DATA COMMUNICATIONS AND COMPUTER NETWORK

CHAPTER ONE

DATA COMMUNICATIONS

Data communication Refers to the exchange of data between A source and A receiver.

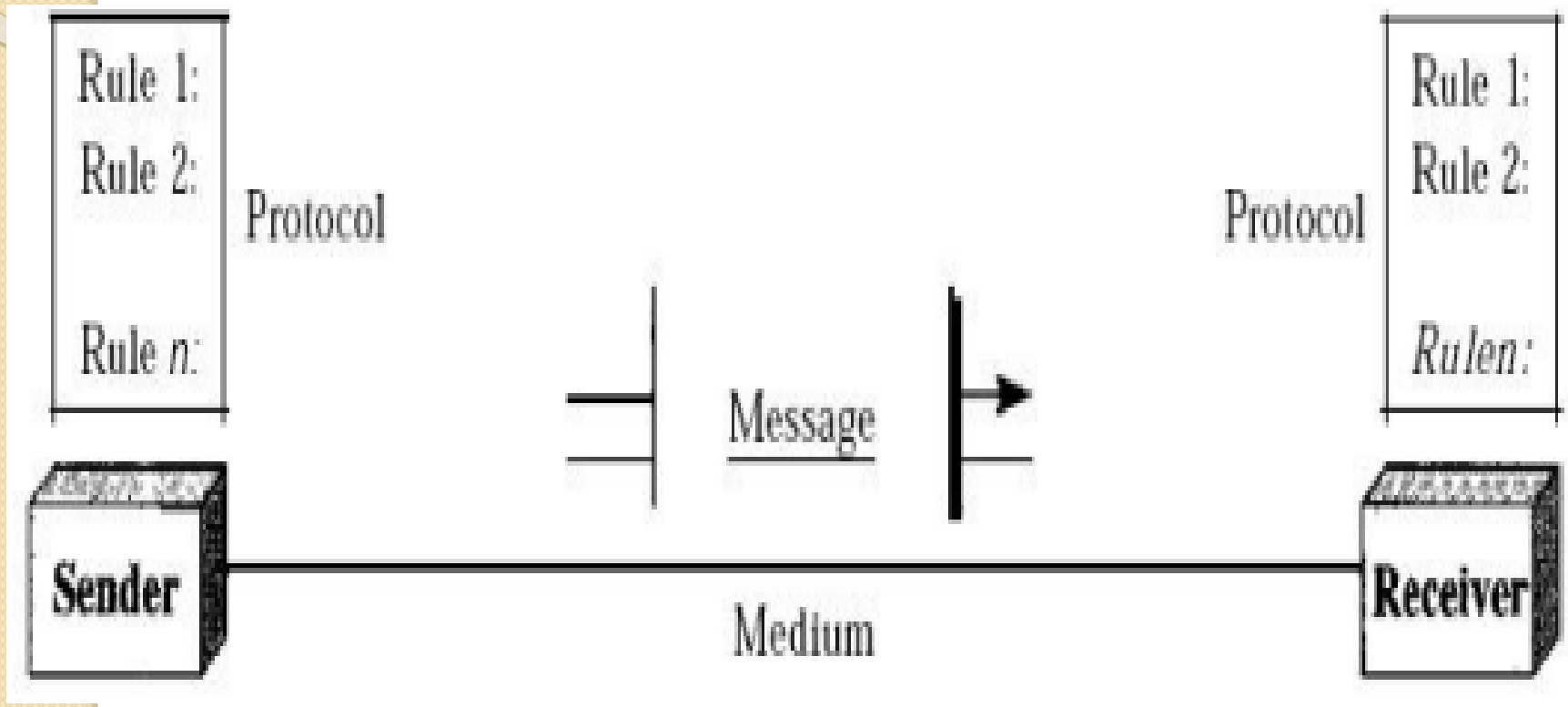
The device that transmits the data is known as source and the device that receives the transmitted

Data is known as receiver.

Data communication Refers to the exchange of data between two devices via some form of transmission medium such as a wire cable using appropriate signal.

Components of Data Communication

A data communications system has five components:



i) **Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

ii) **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

iii) **Receiver:** The receiver is the device that receives the message. It can be a computer,workstation, telephone handset, television, and so on.

iv) **Transmission medium:** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire,coaxial cable, fiber-optic cable, and radio waves.

v) **Protocol:** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking french cannot be understood by a person who speaks only japanese

Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (os or 1s).Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding.

Number:

Numbers are also represented by bit pattern**s,** the number is directly converted to a binary number to simplify mathematical operations.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the resolution.

Audio:

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete.

Video:

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.G., By a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion

Types of Data

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states.

Signal: The electrical wave that is used to represent the data. Can be analog or digital signal.

Cont .....

An analog signal has infinitely many levels of intensity over a period of time. As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path. Ex:-Human voice

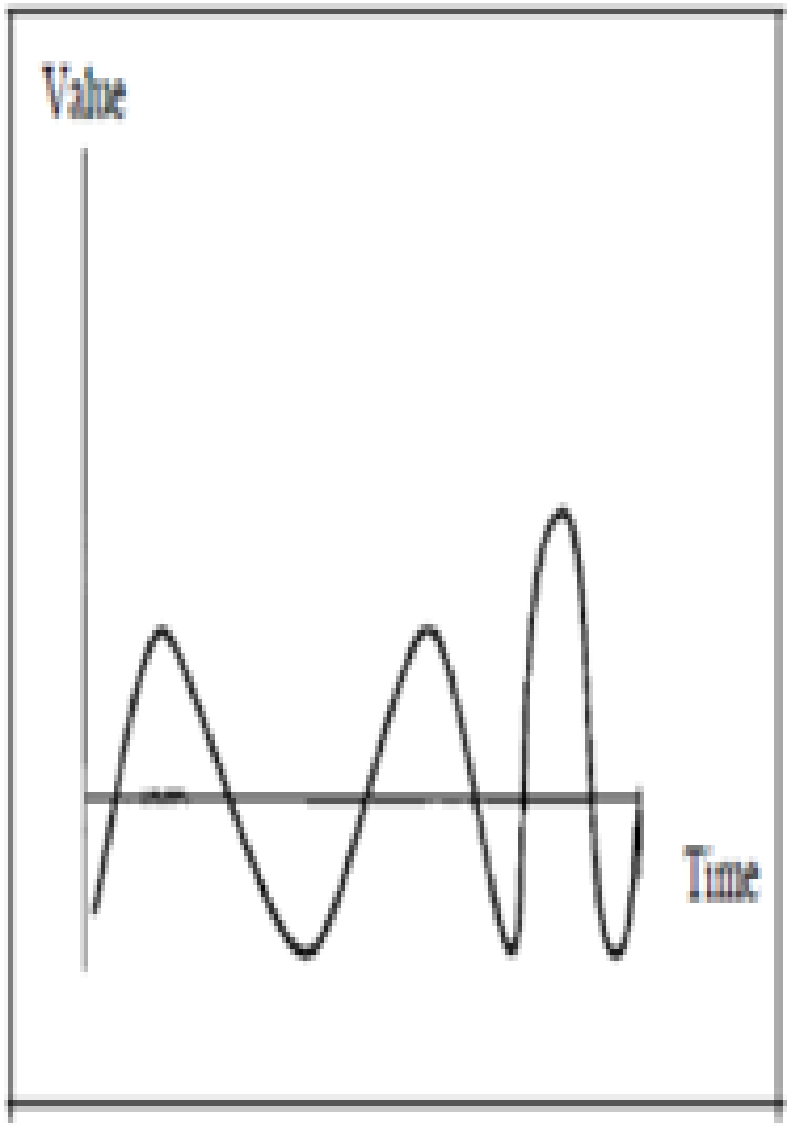
Data => Continuous (e.g. audio)

Signaling =>continuously varying electromagnetic wave

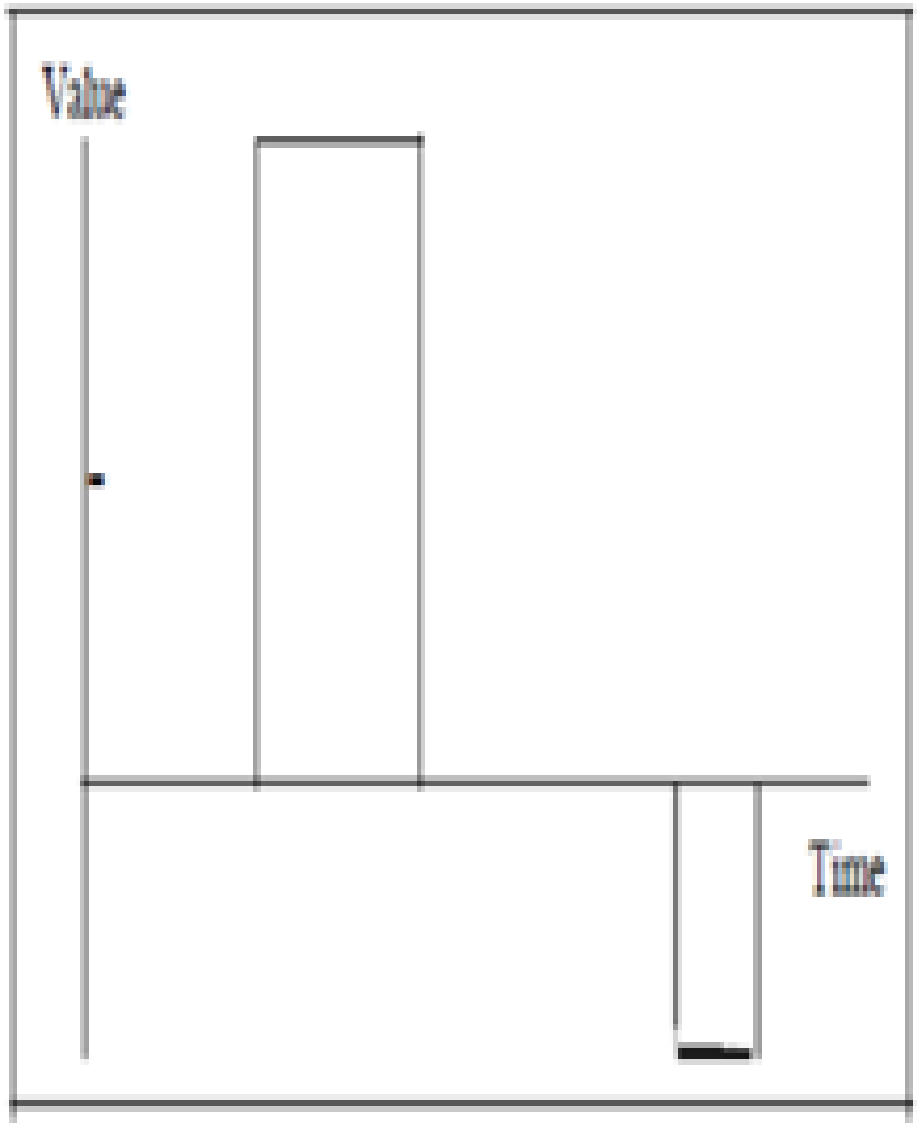
A digital signal, on the other hand, can have only a limited number of defined values. Although each value can be any number, it is often as simple as 1 and 0. Ex:-Digital Watch

Data =>Discrete (e.g. text)

Signaling => Sequence of Voltage pulses



a. Analog signal

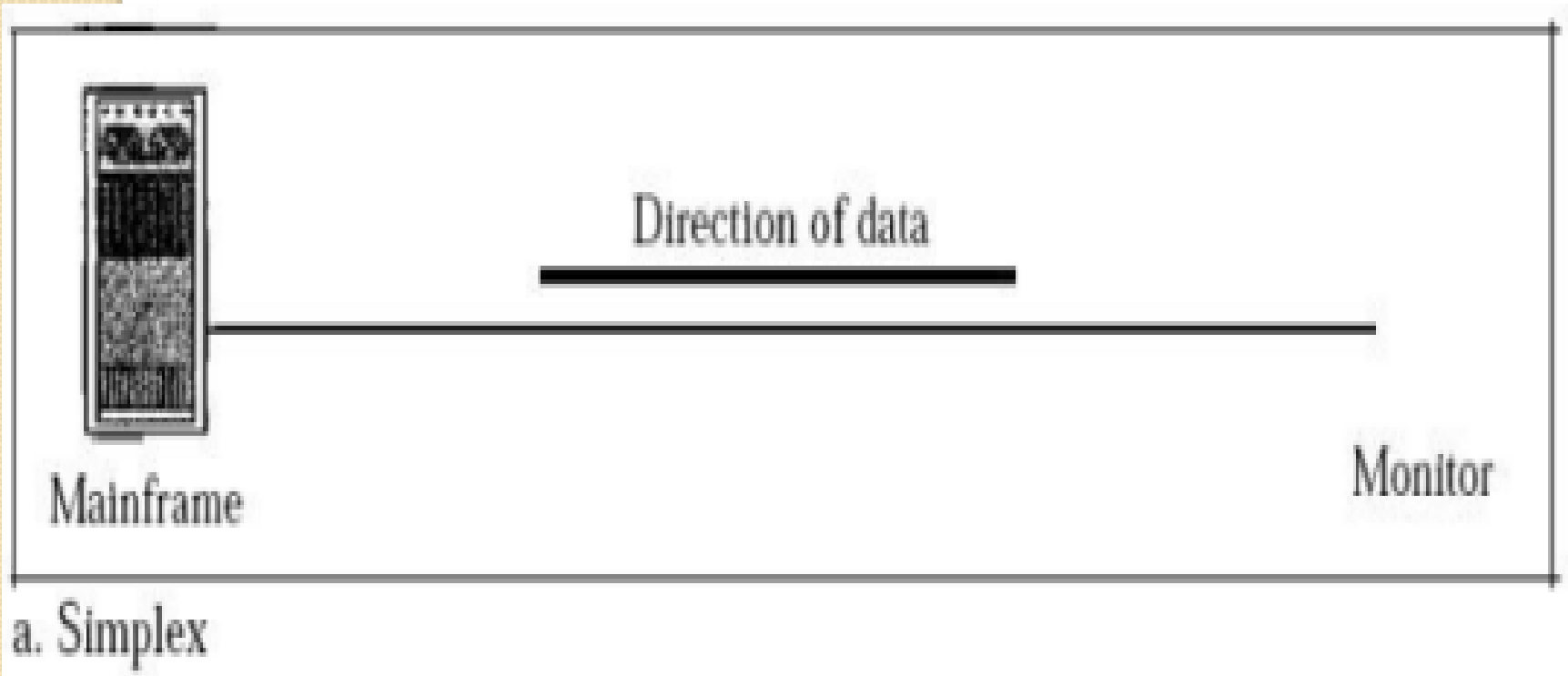


b. Digital signal

Types of Communication Styles

Communication between two devices can be simplex, half-duplex, & full-duplex

1. Simplex

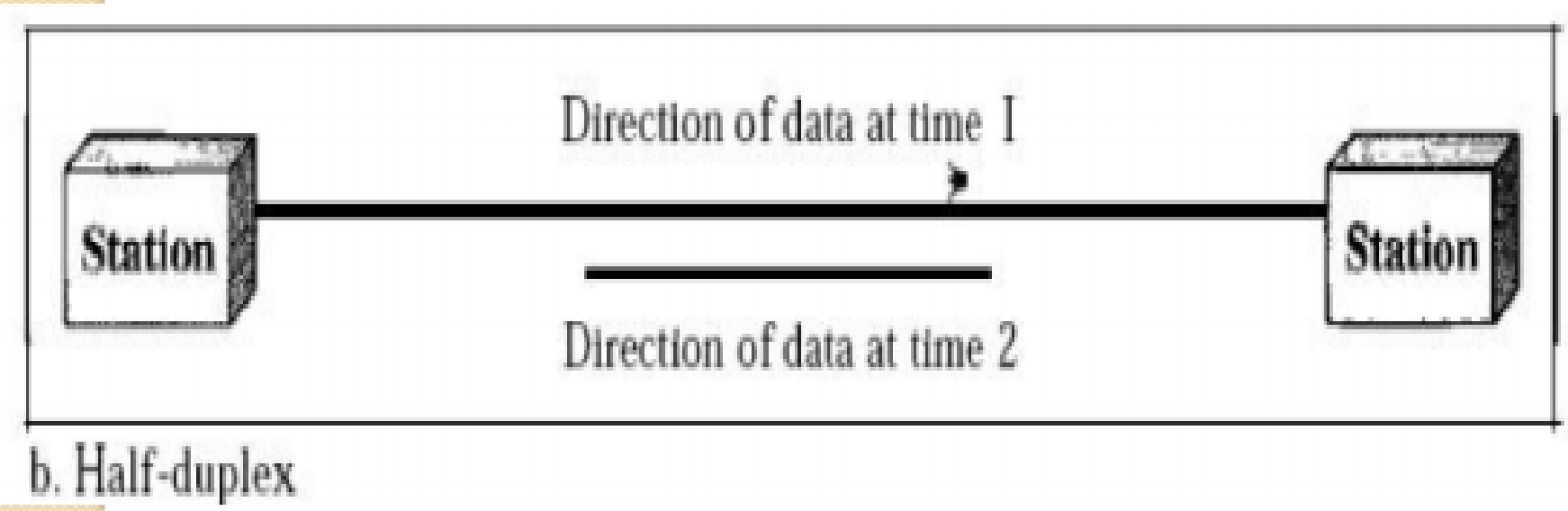


a. Simplex

-In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

- This mode of communication vastly used in Radio and TV where we can see and hear or recive data only but we can't send any information data by the same channel

ii) Half-Duplex



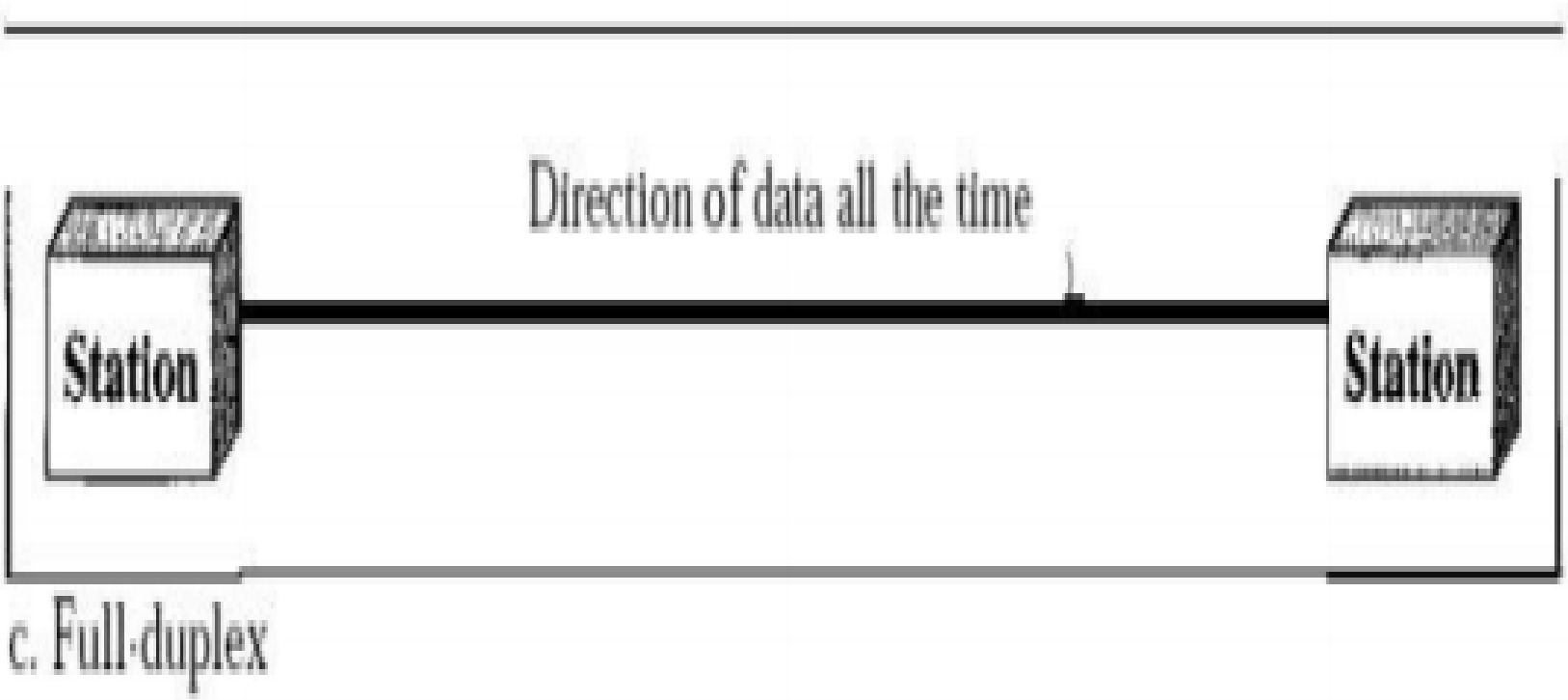
b. Half-duplex

-In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

- The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are travelling in one direction, cars going the other way must wait.

- This mode of communication vastly used in Walkie-talkie, intercom,string phone

iii) Full Duplex



c. Full-duplex

-In full-duplex mode, both stations can transmit and receive simultaneously.

-The full-duplex mode is like a two way street with traffic flowing in both directions at the same time.

-One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

Data Transmission

Data transmission refers to the process of transferring data between two or more digial devices. Data is transmitted from one device to another in analog or digital format.

