves to hybridization. A multitiered WAN can be hybridized by fully or partially meshing the backbone tier of routers
- An effective hybrid topology may be developed in a multitiered WAN by using a fully meshed topology for the backbone nodes only

NETWORK DESIGN CONSIDERATION

- In designing any network either large or small, it is important to determine the needs and desires of the stakeholders for network and the budget for the implementation.
- The critical things needed to be considered in designing a network are as follows:

Connectivity and Security

- Network connectivity today requires access through different channels with greater speed.
- Demand for mobile connectivity is on the increase, users want to access services and networks at their convienent and anyway.
- Balancing these needs while maintaining security is a challenge that must be addressed in design phase of any network.
- These challenges includes: where data is stored either in-house or off- site with cloud-based solutions, what types of information should be accessible, who should be allowed to access it, which devices should be used to secured the network at the same time do not slow down the network.

Redundancy and Backing-up

- Redundancy means having back up devices in place for any mission-critical components of the networks, so that whenever the active server fails or requires maintenance, the redundant server should take over.
- A good rule of thumb is to have redundant components and services in place for any part of the network that cannot be down for more than an hour.
- The redundancy can be on the internet connection, servers, devices (switches, routers, spare parts, etc)
-

Standardization of Hardware and software

- Standardization of hardware and software used in a network is a critical success factor for ensuring the network runs optimally.
- Standardization helps to reduce costs associated with maintenance, upgrade and repairs.
- In designing a network, it is important to conduct a full audit of the current computer systems, software and peripherals to determine what should be standardized.

Disaster recovery plan

- A detailed disaster recovery plan should be part of any network design.
- It includes but not limited to provision of back-up power, procedures to be followed if the network or server crashes.
- It is a good rule of the thumb that data/information should be back-up in an agreed time interval to ensure that in case of system crash, data or information are not lost and that down time is kept to a minimum.
- This should include when and how data is back-up and how it will be recovered.
- Data/information should be backed-up in a secure location off-site in the event of a disaster.

Future Growth of the Organisation

- It is a good practice, that some allowances for future growth is built into the network design.
- It is advisable that, in network design, at least 20% should factor for future growth in a year.
- It includes internet bandwidth, licences, storage capacity, processing speed, etc

OSI Layering

ISO – Organization for Standardization

- ISO is and International standards organization responsible for a wide range of standards, including many that are relevant to networking.
- In 1984, in order to aid network interconnection without necessarily requiring complete redesign.
- The Open System Interconnection (OSI) reference model was approved as an international standard for communication architecture.

The Need for Standard In Networking

- Over the past couple of decades many of the networks that were built used different hardware and software in implementations, as a result they were incompatible and it became difficult for networks using different specifications to communicate with each other.
- To address the problem of networks being incompatible and unable to communicate with each other, the International Organization for Standardization researched various network schemes.
- The ISO recognized there was a need to create a NETWORK MODEL that would help vendors create interoperable network implementations.

The OSI Reference Model

- The Open System Interconnection (OSI) reference model is a descriptive network scheme. It ensures greater compatibility and interoperability between various types of network technology .
- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divided the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems.
- This separation into smaller more manageable functions is known as layering

Network Protocols

- Network Protocol is a set of rules outlining how connected devices communicate across a network to exchange information easily and safely.
- Protocols serve as a common language for devices to enable communication irrespective of differences in software, hardware, or internal processes.
- Most network are organized as layers or levels to reduce their design complexity Each layer is built upon the one below it.

- The number of layers, the name of the layer, the contents of each layer, and the functions of each layers differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

Types of protocol

- Transmission Control Protocol (TCP)
  - Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.
  - TCP organizes data so that it can be transmitted between a server and a client. It guarantees the integrity of the data being communicated over a network
  - TCP establishes a connection between a source and its destination, which it ensures remains live until communication begins.

Types of Protocol

- Internet Protocol (IP)
  - The Internet Protocol (IP) is a set of standards for addressing and routing data on the Internet.
  - Each computer -- known as a host -- on the internet has at least one IP address that uniquely identifies it from all other computers on the internet.
  - message is divided into chunks called packets. Each packet contains both the sender's internet address and the receiver's address.
  - Any packet is sent first to a gateway computer that understands a small part of the internet.
  - The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood -- or domain. That gateway then forwards the packet directly to the computer whose address

Types of Protocol

- User Datagram Protocol (UDP)
  - User Datagram Protocol (UDP) is a communications protocol for time-sensitive applications like gaming, playing videos, etc.
  - UDP results in speedier communication because it does not spend time forming a firm connection with the destination before transferring the data.
  - Because establishing the connection takes time, eliminating this step results in faster data transfer speeds.
  - UDP can also cause data packets to get lost as they go from the source to the destination. It can also make it relatively easy for a hacker to execute a distributed denial-of-service (DDoS) attack.

Types of Protocol

- Post office Protocol (POP)
  - Post Office Protocol is a widely used e-mail application protocol that can be used to retrieve e-mail from an e-mail server for the client application, such as Microsoft Outlook.
  - POP works through a supporting email software client that integrates POP for connecting to the remote email server and downloading email messages to the recipient's computer machine.
  - POP uses the TCP/IP protocol stack for network connection and works with Simple Mail Transfer Protocol (SMTP) for end-to-end email communication, where POP pulls messages and SMTP pushes them to the server
- Assisgment : Distiguish between UDP and TCP

Network Architecture

- Network Architecture is the way network services and devices are structured together to serve the connectivity needs of client devices and applications.
- The purpose of a network architecture is to provide a framework for organizing and managing the network infrastructure. In addition to providing a structure for managing the network infrastructure, the architecture should also provide for the efficient and effective use of the network resources.
- Network architecture specification contains enough information to allow the implementer to develop each layer so that it will correctly obey the appropriate protocol.

Layering

- Each corresponding layers on different machines are called peers. It is the peers that communicate by using the protocol
- No data are directly transferred from layer n on one machine to layer n on another machine even though the layer n on one machine conceptually thinks of their communication as being "horizontal" using the layer n protocol
- Each layer passes data and control information to the layer immediately below it, until the lowest layer is reached.
- Below layer 1 is the physical medium through which actual communication occurs
- Between each pair of adjacent layers is an interface which defines the primitive operations and services the lower layer makes available to the upper one.
- When network designers develop network protocol, one of the most important considerations is defining clean interfaces between the layers.

Layering Issues

- Every layer has a mechanism for identifying senders and receivers – has some addressing mechanism.
- Layers have rules for data transfer protocol – including data direction, number of logical channels and their priorities.
  - Error control protocol
  - Data sequencing guidelines
  - Flow control
- Data multiplexing and demultiplexing
- Layer can offer two different services to the layers above them: connection-oriented and connectionsless
- Quality of service.

The OSI Reference Model

- Open System International (OSI) reference model – deals with connecting open system – i.e. systems that are open for communication with other systems.
- The Open Systems Interconnection (OSI) Model is a conceptual framework that defines how networking systems communicate and send data from a sender to a recipient.
- It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s
- It helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.
- OSI/IEEE 802 specifies the OSI as having seven layers:
  - Physical Layer
  - Data-link layer
  - Network Layer
  - Transport layer
  - Session Layer

The OSI Reference Model

- Presentation Layer
- Application Layer

- The OSI Layering principles are as follows:
  - A layer should be created where a different abstraction is needed
  - Each layer should perform a well-define function
  - The function of each layer should be chosen with an eye towards defining international standardized protocols
  - The layer boundaries are chosen to minimize the information flow across the interfaces
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy

The Physical Layer

- The physical layer is responsible for the physical cable or wireless connection between network nodes. That is, it provides physical interface for transmission of information.
- It defines the connector, the electrical cable or wireless technology connecting the devices.
- Defines rules by which bits are passed from one system to another on a physical communication medium.
- Covers all – mechanical, electrical, functional and procedural.
- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

Physical Layer Installations

- The physical layer plant is concerned with the medium in which the raw bits that makes up the network signals are transported.
- Common network transmission media include: twisted pair wire, coaxial cable, fibre optics cable, radio and satellite link, and magnetic media
- The propagation delay in a twisted pair, coaxial cable, fibre optic cable, and wireless medium is compared below.

COPPER-BASED CABLES

- **Twisted Pair:** This is the common telephone wire (copper) which is very inexpensive, ubiquitous, and already installed in many buildings. It is susceptible to noise from other transmission sources (the twisting is to reduce noise)It can be used repeater – less over distances of a few kilometres and has good multi-tapping qualities. Its transmission bandwidth is dependent on core diameter and distance. It can achieve bandwidths of several megabits/sec over a few kilometres and can be used for both analogue and digital communication.

Coaxial cable: This is a shielded copper wire, which is inexpensive relative to its transmission capacity. It also has relatively better noise immunity than twisted pair and cover longer distance at higher speeds than twisted pair but is more expensive. It has the same good multi-tapping qualities as twisted pair and can be used for both digital (baseband transmission with 50-ohm cable) and analog (broadband transmission with 75-ohm) communication

Fibre Optic Cable Plants

A fibre optic based physical layer generally consist of:

- Transmitter
- Couplers
- Optical Switches
- Slices
- Receiver

Fibre Optic Cables

- Have small weight
- Have no crosstalk
- Low error rate thus producing high fidelity transmission
- They work without repeaters at distance up to tens of kilometres. They are good for high bandwidth communication.
- Due to losses in signal level at tapping points and in couplers, fibre optic cables have multi-tapped problems hence is unsuitable for busing application.
- They are unable to transmit DC voltages and hence unsuitable for CSMA/CD runs.

RADIO TRANSMISSION

- Easy to generate
- Can travel long distance
- Can penetrate obstacles such as building
- it is attractive for its low incremental cost as it can serve an unlimited number of users.
- Network communication radio waves entails sharing the broadcast spectrum.
- since the waves can travel long distances, interference between users is a problem.
- a license is needed for wide area transmission.

MICROWAVE TRANSMISSION

- This transmission use microwave (waves at the high end of the radio spectrum) generated on tower mounted dishes that travel along straight lines.
- The distance between the transmitters and receivers (or repeaters) is dependent on the towers and can be up to 80km apart for fairly tall towers.
- High strengths:
  - Media is free space requiring no right of way
  - Relatively inexpensive.
- The disadvantages include:
  - To communicate, one need to be assigned a broadcast spectrum and spectrum availability is limited.
  - Microwave transmission is affected by atmospheric conditions.

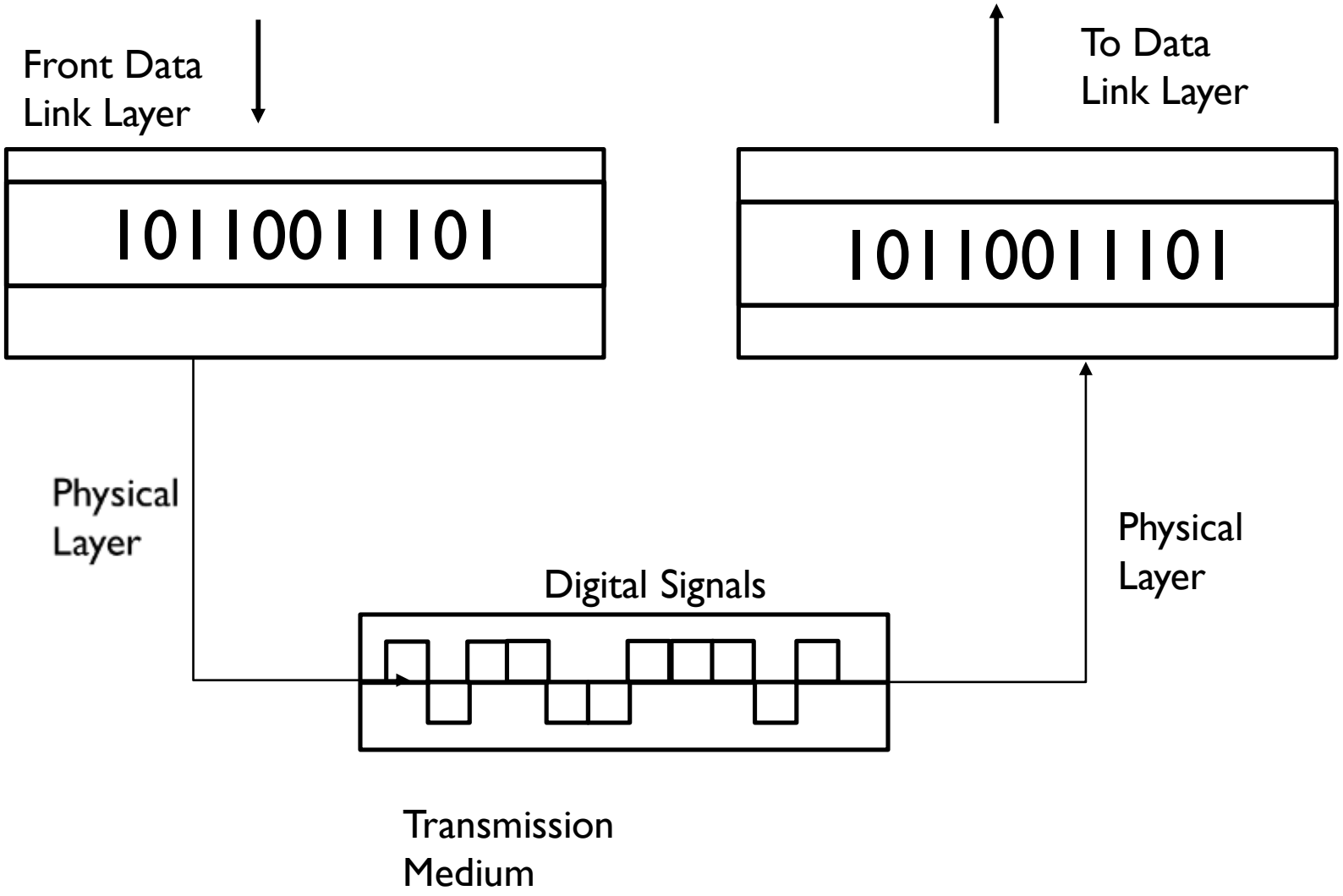
Satellite Communication

- Very suitable for high bandwidth transmission with a low incremental cost.
- is distance independent
- has a high propagation delay (2 X 0.24 seconds earth to satellite and back)
- Even though satellite links is unsuitable for busing applications it can be used in a LAN network to interconnects a LAN to a wider area network.

Comparison Between Fibre Optic and copper Cable Technology

- Copper – and – fibre-based physical layers have their strengths and limitation. Over long distances a single node fibre has many advantages over copper based links. These are
- Fibre-based plants have low signal loss and a bandwidth capacity. While for a coaxial cable, size requirement increases with bandwidth, the core size for a fibre cable plants generally decreases with increasing bandwidth.
- Repeater-less transmission is possible at distances up to 30km with a fibre link while for coaxial links, the maximum repeater-less transmission is limited to 50km or there about.
- Crosstalk and interference between adjacent signal path is a problem in copper cables. Fibre optic cables are non-conductive and are not affected by extraneous signal and noise. Also fibre cables do not radiate or produce interference.
- Fibre optic cable, when compared to copper lines, will carry more traffic. As an example a 3.5 in duct with320 twisted pairs or 20 coaxial have the same information carrying capacity as a 3/8 inch diameter fibre optical cable. Thus for the same bandwidth, a fibre plant has less weight and smaller size.
- for a fibre plant, there is greater difficulty in tapping by an intruder and it is less susceptible to damage by electromagnetic pulse.
- The disadvantage relative to copper are:
  - Because of coupler losses and losses at optical switches and contacts, a fibre plant is not suitable for busing applications.
  - Cost weights against the use of a fibre plant. Comparatively, the cost of installation of a copper plaint is lower than that for a fibre plant.

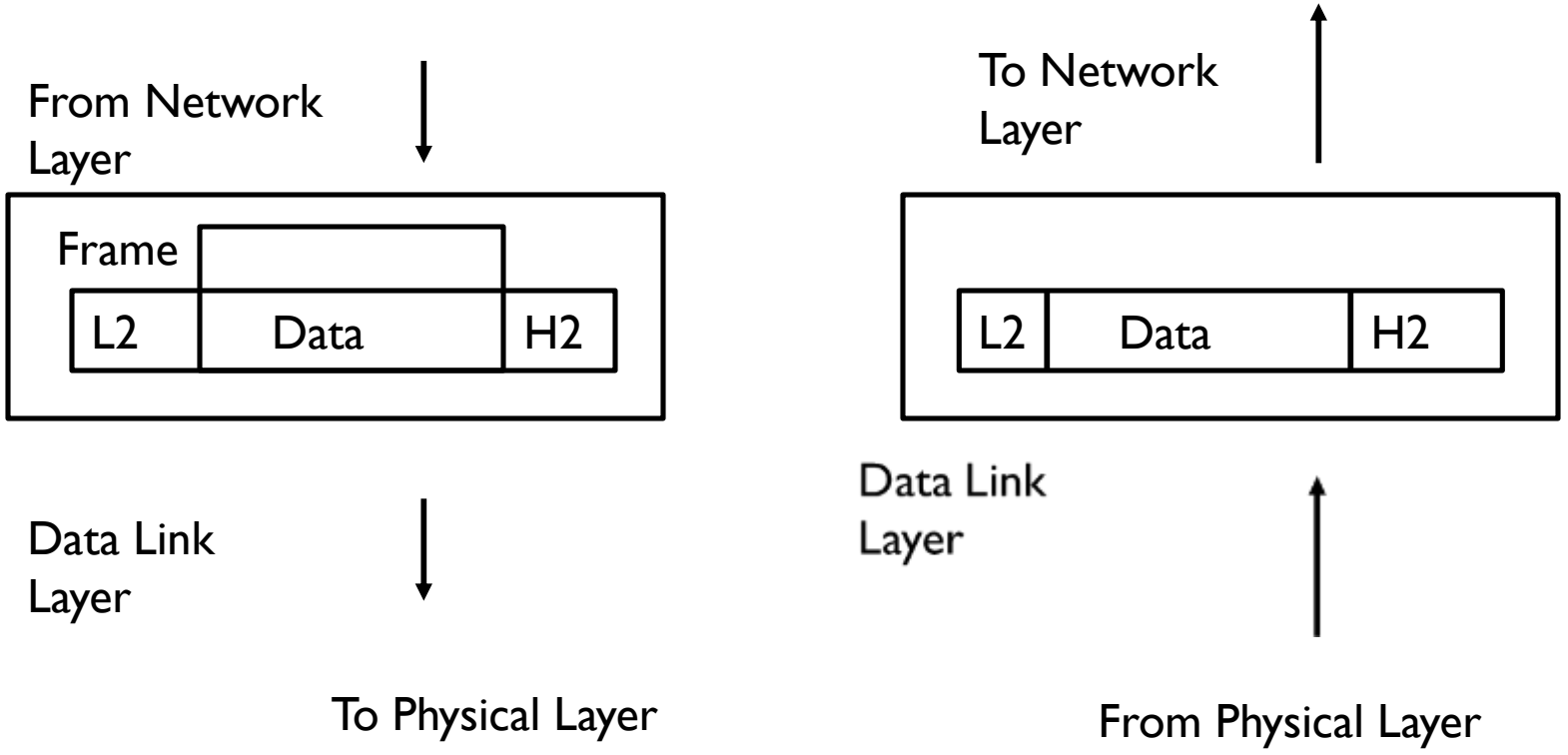
Physical Layer



The Data Link Layer

- The data link layer establishes and terminates a connection between two physically-connected nodes on a network
- Data link layer attempts to provide reliable communication over the physical layer interface.
- Breaks the outgoing data into frames and reassemble the received frames.
- This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.
- Supports points-to-point as well as broadcast communication.
- Supports simplex, half-duplex or full-duplex communication.

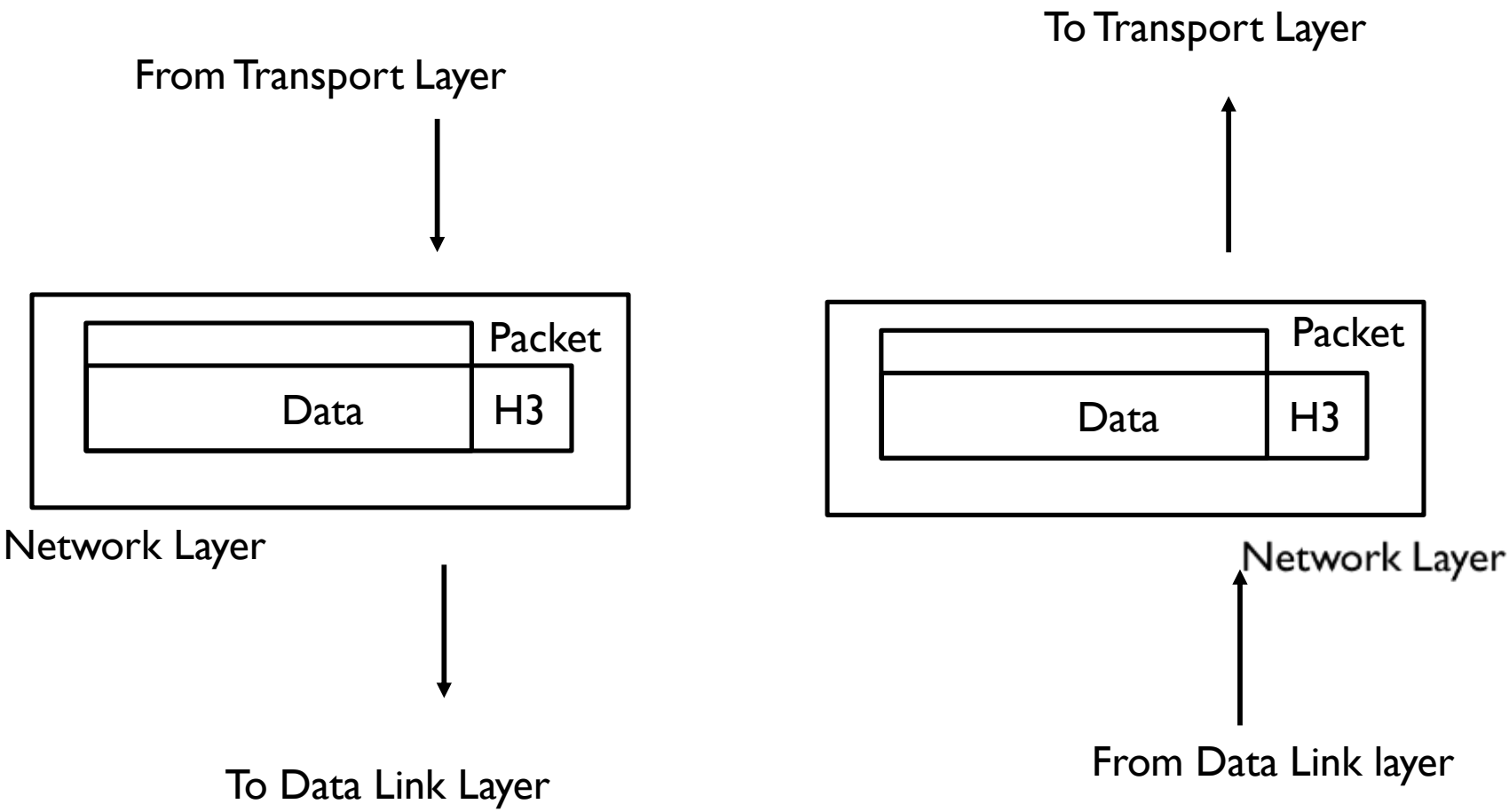
Data Link Layer



The Network Layer

- Implements routing of frames (packets) through the network.
- Defines the most optimum path the packet should take from the source to the destination.
- Defines logical addressing (Internet protocol address)so that any endpoint can be identified.
- Handle congestion in the network.
- Facilitates interconnection between heterogeneous network (Internetworking).
- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

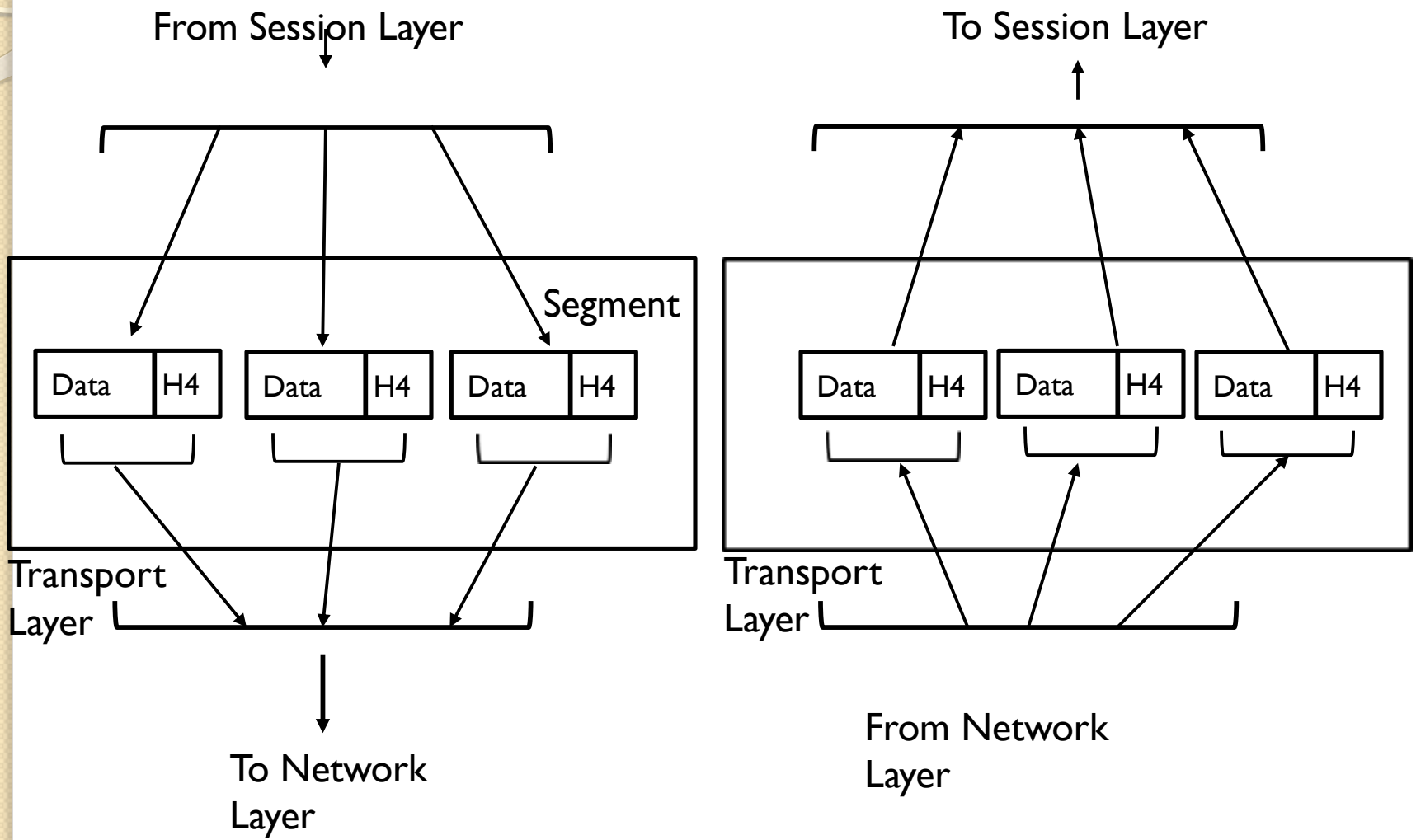
Network Layer



The Transport Layer

- Provide a reliable mechanism for the exchange of data between two processes in different computers.
- Ensure that the data units are delivered error free.
- Ensure that data units are delivered in sequence.
- Ensures that there is no loss or duplication of data units.
- Provides connectionless or connection oriented service.
- Provides for the connection management.
- Multiplex multiple connection over a single channel

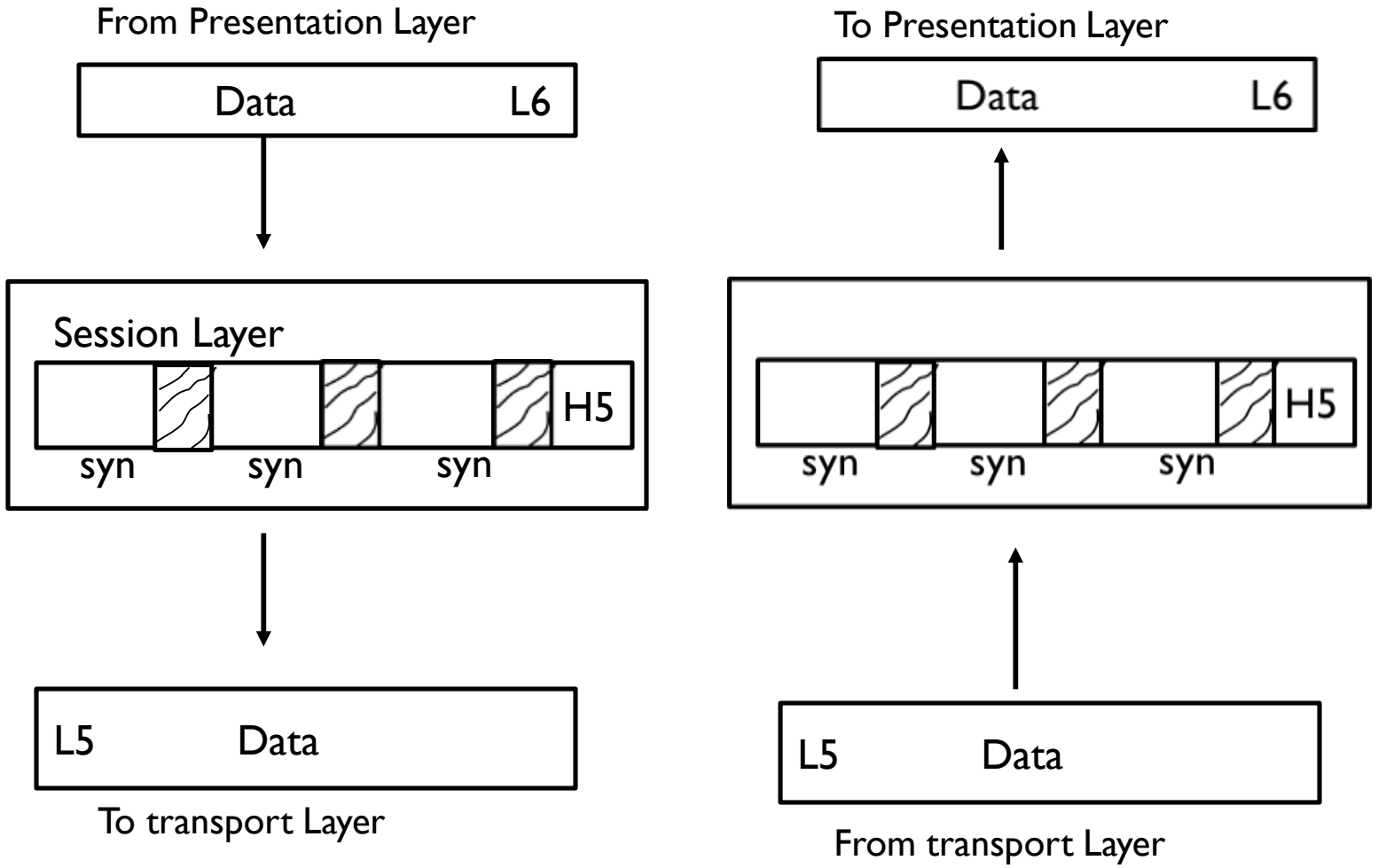
Transport layer



The Session Layer

- Provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.
- This layer requests for a logical connection to be established on an end-user's request.
- Any necessary log-on or password validation is also handled by this layer.
- Session layer is also responsible for terminating the connection.
- This layer provides services like dialogue discipline which can be full duplex or half duplex.
- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted form the last checkpoint.

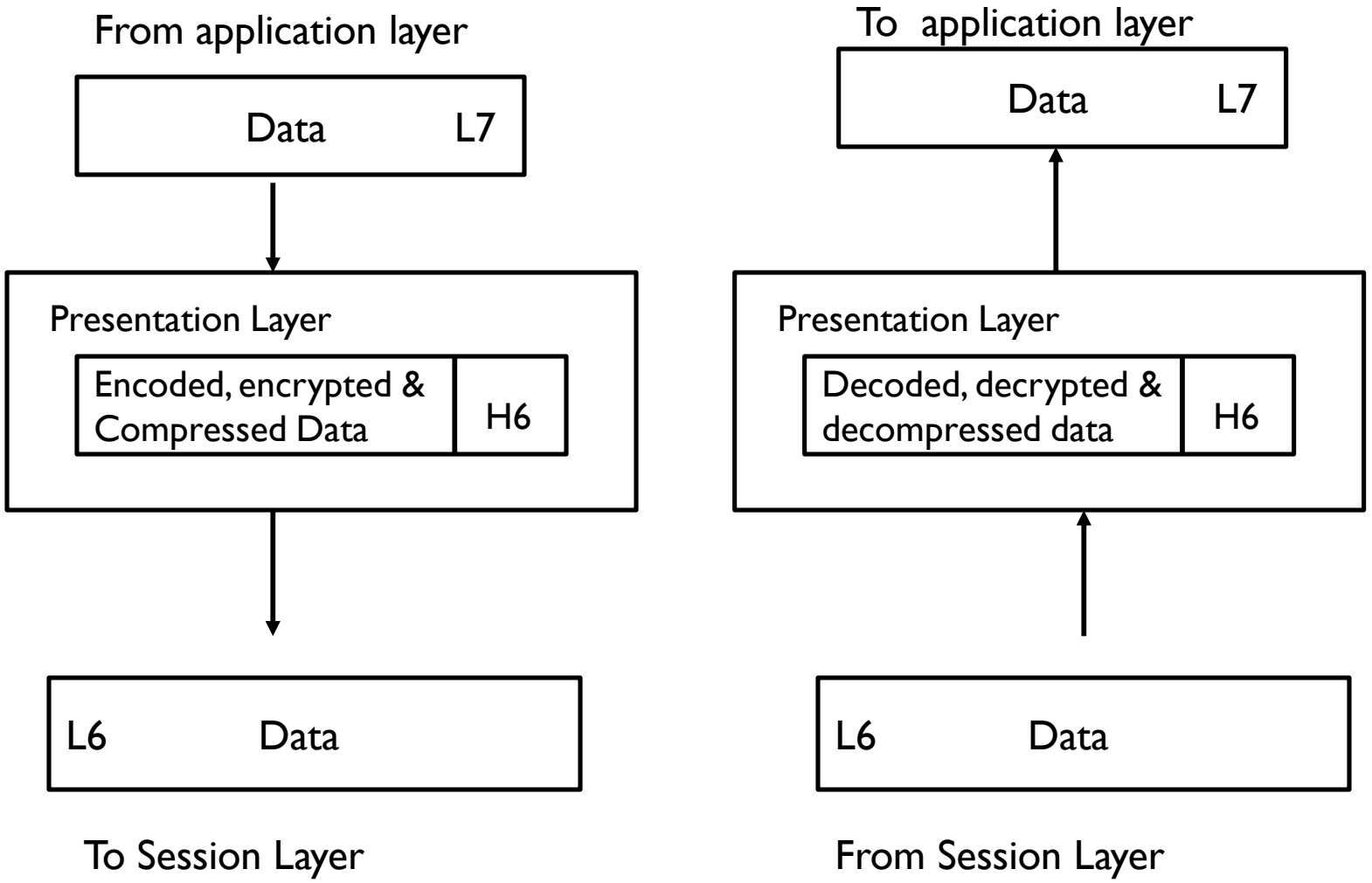
Session Layer



The Presentation Layer

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

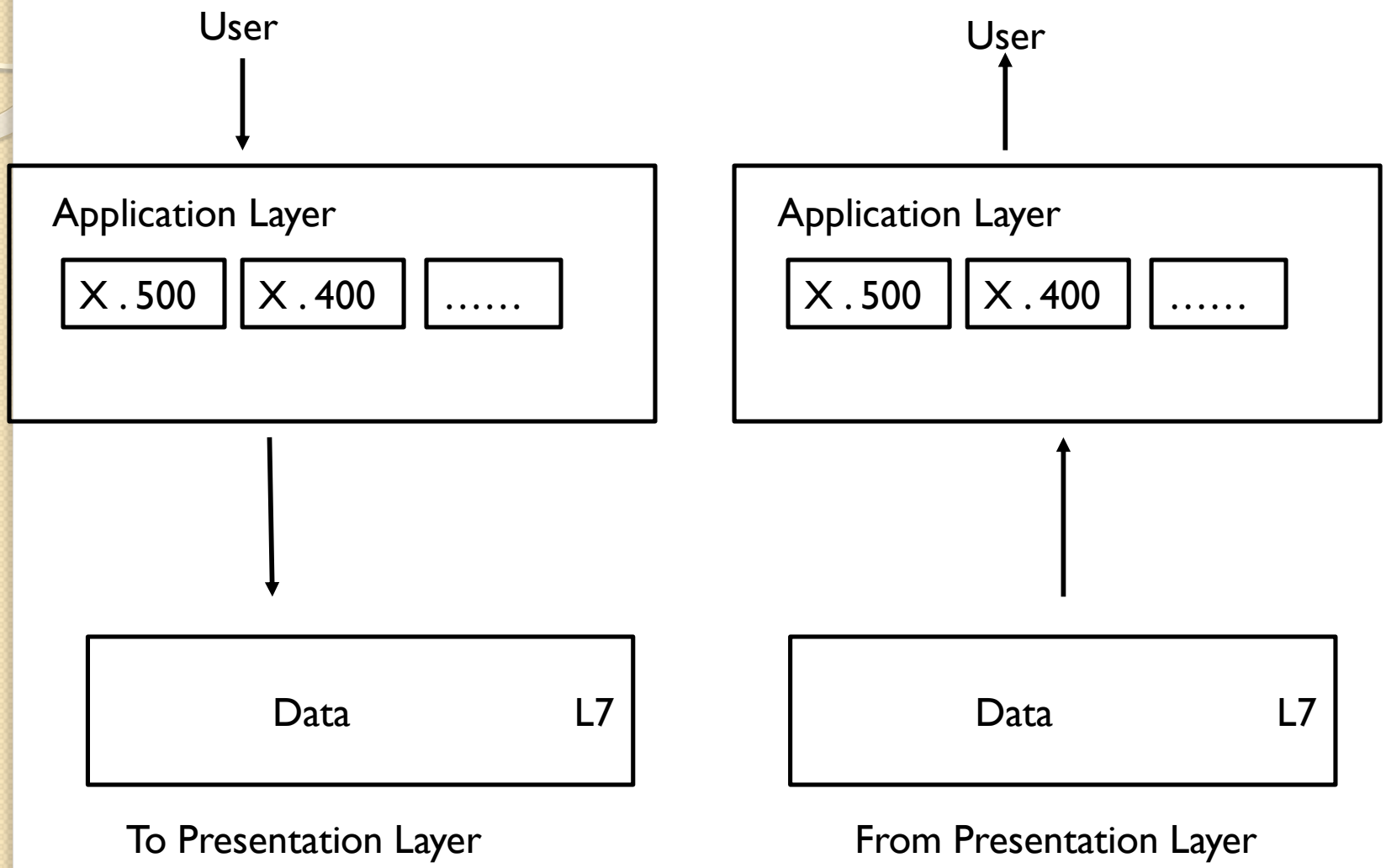
Presentation Layer



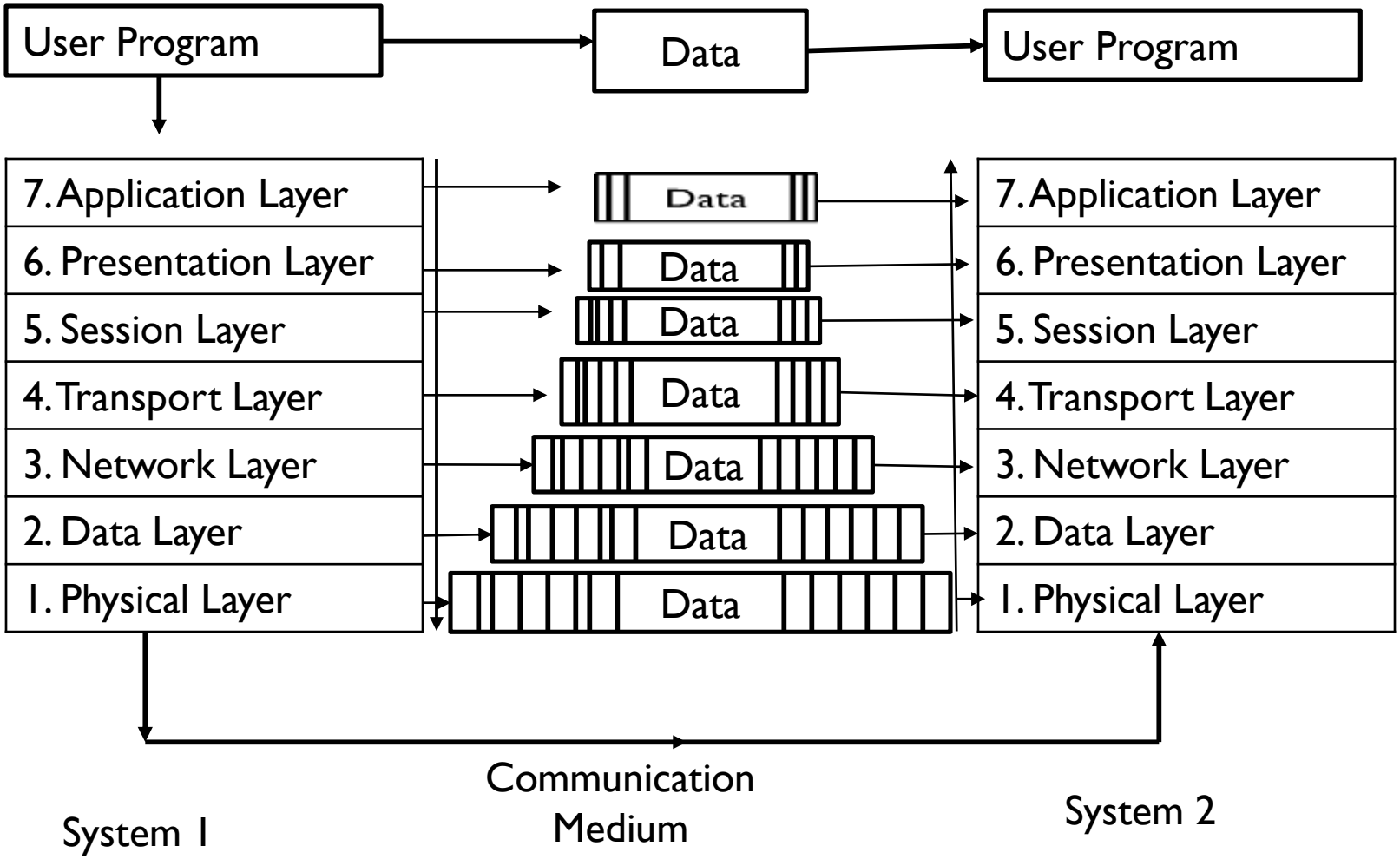
The Application Layer

- The application layer is used by end-user software such as web browsers and email clients
- It provides protocols that allow software to send and receive information and present meaningful data to users.
- Application layer interacts with application programs and is the highest level of OSI model.
- Application layer contains management functions to support distributed applications.
- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

Application Layer



OSI Layers model



Contribution of the OSI Reference Model

- Three concepts are central to the OSI model:
  - Services
  - Interfaces
  - Protocols
- Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicit.
- Each layer performs some services for the layer above it
- The service definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer's semantics.
- A layer's interface tells the process above it how to access it. It specifies what the parameters are and what result to expect, it, too, says nothing about how the layer works inside.
- Finally, the peer protocols used in a layer are the layer's own business. It can use any protocols it want to, as long as it gets the job done (i.e. provides the offered services). It can also change them at will without affecting software in higher layers.