How does data Transmission work between digital devices?

Data is transferred in the form of bits between two or more digital devices. There are two methods used to transmit data between digital devices.Serial data transmission sends data bits one after another over a single channel. Parallel data transmission sends multiple data bits at the same time over mutiple channels.

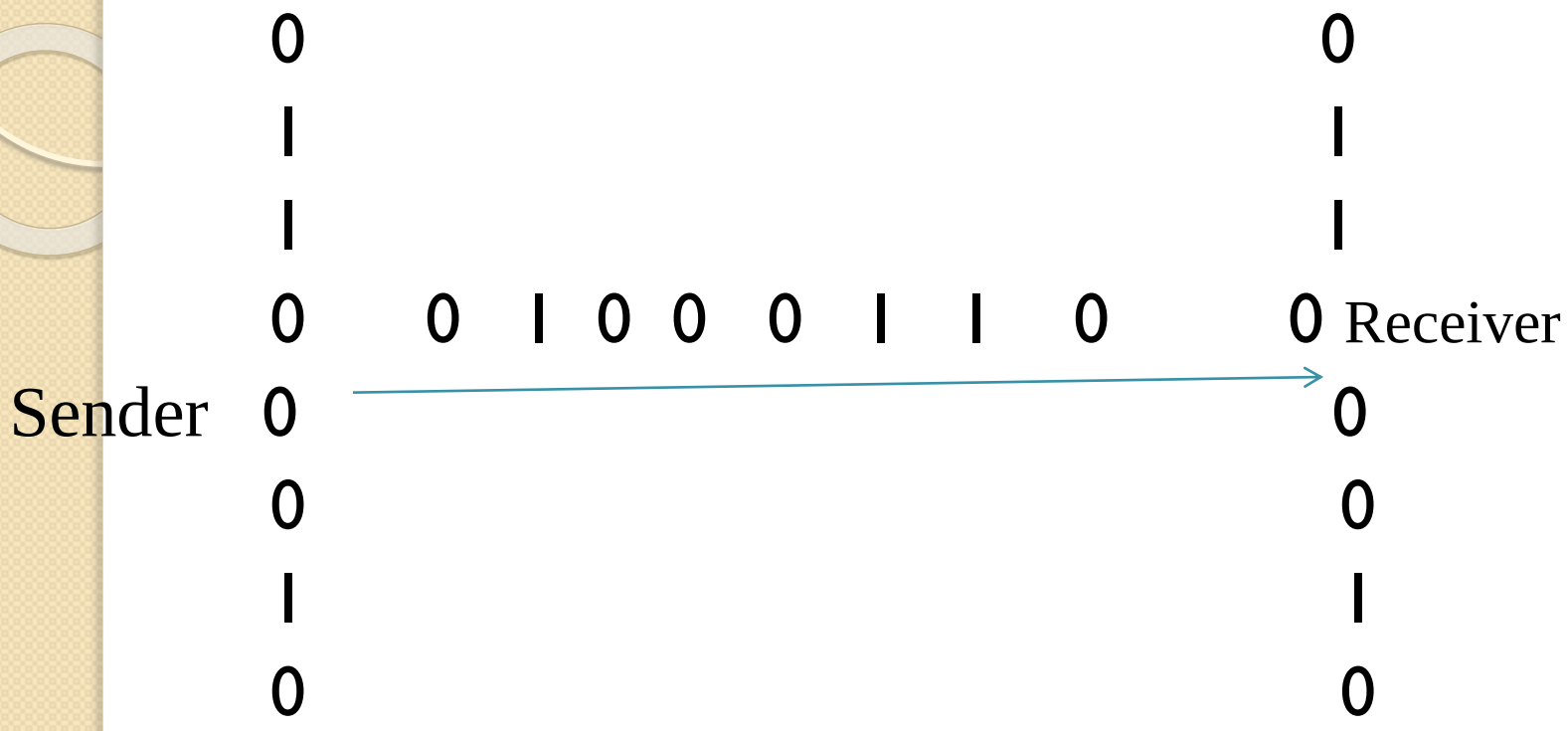
Types of Data transmission

1. **Serial Transmission:** While transferring data b/n two physically separate devices,especially if the separation is more than a few kilometers, for reaons of cost, it is more economical to use a single pair of lines.

- Data is transmitted as a single bit at a time using fixed time interval for each bit. This mode of transmission is known as bit-serial transmission

- In a serial transmission, the various bits of data are transmitted serially one after the other. Slower than parallel

- Serial transmission is used for long distance communication.It is also used in cases where the amount of data being sent is relatively small.



Serial Transmission of 8-bit Data

Classifications of Serial Transmission

Serial transmission has two classfications: asynchronous and synchronous

1. **Asynchronous Serial Transmission: D**ata bits can be sent at any point in time. Stop bits and start bits are used b/n data bytes to synchroniz the transmitter and receiver and to ensure that the data is tranmitted correctly. Time bits isn't constant, so gaps are used to provide time b/n transmissions.

- It is more cost effective method
- The data transmission can be slower, but this is not always

2. Synchronous Serial Transmission

Data bits are transmitted as a continuous stream in time with a master clock. The data transmitter and reciver both operate using a synchronized clock frequency so start bits,stop bits and gaps are not used.

- Data moves faster and timing errors are less frequent b/c time of both is synced.

- In comparison with asynchronous serial transmission ,this method is usually more expensive

2. Parallel Transmission: When data is sent using parallel data transmission, multiple data bits are transmitted over multiple channels at the same time. This means that data can be sent much faster than using serial transmission methods.

A group of bits is transmitted simultaneously by using a

Separate line for each bit.

The main advantage of parallel data transmission over serial transmission are:

- It is easier to program and data is sent faster

As a disadvantage :

- It requires more transmission channels than serial

Cont.....

Parallel transmission is used when:

- A large amount of data is being sent
- The data being sent is time-sensitive
- And the data needs to be sent quickly

Parallel Transmission of 8-bit Data

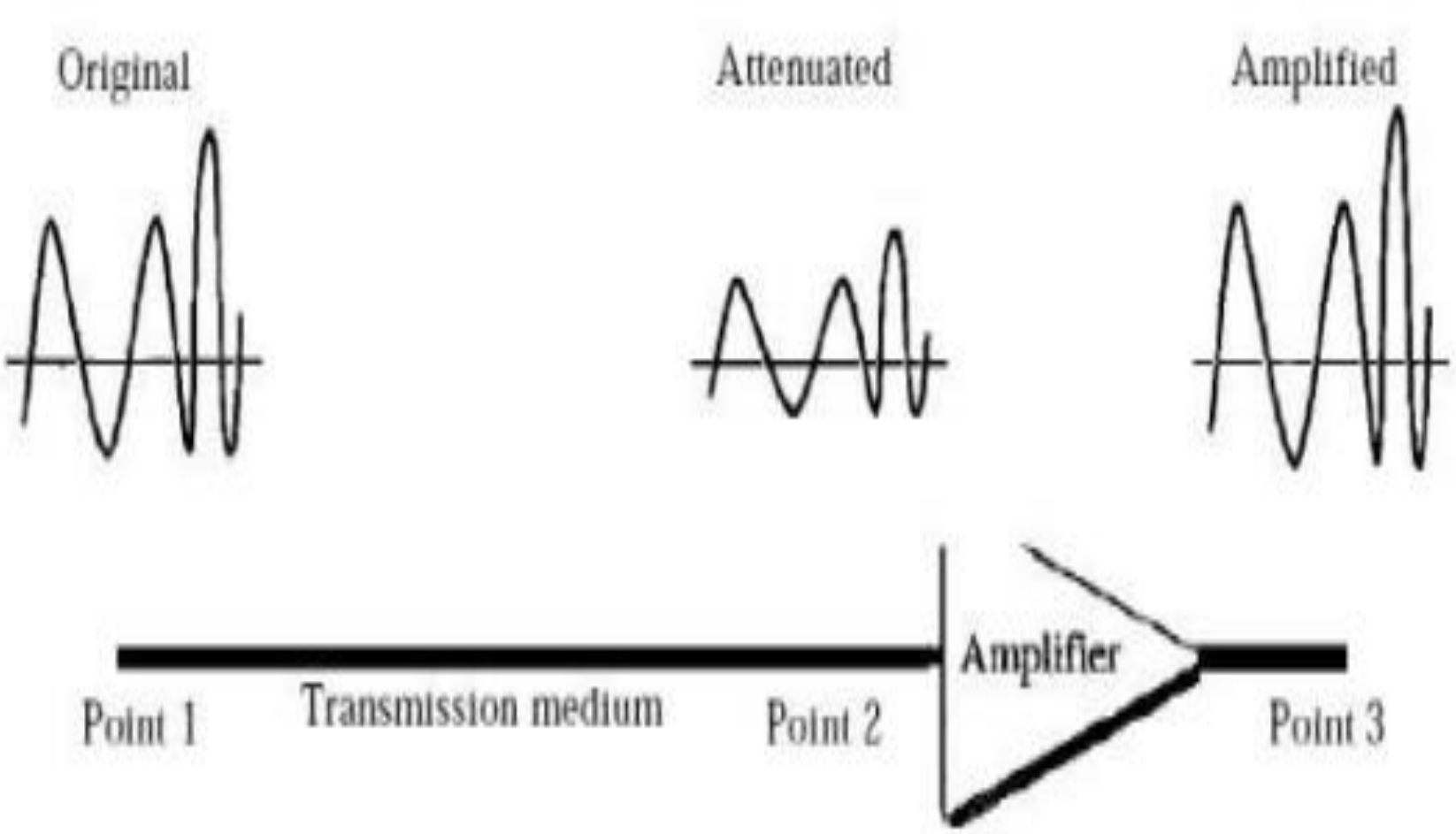
Transmission Impairment

Signals travel through transmission media, which are not perfect.The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are **attenuation, distortion,** and **noise.**

i) Attenuation:

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

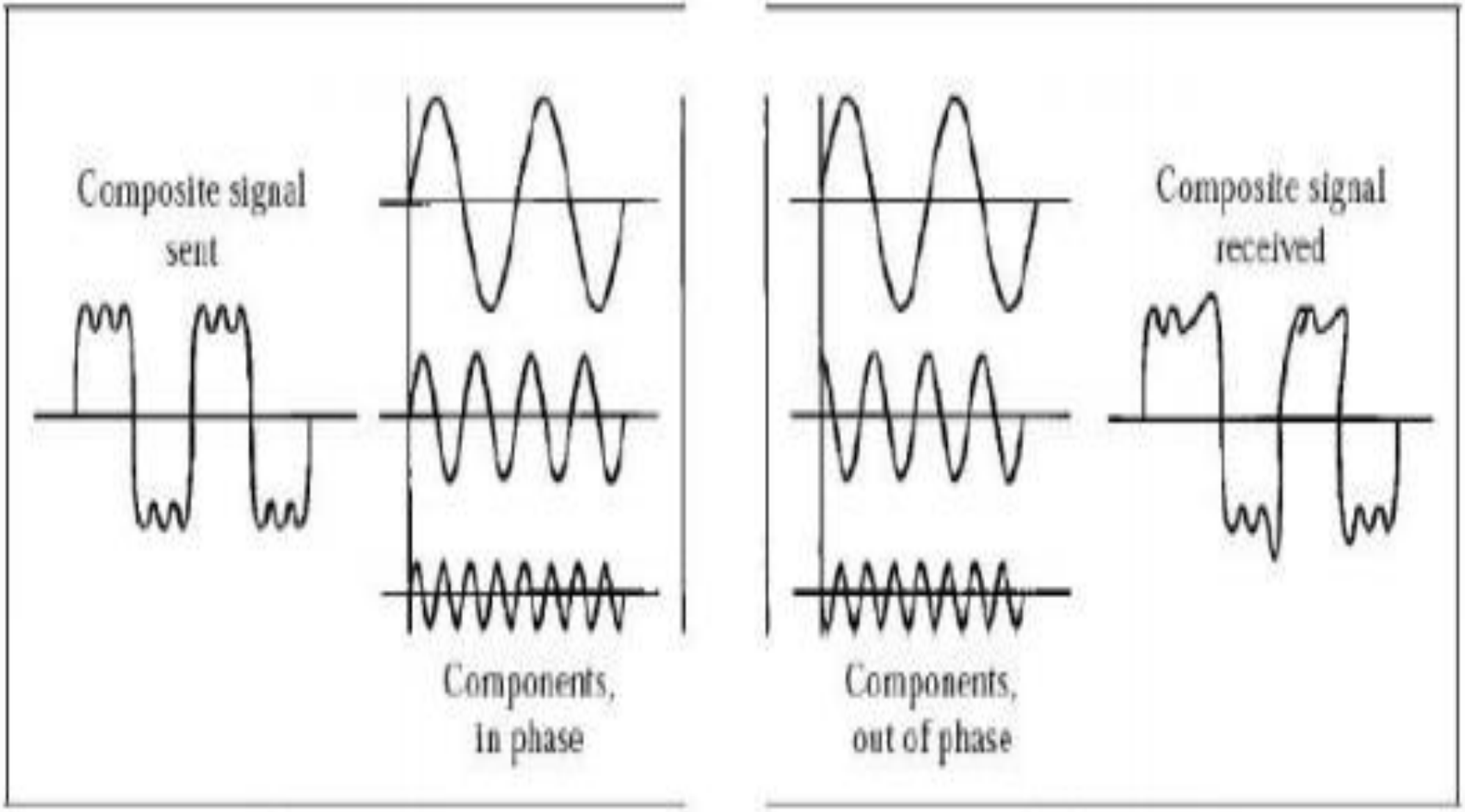
Cont....


Original
Attenuated
Amplified
Amplifier
Point 1
Transmission medium
Point 2
Point 3

ii) Distortion:

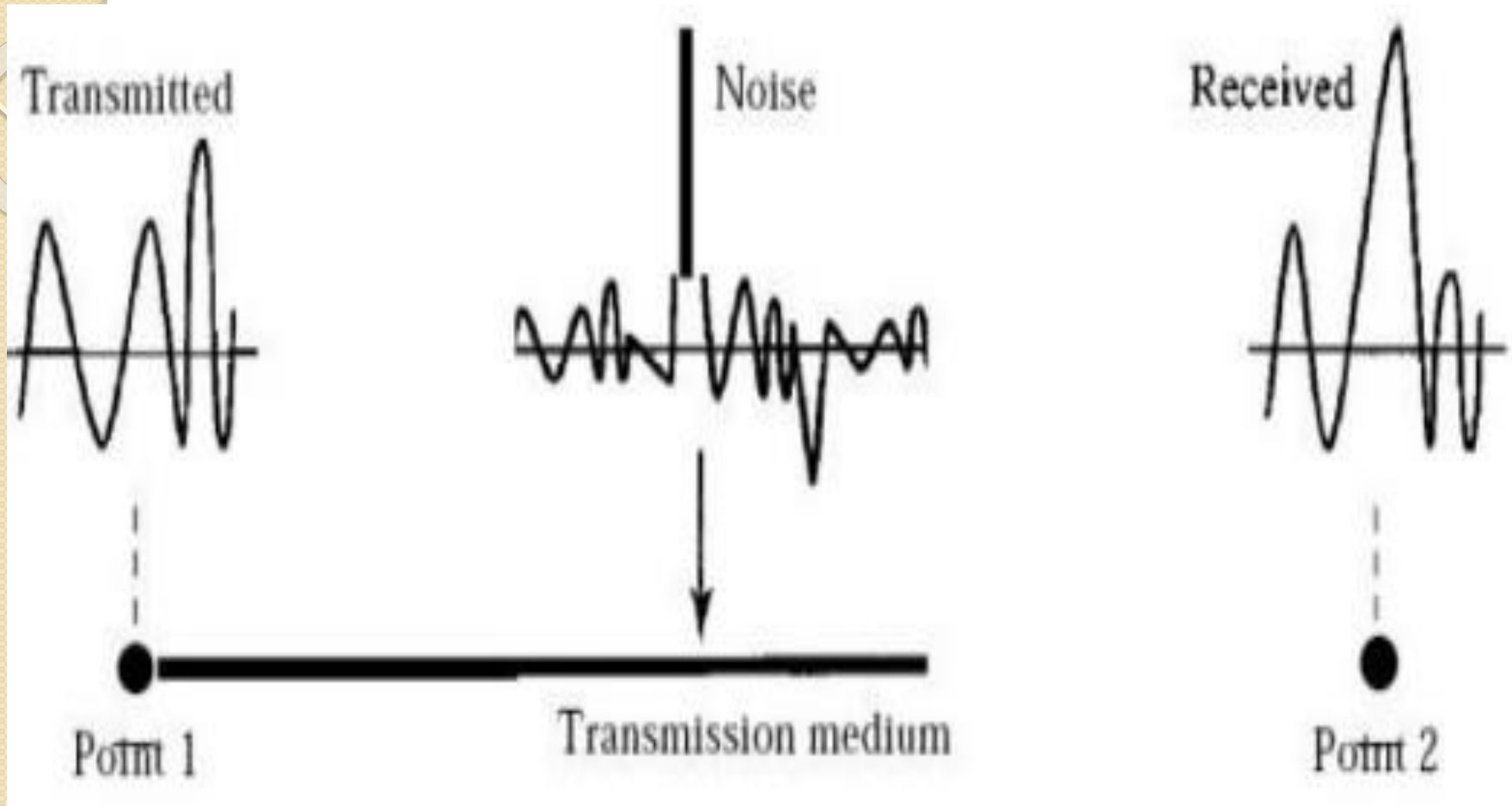
-**Distortion** means that the signal changes its form or shape.

-**Distortion** can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.


Composite signal
sent
Components,
in phase
At the sender
Composite signal
received
Components,
out of phase
At the receiver

iii) Noise:

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal. **Thermal noise** is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter. **Induced noise** comes from sources such as motors and appliances.**Crosstalk** is a disturbance caused by the electric or magnetic fields of one telecommunication signal affecting a signal in an adjacent circuit.**Impulse** is a category of noise which includes unwanted,almost instantaneous sharp sounds. Usually caused by electromagnetic interference,scratches on recording disks....


Transmitted
Noise
Received
Point 1
Transmission medium
Point 2

What is Switching

The mechanism for moving information between different computer network and network segment is called switching in computer network.

The switching functions provides communications pathways b/n two endpoints and manage how data flows b/n them.

The two most common switching methods are **circut switching and packet switching.**

Switching Methods

Circuit switching: Requires a dedicated physical connection b/n the sending and receving devices and also it involves setting up a series of intermediate nodes, in order to propagate the sending node's data to the receiving node.

- The sending system establishes a physical connection, and the data is transmitted b/n the two. When transmission is complete, the channel is closed.

- In particular, it is the method used by the public switched telephone network(PSTN).

Cont....

Packet switching: In here messages are broken into smaller pieces called packets.

Each packets is assigned source and destination addressses. And will be transmitted separately by intermediate nodes and reassembled when they reach the final recipient.