The TCP/IP Reference Model

- The ARPANET was a research network sponsored by the DoD (U.S Department of Defence).
  - This architecture later became known as the TCP/IP reference Model
  - The TCP/IP is the set of communications protocols used for the internet and other similar networks.
  - TCP means Transmission Control Protocol and IP means Internet Protocol
- Furthermore, DoD needed a flexible architecture where applications ranging from transferring files to real-time speech transmission can implemented.

The TCP/IP Reference Model

- The TCP/IP specification defines four layers:
  - Application Layer
  - Transport Layer
  - Internet Layer
  - Host-to-Network (physical) Layer

The Application Layer

- This layer is comparable to the application, presentation and session layers of the OSI model all combined into one.
- It provides a way for applications to have access to networked services.
- It provides the ability to use both TCP and UDP protocols.
- Some of the protocols includes TELNET, FTP, SMTP, DNS, HTTP, Electronic Mail, World Wide Web

The Transport Layer

- This layer acts as the delivery service used by the application layer.
  - This layer also used both TCP and UDP protocols
  - Two transport protocols are defined:
    - Transmission Control Protocol (TCP): A reliable connection-oriented protocol that allows data originating on one machine to be delivered to the other machine in the network
    - User Datagram Protocol (UDP): An unreliable connectionless protocol for applications that don not want TCP sequencing or flow control and wish to provide their own.
    - The choice of protocol is made based on the application's transmission reliability requirements.
    - The transport layer also handles all error detection and recovery
    - It uses checksums, acknowledgement and timeouts to control transmissions

The Internet Layer

- This layer organize or handle the movement of data on the network.
- Permits host to inject packets into any network and have them travel independently to the destination.
- The main protocol used is the internet Protocol (IP)
- Its job is to deliver IP packets where they are supposed to go.

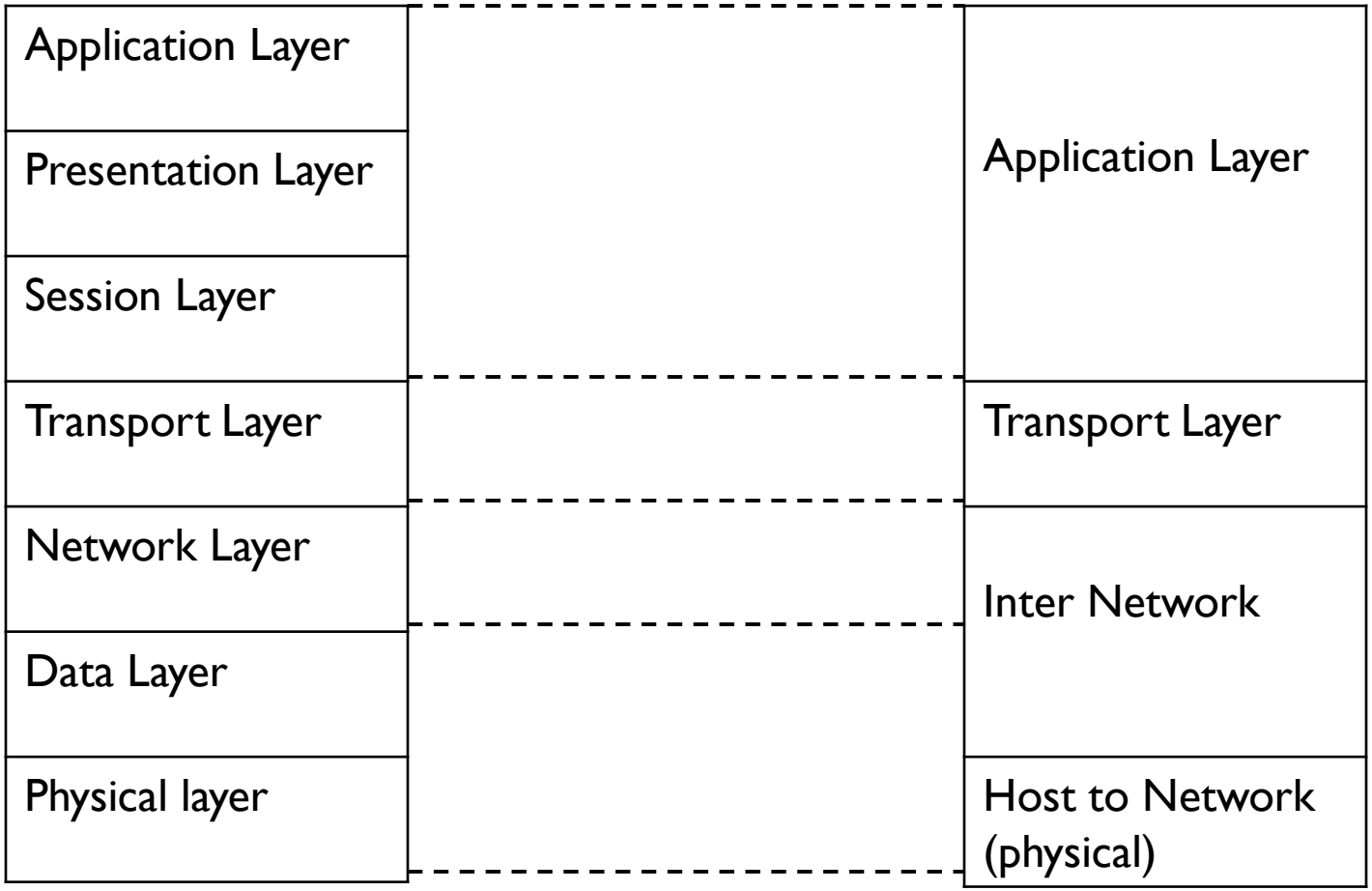
HOST-to-Network Layer

- This layer normally consists of devices drivers in the OS and the network interface card attached to the system.
- It takes care of the communication details on the media being used to transfer the data on the network.
- It consists of IP protocol, IP addresses and Network address translation
- Some of the famous protocols used at this layer include ARP(Address resolution protocol), PPP (Point to Point Protocol), etc.

A Comparison of the OSI and TCP/IP Reference Models

- The OSI and TCP/IP reference models have much in common
  - Both are based on the concept of a stack of independent protocols.
  - The functionality of the layers is roughly similar.
- The two models also have many differences.

OSI model Vs TCP/IP model



OSI vs TCP/IP

- An obvious difference between the two models is the number of layers: the OSI model has seven layers and the TCP/IP has four layers.
- Both has (inter) network, transport, and application layers, but the other layers are different.
- Another difference is in the area of connectionless versus connection-oriented communication.
  - The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer, where it counts (because the transport service is visible to the users).
  - The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer. Giving the users a choice. This choice is especially important for simple request-response protocols.

Introduction to the Internet and Web

Internet

- It is the largest network in the world that connects hundreds of thousands of individual networks all over the world.
- The popular term for the Internet is the “information highway”.
- Rather than moving through geographical space, it moves your ideas and information through cyberspace – the space of electronic movement of ideas and information.
- The basic protocol for internet is TCP/IP (Transmission Control Protocol/ Internet Protocol)

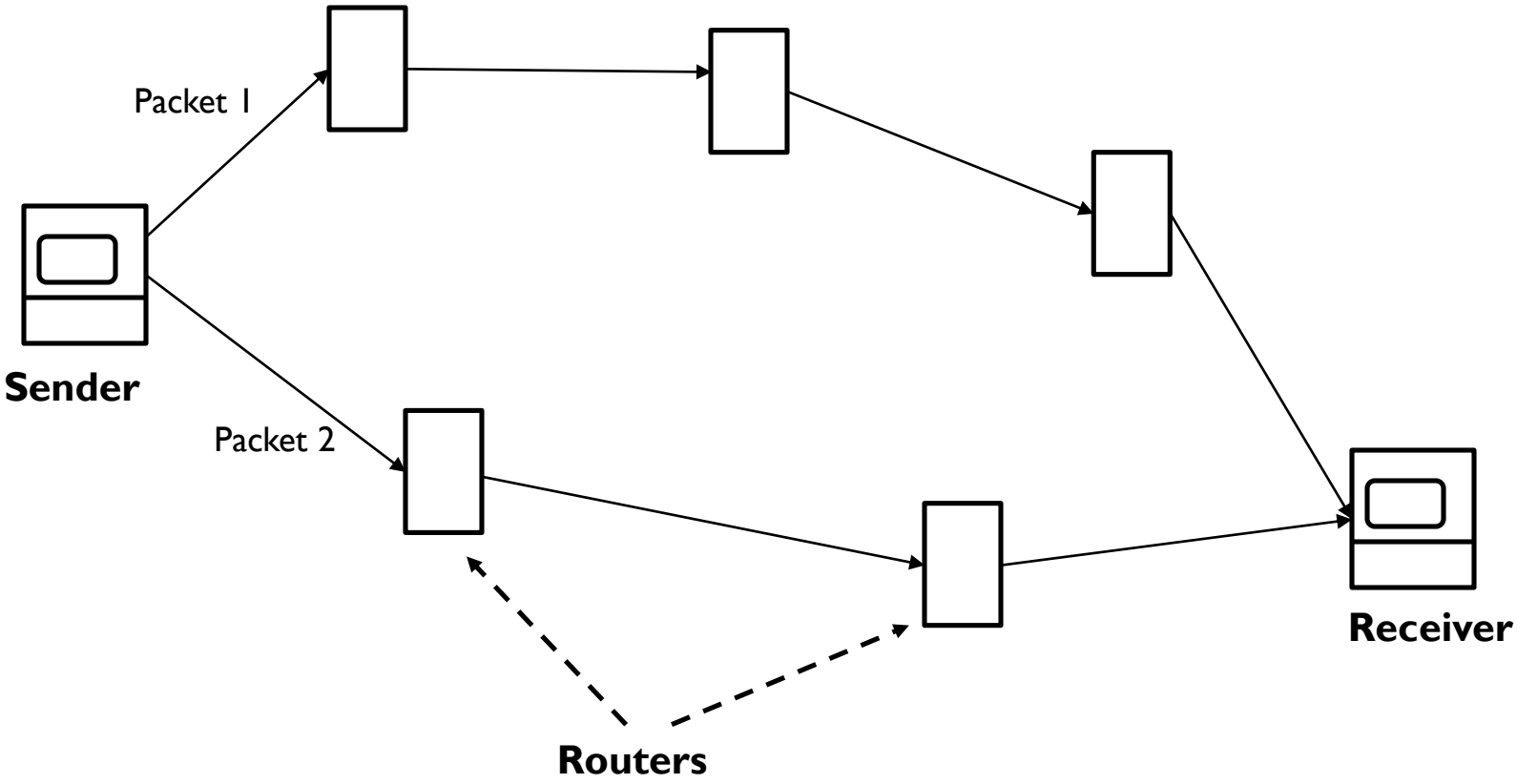
Internet Protocol (IP)

- OVERVIEW
- The IP protocol provides two main functionality:-
  - Decomposition of the initial information flow into packets of standardized size, and reassembling at the destination.
  - Routing of packet through successive networks, from the source machine to the destination identified by its IP address.
  - Transmitted packets are not guaranteed to be delivered (datagram protocol).
  - The IP protocol does not request for connection (connectionless) before sending data and does not make any error detection.

Functions

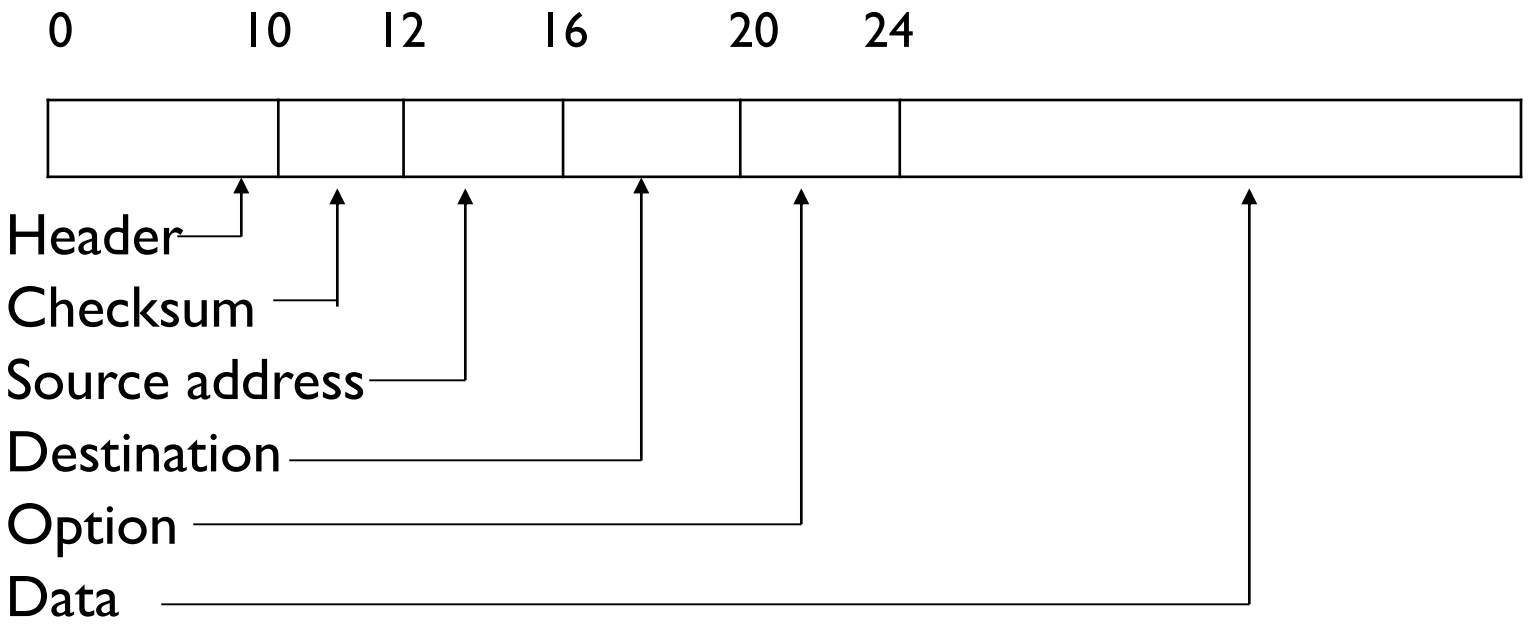
- Decompose the initial data (to be sent) into datagrams.
- Each datagram will have a header including, the IP address and the port number of the destination.
- Datagrams are then sent to selected gateways, e.g IP routers, connected at the same time to the local and to an IP service provider network.

- Datagrams are transferred from gateways to gateways until they arrived at their final destination



Structure of an IP Packet

- The fields at the beginning of the packet, called the frame header, define the IP protocol's functionality and limitations.
- 32 bits are located for encoding source and destination addresses (32 bits for each of these address fields)
- The remainder of the header (16 bits) encodes various information such ad the total packet can be a maximum of 64Kb long.



Transmission Control Protocol (TCP)

Overview

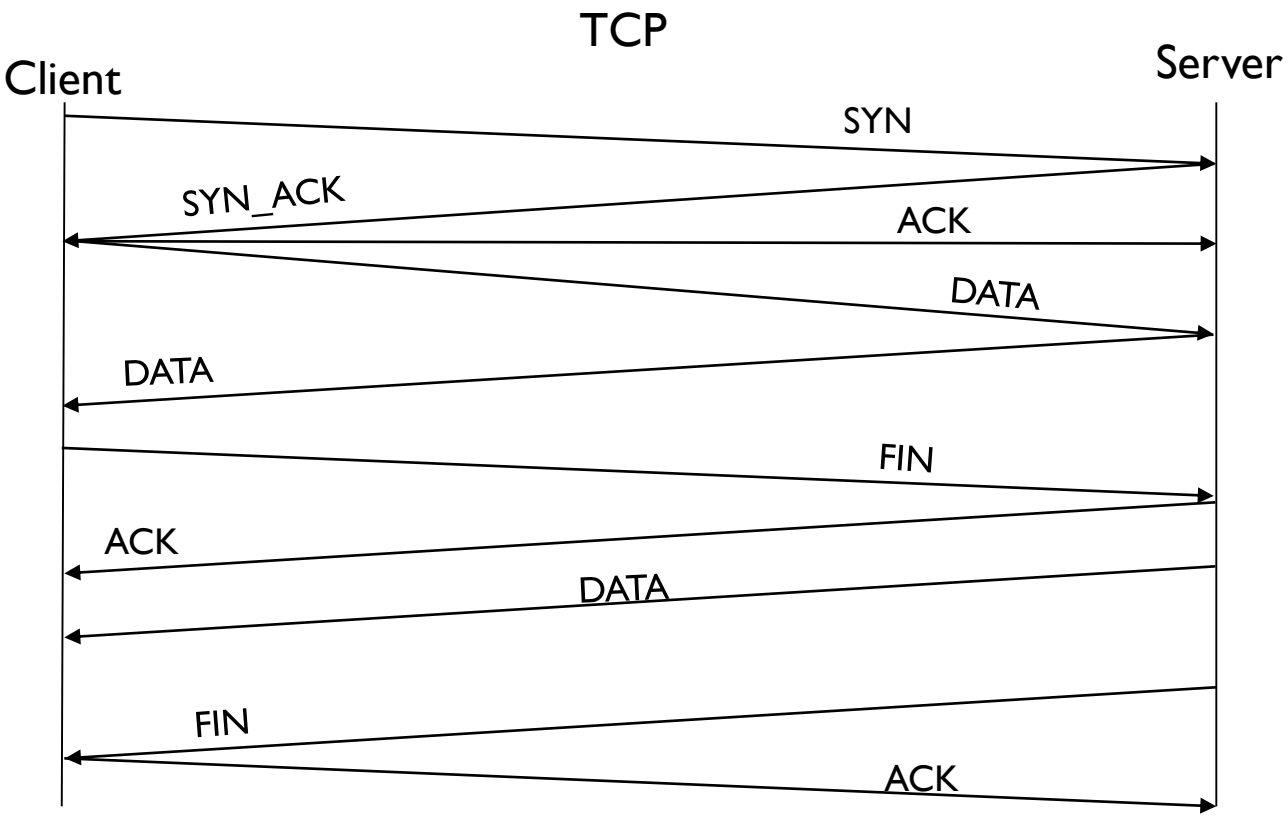
- TCP provides by using IP packets a basic service that does guarantee safe delivery:
  - Error detection
  - Safe data transmission
  - Assurance that data are received in the correct order

- Before sending data, TCP requires that the computers communicating establish a connection (*connection-oriented protocol*).

Transmission control protocol (TCP)

- TCP provides by using IP packets a basic service that does guarantee safe delivery:
- Error detection
- Safe data transmission
- Assurance that that are received in the correct order
- Before sending data, TCP requires that the computers communicating establish a connection (connection-oriented protocol)

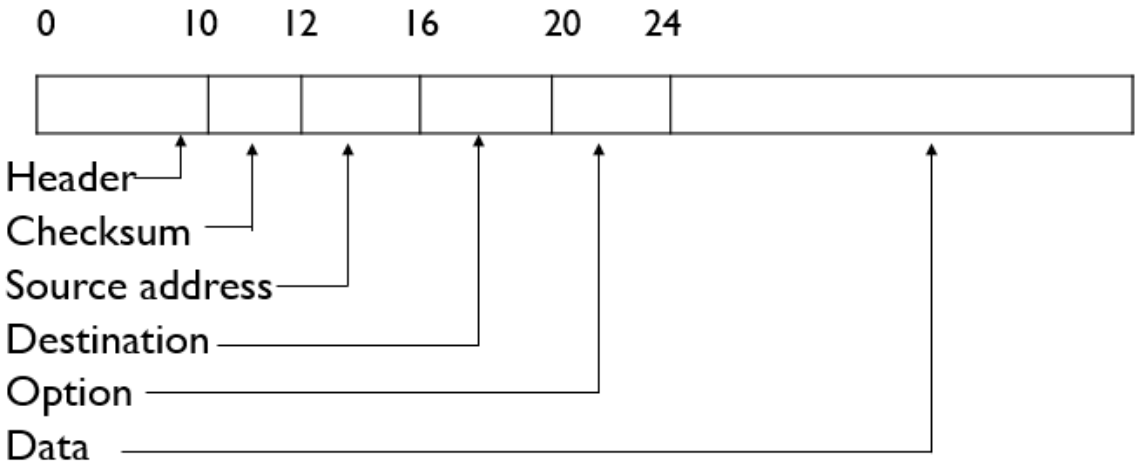
Transmission control protocol (TCP)



- TCP provides support for sending and receiving arbitrary amount
  data as one big stream of byte data (IP is limited to 64Kb).
- Packets are numbered, and reassembled on arrival, using sequence
  sequence acknowledge numbers.
- TCP also improves the capability of IP by specifying port numbers

➢ There are 65,536 different TCP ports (sockets) through which eve
  TCP/IP machine can talk.

Structure of a TCP packet



User Datagram protocol (UDP)

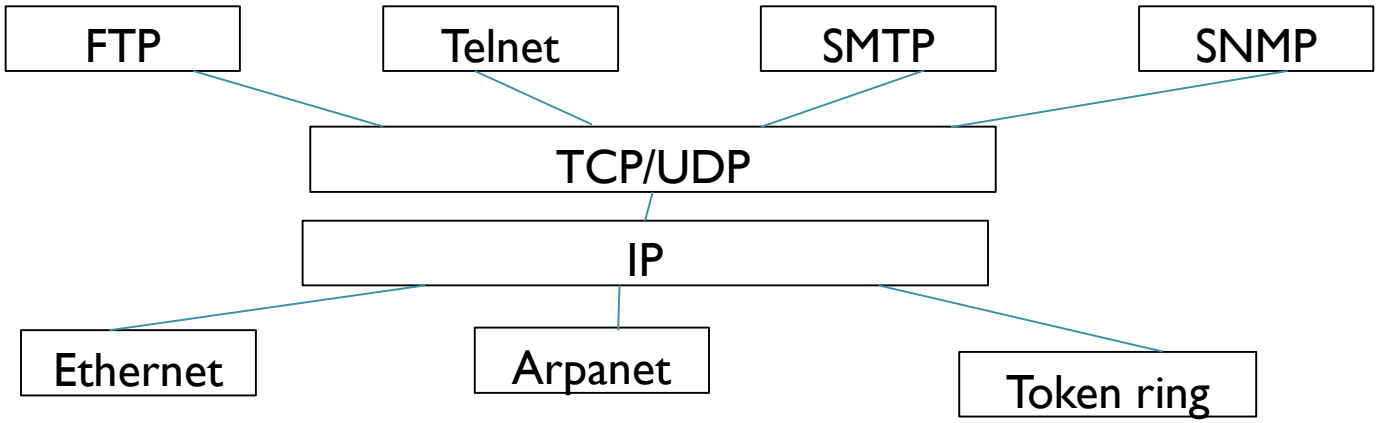
Overview

- Datagram protocol also built on top of IP.
- Has the same packet-size limit (64Kb) as IP, but allows for port number specification.
- Hence, every machine has two sets of 65,356 ports: one for TCP and the other for UDP.
- Connectionless protocol, without any error detection facility.
- Provides only support for data transmission from one end to the other, without any further verification.
- The main interest of UDP is that since it does not make further verification, it is very fast.
- Useful for sending small size data in a repetitive way such as time information.

Internet Application protocols

On top of TCP/IP, several services have been developed in order to homogenize applications of same nature:

- FTP (File Transfer Protocol) allows the transfer of collected to the internet.
- Telnet (Terminal Protocol) allows a user to connect to a remote host in terminal mode.
- NNTP (Network News Transfer Protocol) allows the constitution of communication groups (newsgroups) organized specific topics.
- SMTP (Simple Mail Transfer Protocol) defines a basic service for electronic mails.
- SNMP(Simple Network Management Protocol) allows the management of the network.



What is Web?

- The **Web (World Wide Web)** consists of information organized into Web pages containing text and graphic images.
- It contains hypertext links, or highlighted keywords and images that lead to related information.
- A collection of linked Web pages that has a common theme or focus is called a **Web site**.
- The main page that all of the pages on a particular Web site are organized around and link back to is called the site's **home page**.

Client/Server Structure of the Web

- Web is a collection of files that reside on computers, called **Web servers**, that are located all over the world and are connected to each other through the Internet.
- When you use your Internet connection to become part of the Web, your computer becomes a **Web client** in a worldwide client/server network.
- A **Web browser** is the software that you run on your computer to make it work as a web client.

Addresses on the Web IP Addressing

- Each computer on the internet does have a unique identification number, called an IP (Internet Protocol) address.
- The IP addressing system currently in use on the Internet uses a four-part number.
- Each part of the address is a number ranging from 0 to 255, and each part is separated from the previous part by period,
- For example, 106.29.242.17

IP Addressing

- The combination of the four IP address parts provides 4.2 billion possible addresses (256 x 256 x 256 x 256).
- This number seemed adequate until 1998.
- Members of various Internet task forces are working to develop an alternate addressing system that will accommodate the projected growth.
- However, all of their working solutions require extensive hardware and software changes throughout the Internet.

Domain Name Addressing

- Most web browsers do not use the IP address to locate Web sites and individual pages.
- They use domain name addressing.
- A **domain name** is a unique name associated with a specific IP address by a program that runs on an Internet host computer.
- This program, which coordinates the IP addresses and domain names for all computers attached to it, is called **DNS (Domain Name System) software**.
- The host computer that runs this software is called a **domain name server.**

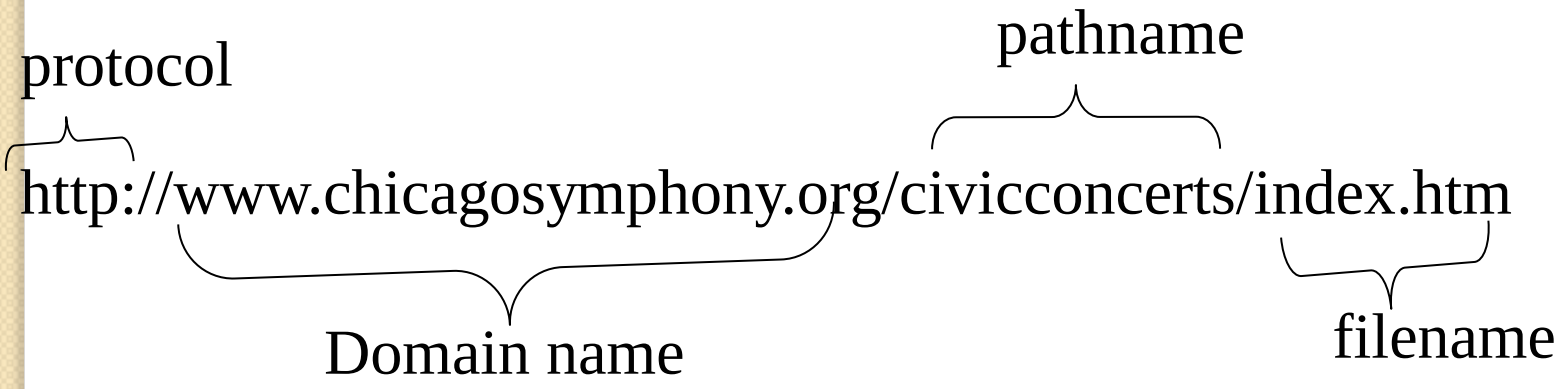
Domain Name Addressing

- Domain names can include any number of parts separated by periods, however most domain names currently in use have only three or four parts.
- Domain names follow hierarchical model that you can follow from top to bottom if you read the name from the right to the left.
- For example, the domain name gsb.uchicago.edu is the computer connected to the Internet at the Graduate School of Business (gsb), which is an academic unit of the University of Chicago (uchicago), which is an educational institution (edu).
- No other computer on the Internet has the same domain name.

Uniform Resource Locators

- The IP address and the domain name each identify a particular computer on the Internet.
- However, they do not indicate where a Web page's HTML document resides on that computer.
- To identify a Web pages exact location, Web browsers rely on Uniform Resource Locator (URL).
- URL is a four-part addressing scheme that tells the Web browser:
  - What transfer protocol to use for transporting the file
  - The domain name of the computer on which the file resides
  - The pathname of the folder or directory on the computer on which the file resides
  - The name of the file

Structure of a Uniform Resource Locators



http => Hypertext Transfer Protocol

HTTP

- The transfer protocol is the set of rules that the computers use to move files from one computer to another on the Internet.
- The most common transfer protocol used on the Internet is the Hypertext Transfer Protocol (HTTP).
- Two other protocols that you can use on the Internet are the File Transfer Protocol (FTP) and the Telnet Protocol

- Data Communication

Concept of Data Communication

- Data Communication consists of two words: Data and Communication
- Data can be any text, image, audio, video and multimedia files.
- Communication is an act of sending and receiving data.
- Data Communication refers to the exchange of data between two or more networked or connected devices
- These devices must be capable of sending and receiving data over a communication medium

DATA COMMUNICATION

- Computer is use to capture, process, store, generate and communicate data/ information.
- DC is the active process of transporting data/ information from one point to another
- Data communication can be on wired or wireless connectivity
- Effectiveness of data communication system depends on the following fundamental characteristics.
  - Delivery: The system must deliver data to the corrected destination
  - Accuracy: The system must deliver data accurately
  - Timeliness: The system must deliver data in a timely manner.

Standards Organisations for Data Communications

- International Standard Organization (ISO)
- International Telecommunications Union-Telecommunication Sector (ITU-T)
- Institute of Electrical and Electronics Engineers (IEEE)
- American National Standards Institute (ANSI)
- Electronics Industry Association (EIA)
- Telecommunications Industry Association (TIA)
- Internet Architecture Board (IAB)
- Internet Engineering Task Force (IETF)
- Internet Research Task Force (IRTF)

DATA COMMUNICATION COMPONENT

1) **Transmitter**: is the device that sends the message, it can be a computer, workstations, telephone e.t.c

2) **Receiver**: Is the device that receives the message. It can be a computer, workstation telephone e.t.c

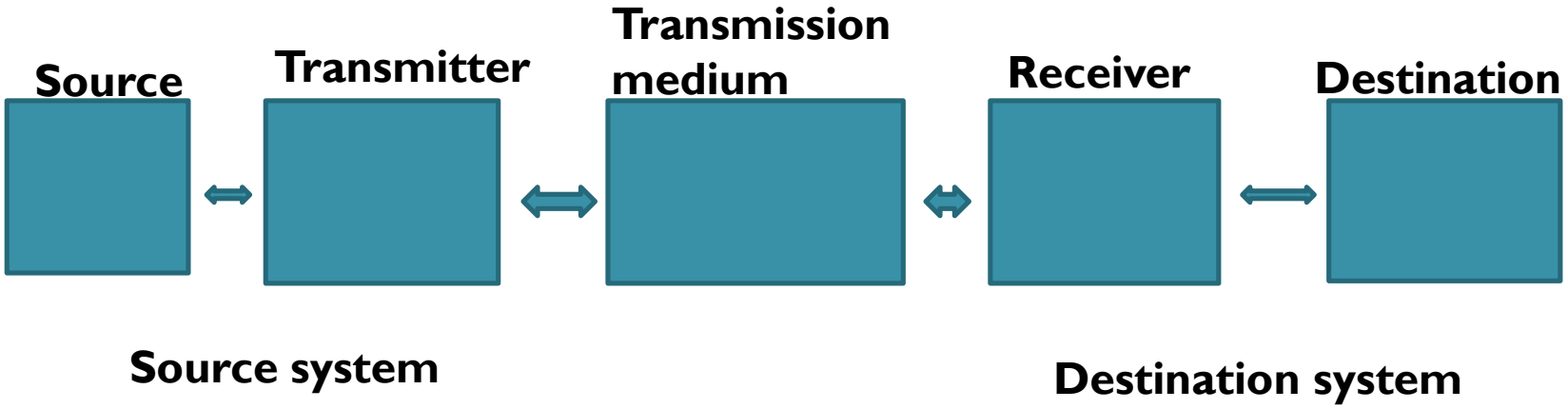
3) **Medium**: is the physical path by which a message travels from the sender to receiver through pair wire, coaxial cable, fiber-optic cable, radio waves etc

4 Message: is the transmission (data) to be communicated. It can be consist of text, number, picture, sound, video. etc

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

Data Communication Circuits

- Data communication circuit provides a transmission path between locations and transfers digital information from one station (node, where computers or other digital equipment are located) to another using electronic circuits.
- Data communications circuit utilize electronic communications equipment and facilities to interconnect digital computer equipment.



Data Communication Circuit

- Source: - This device generates the data to be transmitted; examples are mainframe computer, personal computer, workstation Mobile Station etc. The source equipment provides a means for humans to enter data into system.

- Transmitter: - A transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of transmission system. For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by the telephone network.

- Transmission medium: - The transmission medium carries the encoded signals from the transmitter to the receiver. Different types of transmission media include free-space radio transmission (wireless transmission) and physical facilities such as metallic and optical fiber cables.

Data Communication Circuits

- Receiver: - The receiver accepts the signal from the transmission medium and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

- Destination: - Takes the incoming data from the receiver and can be any kind of digital equipment like the source

Measuring Capacity of Communication Media

- In data communication, the transmission medium is known as Channel.
- The capacity of a channel is the maximum amount of signals or traffic that a channel can carry, it is measured in terms of bandwidth and data transfer rate.
- The bandwidth of a channel is the range of frequencies available for transmission of data through that channel
- The higher the bandwidth, the higher the data rate.
- Bandwidth is measured in Hertz. (1KHz = 1000 Hz

Measuring Capacity of Communication Media

- Data travels in the form of signals over a channel.
- Data signal carries one or two bits over the channel.
- Data transfer rate is the number of bits transmitted between source and destination in one second. It is measure in terms of bits per second (bps).
- 1 Kbps = 1024 bps, 1 Mbps = 1024 Kbps, 1 Gbps = 1024 Mbps, 1Tbps = 1024 Gbps

How to Calculate Data Transfer Rate Speed, Time and Data

- The main equation for solving data transfer rate, Speed and Time is given as: S = A ÷ T, in which A is the amount of data and T is the transfer time to solve for S, the speed, or rate, of transfer.
- For example, determine the speed or the rate of transfer of 25 megabyte in 2 min.
- S = ?
- A = 25Mb
- T = 2mins = 2*60 = 120 sec.
- S= 25mb /120 sec = 0.208 mbps
- 0.208mbps * 1024 = 212.9 Kbps.

How to Calculate Data Transfer Rate Speed, Time and Data

- For instance, you transferred 100 GB at a rate of 7 MB/s. Compute the Time required for the transfer.
- First, convert Gigabyte to Megabyte so you're working with the same units in every part of the equation. 100 x 1,024 = 102400.
- To solve for T = A/S = 102400/ 7= 14628.57. Therefore, it took 14628.57 sec. Now convert this to hours, divide by 3,600, which is 4.07.
- In other words, it took 4.06 hrs to transfer 100 GB at a rate of 7 MB/s.

Data Transfer Rate computation

- A user wants to upload a text document at the rate of 10 pages per 20 seconds. What will be the required data rate of the channel ?. Assume that 1 page contains 1600 characters and each character is of 8 bits.

Solution

Number of pages = 10

Number of characters per page = 1600

Number of bits per characters = 8

Total number of bits = 10*1600*8

Expected upload time = 20 seconds

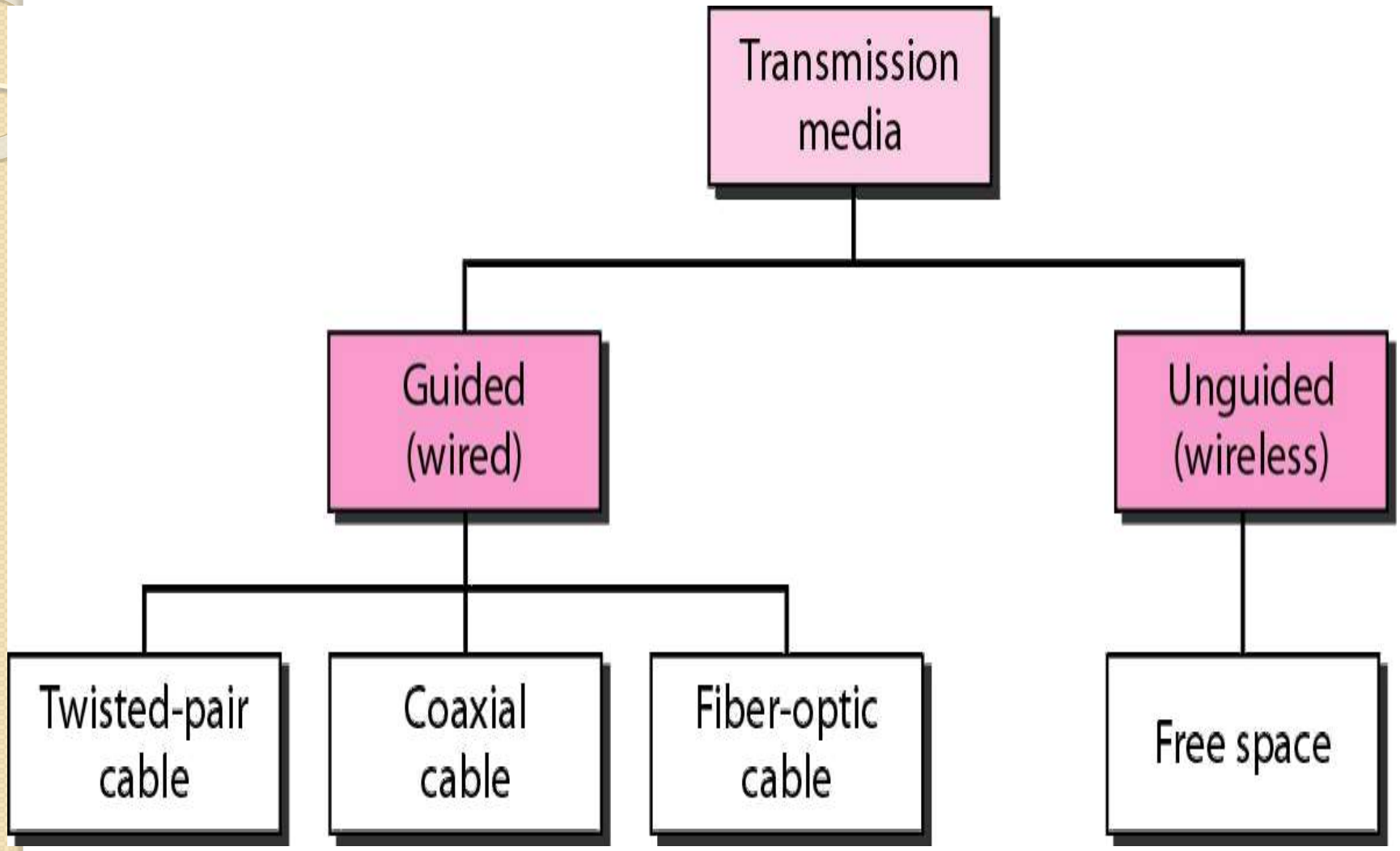
Required data rate = (10 * 1600 * 8)/20

= 6400bps = 6.25Kbps.

Communication/Transmission medium

- The transmission medium is the physical path between transmitter and receiver in a data transmission system.
- It is included in the physical layer of the OSI protocol hierarchy.
- Transmission media can be generally categorized as either unguided or guided,
- Guided Transmission Media uses a "cabling" system (or some sort of conductor) that guides the data signals along a specific path. Guided Media is also known as Bound Media.
- The data signals are bound by the "cabling" system. The conductor directs the signal propagating down it.
- Examples of guided transmission media are copper wire and optical fiber.

Communication/Transmission medium



Communication/Transmission medium

- Unguided Transmission Media is a means for data signals to travel without anything to guide them along a specific path.
- The data signals are not bound to a cabling media and as such are often called Unbound Media.
- Unguided transmission media are wireless systems.
- Signals propagating down an unguided transmission medium are available to anyone who has a device capable of receiving them.

Electromagnetic Waves

- A wave is a disturbance in a medium that carries energy without a net movement of particles.
- The two basic kinds of waves are longitudinal and transverse.
- With longitudinal waves, the displacement is parallel in the direction of propagation.
- Examples of longitudinal wares are earthquake, ultrasound, sound waves in air, etc.
- While Transverse waves, the displacement is perpendicular to the direction of propagation.
- examples of Transverse waves are electromagnetic waves, guitar string, etc.

Characteristics of Electromagnetic waves

- The three main characteristics are wave velocity, frequency and wavelength.
- Wave velocity is the distance travelled by a wave per unit time. it is the speed withwhich a disturbance of the particle propagates through a medium. Wave velocity is compute using the equation $V = f \lambda$.
- Frequency is the number of waves that pass a given point in one second. The frequency formula is given by $F = V/\lambda$.
- Wavelength is the distance between two successive crests or troughs of a wave. it is measured in the direction of the wave. Formula is $\lambda = V/f$

Computation for wavelength, frequency, and velocity

- A harmonic wave is moving along a rope. The source generating the waves completes 50 to and fro motions in 20 s. A trough travels 3m in 4s; determine the wavelength of the wave.

- Solution:
- Time taken for 50 oscillations = 20 s
- Time for 1 oscillation, t = 20/50= 0.4 s
- Frequency of 1 oscillation, f = 1/0.4 = 2.5 Hz
- The wave travels a distance of 3m in 4s.
- The wave speed is calculated by v = 3 / 4 = 0.75 ms-1
- The wavelength formula is given by $\lambda = v / f = 0.75/2.5$
- $\lambda = 0.3$ m.

Computation for wavelength, frequency, and velocity

- 1) A wave has frequency of 50 Hz and a wavelength of 10 m. What is the speed of the wave?
- Solution:
- f = 50 Hz, λ =10 m
- V = ?
- V = f * λ = 50Hz * 10 m = 500 m/s

- 2) A wave has wavelength of 10 m and a speed of 340 m/s. What is the
- frequency of the wave?
- Solution:
- λ = 10 m, V = 340 m/s
- F = ? □ □ □
- F = V/ λ = 340 m/s / 10m = 34 Hz

COMMUNICATION MEDIA

- The major communication media are:

1) **Wire Pairs**:- Wire pairs are commonly used in local telephone communication and for short distance digital data communication. They are usually made up of copper. The data transmission speed is normally 9600 bits per second in a distance of 100 meters.