As an example we can take Internet (connectionless) by it self

Characteristics of Data Communication

The effectiveness of Data Communication depend on four fundamental characteristics

1. **Delivery _ the system must deliver data to correct destination**

2. **Accuracy_the system must deliver data to correct destination accurately**

3. **Timeliness_ the system must deliver data on time**

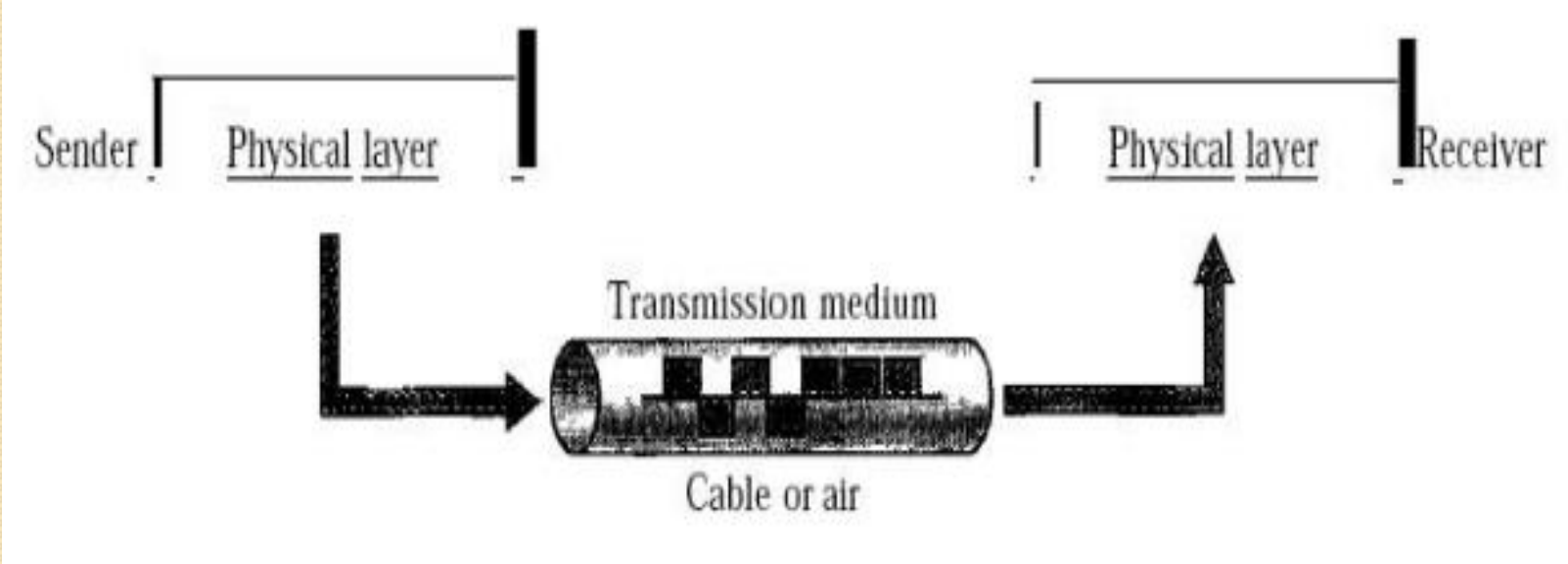
4. **Jitter_ is refer to the variation in packet arrival time**

End Of Chapter One

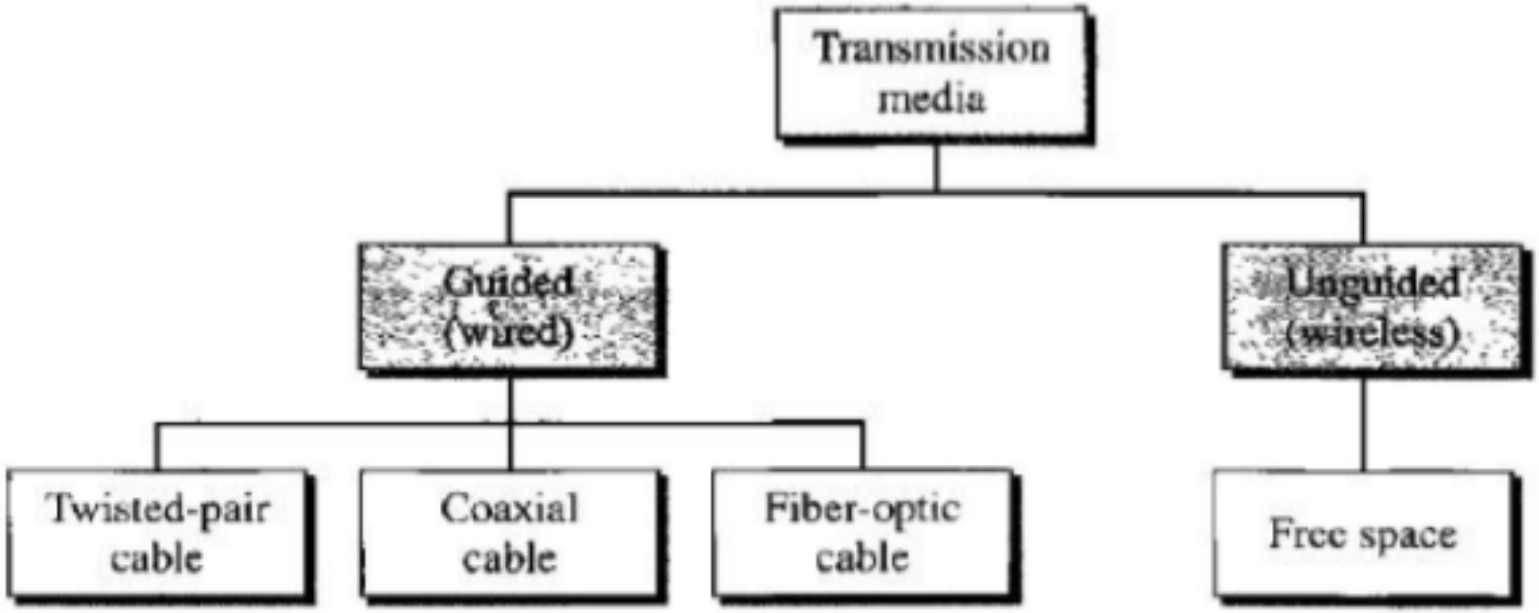
Chapter Two

Transmission Media

The medium over which the information between two computer systems is sent, called transmission media (or) transmission media is a pathway that carries the information from sender to receiver. Transmission media is also called as communication channel.



-In telecommunications, transmission media can be divided into two broad categories: **Guided/Wired and Unguided/Wireless**. **Guided media** include **twisted-pair cable, coaxial cable, and fiber-optic cable**. **Unguided medium** is free space.



1. **Guided/Bounded Media**

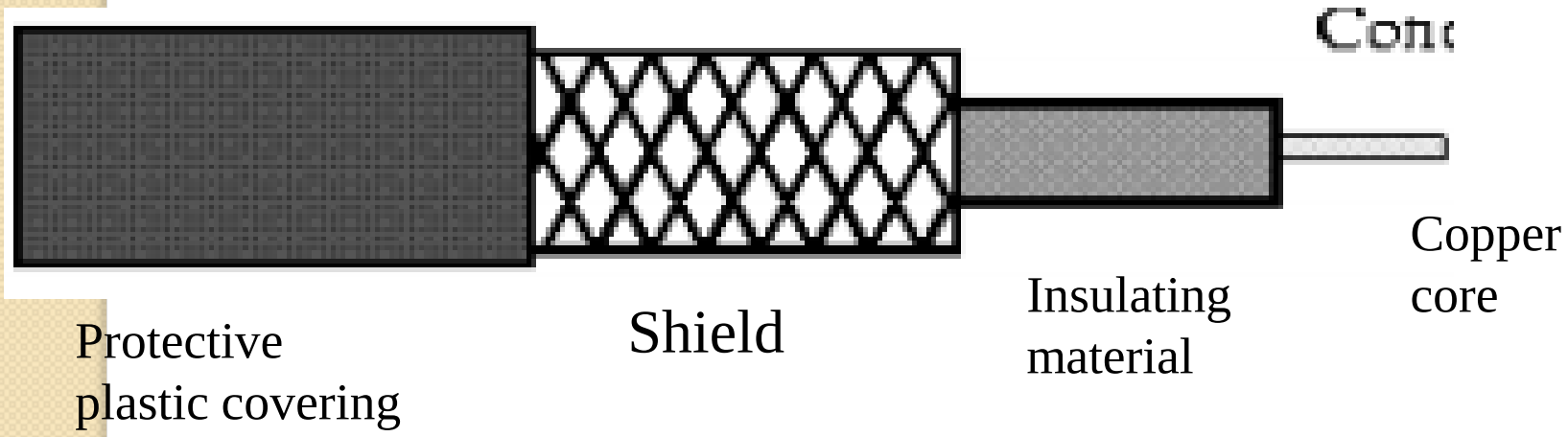
Guided media are the physical links through which signals are confined to narrow path.

Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography. Three common types of bounded media are used of the data transmission. These are **coaxial cable, twisted pair cable and fiber optics cable**

1. **Coaxial Cable**

Coaxial cable is very common and widely used commutation media. For example TV wire is usually coaxial.

Coaxial cable has two wires of copper. The core wire lies in center and is made of solid conductor. Core is enclosed in an insulating sheath. Over the sheath the second wire is wrapped around and that too in turn encased by insulator sheath. This all is covered by plastic cover.



Characteristics Of Coaxial Cable

- Low cost
- Easy to install
- Mostly used in LAN
- Coaxial cables provide high bandwidth rates of up to 450 mbps.

Advantages of Coaxial Cable

- Inexpensive
- Easy to wire
- Easy to expand

Disadvantages of Coaxial Cable

- Single cable failure can take down an entire network

2. Twisted-Pair Cable

A twisted pair consists of two conductors (Normally copper), each with its own plastic insulation,twisted together in pairs. The most popular network cabling is Twisted pair.it is a light weight,easy to install ,inexpensive and support many different types of network. It also supports the speed of 100mps.There are two types of twisted pairs cabling

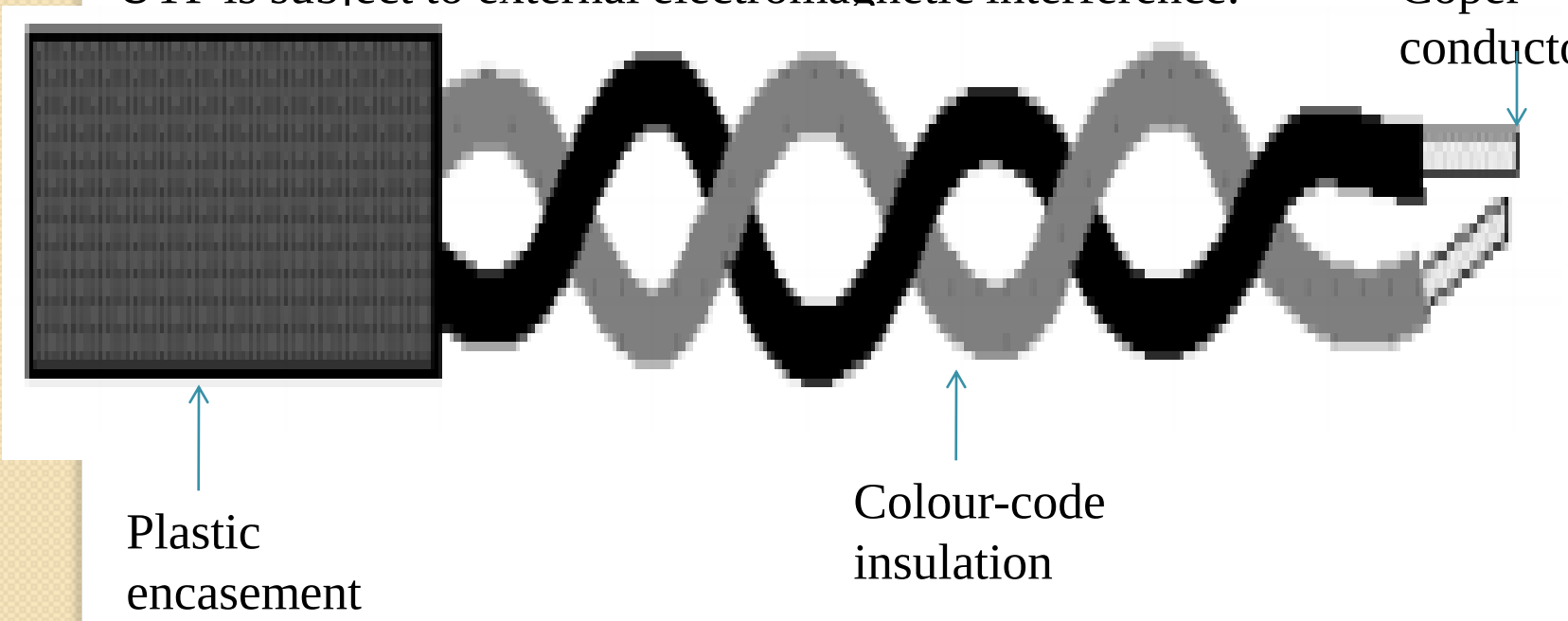
1. **Unshielded twisted pair (UTP)**
2. **Shielded twisted pair (STP)**

1. Unshielded twisted pair (UTP)

UTP is a set of twisted pair of cable within a plastic sheath. Cables without a shield are called UTP.

Cont.....

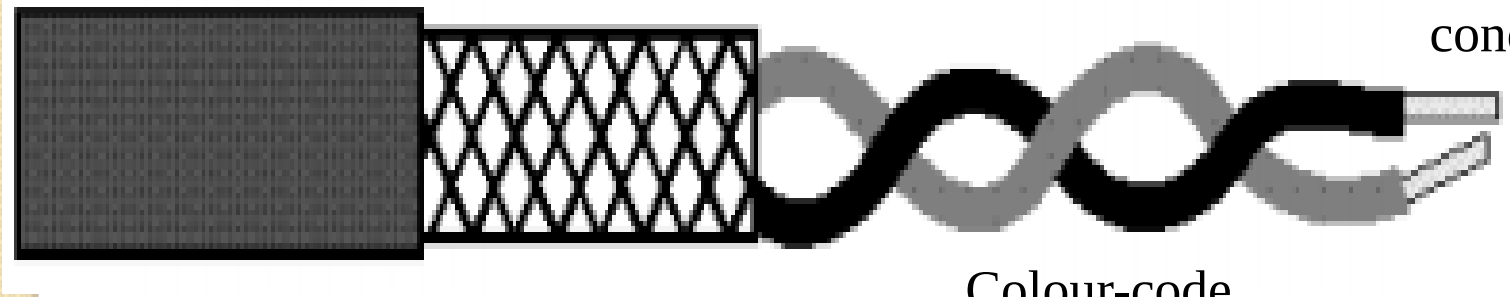
- UTP is ordinary telephone wire
- UTP is a least expensive of all the transmission media commonly used for LAN.
- Is easy to work with
- Is easy to install
- UTP is subject to external electromagnetic interference.



2. Shielded twisted pair (STP)

STP offers a protective sheathing around the copper wire.

- STP provides better performance at lower data rates
- STP are not commonly used in networks
- Installation is easy
- Cost is moderately expensive
- It still suffer from outside interference but not as much UTP.

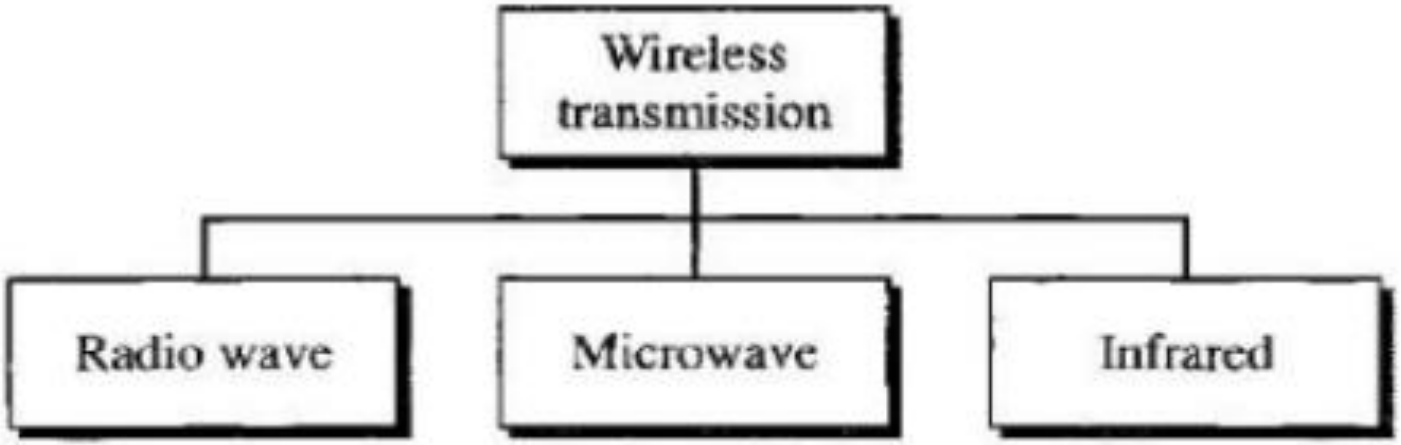


3. Fiber optic cable (FOC)

Fiber Optic works on the properties of light.FOC is a light pipe which is used to carry a light beam from one place to another. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data form. Fiber Optic provides the highest mode of speed. It comes in two modes, one is **single mode fiber** and s econd is **multimode fiber**. **Single mode** fiber can carries single ray of light whereas **multimod**e is capable of carrying multiple beams of light.

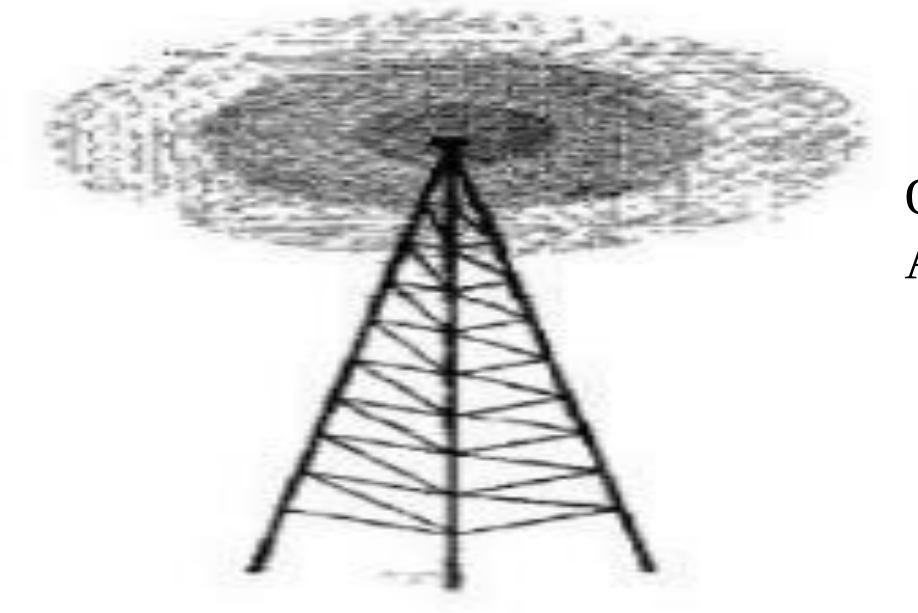
2.Unguided/Unbound Media

Unbound transmision media are the way of transmitting data without using any cables. These media are not bounded by physical greography. There is no connectivity between the sender and receiver. Information is spread over the air, and anyone including the actual recipient may collect the information. This type of transmission is called wireless.



I. Radio Waves

Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. Radio waves, for the most part, are omni-directional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.



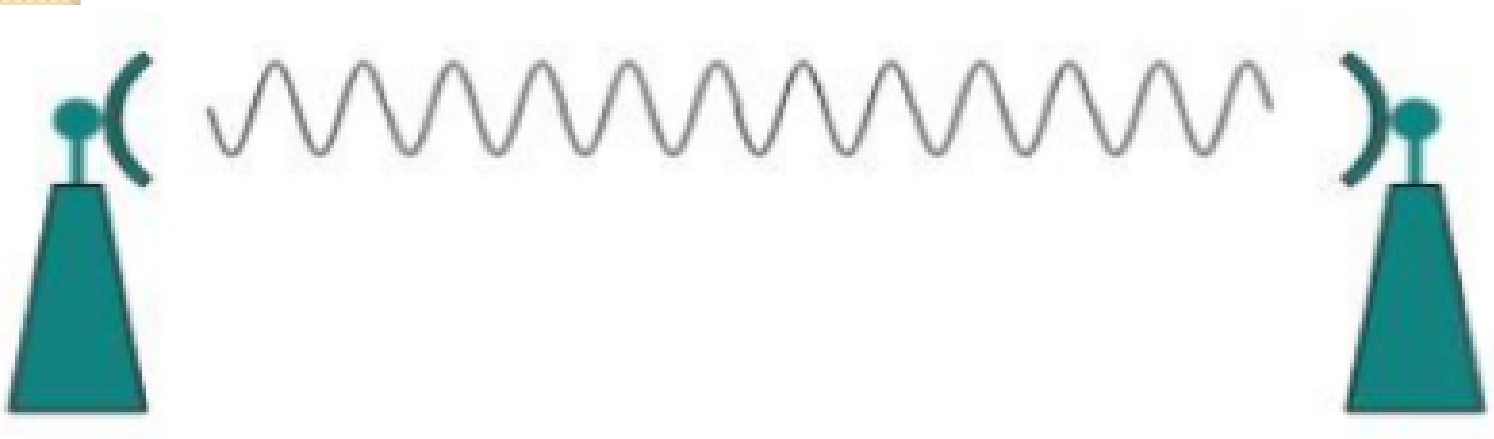
Omni directional Antenna

CONT...

The omni-directional property has a disadvantage, too. The radio waves transmitted by oneantenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

II. Microwaves

Electromagnetic waves having frequencies between I and 300 GHz are called microwaves.Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.Ex:-nsatellite TV dish



[*Image: Microwave Transmission*]

III. Infrared

Infrared waves, with wavelengths from 1 mm to 770 mm, can be used for short-range communication.the remote control used in TV,VCR and stereos all use infrared communication they are relatively directional,cheap and easy to build, but have a major drawback: they do not pass through solid object(cannot penetrate walls).infrared light is suitable for indoor wireless LAN.