2) **Twisted Pair:-** Is the most widely used medium for telecommunication, it consist of copper wires that are twisted into pairs. The use of two wires twisted together helps to reduce cross talk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 10 million bits per second. Twisted pair can be unshielded twisted pair (UTP) and shielded twisted pair (STP)

COMMUNICATION MEDIA Continuation

3) Coaxial Cable:- is widely used for cable television system, office building for local area networks. The cables consist of coppers or aluminum wire wrapped with insulating layer of a flexible material with a high dielectric constant, all of which are surrounded by a conductive layer. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per seconds.

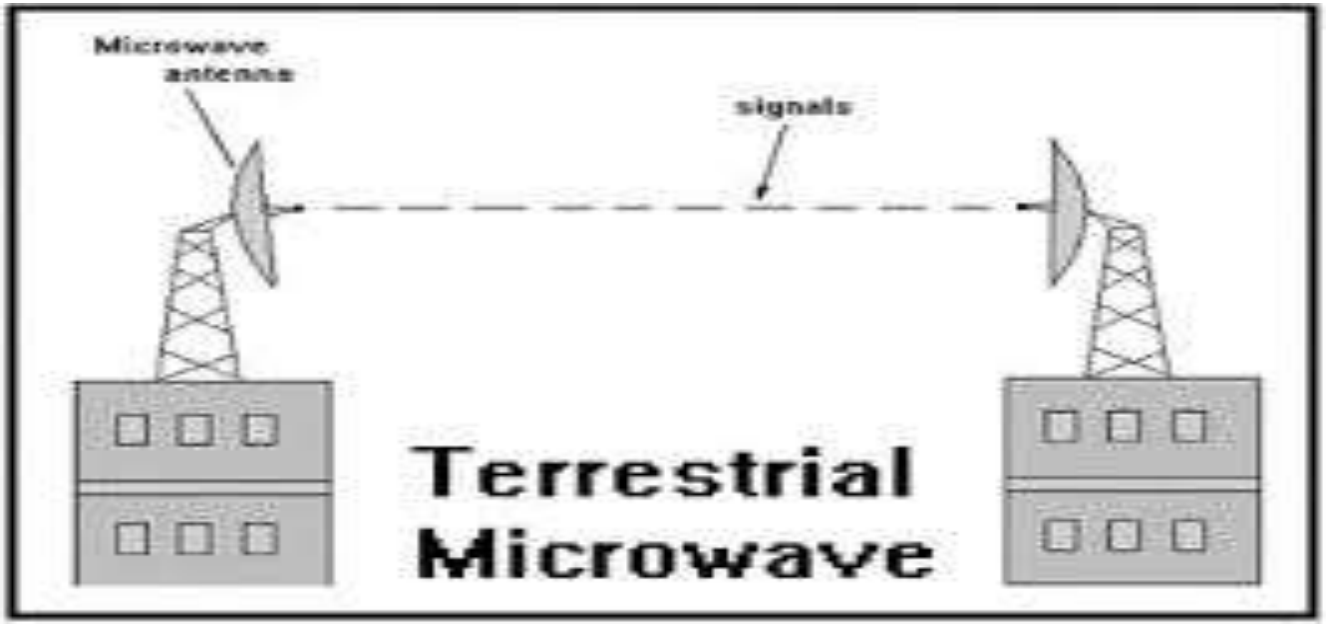
4) Optical Fiber:- It consist of one or more filaments of glass fiber wrapped in protective layers that carries data by means of pulses of light which can travel over extended distances. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed may reach trillions of bits per second.

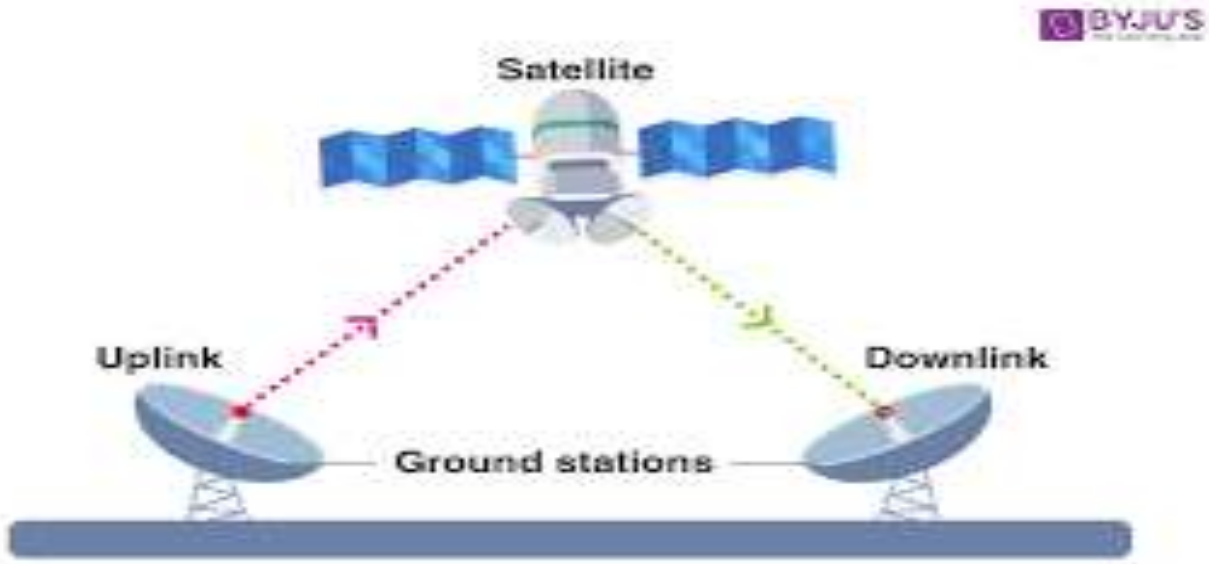
COMMUNICATION MEDIA Continuation

5) Wireless Technology

(a) **Terrestrial Microwave:-** It use earth based transmitter and receiver. It use low giga hertz range, which limits all communications to line-of-sight. Path between relay station spaced approximately 48km apart. Microwave antennas are usually placed on top of buildings towers, hills and mountain peaks.

(b) **Communication Satellites:-** The satellites use microwave radio signal as their medium for transmission which are not deflected by the earth's atmosphere. The satellites are stationed in space, typically 35,400km above the equator. They are capable of recovering and relaying voice data to signal


Microwave antenna
signals
Terrestrial Microwave


BYJU'S
Satellite
Uplink
Downlink
Ground stations

Wireless Technologies

- Bluetooth – is a short-range wireless technology that can be used to connect mobile-phones, mouse, headphones, keyboards, computer, etc wirelessly over a short distance.
- All Bluetooth-enabled devices have a low cost transceiver chip.
- The chip uses the unlicensed frequency band of 2,4 Ghz to transmit and receive data.
- These devices can send data within a range of 10 meters with a speed of 1-2 Mbps.

Wireless Technologies

- Wireless LAN – it is a local area network and it is a popular way to connect to the internet.
- The wireless LAN is number as 802.11 by IEEE and it is popularly known as wi-fi.
- These networks consist of communicating devices such as laptops, mobile phones, etc and network device called Access points (APs).
- An Access point is a device that is used to create a wireless local area network, by connecting to a wired router, switch or hub.
- The wi-fi gives users the flexibility to move around within the network area while being connected to the network,

TYPES OF COMMUNICATION SERVICES

- The general classes of communication carries service for both voice and data are:

(1) Narrowband is a limited-capacity communication type that uses a narrow range (or band) of frequencies to transmit information. Narrowband is commonly used in radio communication, emergency services, and internet connections. This communication type utilizes limited bandwidth, making transmitting information over long distances easier. It handles moderate data transmission volumes between 300 and 9600 band. Example are line printer, telephone voice, etc.

(2) Broadband- handles very large volumes of data . Data transmission rates are in millions or more. Examples are high-speed data analysis and satellite communication. Broadband refers to various high-capacity transmission technologies that transmit data, voice, and video across long distances and at high speeds. Common mediums of transmission include coaxial cables, fiber optic cables, and radio waves.

Serial and Parallel Data Transmission

- There are two methods of transmitting digital data namely parallel and serial transmissions.
- In parallel data transmission, all bits of the binary data are transmitted simultaneously.
- For example, to transmit an 8-bit binary number in parallel from one unit to another, eight transmission lines are required.
- Each bit requires its own separate data path. All bits of a word are transmitted at the same time.
- This method of transmission can move a significant amount of data in a given period of time.
- Its disadvantage is the large number of interconnecting cables between the two units.
- For large binary words, cabling becomes complex and expensive.
- This is particularly true if the distance between the two units is great. Long multiwire cables are not only expensive, but also require special interfacing to minimize noise and distortion problems.
- Parallel communication is used for short-distance data communications and within a computer,

Serial and Parallel Data Transmission

- Serial data transmission is the process of transmitting binary words a bit at a time.
- Since the bits time-share the transmission medium, only one interconnecting lead is required.
- While serial data transmission is much simpler and less expensive because of the use of a single interconnecting line, it is a very slow method of data transmission.
- Serial data transmission is useful in systems where high speed is not a requirement.
- Serial transmission is used for long-distance data communications

Classification of transmission waves and their properties

Transmission Wave	Properties
Radio waves	1. waves of frequency range 3KHz – 1 GHz 2. Omni-directional, these waves can move in all directions 3. Radio waves of frequency 300KHz -30 MHz can travel long distance. 4. Susceptible to interference 5. Radio waves of frequency -300KHz-30MHz can penetrate walls 6. These waves are used in AM and FM radio, television, etc
Microwaves	1. Electromagnetic waves of frequency range 1 GH-300GH2' 2. Unidirectional can move in one direction. 3 Cannot penetrate solid objects such as walls, hills or mountains. 4. Need line – of – sight propagation ie both communicating antenna must be in the direction of each other. 5. Used in point –to-point communication or unicast communication such as radar and satellite 6. Provide many large information- carrying capacity.
Infrared waves	1. Electromagnetic waves of frequency range in 300GHz-400THz. 2. Very high frequency waves 3. Cannot penetrate solid object such as waves. 4. Used for short – distance point to- point communication such as mobile-to-mobile, mobile-to-printer, remote-control-to- TV ., Bluetooth to enable devices to other devoces like mouse, keyboard,etc.

COMMUNICATION DEVICES

MODEM

- A modem (modulator – Demodulator) is a device that modulates an analog carrier signal to encode digital information and also demodulates such a carrier signal to decode the transmitted information
- A modem modulates outgoing digital signals from a computer as other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it into a digital signal for the digital device.
- Speed of modem are 2400 bits per second modem,14.4kbps, 28.8kbps, 56kbps, 12.8kbps

Mobile Telecommunication Technologies

- Today, the mobile phone network is the most used network in the world.
- It has the ability to be connected to the network on-the-go, which makes it very convenient to communicate with people via call or instant messages.
- It is handy to access the internet using the mobile phone network through wireless connection.
- The architecture of the mobile network has rapidly evolved, it is classified in generation, such as 1G, 2G, 3G, 4G and 5G.

First Generation (1G)

- The first generation (1G) mobile network system came around 1982.
- It was used to transmit only voice calls.
- The analog signals were used to carry voices between the caller and receiver,

Second Generation (2G)

- The second generation mobile network system came around 1991.
- Digital signals are used to carry voice calls, hence improved call quality.
- Enhance security as the signals can be encrypted
- It also enabled an additional service to send SMS and MMS (Multimedia messages)

Third Generation (3G)

- The third generation mobile network technology was developed around late 1990, but it was commercially used around 2000.
- It offered both digital voice and data services, and provided internet access.
- It facilitated greater voice and data capacity, with significantly faster data transfer speed.

Fourth Generation (4G)

- It provided faster data and voice services than the 3G.
- It revolutionised the telecommunication industry by bringing the wireless experience.
- It supported interactive multimedia, voice, video, wireless internet and other broadband services.

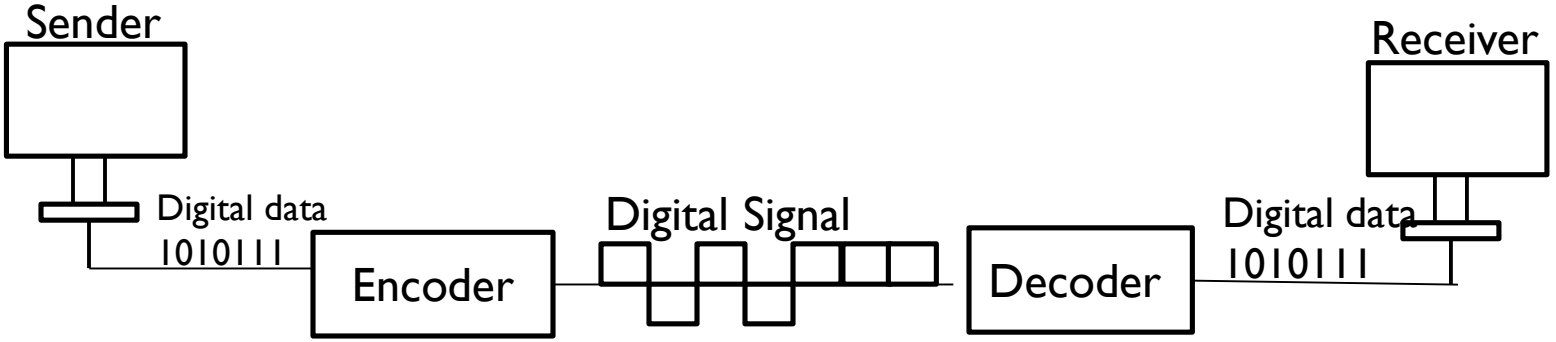
Fifth Generation (5G)

- The fifth generation (5G) is currently under development and implementation.
- It is expected to be a milestone development for the success of IoT and Machine to Machine (M2M) communications.
- Machine to Machine (M2M) is direct communication between devices – wired or wireless.
- 5G is expected to allow data transfer in Gbps, Tbps which is much faster than 4G.

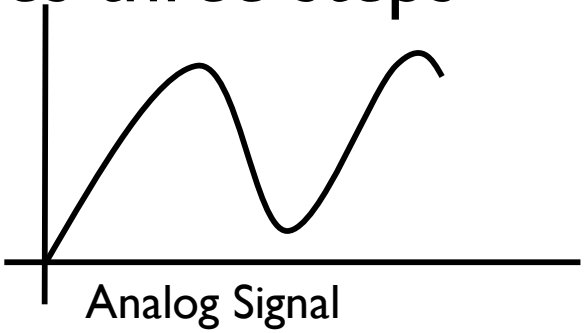
Data Transmission

- General Data or information can be stored in analog or digital format.
- For a computer to use the data/information, it must be in discrete digital form.
- Similar, signals can be in analog and digital form.
- To transmit digital data, it must be converted into digital signals.
- Digital data can be converted into digital signals in two ways: line coding and block coding.
- Note that for all communications, line coding is necessary where as block coding is optional
- Digital data are represent in binary format of 1s and 0s. While digital signals are represented in voltage level.

Data Transmission Cont……

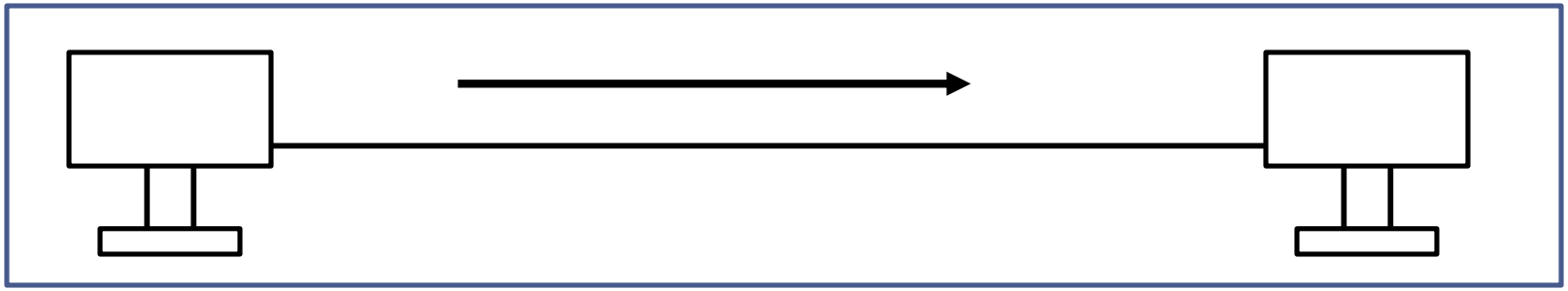


- Block coding is used to ensure accuracy of the data transmitted, this is achieved by using redundant bits.
- Analog data is a continuous stream of data in the wave form where as digital data is discrete.
- Analog data can be converted into digital data using pulse code modulation (PCM)
- This conversion involves three steps
  - Sampling
  - Quantization
  - Encoding

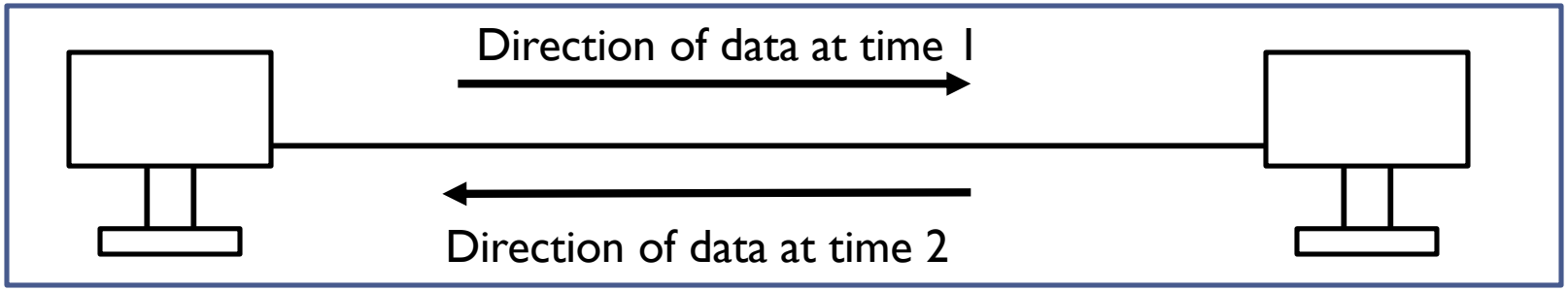


Data Flow

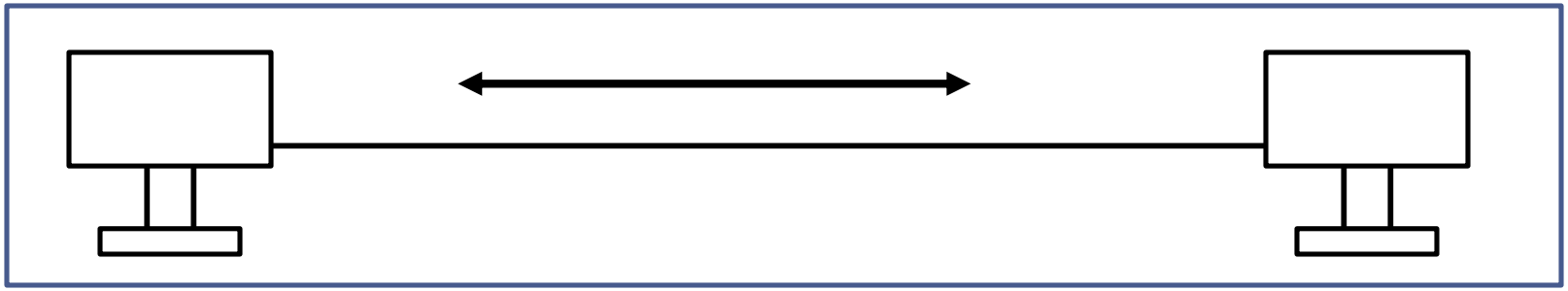
Simplex



Half duplex



Full Duplex



Data Flows

- Simplex communication – it is a one way or unidirectional communication between two devices, in which one device is sender and other is receiver. Devices use the entire capacity of the link to transmit the data. Example printer, keyboard, speaker, etc.
- Half-duplex communication- it is two way or bidirectional communication between two devices, in which both the devices can send and receive data or control signals in both directions, but not at the same time. While one device is sending data, the other one will receive and vice-versa. Example is walkie-talkie

Data Flows

- Full-duplex communication – it is two way or bidirectional communication in which both devices can send and receive data simultaneously. Example is mobile phones and landline telephones, etc.

- Multiplexing

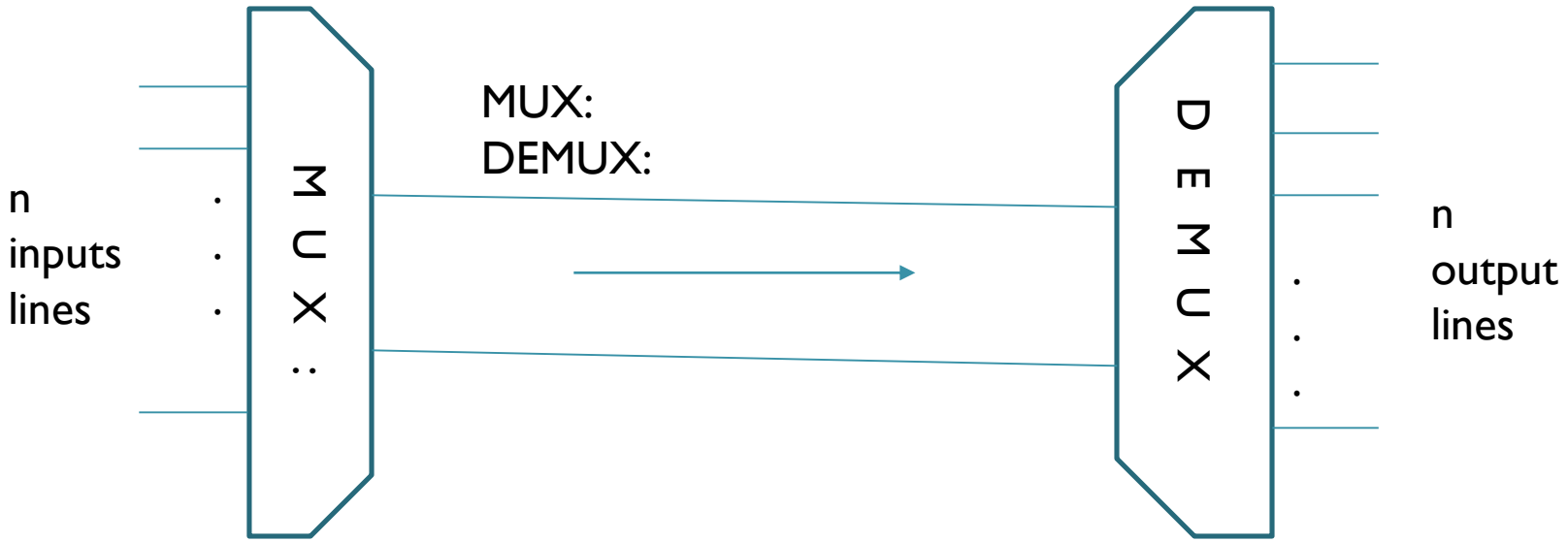
Multiplexing

- A single cable or radio link can handle multiple signals simultaneously using a technique known as multiplexing. Multiplexing permits hundreds or even thousands of signals to be combined and transmitted over a single medium.
- It is the set of techniques that allows the simultaneous transmission of multiple data or signals across a single communication medium or link.
- Is the process of making the most effective and efficient use of the available communication channel capacity to transmit individual signals or share among a number of communicating stations.
- The channel in this context could be a transmission line, e.g. a twisted pair or co-axial cable, a radio system or a fibre optic system etc
- Bandwidth utilization is the wise use of available bandwidth to achieved efficiency in data communications

Multiplexing

- Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.
- Multiplexing is done using a device called multiplexer (Mux) that combine input lines to generate one output line i.e (Many to one).
- At the receiving end a device called demultiplexer (DEMUX) is used to separate signal into its component Signal i.e. (one to many)
- Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium and identifies each and send to different receivers

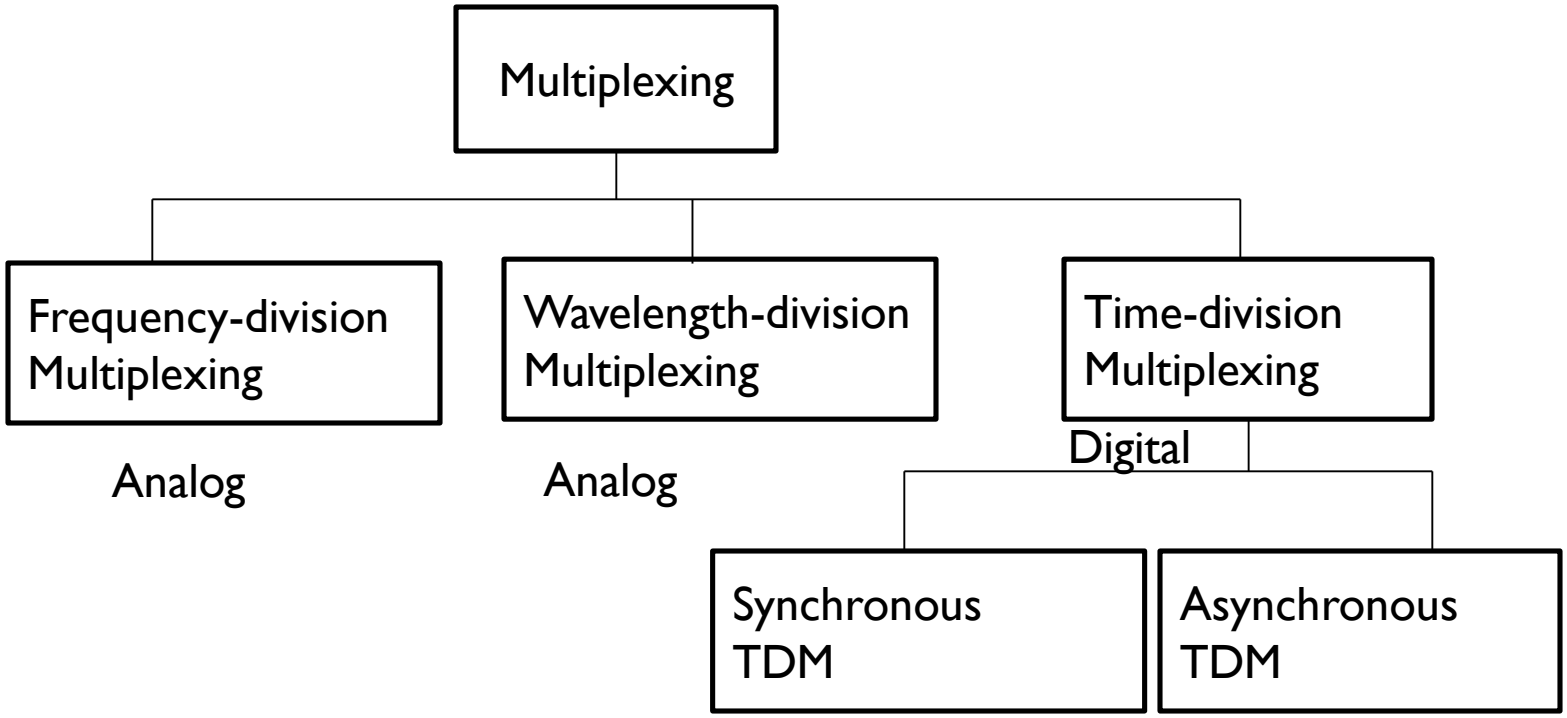
Multiplexing



Advantages of multiplexing

- More than one signals can be sent over single medium or link.
- Effective use of the bandwidth of medium.

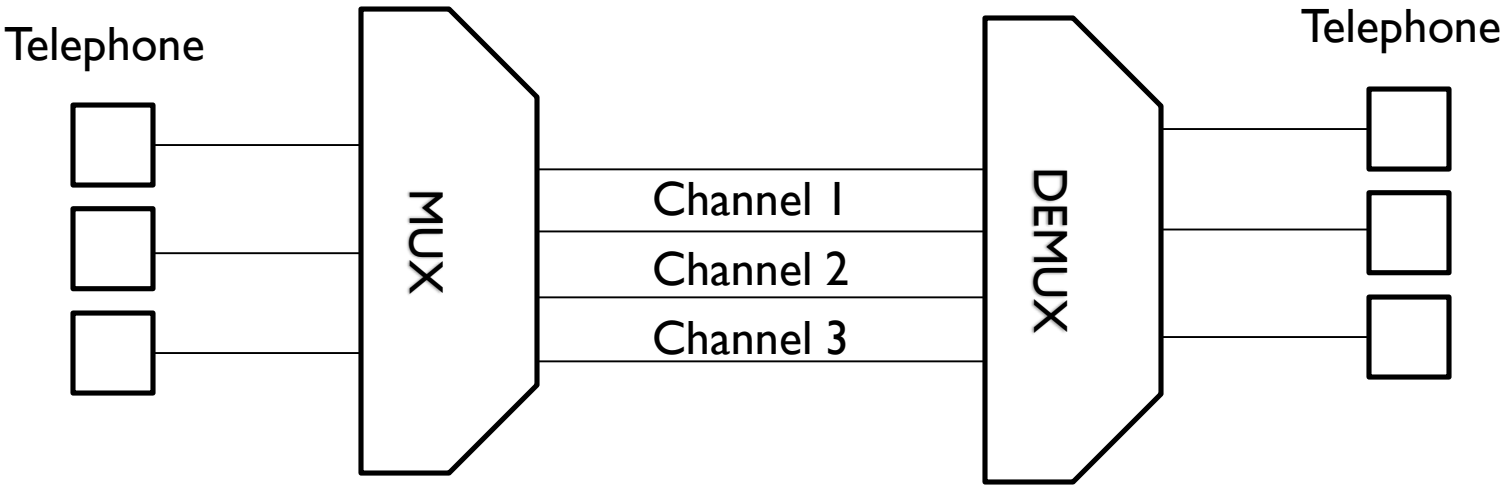
Types of Multiplexing



Frequency Division Multiplexing

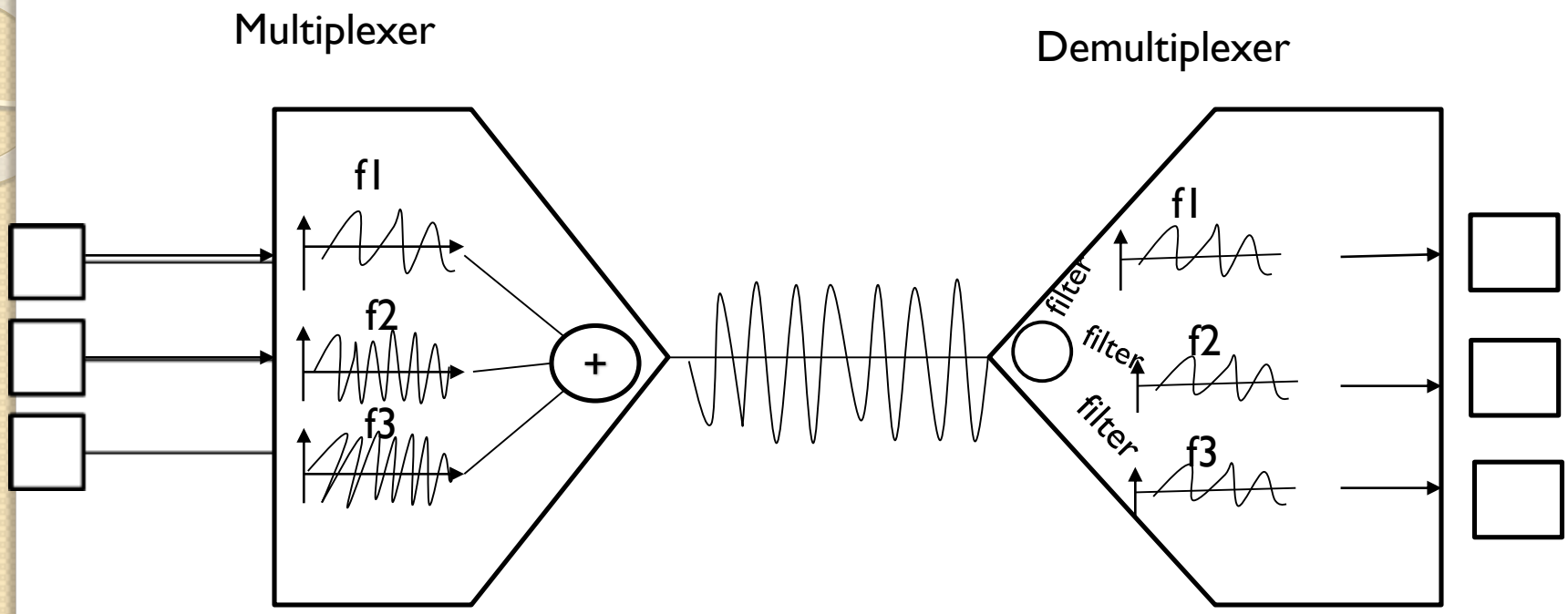
- It is an analog techniques.
- Signals of different frequencies are combine into a composite signal and is transmitted through a single link.
- Bandwidth of the link should be greater than the combined bandwidth of the various channels.
- Each signal is having different frequency.
- Channels are separated by the strips of unused bandwidth called Guard Bands (to prevent overlapping)

Frequency Division Multiplexing



Application for FDM

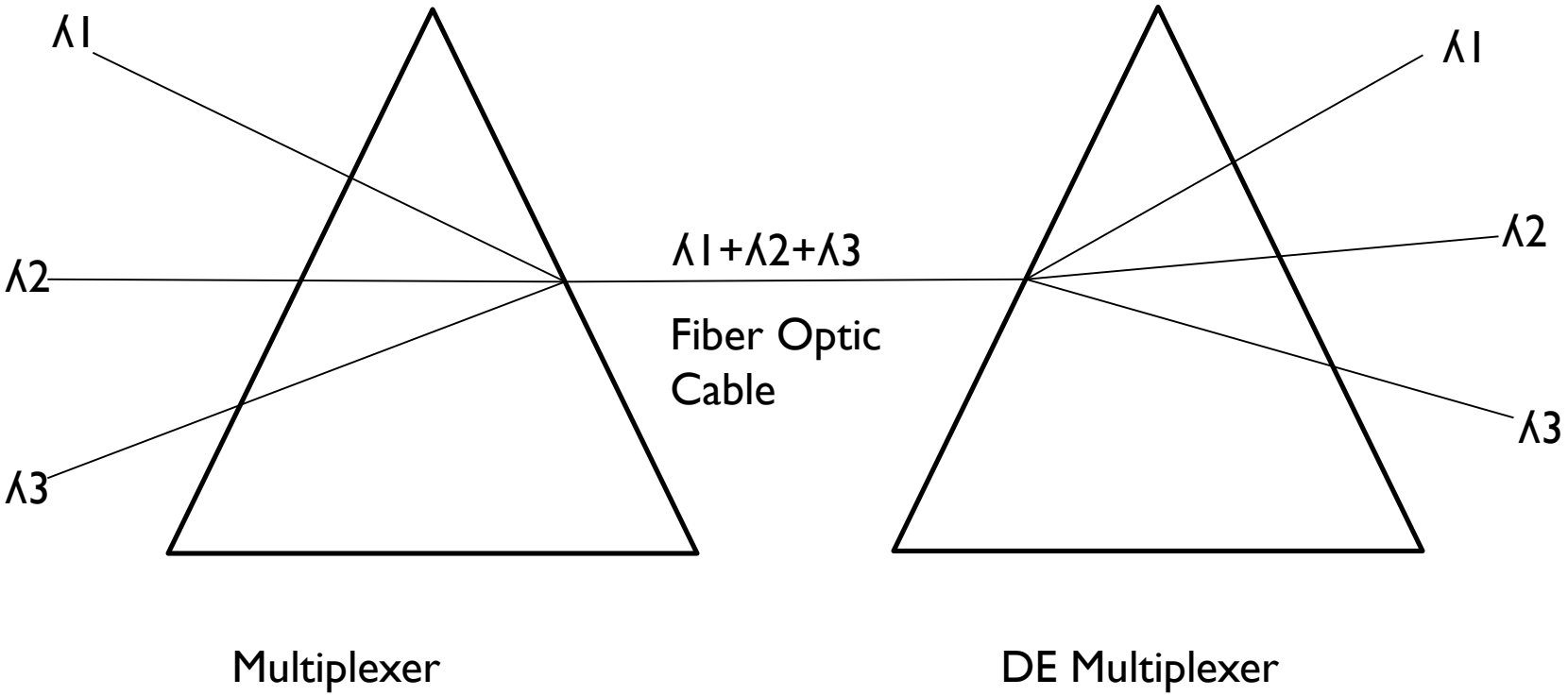
- FDM is used for FM and AM radio Broadcasting
- AM frequency is 530 to 1700 KHZ
- FM frequency is 88 to 108 MHZ
- FDM is used in television broadcasting.
- First generation cellular telephone also used FDM


Multiplexer
Demultiplexer
f1
f2
f3
+
filter
filter
filter
f1
f2
f3

Wave Division Multiplexing

- WDM is an analogue multiplexing technology.
- Working is same as FDM
- In WDM different signals are optical or light signals that are transmitted through optical fiber.
- Various light wires from different sources are combined to form a composite light signal that is transmitted across the channel to the receiver.
- At the received end, this composite light signal is broken into different light waves by demultiplex.
- This combination and the splitting of light waves is done by using a PRISM. Prism bends beam of the light based on the angle of incidence and the frequency of light wave.

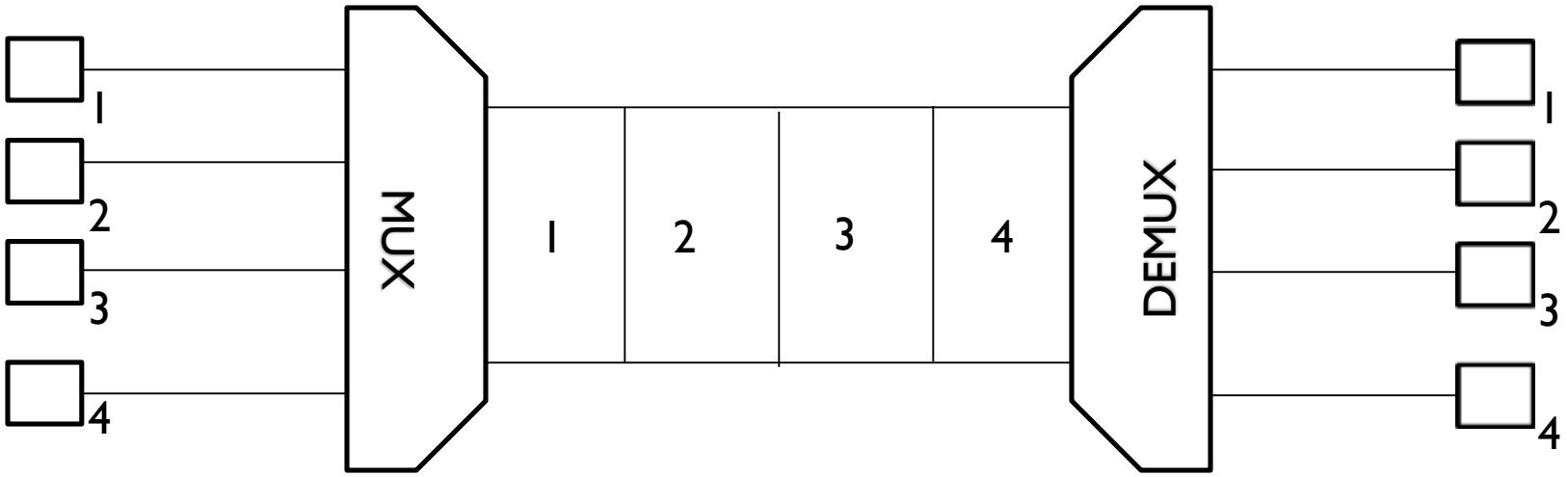
Wave Division Multiplexing



Time Division Multiplexing

- It is the digital multiplexing technique
- Channel or link is divided on the basis of time.
- Total time available in the channel is divided between several users.
- Each user is allotted a particular time interval called time slot or slice.
- In TDM the data rate capacity of the transmission medium should be greater than the data rate required by sending and receiving devices.

Time Division Multiplexing



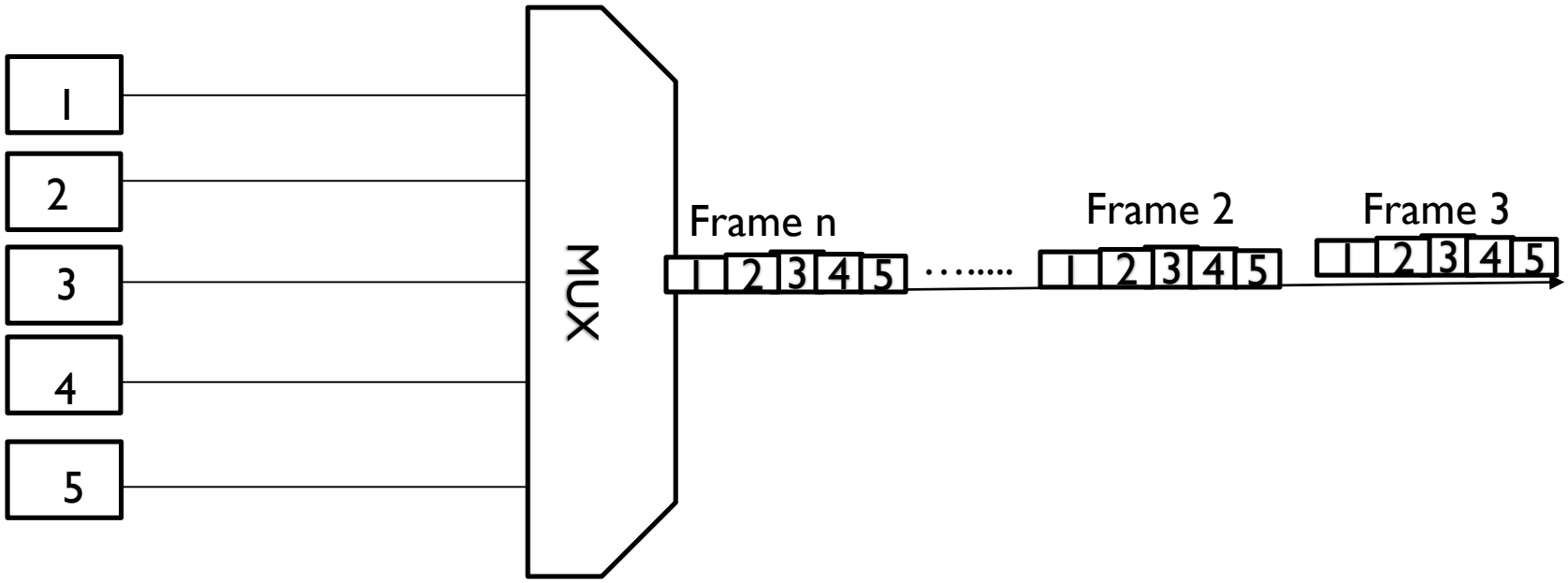
Types of TDM

- Synchronous TDM
- Asynchronous TDM

Synchronous TDM

- Each device is given same time slot to transmit the data over the link, whether the device has any data to transmit or not.
- Each device places its data onto the link when its time slot arrives, each device is given the possession of line turn by turn.
- If any device does not have data to send then its time slot remain empty.
- Time slots are organised into frames and each frame consists of one or more time slots.
- If there are in sending devices there will be n slots in frame.