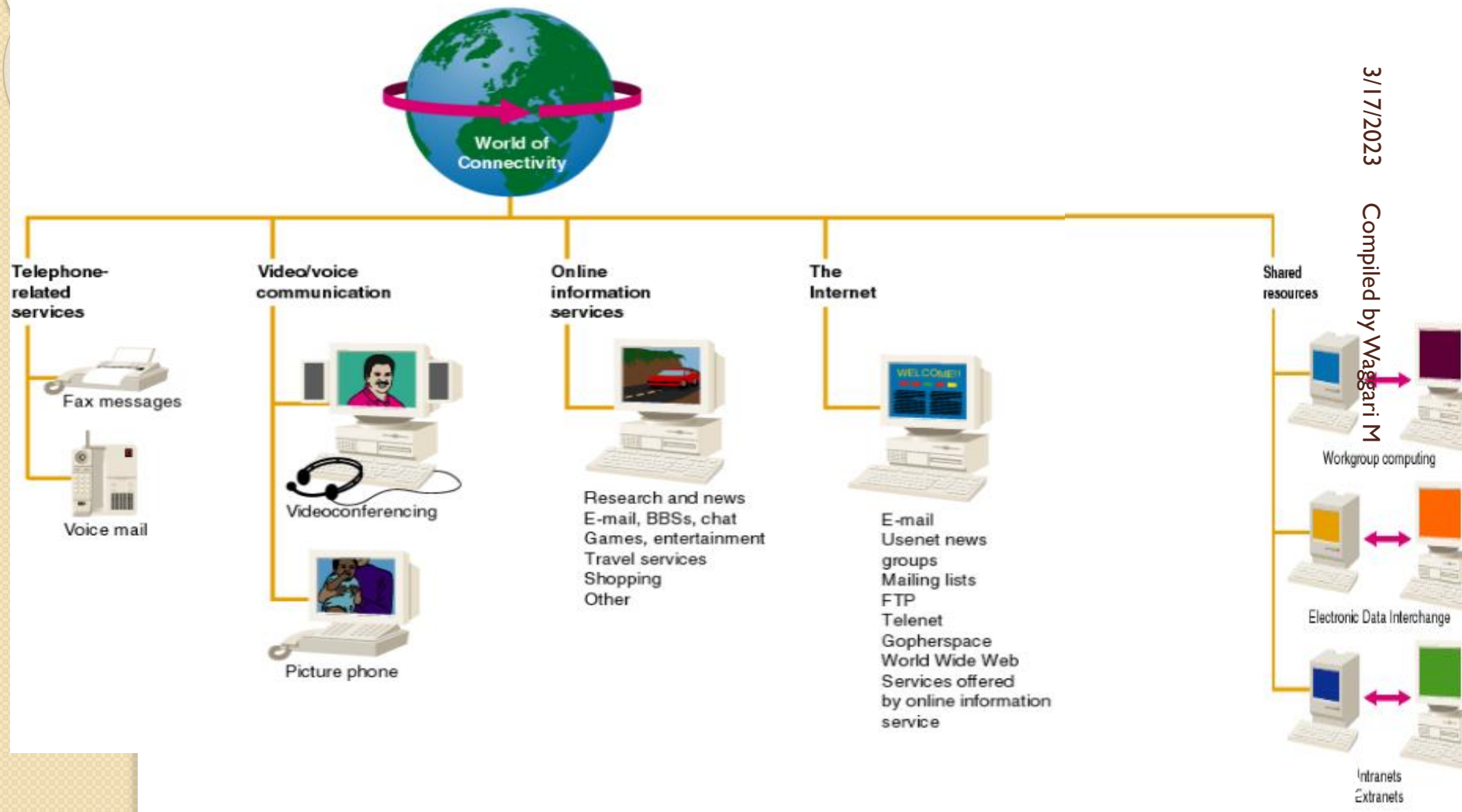
Introduction to Computer Networks

Computer Networking

A computer network is a set of computers connected together for the purpose of sharing resources. Computers on a network are called nodes. The connection between computers can be done via cabling, most commonly Ethernet cable, or wirelessly through radio wave. Connected computers can share resources like internet,printers,file servers,and other.

A network is a multipurpose connection,which allows a single computer to do more.

Uses of Computer Networks

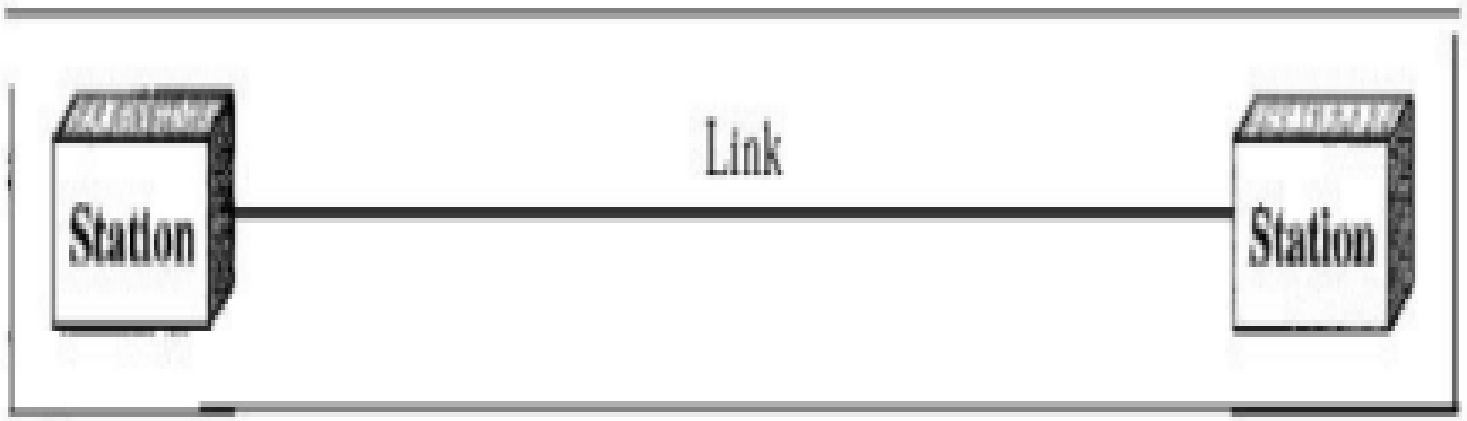


Network Line Configuration:

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time.There are two possible types of connections: **point-to-point** and **multipoint**.

1. **Point-to-Point:** A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

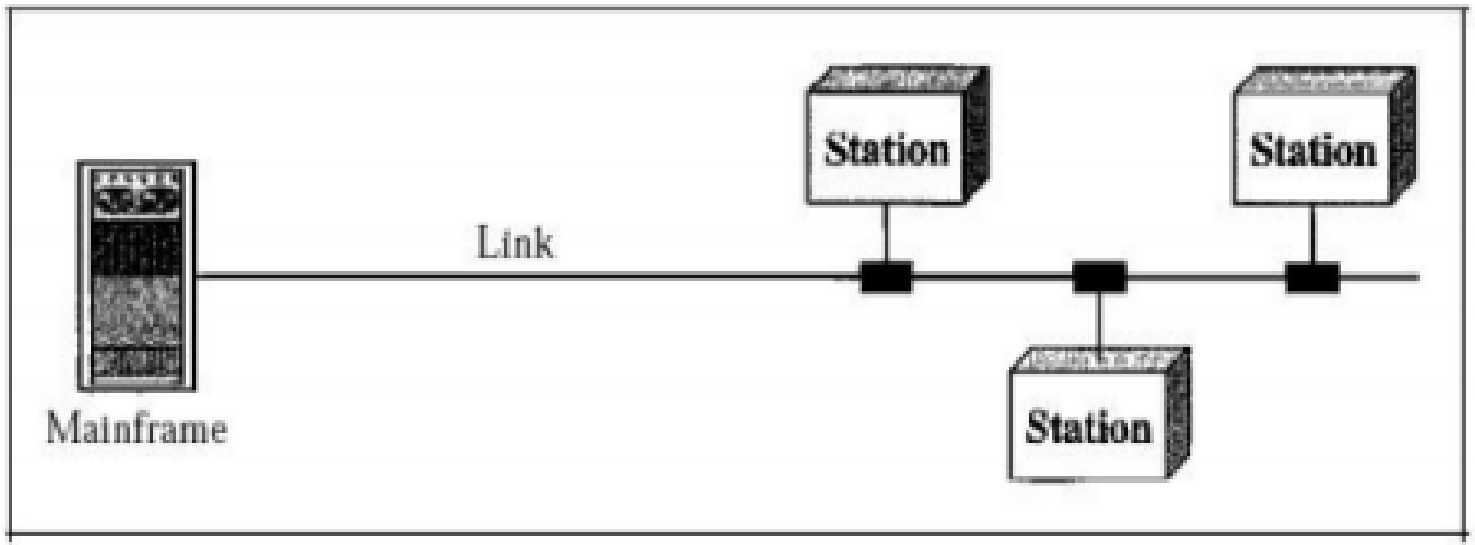
   When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.



a. Point-to-point

2. Multipoint: A multipoint (also called multi drop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.

If several devices can use the link simultaneously, it is a **spatially shared connection.** If users must take turns, it is a **timeshared connection**



b. Multipoint

Network Topologies

The topology defines how the devices (computers,printers..etc) are connected and how the data flows from one device to another. There are two conventions while representing the topologies. The physical topology defines how the devices are **physically wired**. The **logical topology** defines how the data flows from one device to another.

Physical Topology consists of four different topologies. They are:

i) Mesh Topology
ii) Star Topology
iii) Bus Topology
iv) Ring Topology

Mesh Topology

The meshtopology incorporates a unique networkdesign in which each computer on the network connects to every other, creating a point-to-point connection between every device on the network. The purpose of the meshdesign is to provide a high level of redundancy. If one network cable fails, the data always has an alternative path to get to its destination.

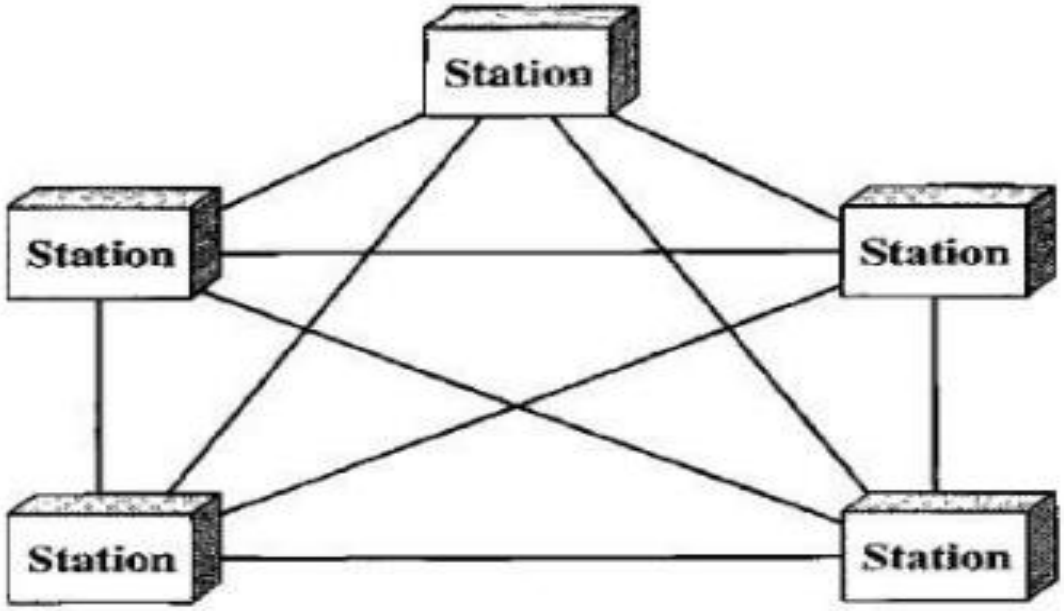


Fig. Mesh Topology

Advantages

- Provides redundant paths between devices
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.
- Point-to-point links make fault identification and fault isolation easy.
- The network can be expanded without disruption to current users.

Disadvantages

- Requires more cable than the other LAN topologies
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
- Complicated implementation.

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller,usually called a hub.
- The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

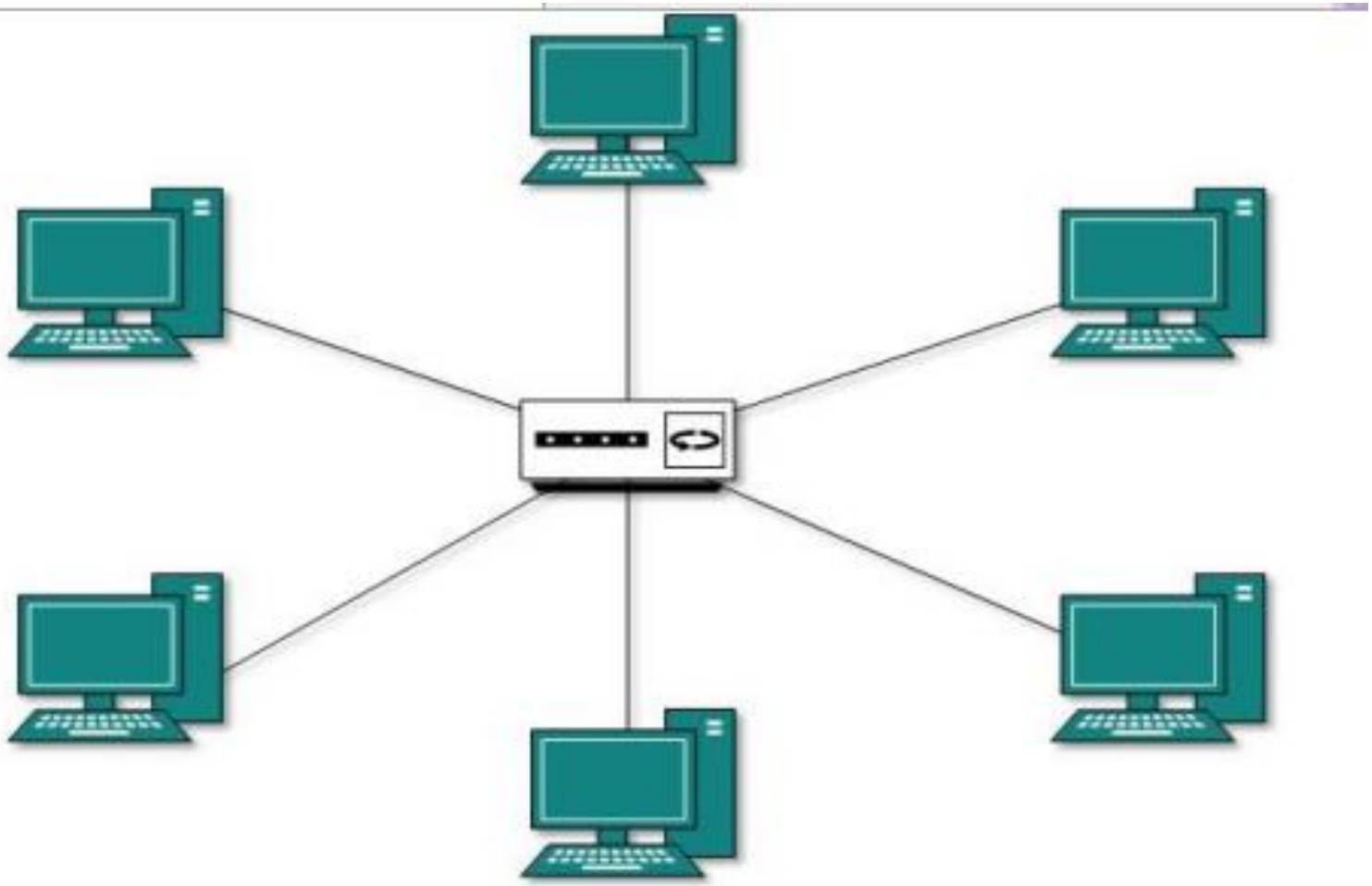


Fig. Star Topology

Advantages

- A star topology is less expensive than a mesh topology.
- In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- Cable failure affects only a single user.
- Easy to troubleshoot and isolate problems.
- Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

Disadvantages

- The dependency of the whole topology bon one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub
- Requires more cable than most of the other topologies.
- More difficultthan other topologies to implement.

Bus Topology

A bus networkuses a trunk or backbone to which all of the computers on the network connect. In a bus topology all devices are connected to the transmission medium as backbone. There must be a terminator at each end of the bus to avoid signal reflections, which may distort the original signal. Signal is sent in both directions, but some buses are unidirectional.

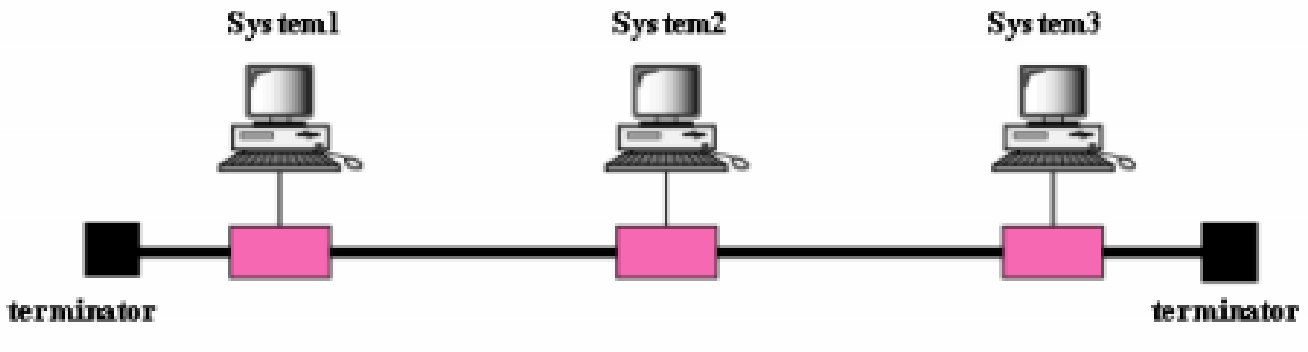


Fig. Bus Topology

Advantages

- Compared to other topologies, a bus is cheap and easy to implement.
- A bus uses less cabling than mesh or star topologie
- Good for small networks
- Does not use any specialized network equipment.

Disadvantages

- Difficult reconnection and fault isolation.
- A fault or break in the bus cable stops all transmission, even between devices on the same sideof the problem.
- There might be network disruption when computers are added or removed.

Ring Topology

In Ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure administrator may need only one more extra cable.

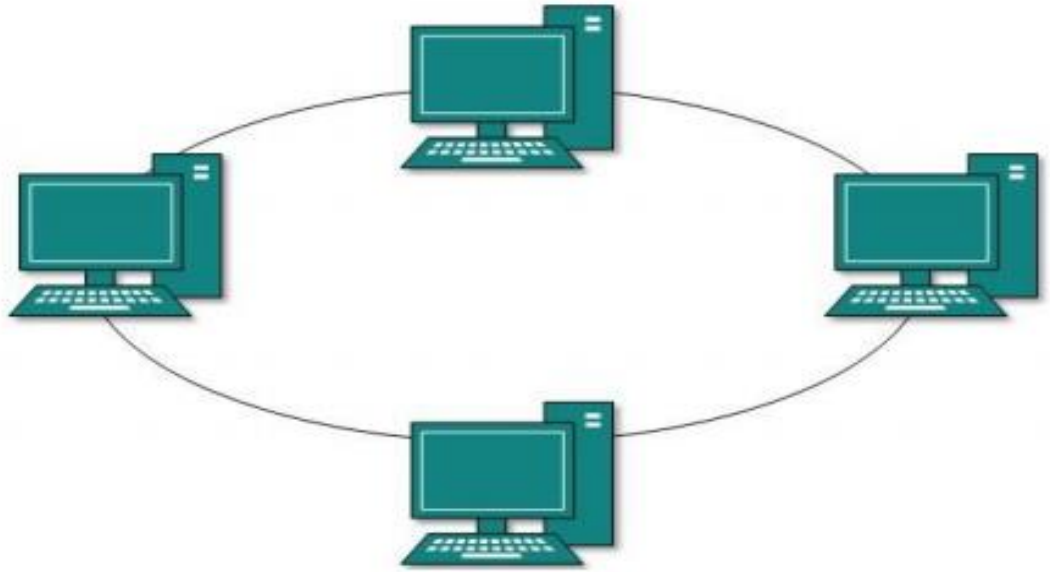


Fig. Ring Topology

Advantages

- A ring is relatively easy to install and reconfigure.
- Fault isolation is simplified
-Cable faults are easily located, making troubleshooting easier

.

Disadvantages

- Unidirectional traffic can be a disadvantage.
- In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.
- Expansion to the network can cause network disruption.

Tree/Hybrid Topology

Also known as Hierarchical Topology is the most common form of network topology in use present day. This topology imitates as **extended Star Topology** and inherits properties of **Bus topology**. This topology divides the network into multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The **lowest most is access-layer** where user‟s computer are attached. The **middle layer is known as distribution layer**, which works as mediator between upper layer and lower layer. The **highest most layer is known as Core layer**, and is central point of the network, i.e. root of the tree from which all nodes fork.