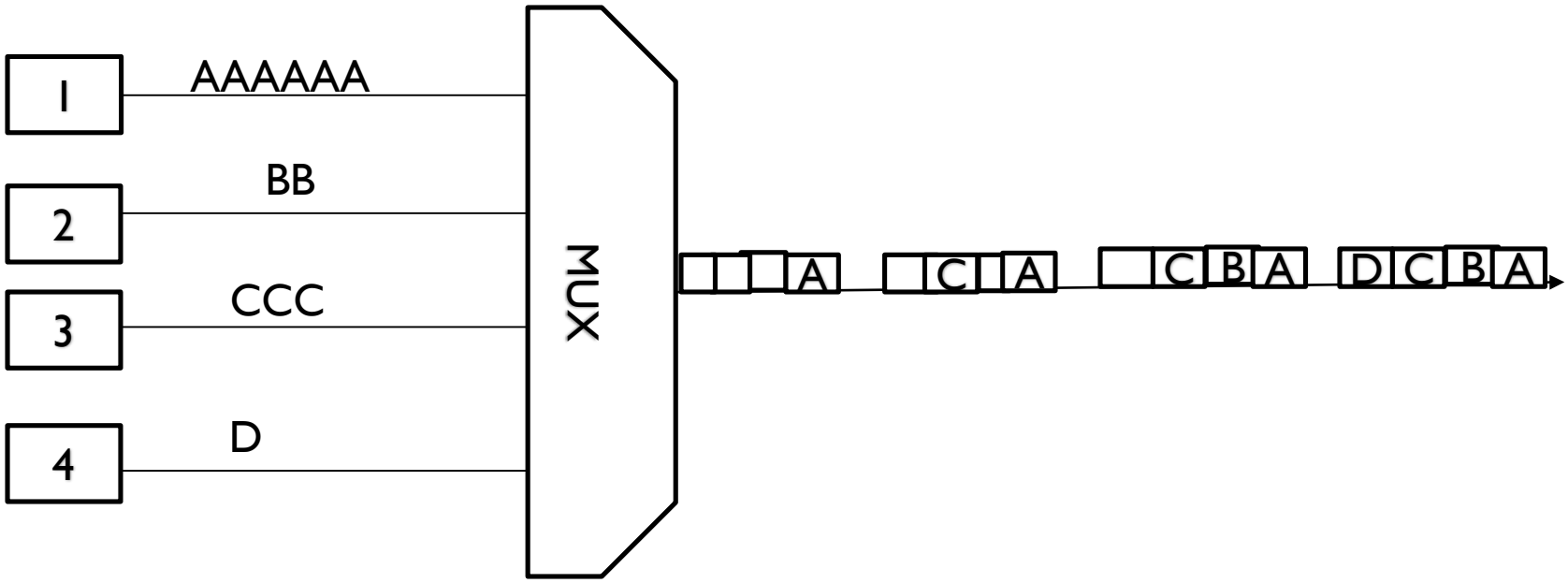
Synchronous TDM



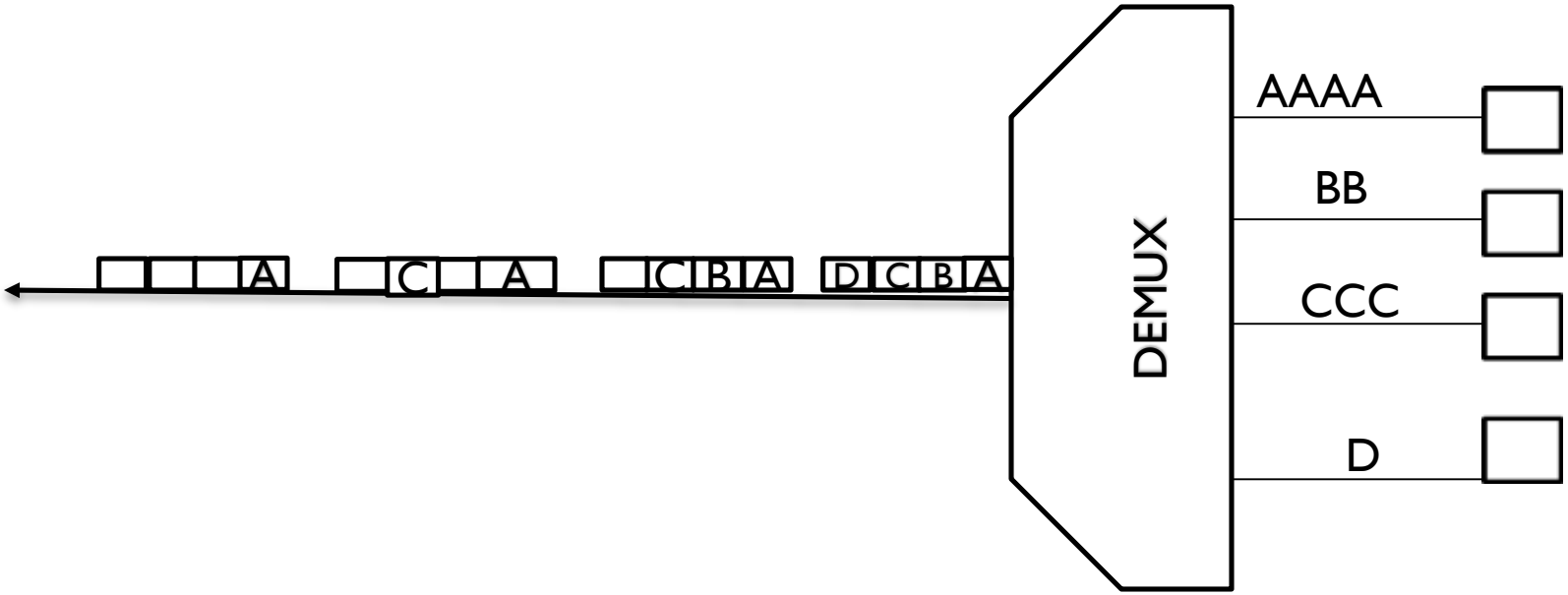
Multiplexing Process in STDM

- In STDM every device is given opportunity to transmit a specific amount of data onto the link.
- Each device gets its turn in fixed under and for fixed amount of time called interleaving.
- Interleaving is done by a character (one byte)
- Each frame consist of four slots as there are four input devices.
- Slots of some devices go empty of they do not have any data to send.

TDM Multiplexing



TDM Demultiplexing



DISADVANTAGE OF STDM

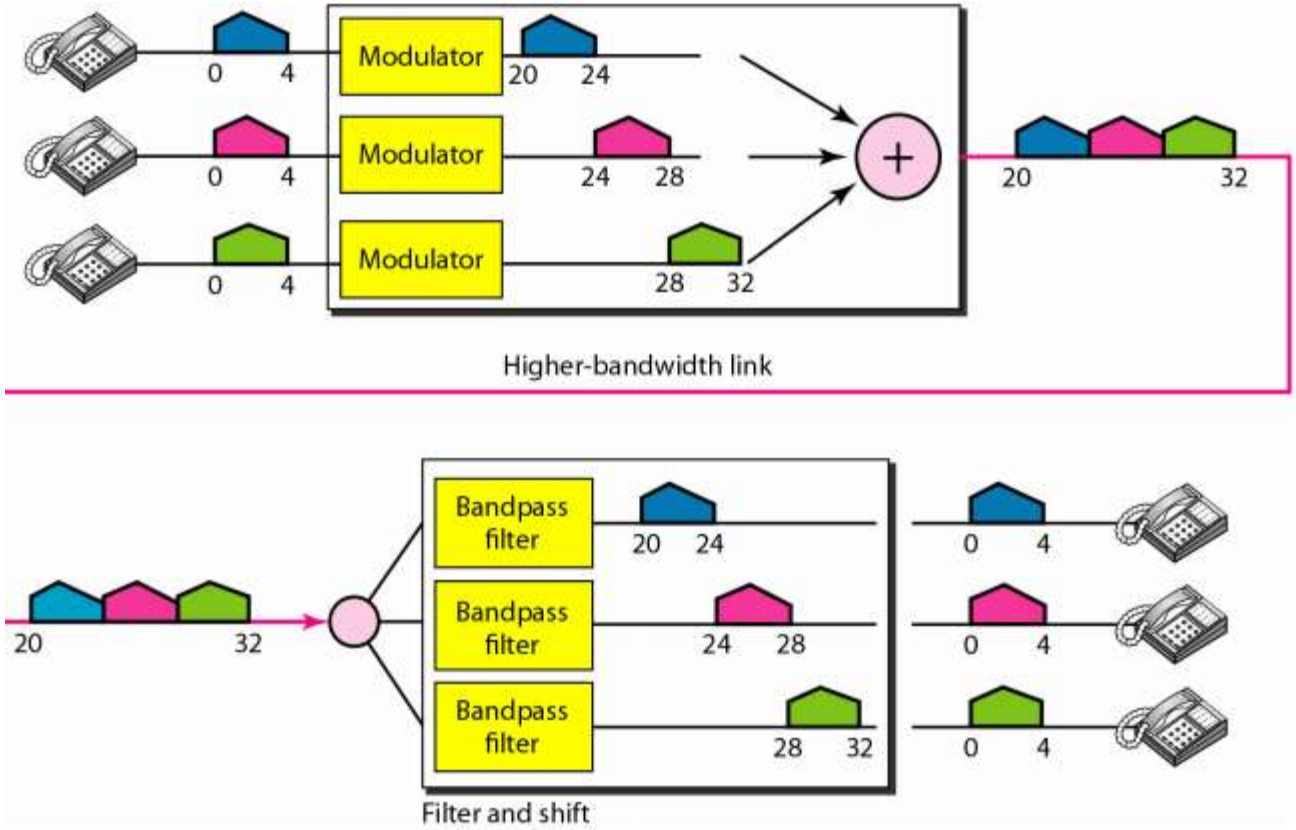
- The channel capacity cannot be fully utilised some of the slots go empty in certain frames.

Asynchronous TDM

- Also known as statistical time division multiplexing.
- In this time slots are not fixed i.e slots are flexible.
- Total speed of the input line can be greater than the capacity of the path.
- In ASTDM we have n input lines and m slots i.e. m less than n (m < n)
- Slots are not predefined rather slots are allocated to any of the device that has data to send

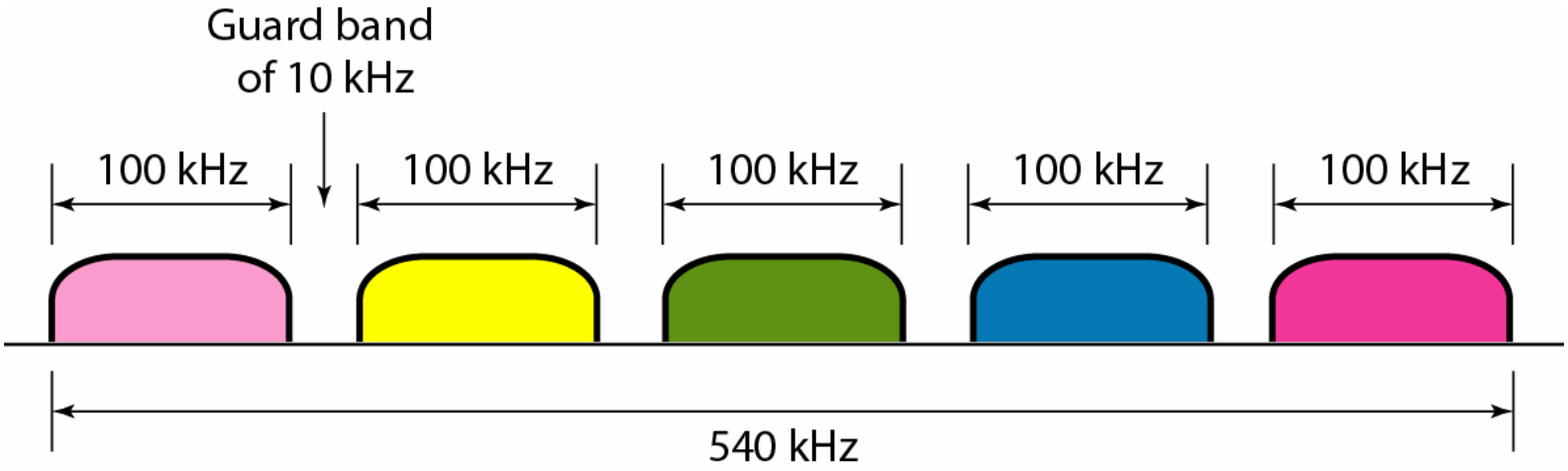
Computation on Multiplexing

- Assume that a voice channel occupies a bandwidth of 4 kHz. We need to combine three voice channels into a link with a bandwidth of 12 kHz, from 20 to 32 kHz. Show the configuration, using the frequency domain. Assume there are no guard bands.
- Solution
  - Each voice channel bandwidth is 4kHz.
  - Available bandwidth is 20 to 32 kHz.
  - First voice channel is 20-24 kHz bandwidth
  - Second voice channel is 24-28 kHz bandwidth
  - Third voice channel is 28-32 kHz bandwidth. Then we combine them as shown in the figure.


Modulator
Modulator
Modulator
0
4
20
24
28
32
+
Higher-bandwidth link
Bandpass filter
Bandpass filter
Bandpass filter
Filter and shift

Computation on Multiplexing

- Five channels, each with a 100-kHz bandwidth, are to be multiplexed together. What is the minimum bandwidth of the link if there is a need for a guard band of 10 kHz between the channels to prevent interference?
- Solution
  - Each channel is 100kHz
  - The five channels will be 100kHz * 5 = 500kHz -------- (A)
  - Each guard band is 10kHz,
  - The four guard band will be 10 kHz * 4 = 40 kHz ------- (B).
  - Therefore the mininum bandwidth requirement for the link will be (A) + (B) = 500kHz + 40 kHz = 540kHz


Guard band
of 10 kHz
100 kHz
100 kHz
100 kHz
100 kHz
100 kHz
540 kHz

Computation on Multiplexing

- The Advanced Mobile Phone System (AMPS) uses two bands. The first band of 824 to 849 MHz is used for sending, and 869 to 894 MHz is used for receiving. Each user has a bandwidth of 30 kHz in each direction and support 42 channels are use for control. How many people can use their cellular phones simultaneously?
- Solution

  - Each band is 25 MHz. = 25 *1000 = 25,000 kHz
  - Each user bandwidth is 30 kHz
  - The numbers of channels in the band will be 25,000/30 = 833.33 kHz appro. 833 kHz.
  - Control channels is 42 kHz
  - Available channel 833 - 42 = 791 kHz

    791 channels are available for cellular phone users.

Network Switching

Switching Networks

- The technique of transferring data or information from one computer network to another network is known as switching.
- Switching is the process of forwarding data coming in from one port/node to another port or node leading towards the destination.
- Switching in a computer network is achieved by using switches. A switch is a hardware device which is used to join multiple computers together with one local area network (LAN).
- A Computer Network may include number of switches and nodes
- The incoming data to a port/node is called ingress.
- The out going data from a port/node is called egress.

Switching Networks

- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.

Why is Switching Concept required?

- Bandwidth: It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- Collision: Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

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.

What is a Switch in a Computer Network?

- Switches refer to the networking devices that operate at an OSI model's layer 2 or data link layer.
- They establish connections between networked devices and employ packet switching to transmit, receive, or forward data packets or frames over the network.
- There are numerous ports on a switch where computers can be connected.
- A network switch evaluates the destination address of each data frame that enters one of its ports, runs any necessary checks, and then sends the frame to the appropriate device(s).
- It enables broadcast, multicast, and unicast communication.

Features of Switches

- Switches function in the OSI model's layer 2 or data connection layer.
- It is a smart network appliance that resembles a multiport network bridge.
- The media access control (MAC) sublayer addresses are used to transport data packets to certain target ports.
- To accept and transmit data packets from the source device to the target device, it employs packet switching technology.
- It allows one-to-one (unicast), one-to-many (multicast), and one-to-all (broadcast) communications.
- Full duplex transmission means that communication in the channel happens in both directions at once. As a result, collisions do not happen.
- Switches are operational hardware that has network management and software capabilities.
- Switches have the ability to carry out some error checking before sending data to the target port.
- There are a total of 24/48 ports, which is more than usual

Types of Switches

- **Unmanaged Switch**
  - These affordable switches are frequently used in small enterprises and household networks.
  - They are easy to set up, and once connected to the network, they are ready to use right away.
  - This plug-and-play approach makes it easy to add more switches when new devices need to be added.

Managed Switch

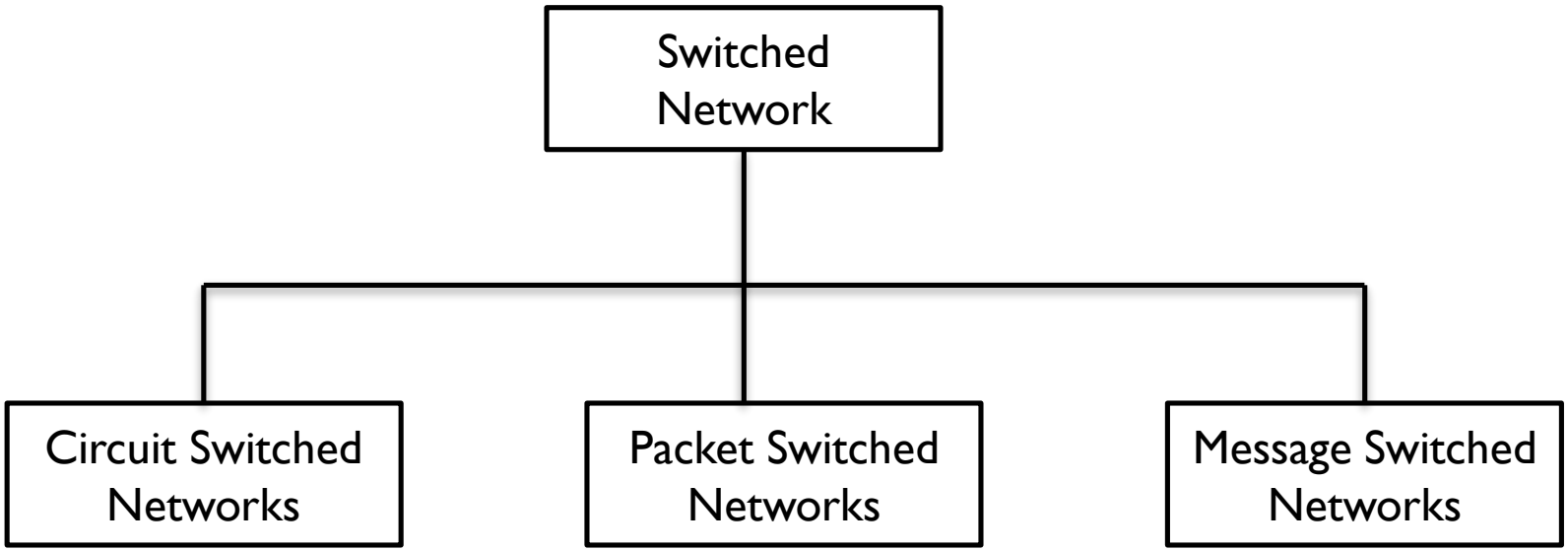
- These switches have addition functionality to a regular switch, they used in organisations with large and complicated networks.
- The added features could include QoS (Quality of Service) enhancements, including more precise control, stronger security standards, and total network administration.
- They are valued in expanding organisations despite their expense because of their scalability and adaptability.
- The Switches are monitored are configured using the Simple Network Management Protocol (SNMP).