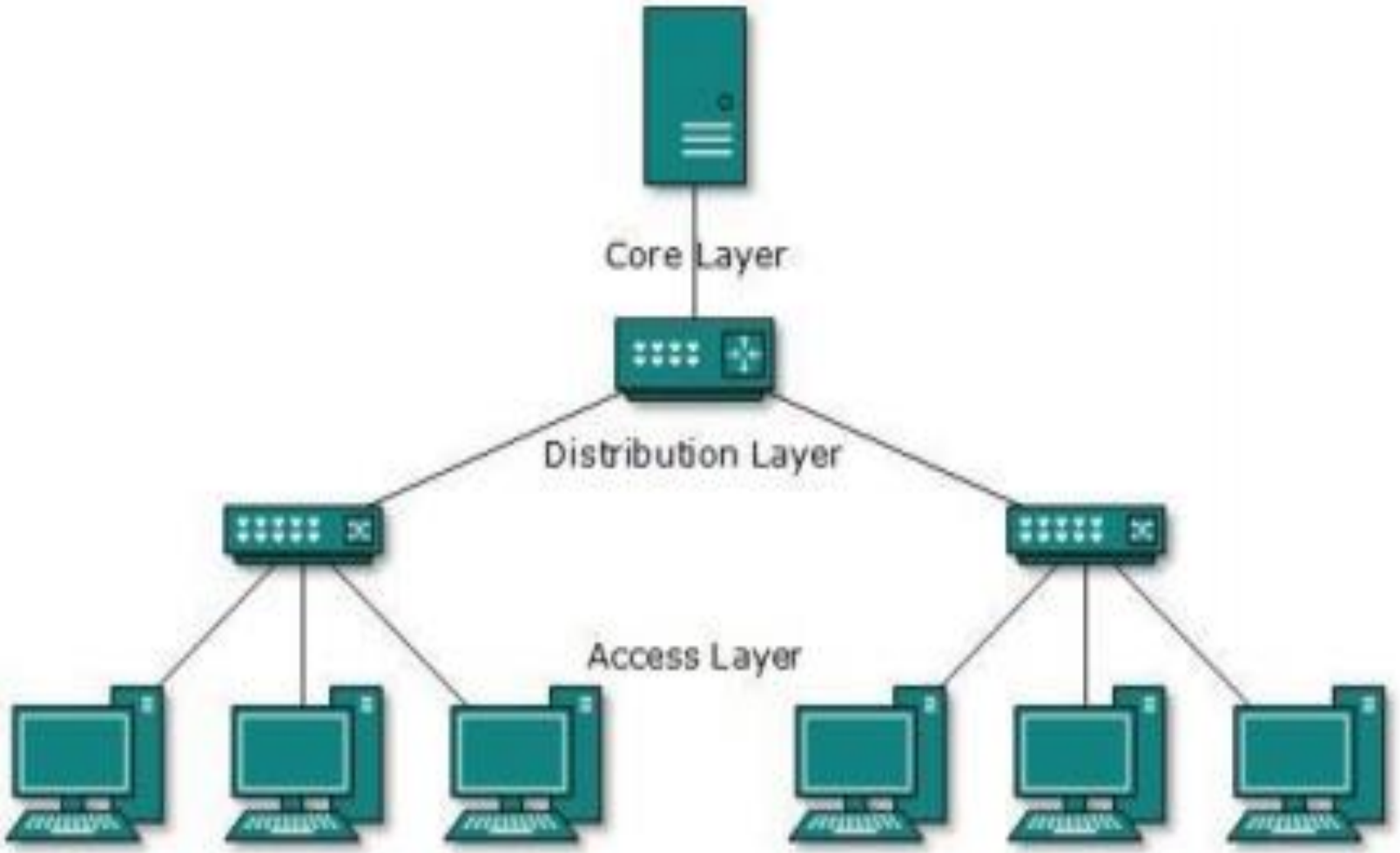


Fig.Tree Topology

All neighbouring hosts have point-to-point connection between them. Like bus topology, if the root goes down, the entire network suffers. Though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment and so on.

Network Types

There are basically three categories of networks based on its size and geographical coverage

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)

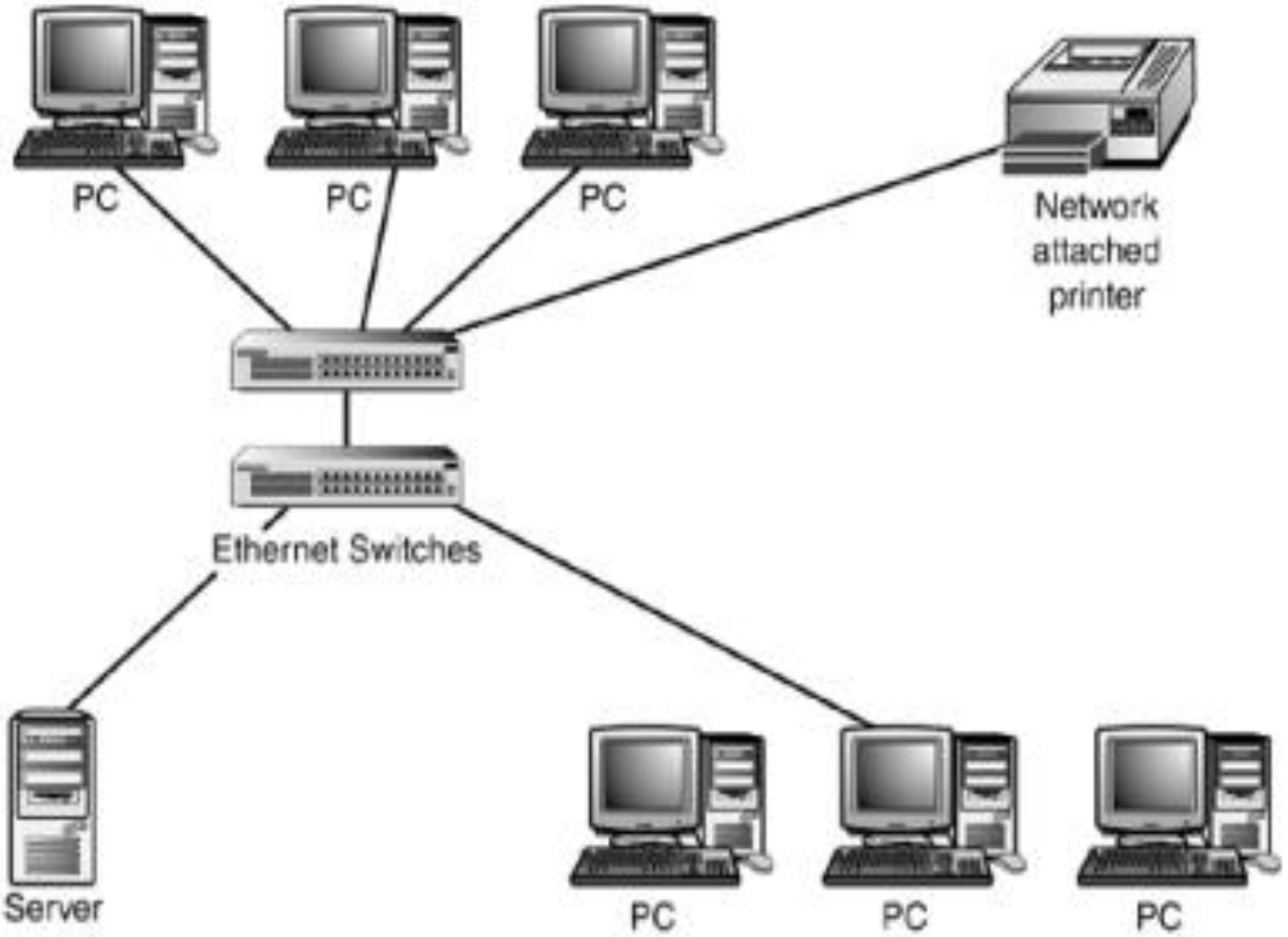
Local Area Network (LAN)

This is one of the original categories of network,and one of the simplest. LAN is a privately owned computer network covering a small networks geographical area,like a home,office,or groups of buildings. The function of the LAN is to interconnect workstation computers for the purposes of sharing files and resources. Because of its localized nature, the LAN is typically high speed and cheaper to set up than a WAN, Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

- Smallest LAN may only use two computers,while larger LANs can accommodate thousands of computers. High speed and relatively low cost are the defining characteristics of LANs.

- If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network (WLAN)

Figure 1. Local area network.

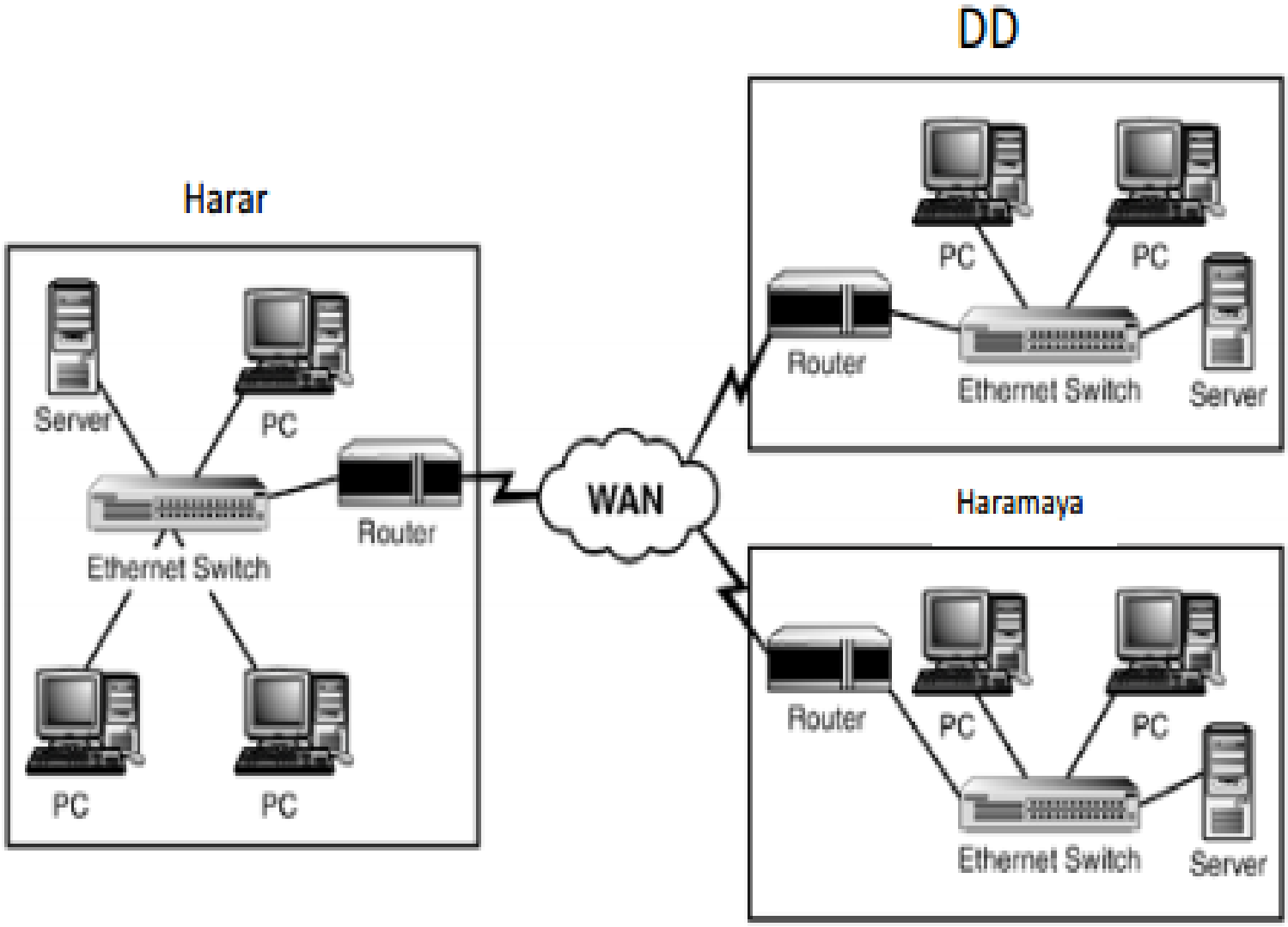


Wide Area Network (WAN)

WAN is a telecommunication network. It is simply a LAN of LANs (network of networks). A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

- WAN are characterized by the slowest data communication rates and the largest distances. It generally utilize different and much more expensive networking equipment than do LANs.
- Organizations supporting WANs using the internet protocol are known as Network Service Providers (NSPs). These form the core of the internet.by connecting the NSP WANs together using links at Internet Packet Interchanges a global communication infrastructure is formed.

Figure 2 Wide area network.



Metropolitan Area Network (MAN)

This is a network which is larger than a LAN but smaller than a WAN, and incorporates elements of both it typically spans a town or city and is owned by a single person or company.

- ✓ MANs rarely extend beyond 100 KM and frequently compise a combination of different hardware and transmission media
- ✓ The two most important components of MANs are security and standardization. Security is important because information is being shared between dissimilar systems. Standardization is necessary to ensure reliable data communication.

Personal Area Network (PAN)

A personal area network is a computer network organized around an individual person within a single building. A typical PAN would include one or more computer,telephones,peripheral devices,video game consoles and other personal entertainment devices.PAN can be constructed with cables or wirelessly.This type of network provides great flexibility for example:-

- Send a document to printer in the office upstaires while you are sitting on the couch with ur laptop
- Upload a photo from your cell phone to your desktop computer
- Watch movies from an online streaming service to your TV

Network Models

There are two basic wired network models from which to choose the peer-to-peer network model and the client/server model. The model used for a network is determined by several factors, including how the network will be used, how many users will be on the network, and budgetary considerations.

1. Peertopeer Networking Model

A peer-to-peer network is a decentralized network model offering no centralized storage of data or centralized control over the sharing of files or resources.Each computers acts as both the client and the server, communicating directly with the other computer

Peer-to-peer networks are typically found in small offices or in residential settings where only a limited number of computers will be attached and only a few files and resources shared. A general rule of thumb is to have no more than 10 computers connected to a peer-to-peer network.

2. Client/Server Networking Model

A client/Server computer network is one which has a centralized infrastructure. It allows for centralized network management of all network services,including user management, security, and backup procedures.

- Most data and applications are installed on the server. When clients need access to these resources, they access them from the server.

Table 1 Comparison of Networking Models

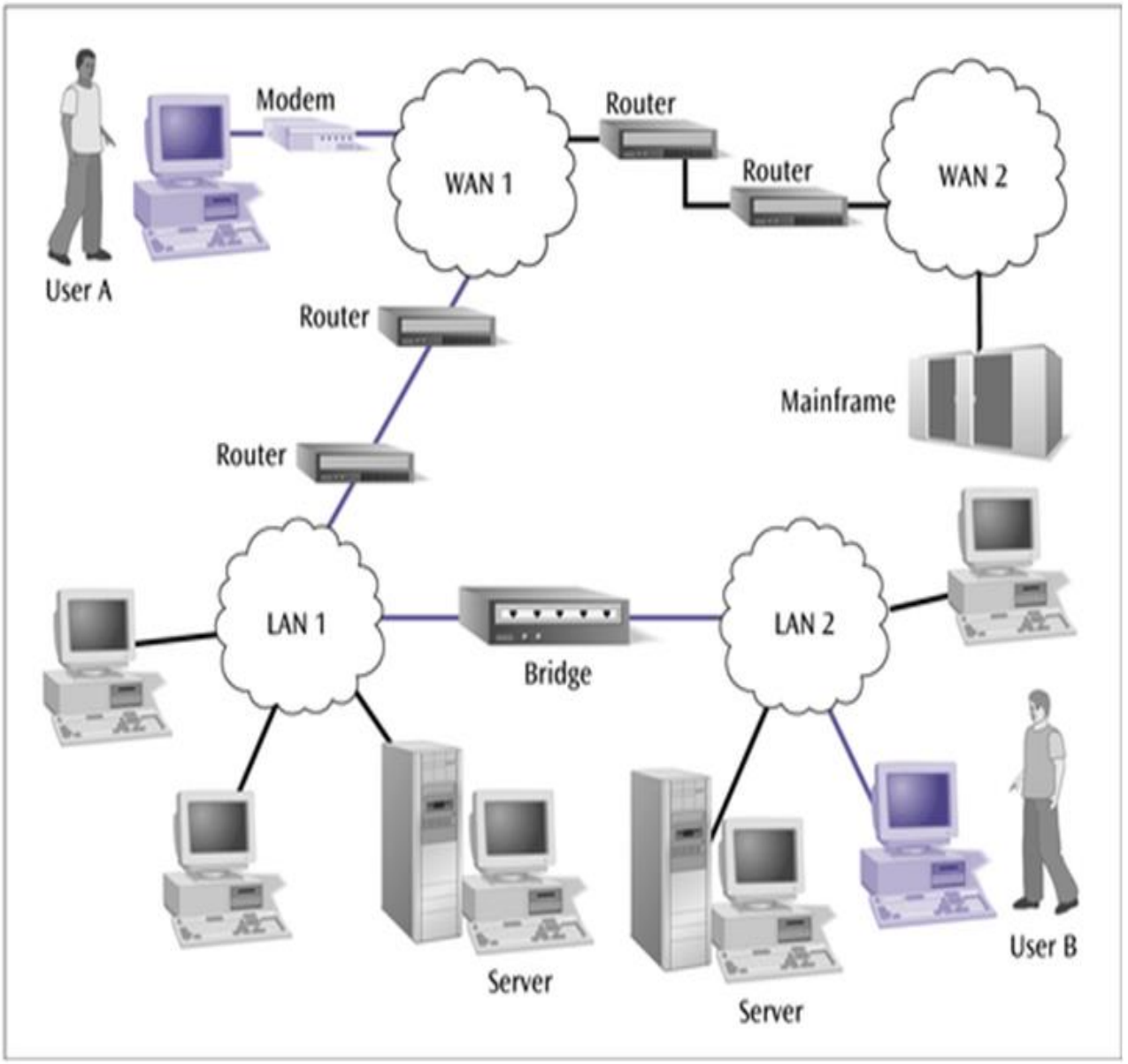
Attribute	Peer-to-Peer Network	Client/Server Network
Basic	Clients and server are not distinguished,each node act as client and server	There is a specific server and specific clients connected to the server
Size	Restricted to a maximum of 10 computers.	The size of the network is limited only by server size and network hardware, and it can have thousands of connected systems.
Service	Each node can request for services and can also provide the services	The client request for service and server respond with the service

Focus	connectivity	Sharing the information
Data	Each peer has its own data	The data is stored in a centralized server
Administration	Each individual is responsible for the administration of his or her own system. A administrator is not needed.	A skilled network administrator is often required to maintain and manage the network.
Security	Each individual is responsible for maintaining security for shared files or resources connected to the system.	Security is managed from a central location but often requires a skilled administrator to correctly configure.
Cost	Minimal startup and implementation cost.	The client-server are expensive to implement
Stability	Peer-to-peer suffer if the number of peers increases in the system	Client-server is more stable and scalable

Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another.When two or more networks are connected, they become an internetwork, or internet.

An overall view of the interconnection between local area networks and wide area networks

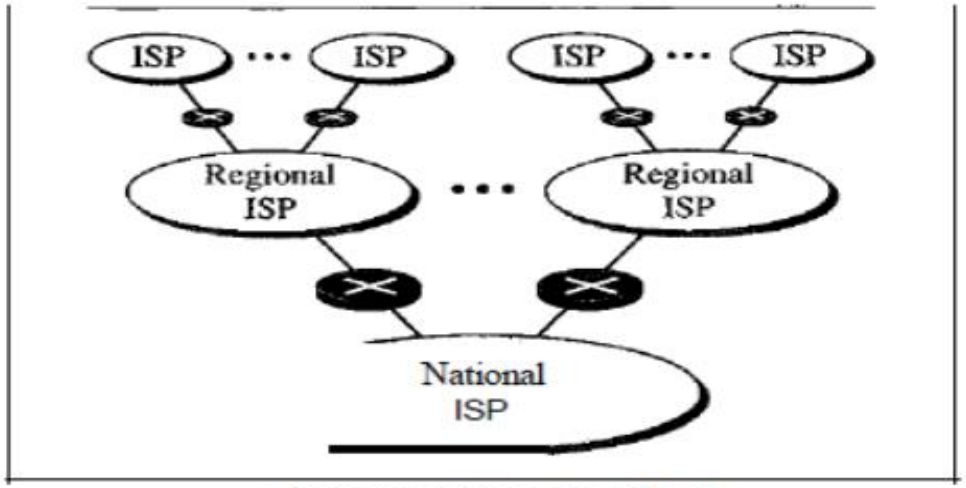


Network, internet, and Internet

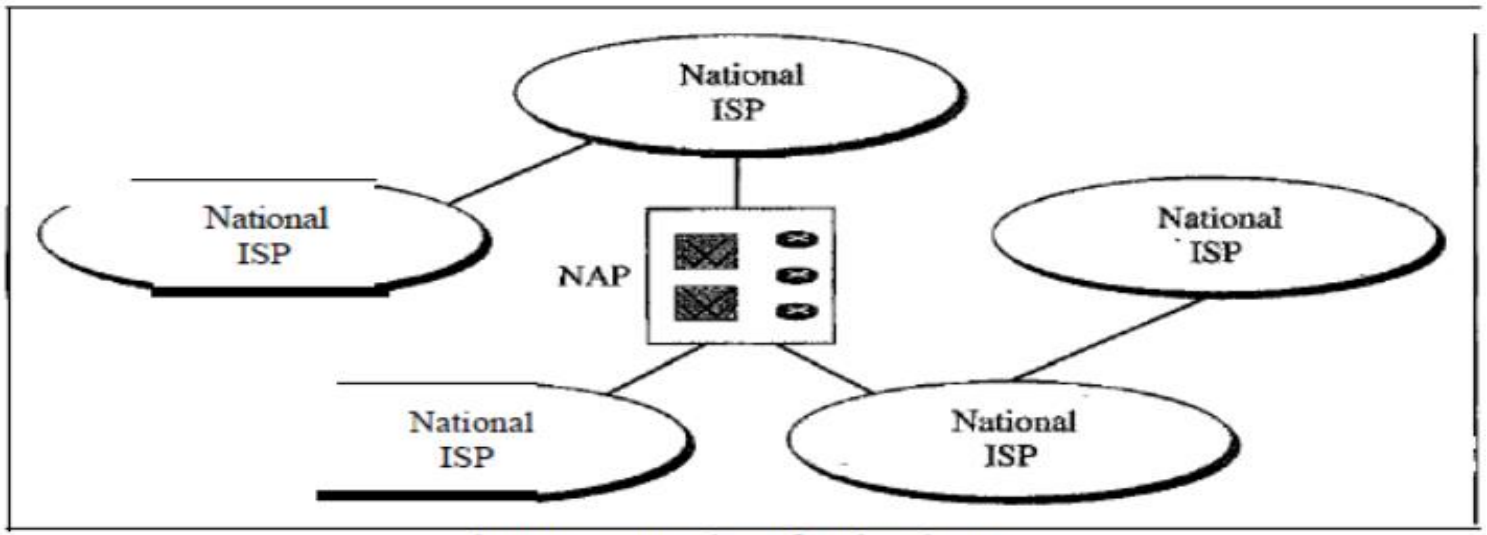
- A network is a group of connected communicating devices such as computers and printers.
- An internet (note the lowercase letter i) is two or more networks that can communicate with each other.
- The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.
- Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet.

End of Chapter 2

Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

Difference between Internet and Intranet

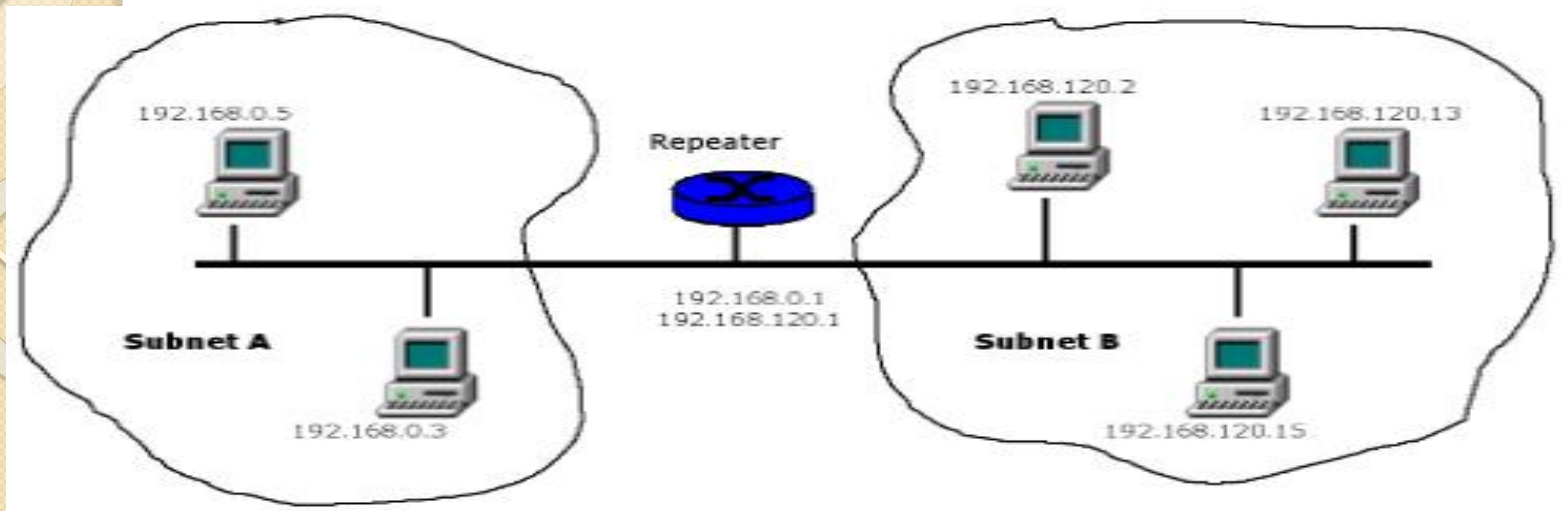
Internet	Intranet
Internet is wide network of computers and is open for all	Intranet is also a network of computers designed for specific group of users
Internet itself contains a large number of intranets.	Intranet can be accessed from internet but with restrictions
The number of users who use internet is unlimited	The number of users is limited
The visitors traffic is unlimited	The traffic allowed is also limited
Internet contains different source of information and is available for all	Intranet conatins only specific group information.

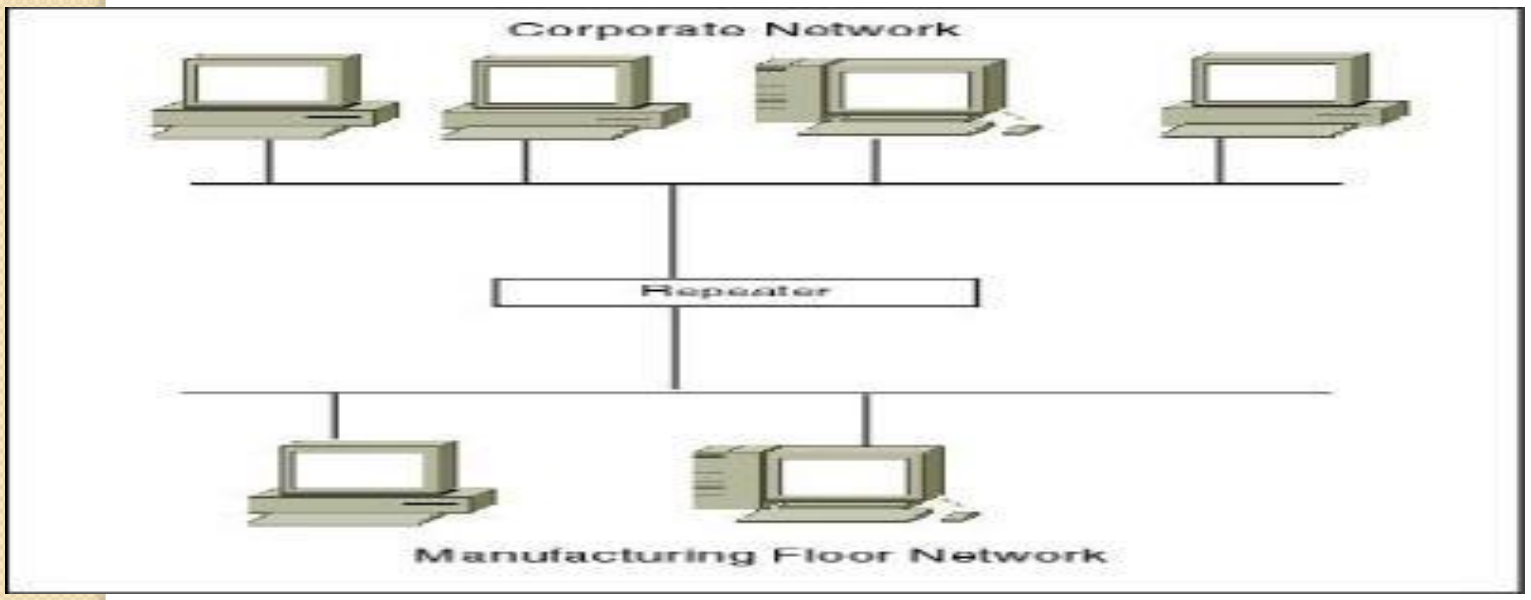
Networking Devices

Repeater

A repeater is an electronic device that amplifies the signal it receives, or else, you can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances.

- ✓ It can regenerate signals at the bit level to allow them to travel a longer distance on the media.
- ✓ It operates at Physical Layer of OSI
- ✓ A repeater does not actually connect two LANs; it connects two segments of the same LAN. The segments connected are still part of one single LAN. A repeater is not a device that can connect two LANs of different protocols.
- ✓ A repeater forwards every frame; it has no filtering capability.


192.168.0.5
Repeater
192.168.120.2
192.168.120.13
192.168.0.1
192.168.120.1
Subnet A
Subnet B
192.168.0.3
192.168.120.15


Corporate Network
Repeater
Manufacturing Floor Network

Hub

Hubs are used in networks that use twisted-pair cabling to connect devices. Hub is also used to do data transfer, when a host sends a data packet to a network Hub, the Hub copies the data packet to all of its ports connected to.

However, because of its working mechanism, a hub is not so secure and safe.Moreover, copying the data packets on all the interfaces make it slower and more congested which lead to use of switch.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly referred to as workgroup hubs. Others can accommodate larger numbers of devices (normally up to 32).

Types of Hubs

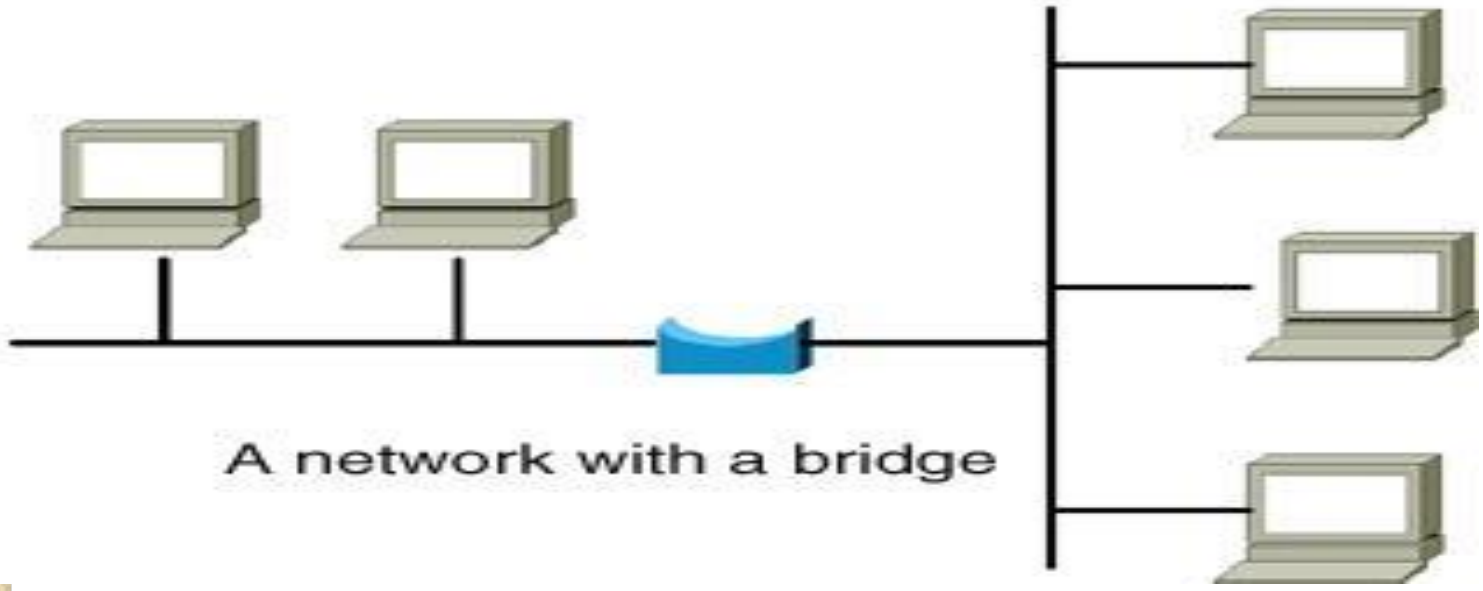
Passive Hubs:- In its most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a passive hub. do not amplify the electrical signal of incoming packets before broadcasting them out to the network. It is just a connector. It connects the wires coming from different branches.

Active Hubs:- a type of hub that can perform amplification, as does a repeater. Far more common nowadays is an active hub, which, as well as providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices.

Intelligent hubs:- add extra features to an active hub that are of particular importance to businesses.

Bridge

- Bridges are used to logically separate network segments within the same network.
- The function of the bridge is to make intelligent decisions about whether or not to pass signals on to the next segment of a network. When a bridge receives a frame on the network, the destination MAC address is looked up in the bridge table to determine whether to filter, flood, or copy the frame onto another segment.
- If a router connects two different types of networks,then a bridge connects two subnetworks as a part of the same networkyou can think of two different labs or floors connected by bridge.
- Broadcast Packets are forwarded to all directions.

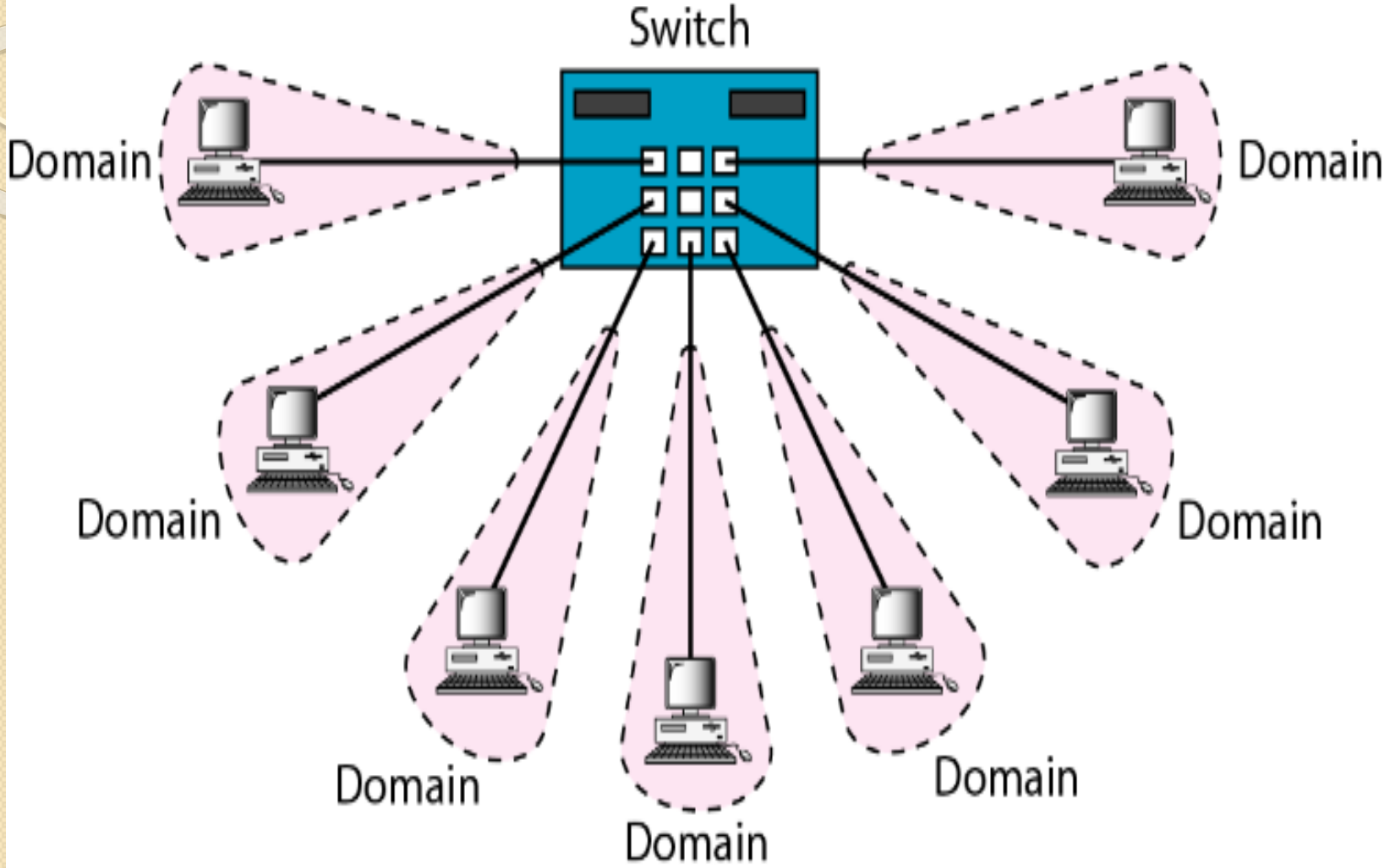


A bridge has filtering capability. It can check the destination address of a frame and decide if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision must specify the port.

Switch

Switches provide a unique network segment on each port, thereby separating collision domains. Today, network designers are replacing hubs in their wiring closets with switches to increase their network performance and bandwidth while protecting their existing wiring investments.

- Switch is more intelligent than Hub.while hub just does the work of data forwarding, a switch does ‘filter and forwarding’ more intelligent way of dealing with data packets.
- When packet is received at one of the interfaces of the switch,it filters the packet and sends only to the interface of the intended receiver.


Switch
Domain
Domain
Domain
Domain
Domain
Domain
Domain

Types of Switches

1.Cut-through switch

In a cut-through switching environment, the packet begins to be forwarded as soon as it is received. This method is veryfast, but creates the possibility of errors being propagated through the network, as there is no error checking.

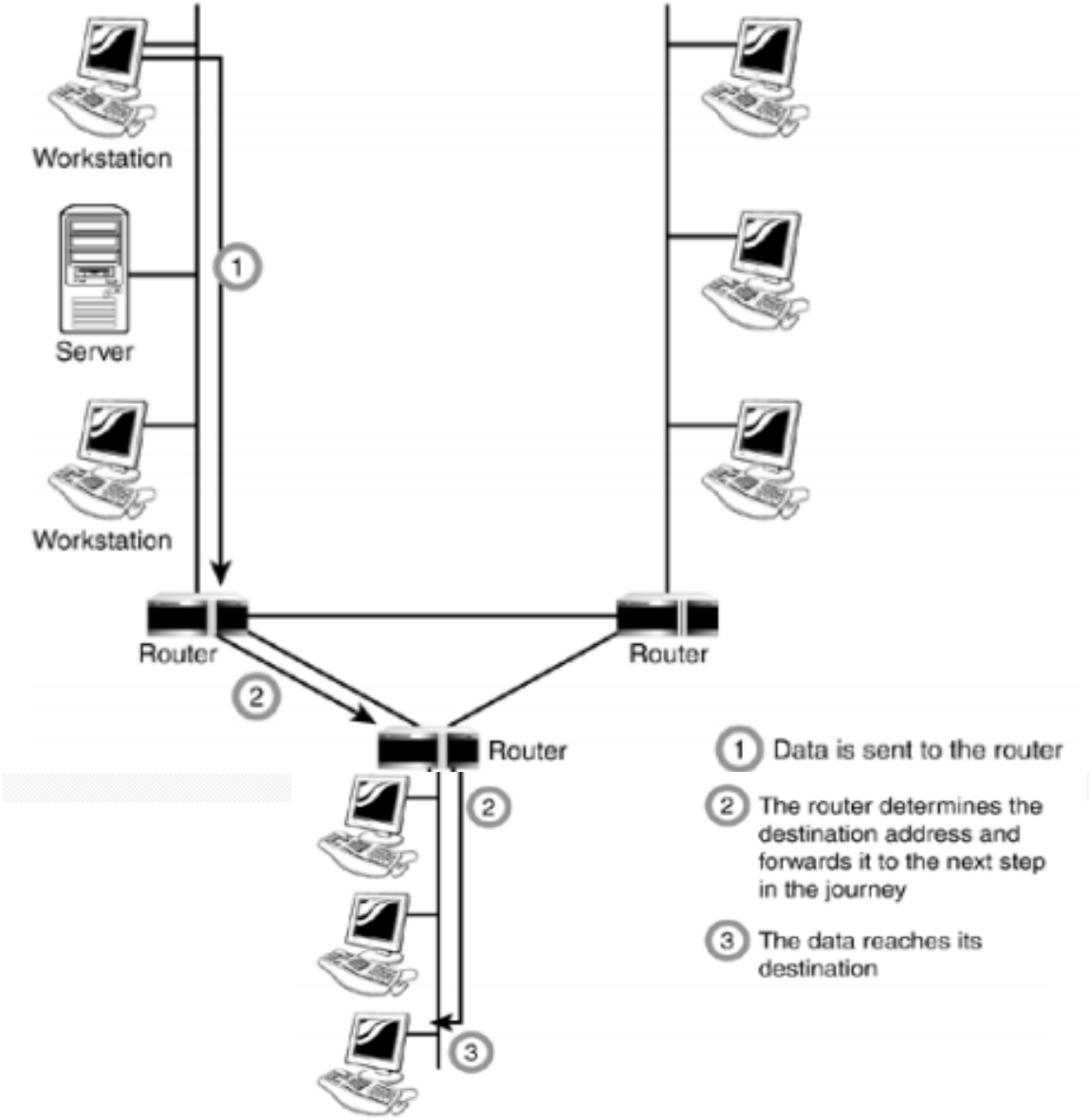
2.Store and Forward Switch

Unlike cut-through, in a store-and-forward switching environment, the entire packet is received and error checked before being forwarded. The upside of this method is that errors are not propagated through the network. The downside is that the error checking process takes a relatively long time, and store-and-forward switching is considerably slower as a result.

Router

A router is a network device which is responsible for routhing traffic from one to another network. These two could be a private company net to public network. You can think a router as a traffic police who directs different net traffic to different directions.

- A router can be a dedicated hardware device or a computer systemwith more than one network interface and the appropriate routing software.
- When a router receives a packet of data, it reads the header of the packet to determine the destination address. Once it has determined the address, it looks in its routing table to determine whether it knows how to reach the destination and, if it does, it forwards the packet to the next hop on the route. The next hop might be the final destination, or it might be another router.


Workstation
Server
Workstation
Router
Router
Router
1
2
2
3
1 Data is sent to the router
2 The router determines the destination address and forwards it to the next step in the journey
3 The data reaches its destination

Modem

A modem, short for modulator/demodulator, is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines.

Our computer generates binary data or digital data in forms of 1s and 0s and on the other hand, a wire carries an analog signal and that's where a modem comes in.

A modem stands for (Modulator+Demodulator) That means it modulates and demodulates the signal between the digital data of a computer and analog signal of a telephone line.

Network Interface Card (NIC): is a hardware device that acts as an interface through which a computer connects to a network. NICs work at both data link layer (layer 2) and the Physical layer (layer 1) of the OSI model. At the data link layer, the NIC converts the data packets into data frames; at the physical layer, it is responsible for converting the data into signals, and transmitting them across the communication medium. NIC is usually an expansion card on the computer with a port to plug in the network cable. NIC has its own MAC address.

- ✓ NIC turns data into an electrical signal that can be transmitted over the network.