Types of Switches

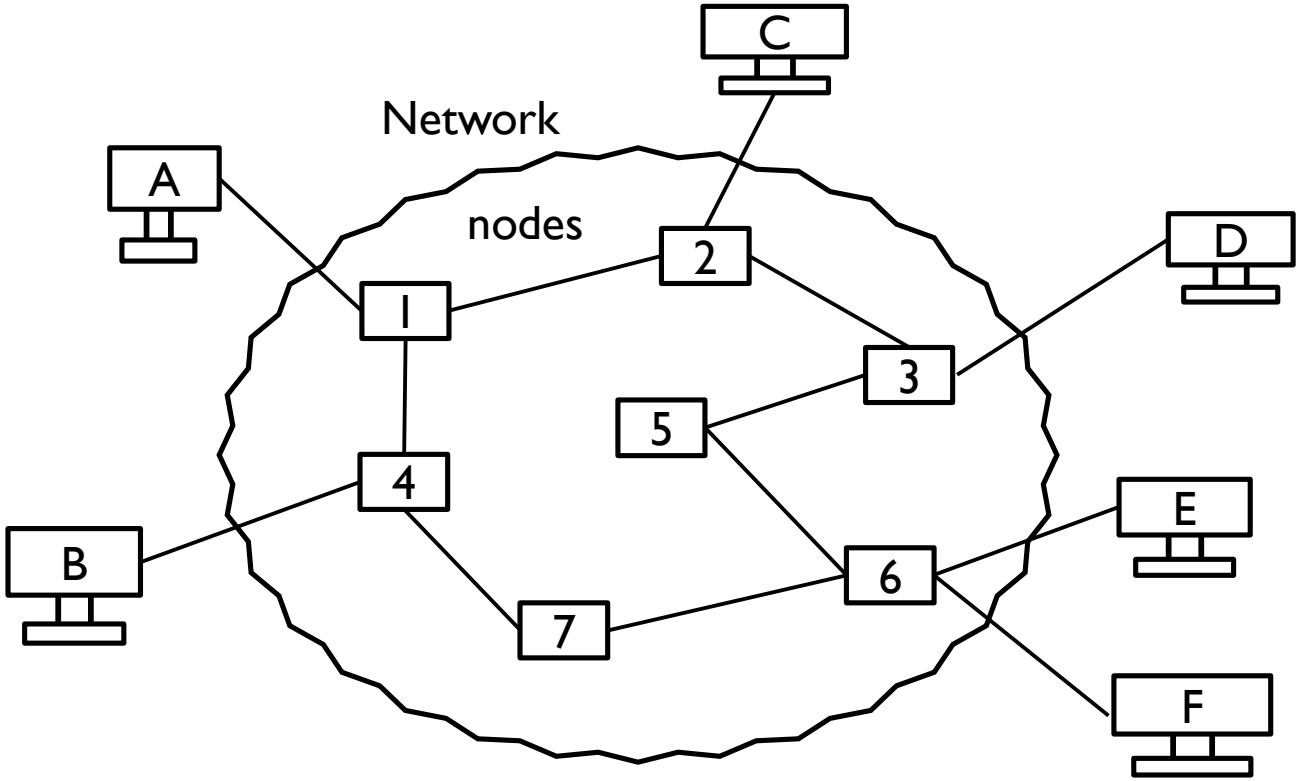
- **LAN Switch**
  - Devices connected to a company's internal LAN are connected by LAN switches.
  - They are also known as data switches or Ethernet switches.
  - These switches are very useful for easing network bottlenecks or congestion.
  - They do this in a way that prevents data packets in a network from overlapping.

- **PoE Switch**
  - In PoE Gigabit Ethernets, Power over Ethernet (PoE) switches are used.
  - Devices linked to it can receive both energy and data over the same line due to PoE technology, which combines data and power communication over the same connection.
  - PoE switches provide more flexibility and make cable hookups easier.

Taxonomy of Switched Network



Sample Switched Network



- Nodes are connected to one another by transmission Link.
- Each work station attaches to the node.
- The collection of nodes is a switched communication Network.

Circuit Switching

- Transmission of data between two nodes are done over a dedicated communication path.
- A pre-specified route is created for which data travels and no other data is permitted.
- Transmission in circuit switching have to go through three phases.
  - Establish a circuit
  - Transfer the data.
  - Disconnect the circuit

◦Circuit switching are primarily design for voice communications. Before a user can make a call, a virtual path between caller and callee is established over the network.

Packet Switching

- Transmission data is broken down into smaller chunks called packets.
- A switching information is added in the header of each packets.
- Data transmission of packets over the network is done independently.
- These packets are sometime store on the intermediate networking devices and they do not take much resources either on carried path or in the memory of switches.
- Packets switching enhances transmission efficiently as packets from multiple communication channels can be multiplexed.
- The internet uses packets switching techniques.
- Packet are stored and forwarded according to their priority to provide quality of service.

Type of Packet switching

- Connectionless communication: data are forward from the originating point / sender to the destination point / receiver without any handshaking or established path and acknowledgements are optional.
- Connection oriented communication : data are forwarded to destination based on a pre-established circuit along the path between both end points.

Message Switching

- This technique is somewhere in middle of circuit switching and packets switching.
- In message switching, the whole data is treated as a data units, and is transmitted in its entirety (whole).
- A switch receives the whole data unit and buffers it until there are resources available to transfer it to the next node.
- If the next node does not have enough resource to accommodate the data unit, the data unit have to waits on the current node.
- Message switching has the following drawbacks
  - Every switch in the transit path needs enough storage to accommodate entire message.
  - Because of the store-and-forward technique and waits of the availability of resources, message switching is very slow.
  - Message switching is not suitable for real time application.

Packet Switching Vs. Other Switching

- Packets switching ensures that no user monopolize any transmission line very long, enhance it is suited for handling interactive traffic.
- Packet switching reduce delay and improve throughput than message switching.
- Packet switching does not require any advance setup, while circuit switching requires that a circuit be set up end to end before communication begins.
- In packets switching, different packets can follow different paths depending on the network conditions at the time they are sent, hence packets may arrive out of order. While in circuit switching, reservation of bandwidth all the way from the sender to the receiver are made, all packets follow the same path hence they cannot out of order.

Packet Switching Vs. Other Switching Continuation ……..

- Packet switching is more fault tolerant than circuit switching. That is if a switch goes down in packets switching, packets can be routed around dead switches, but in circuit switching, all packets are terminated and no more traffic can be send.
- Packet switching does not waste bandwidth. It is more efficient from a system wide perspective, while circuit switching reserved bandwidth and where there is no traffic to send, the bandwidth is wasted.
- Packet switching cause delay in transmission because of the store and forward techniques while in circuit switching the packets just flow through the medium continuously because of the reservation of bandwidth

Data Link Layer

- This layer is one of the most complicated layers and has complex functionalities and liabilities.
- The layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.
- This layer is responsible for converting data stream to signals bits by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognisable frame format, and hands over to upper layer.
- Data link layer has two sub-layers:-

  - Logical Link Control:- It deals with protocol flow-control and error control

  - Media Access Control:- It deals with actual control of media

Functionality of Data-Link Layer

- Framing:-Data-link layer takes packets from Network layer and encapsulates them into frames. Then, it sends each frame bit-bit on the hardware and at the receiver end, it pricks up signals from the hardware and assembles them into frames

Addressing:- Data link layer provides layer – 2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware a the time of manufacturing

Synchronization:- when data frames are sent on the link, both machines must be synchronised in order for transfer to take place.

Error Control:- sometimes signals may have encountered problem in transmission and the bit are corrupted. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to other sender.

Flow Control:- Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on the same speed.

Multi – Access: When host on the shared link tries to transfer data, it has a high probability of collision. Data link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple systems

- Error Detection and Correction

Basic Concept

- Network must be able to transfer data from one device to another with complete accuracy.
- Data can be corrupted during transmission,
- Environmental Interference and physical defects in the communication medium can cause random bit errors during data transmission,
- For reliable communication, errors must be detected and corrected.
- Error detection and correction are implemented either at the data link layer or the transport layer of the OSI model.

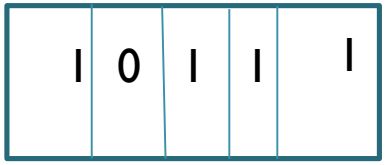
TYPES OF ERRORS

- ERROR

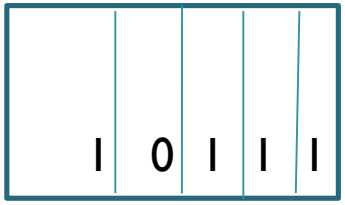
SINGLE BIT

MULITPLE BIT

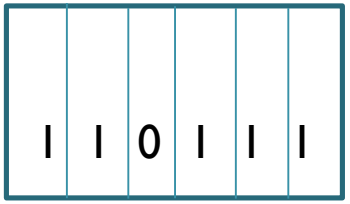
BURST

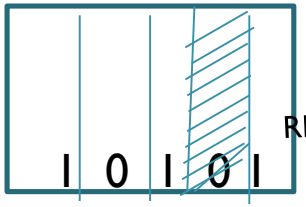


SENT

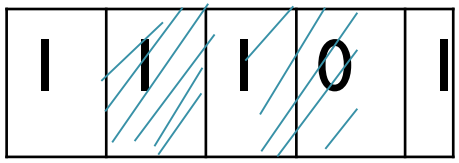


SENT

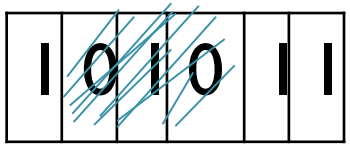




RECEIVED



RECEIVED



SINGLE – BIT ERROR

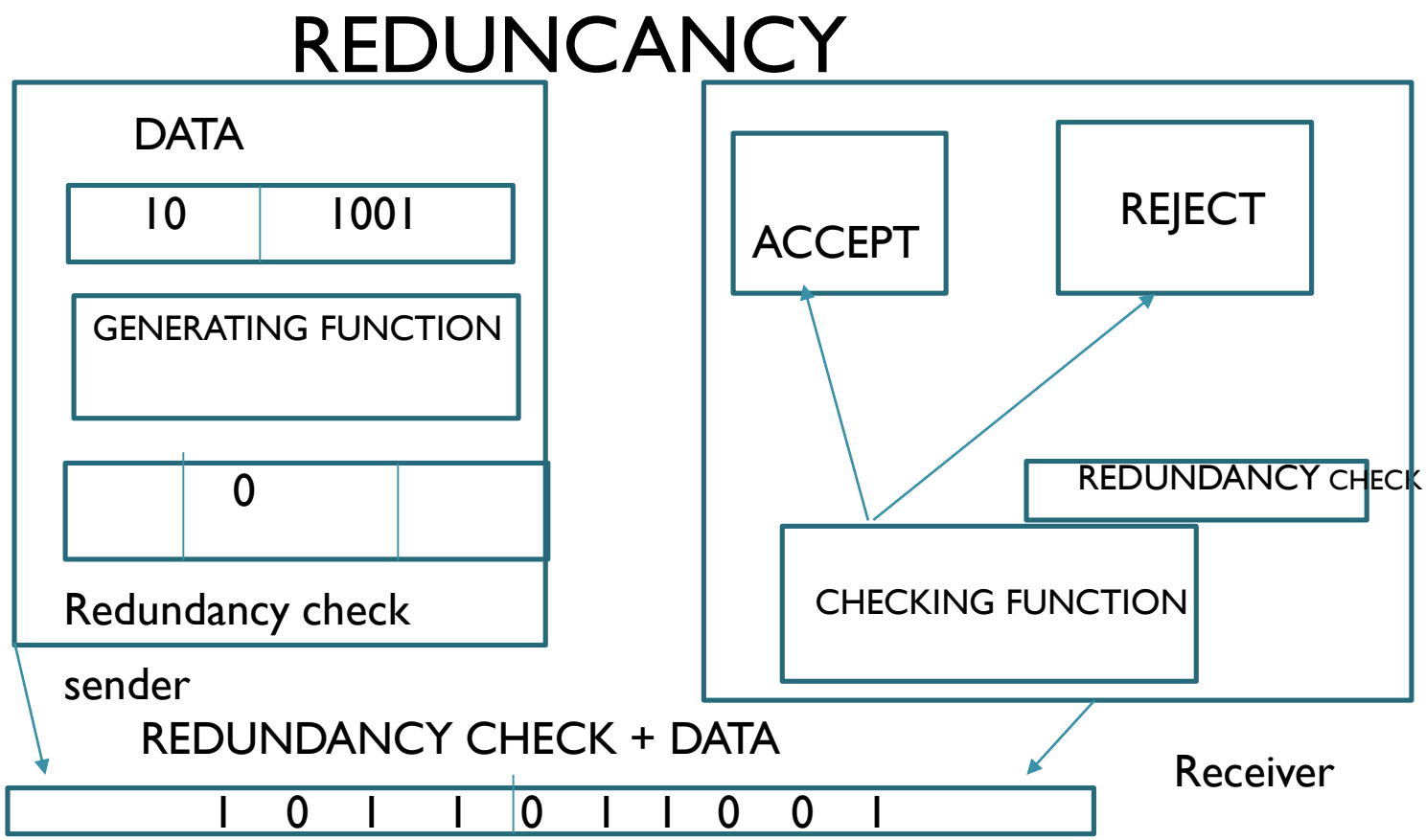
- Single bit error are the least likely type of errors in serial data transmissions because the noise must have a very short duration which is very rare
- However, this kind of errors can happen in parallel transmission.

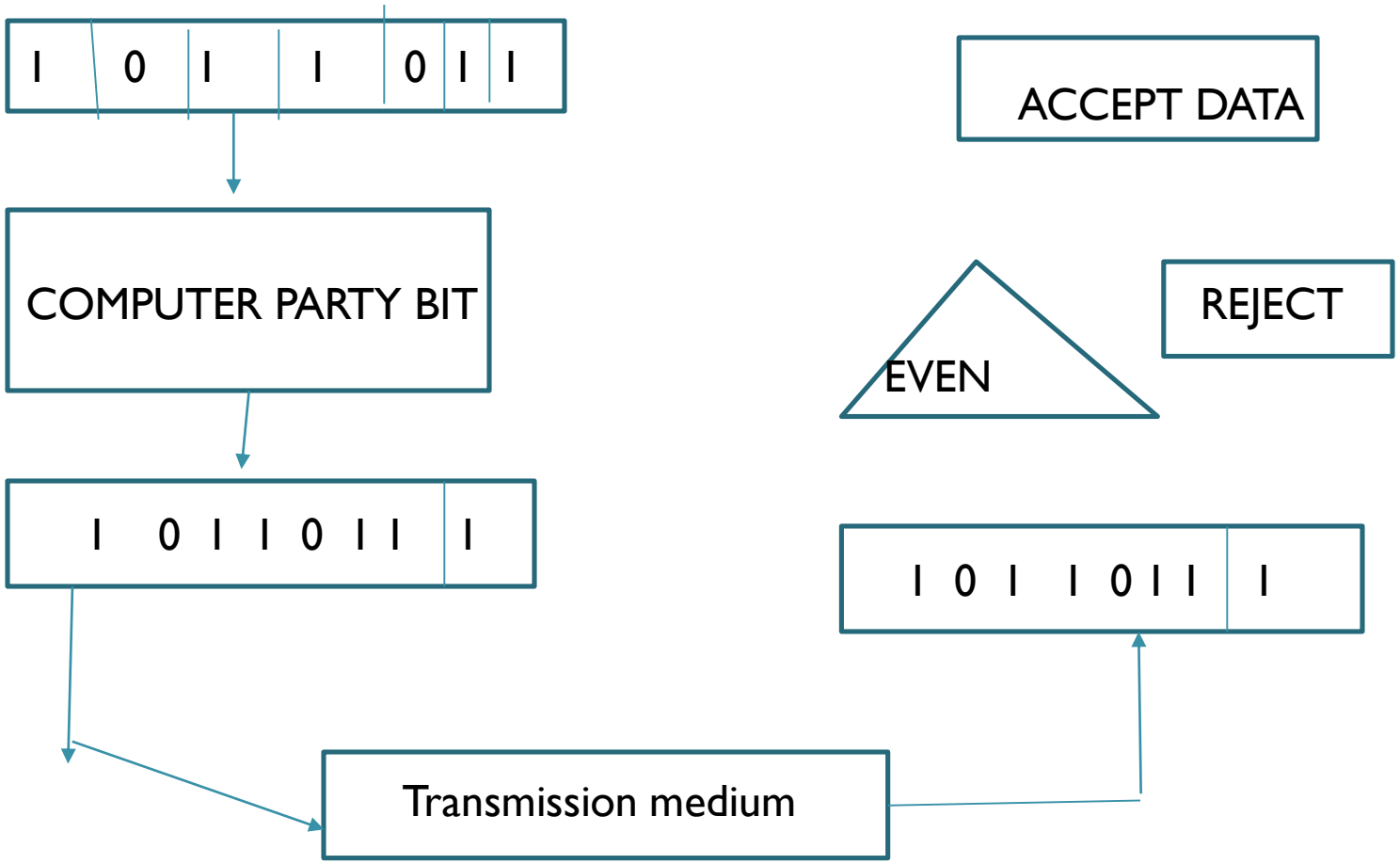
BURST ERROR

- The term burst error means that two or more bit in the data unit changed from 1 to 0 or from 0 to 1.
- The length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between many not have been corrupted
- Burst error is most likely to happen in serial data transmission since the duration of voice is normally longer than the duration of a bit.
- The number of bits affected depends on data rate and duration of noise.

ERROR DETECTION

- Error detection means to decide whether the received data is correct or not without having a copy of the original message,
- Error detection uses the concept of redundancy, which means adding extra bits for errors at the destination.



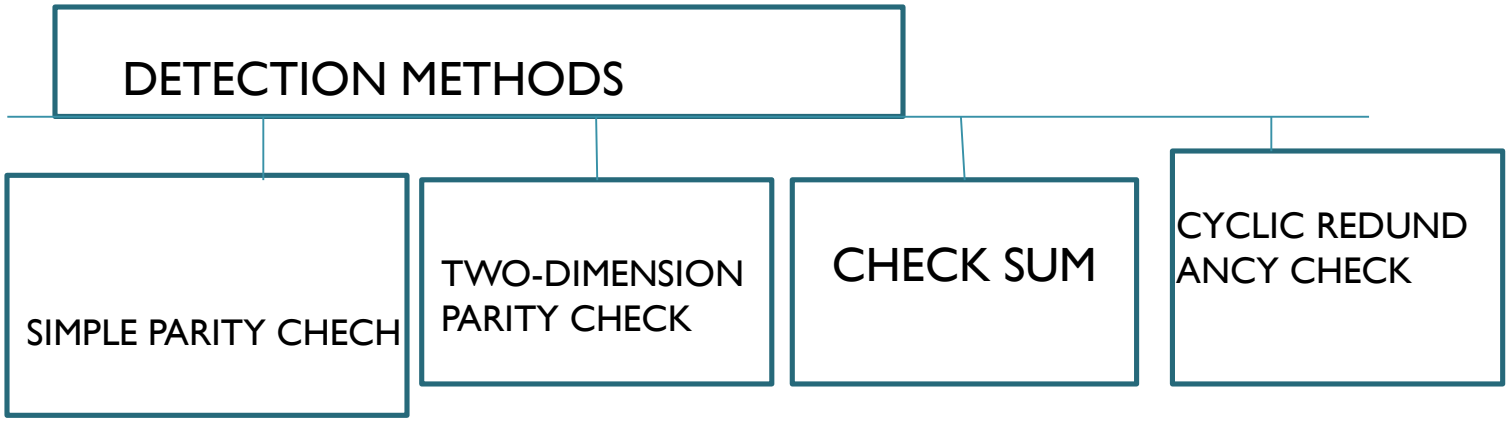

1 0 1 1 0 1 1
ACCEPT DATA
COMPUTER PARTY BIT
EVEN
REJECT
1 0 1 1 0 1 1 1
1 0 1 1 0 1 1 1
Transmission medium

EVEN – PARITY CHECKING SCHEME

- EXAMPLE

DATA BLOCK	PARTITY BIT	CODE WORD
0010	1	00101
0101	0	01010
0111	1	01111
1100	0	11000

DETECTION METHOD



- Simple Parity Check

- Is the most common and least expensive mechanism for error detection.
- In this technique, a redundant bit called parity bit, is appended to every data unit.
- Such that the number of 1s in the unit and the parity become even.
- Block of data from the source are subjected to a parity bit generator, where a parity bit 1 is added to the data unit of the number of 1s are odd and parity bit 0 is added to the data unit of the number of 1s are even

TWO – DIMENSION PARITY CHECK

- Efficiency of error defection can be improved by using two-dimensional parity check
- In this technique, Parity check bits are calculated for each row and all columns and both are sent along with the data,
- At the receiving end these are compared with the parity bits calculated on the received data.

ORIGINAL DATA

10110011	10101011	01011010	1101010

10110011	1	1
10101011	1	1
01011010	0	0
11010101	1	1
100100111	1	1

ROW PARITIES

COLUMN PARITY

SENT DATA

101100111	101010111	010110100	11010111	100101111

PERFORMANCE

- It has increase the likehood of detecting burst errors.

CHECK SUM

- In check sum error detection scheme, the data is divided into K segments each of m bits.
- In the send's end the segments are added using 1's complement arithmetic to get the sum.
- The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segment.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum.
- The sum is complemented
- If the result is zero, the received data is accepted, otherwise rejected.

EXAMPLE OF CHECKSUM

Original

CYCLIC REDUNDANCY CHECK (CRC)

- This CRC is the most powerful and easy to implement technique.
- It is based on binary division
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are generated and appended to the end of data unit.
- The data unit and the CRC bits are divisible by a predetermined binary number.
- At the destination, the incoming data unit is divided by the same number (predetermined binary number)
- If there is no reminder, the data unit is assumed to be correct and is therefore accepted.
- If there is remainder, it indicates that the data unit has been damaged in transit and therefore must be rejected.

DATA = 11001 DIVISION = 101

ERROR CORRECTING CODES

- Error correction can be handled in two ways:-
- First, when an error is discovered, the receiver can have the sender retransmit the entire data unit. This is known as backward error correction.
- Secondly, when an error is discovered, the receiver can use an error-correcting code, which automatically corrects the errors. This is known as forward error correction

NETWORK LAYER FUNCTIONALITIES

- Addressing devices and networks
- Populating routing tables or static routes
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provide connection oriented and connectionless mechanism

NETWORK LAYER FEATURES

- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different protocols and subnets with different scheme
- Different logical network design over the physical network design.
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

NETWORKS ADDRESSING

- Internet protocol helps to communicate end to end devices over the internet.
- There are two internet protocol (IP) that is IPV4 and IPV6.
- IPV4 have been in used for decades and now is running out of address space.
- IPV6 is created to replace IPV4 and hopefully mitigated limitations of IPV4.
- Network address are always logical, that it they are software based address which can be changed by appropriate configuration unlink physical address.
- Network address points to host, node or server and it is configured on network interface card. e.g 192.168.1.10.
- IP Address can be assigned dynamically or static.