Whether you work in wired network office or a wireless one, one thing is common for both environments: it takes both network software and hardware (cables,routers,etc) to transfer data from your computer to another or from a computer thousands of miles away to yours. And at the end ,to get the data you want right to you, it comes down to addresses, so along with an IP address(logical address), there is also a hardware address(physical address) Typically it is tied to a key connection

Chapter 3

Communication Standards

- OSI Reference Model
- TCP/IP Protocol Model

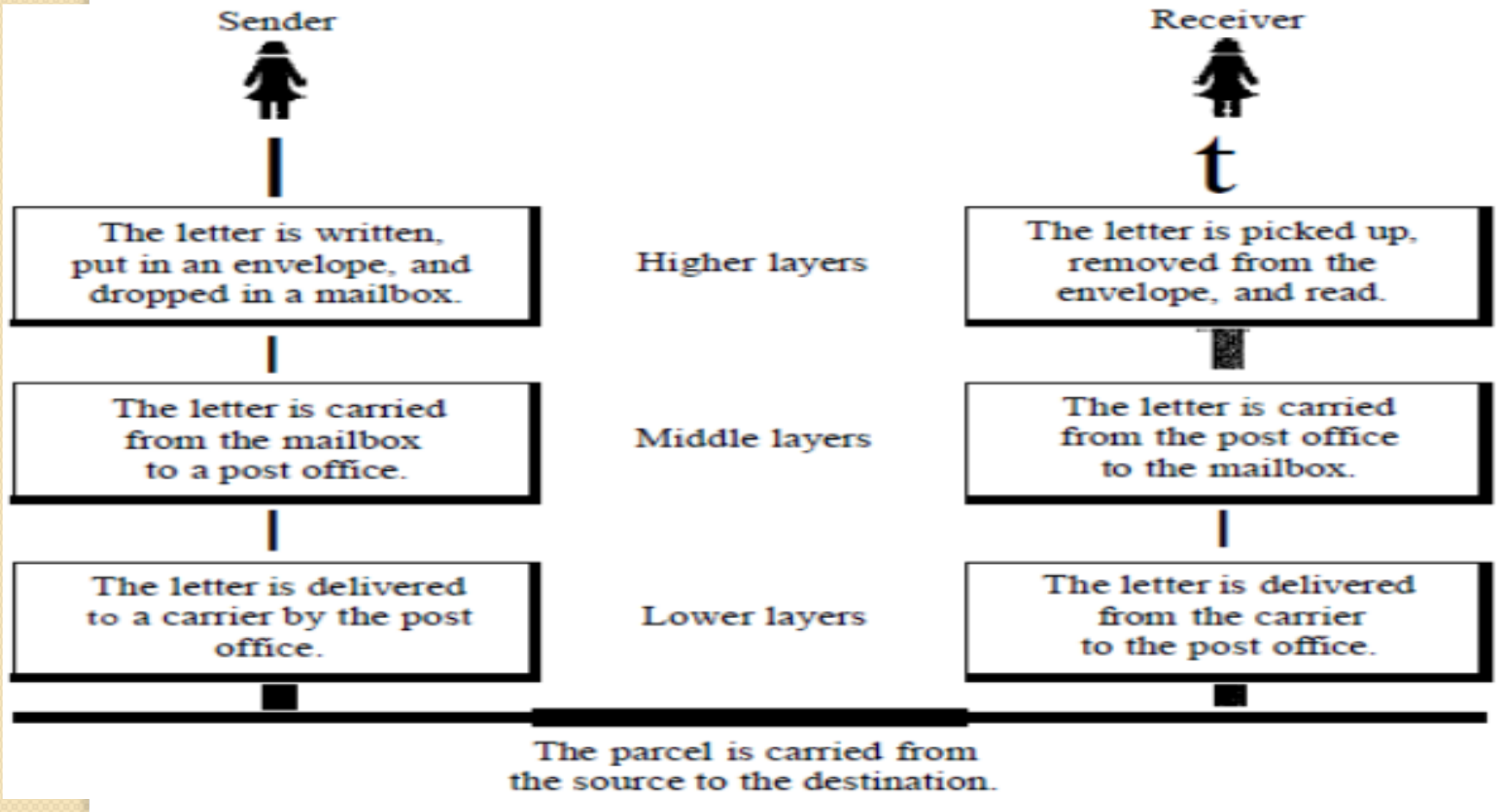
Communication and Layer Architecture

- A network is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network to another.
- The software consists of instruction sets that make possible the services that we expect from a network For example, the task of sending an e-mail from one point in the world to another can be broken into several tasks, each performed by a separate software package.

Layered Tasks

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail.

The process of sending a letter to a friend would be complex if there were no services available from the post office.



- Layers describe the logical groupings of the functionalityandcomponents in an applicaton
- Layer architecture simplifies the network design.
- It is easy to debug network applications in a layered architecture network.
- The network management is easier due to the layered architecture.
- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

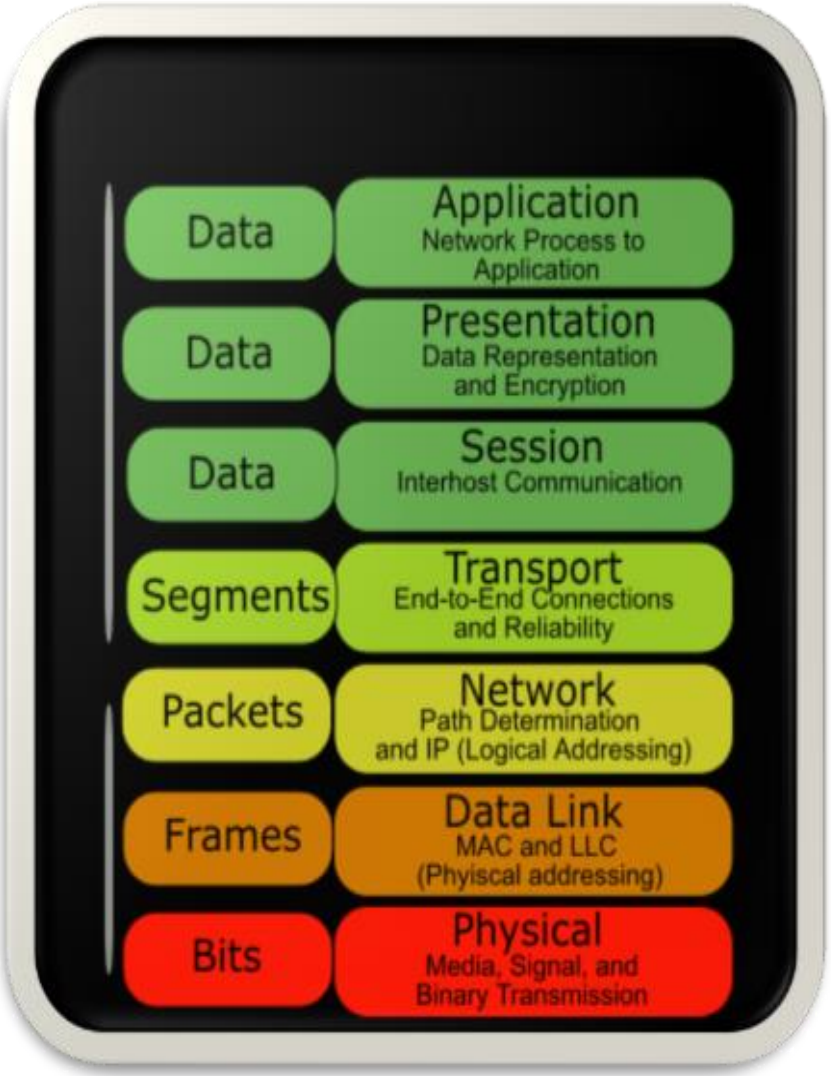
Open Systems Interconnection (OSI)

1. **OSI Model**

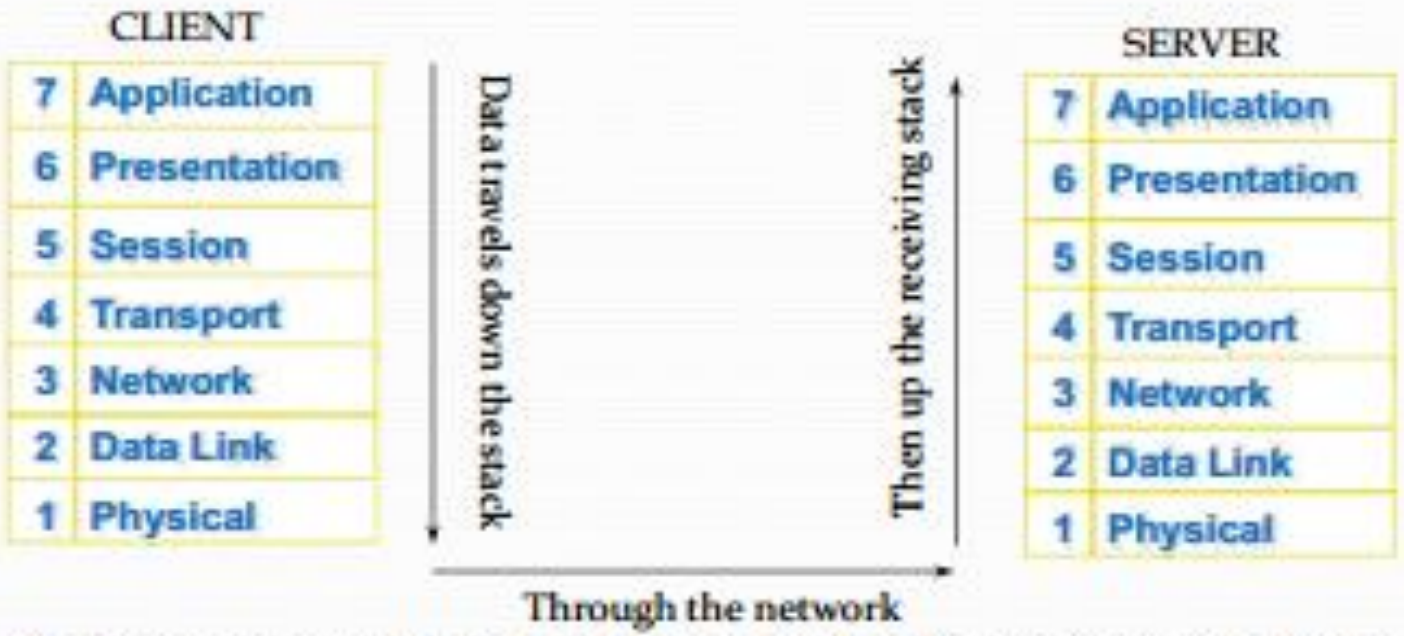
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust and interoperable
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- The OSI model 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 divides 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.

OSI Model Layers

7	Application	Network Processes to Applications
6	Presentation	Data Representation
5	Session	Interhost Communication
4	Transport	End-to-end Connections
3	Network	Address and Best Path
2	Data Link	Access to Media
1	Physical	Binary Transmission



OSI Model Data Flow



As the data passes through each layer on the client information about that layer is added to the data.. This information is stripped off by the corresponding layer on the server.

- **Layer 7 – Application Layer**

  The Application Layer represents the interface between the end-user and the network. Some of the protocols that reside here are HTTP, SMTP, or FTP. Generally speaking all applications that you use to connect to something resides here: Internet Explorer, Mozilla Firefox, Outlook Express, Yahoo Messenger, etc.

- **Layer 6 – Presentation Layer**

  The Presentation Layer transforms data to make a general interface to the Application layer.It decodes, encodes and compresses data for the upper layer. You will notice that every layer serves the layer above it. Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data .

The following are the various services in presentation layer:

POP, SMTP (e-mail, Post office protocol, Simple MailTransfer Protocol), Usenet (for news groups), HTTP (hyper text transfer protocol for web applications), FTP, TFTP (File transfer protocol, trivial FTP for file transfer), Telnet (Terminal Network),DNS(Domain name server,) SNMP (Simple Network Management Protocol).

Layer 5 – Session Layer:

The Session Layer includes the sessions between computers. It opens,maintains and terminates the connections p, between the client and the foreign server

Allows applications on connecting systems to standard ports & establish a session. Provides synchronization between communicating computers. Messages are sent between layers.

Protocols and Implementations:

Video: Quicktime, MPEG

Graphics: Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG)

- On layers 5-7 the data package is in the form of data stream.

Layer 4 Transport Layer:

- The Transport Layer provides data flow between computers; it relieves the upper layers of the concern of getting and sending the data of getting and sending the data.
- Responsible for packet handling. Ensures error-free delivery. Repackages messages (while receiving), divides messages into smaller packets (while transmitting), and handles error handling. segments of message fragments are sent between layers.

Protocols:

- Transmission Control Protocol (TCP) – Connection Oriented
- User Datagram Protocol (UDP) – Connectionless.

TCP - connection-oriented communication for applications to ensure error free delivery; UDP -connectionless communications and does not guarantee packet delivery between transfer points.

Layer 3 Network Layer:

Translates system names into addresses. Responsible for addressing, determining routes for sending, managing network traffic problems, packet switching, routing, data congestion, and reassembling data. Datagrams are sent between layers.

Depends on source

Only two devices whichare directly connected by the same "wire"can exchange data directly

- Devices not on the same network must communicate via intermediate system
- Router is an intermediate system
- The network layer determines the best way to transfer data. It manages device addressing and tracks the location of devices.

Hardware:

The router operates at this layer.

Layer 2 Data link Layer:

Sends data from network layer to physical layer. Manages physical layer communications between connecting systems. Data frames are sent between layers.

- The Data Link Layer takes the bits from layer one andarranges them into data structures called frames.
- It also uses a Frame Header stating the sender MAC address and destination MAC address in it.
- Note that these values change by passing through network nodes like router interfaces or servers.

Hardware:

- Bridges
- Switch
- WAP (Wireless Access Point

Layer 1 – Physical Layer:

- The Physical Layer defines the electrical part of the communication: the binary signals that are transmitted and received in the data exchange.
- Transmits data over a physical medium. Defines cables, cards, and physical aspects. Data bits are sent.

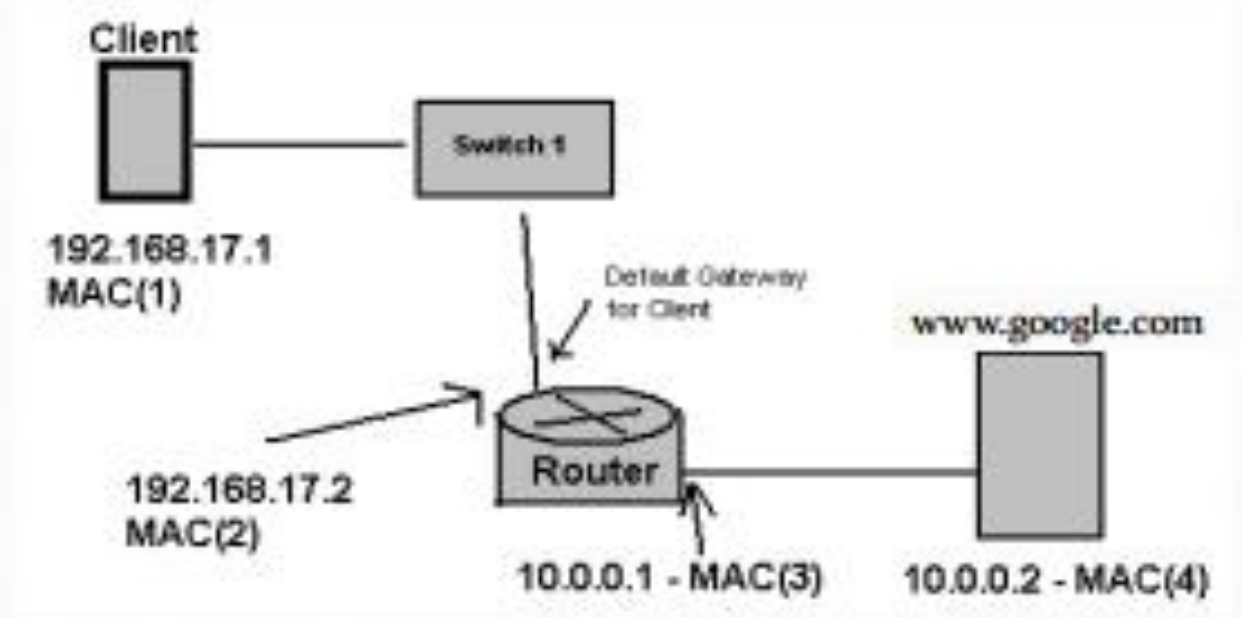
As you probably expected, the data packet looks here something like 1100110000011001100.

Hardware:

- Cabling
- Transceiver
- Hub
- repeater

OSI …

- To make it clearer, look at the following example



A client that is part of a network attached to the Internet sends a packet to www.google.com.

The packet will have:

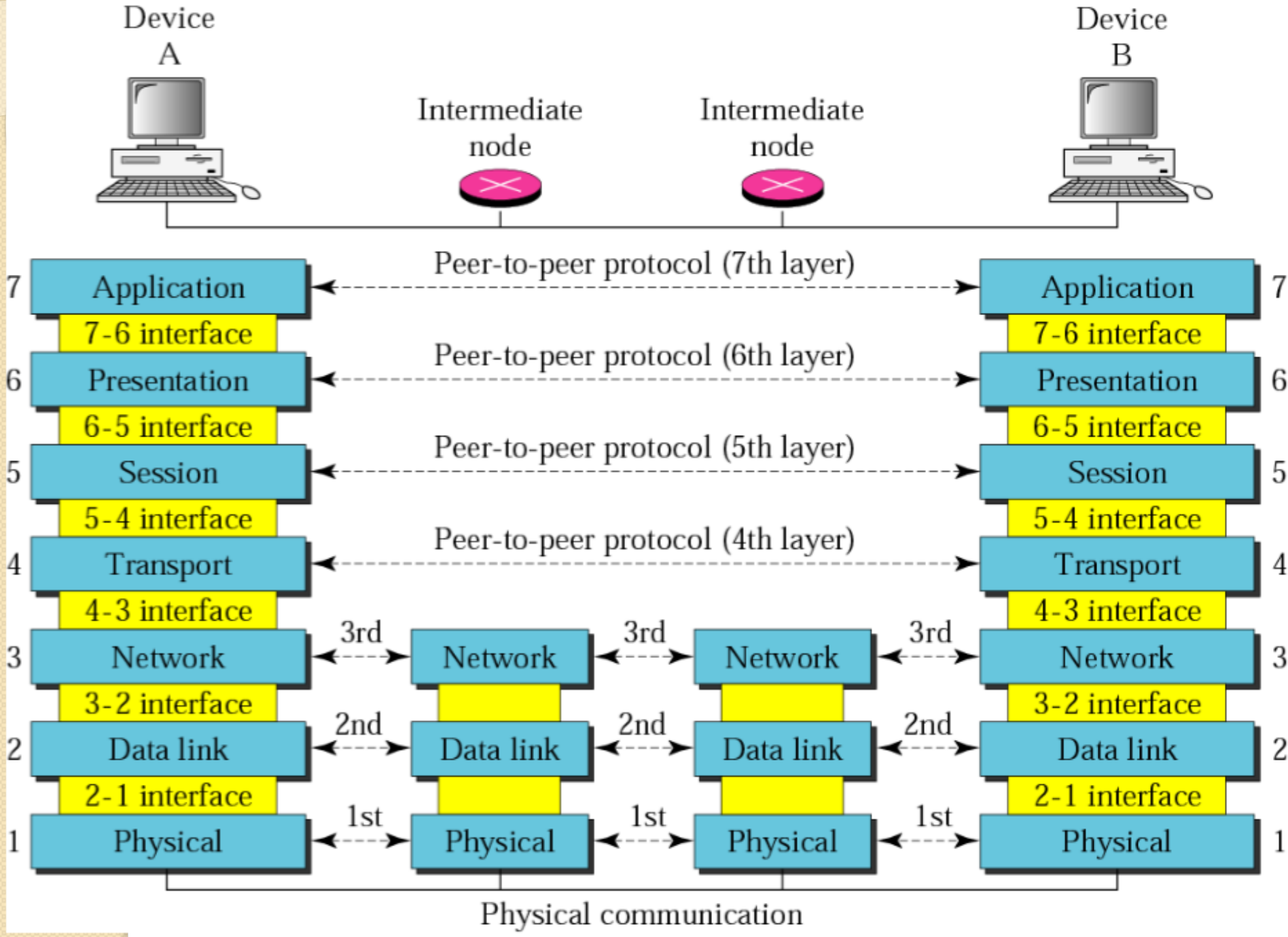
- Sender's IP: 192 168 17 1 Sender s IP: 192.168.17.1
- Sender's MAC: MAC (1)
- Destination IP: 10.0.0.2
- Destination MAC: MAC (2) => Gateway's address

After leaving the router, the sender's MAC becomes

MAC (3) and the destination MAC becomes MAC

(4).

- The figure in the next slide shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes.
- These intermediate nodes usually involve only the first three layers of the OSI model.
- Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.


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

Organization of the Layers

- The seven layers can be thought of as belonging to three subgroups. Layers 1, 2, and 3 - physical, data link, and network - are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
- Layers 5, 6, and 7- session, presentation, and application - can be thought of as the user support layers; they allow interoperability among unrelated software systems.
- Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
- The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

TCP/IP Model

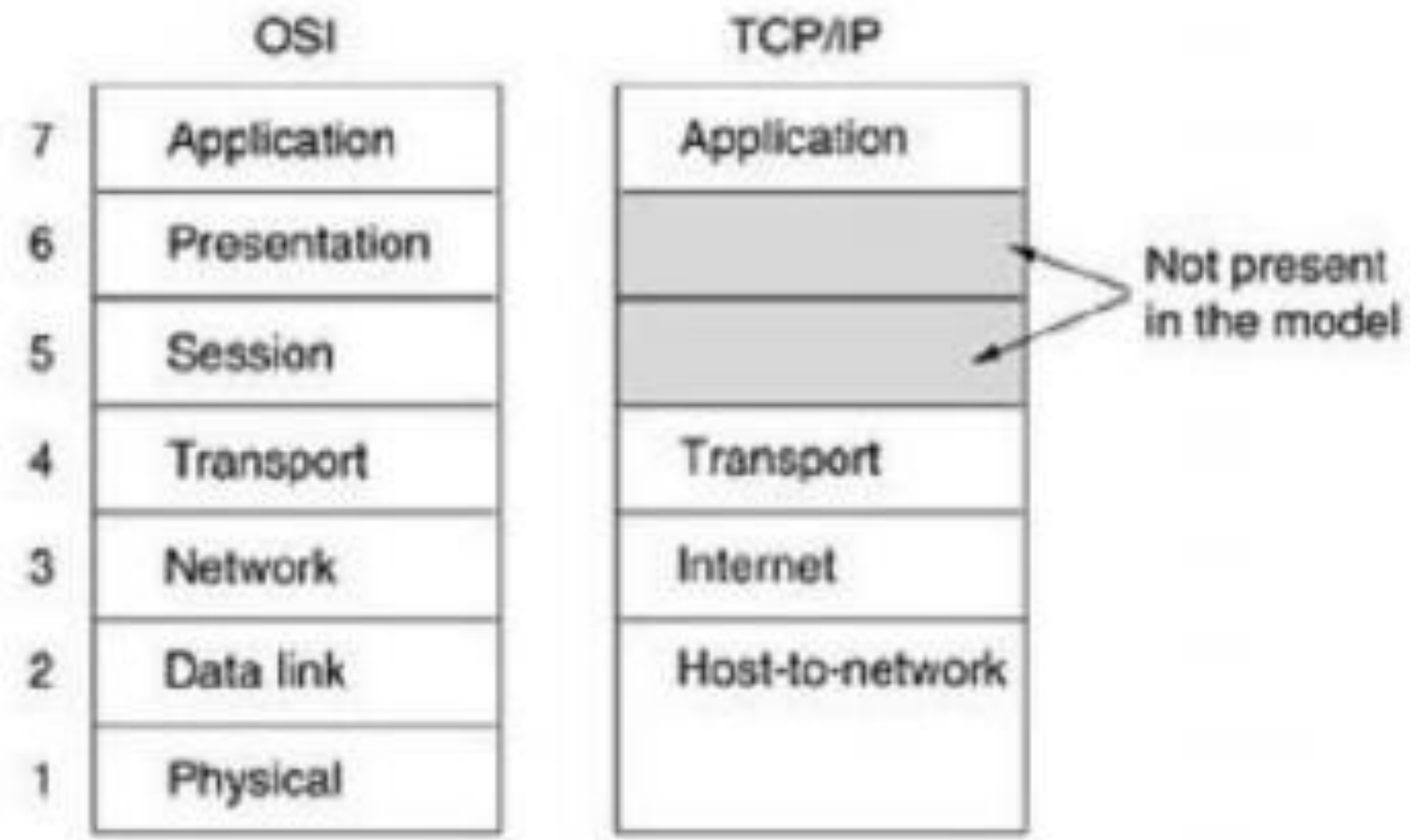


Fig. TCP/IP Reference Model

i) Application Layer:

- The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer.
- It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP)..

ii) Transport Layer:

- It has two protocols. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- TCP is a reliable protocol that allows two application layers to converse with each other.
- The other protocol UDP is a simpler protocol. It ignores some of the duties of the transport layer defined in OSI model. It is used when fast delivery of packets is needed without worrying much about error control.

iii) Internet Layer:

- The main protocol is IP (Internet Protocol) is responsible for creating network layer packets called IP datagrams.
- The datagrams travel network to network or LAN to WAN and the packets may reach out of sequence. It is the responsibility of upper layers to put them into proper order.

iv) Host-to-Network Layer:

- The Internet model does not discuss much about these layers making this protocol machine independent to a large extent. It is left to the user to choose the proper standard or protocol according to what they desire.

PROTOCOL, STANDARDS AND STANDARDIZATION BODIES

PROTOCOL

- A protocol is a set of rules that govern data communications.
- A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are syntax, semantics, and timing.
- Syntax refers to the structure or format of the data, meaning the order in which they are presented.
- Semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
- Timing refers to two characteristics: when data should be sent and how fast they can be sent.

STANDARDS

- Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers.
- Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers.
- Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").
- **De facto:** Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards.
- **De jure:** Those standards that have been legislated by an officially recognized body are de jure standards.

STANDARDIZATION BODIES

- Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.
- International Organization for Standardization (ISO).
- International Telecommunication Union-Telecommunication Standards Sector (ITU-T).
- American National Standards Institute (ANSI).
- Institute of Electrical and Electronics Engineers (IEEE).
- Electronic Industries Association (EIA).

CHAPTER FOUR

Internet Protocol (IP), IP Addressing and Subnetting

IP

- IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation.

- The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6) is being deployed actively worldwide.

IP Address

3

- An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network.
- An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points.
- This is known as "dotted decimal" notation.

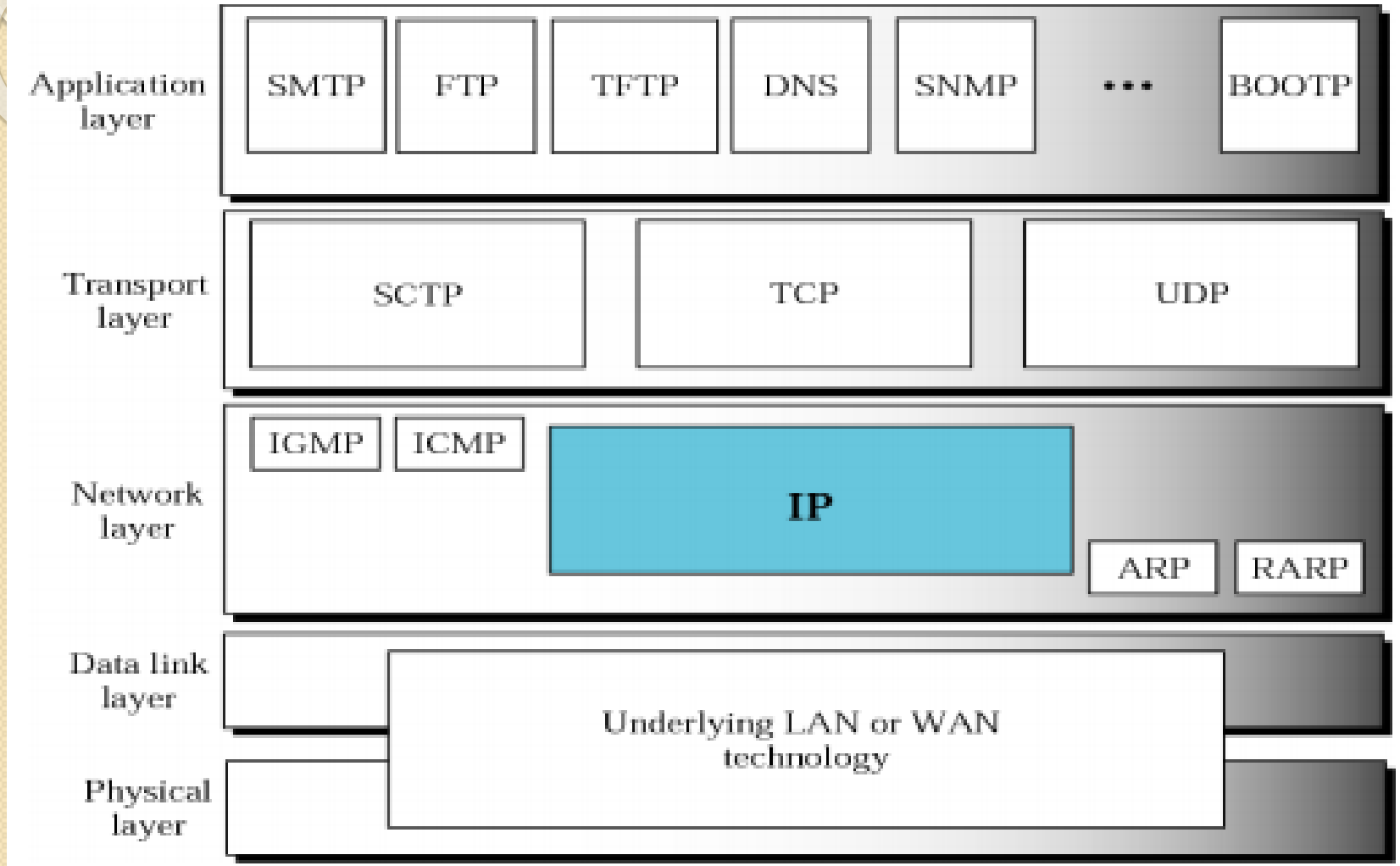
IP Address

- Example: 140.179.220.200
- It is sometimes useful to view the values in their binary form.
- 140 .179 .220 .200 is equivalent to 10001100.10110011.11011100.11001000
- Every IP address consists of two parts, one identifying the network and one identifying the node.

IP Addressing

- Communication at the network layer is host-to-host (computer-to-computer); a computer somewhere in the world needs to communicate with another computer somewhere else in the world.
- Usually, computers communicate through the Internet.
- The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.
- For this level of communication, we need a global addressing scheme; we use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite.

Position of IP in TCP/IP protocol suite



- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.
- IPv4 addresses are unique and universal.
- They are unique in the sense that each address defines one, and only one, connection to the Internet.
- Two devices on the Internet can never have the same address at the same time.

Notations

There are two prevalent notations to show an 1Pv4 address: binary notation and dotted-decimal notation.

Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:

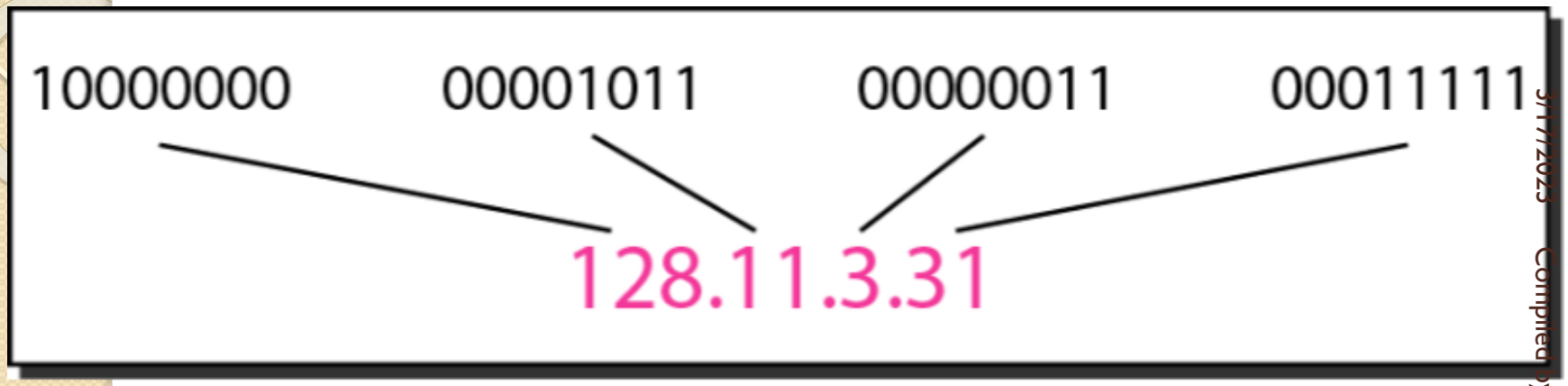
01110101 10010101 00011101 00000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted-decimal notation of the above address:

117.149.29.2

Example: Dotted-decimal notation and binary notation for an IPv4 address



Find the error, if any, in the following IPv4 addresses

a. 111.56.045.78
b. 221.34.7.8.20
c. 75.45.301.14
d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).

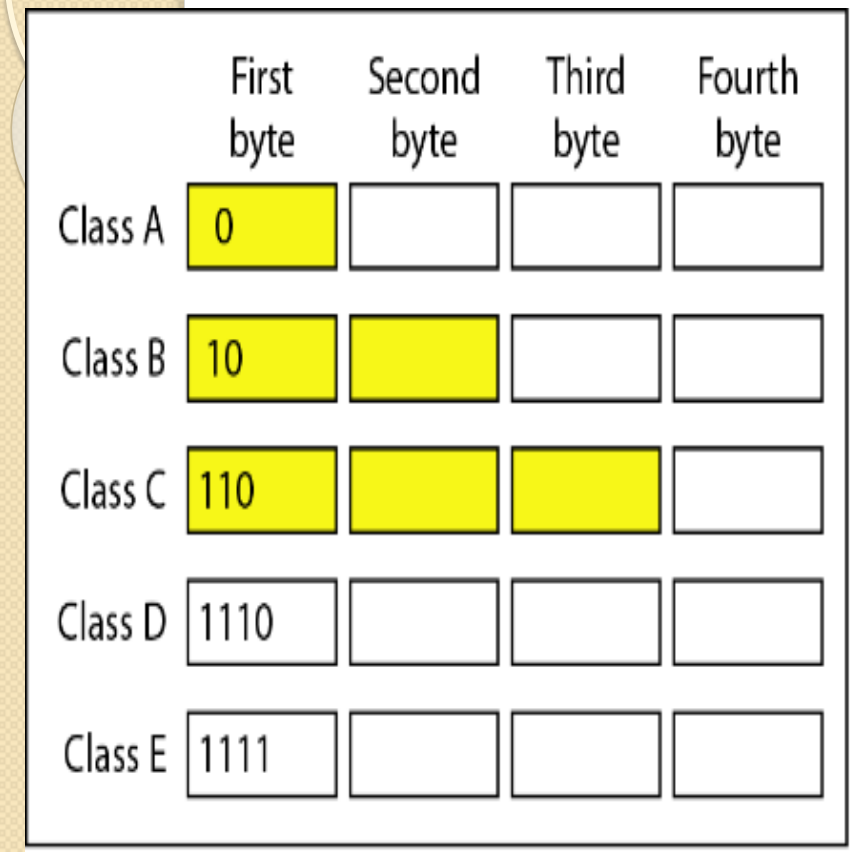
b. There can be no more than four numbers.

c. Each number needs to be less than or equal to 255.

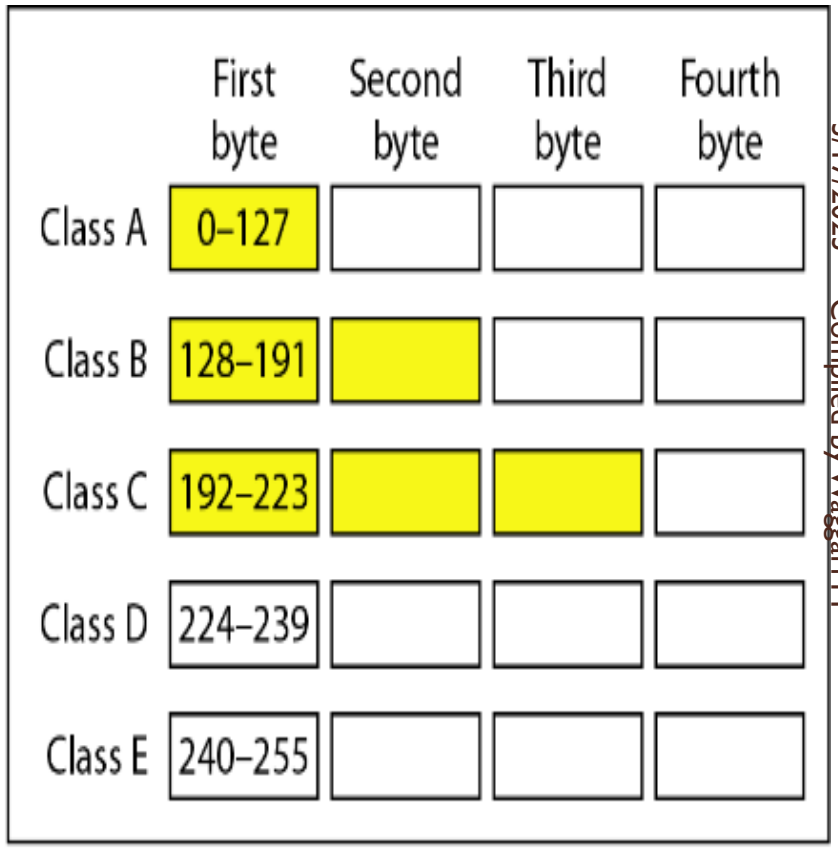
d. A mixture of binary notation and dotted-decimal notation is not allowed.

Address classes

- The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.
- There are 5 different address classes.
- The address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.



a. Binary notation



b. Dotted-decimal notation

Class A addresses begin with 0xxx, or 0 to 127decimal.

Class B addresses begin with 10xx, or 128 to 191decimal.

Class C addresses begin with 110x, or 192 to 223decimal.

Class D addresses begin with 1110,or 224 to 239decimal.

Class Eaddresses begin with 1111, or 240 to 255decimal.

Class D addresses are reserved for multicasting;

Class E addresses are reserved for future use.

Class D and E should not be used for host addresses

Previously, when an organization requested a block of addresses, it was granted one in class A, B, or C.

- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- Class C addresses were designed for small organizations with a small number of attached hosts or routers.

IP address can be one of the 3 classes A, B or C

Now we can see how the Class determines, by default, which part of the IP belongs to the network (N) and which part belongs to the node (h).

Class A -- NNNNNNNN.hhhhhhhh.hhhhhhhh.hhhhhhhh

Class B -- NNNNNNNN.NNNNNNNN.hhhhhhhh.hhhhhhhh

Class C -- NNNNNNNN.NNNNNNNN.NNNNNNNN.hhhhhhhh

Netid and Hostid

- Class A : 255.0.0.0
- Class B :255.255.0.0
- Class C :255.255.255.0

Mask

- Although the length of the netid and hostid (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of contiguous 1s followed by contiguous 0s. The masks for classes A, B, and C are shown below
- The mask can help us to find the netid and the hostid. For example, the mask for a class A address has eight 1 s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Network Addresses

- A very important concept in IP addressing is the network address.
- When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet.
- The first address in the class, however, is normally (not always) treated as a special address.
- The first address is called the network address and defines the organization network.
- It defines the organization itself to the rest of the world.
- The first address is the one that is used by routers to direct the message sent to the organization from the outside.

- The n leftmost bits of the address x.y.z.t/n define the network (organization network); the 32 – n rightmost bits define the particular host (computer or router) to the network.
- The two common terms are prefix and suffix.
- The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix.
- The prefix is common to all addresses in the network; the suffix changes from one device to another.

Simply this means IP address has 2 components (portgens)

1) Network portion (network bits) – hold left portion of the address up to some boundary

2) Host portion (host bits) – hold right portion of the address remaing from network bits

How to identifiy the network bit of address from host bit??

1) by CIDR
2) by class
3) by Mask

For a given IP network

- The n/w bits remains fixed
- The host bits vary
- The n/w address is the one that result when all host bits are not set (make 0)
- Broad cast address:-is the one that results when all the host bits are set (make all 1)
- For n number of host bits the maximum no of hosts for that specific n/w is 2n-2, where n is a number of host
- 1st host address:- address of a host that is one greater than the n/w address
- Last host address:- address of a host that is one less than the broadcast address

Example 1: givin an IP address of 172.16.0.10/29 then find

A. Network Address
B. 1st host Address
C. 2nd host address
D. Broad cast address
E. Last host address
F. Host address range
G. Max no of hosts within this n/w

Soln

172.16.0.10/29

the 1st 29 bits are for n/w bit and the remaining 3 bits are a host bits

10101100.00010000.00000000.00001010

all host should be zero

10101100.00010000.00000000.00001000

a) n/w address=172.16.0.8/29
b) 1st host add=172.16.0.9/29
c) 2nd host add=172.16.0.10/29
d) BA (set host to 1),00001111 =172.16.0.15/29
e) Last host add= 172.16.0.14/29
f) Range =172.16.0.9/29-172.16.0.14/29
g) 2(3)-2= 6

Subnetting

- Subnetting is a process of breaking down one network into multiple network segments by placing a router in b/n each network segments .
- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.
- Subnetting increases the number of 1s in the mask. And it creates many other networks from a network.

- During the process of sub-netting , we borrow some bits from the host portion in order to divide the large network into smaller network.
- Borrowing bits from the host portion reduces the number of hosts
- In the process of sub-netting we don’t have control over the network bits. We must borrow the sub-netting bits from the host portion.
- Communication between these sub-networks is achieved through a router

What Is The Favore Of Subnetting

1, Reduce n/w traffic

2, To improve network performance and security

3, Easy for managment

4, Faster data rate

5, Non-sub-netted networks waste a lot of IPv4 addresses

Subnetting example

There are 4 types of subnetting examples

1. Subnetting when given the require number of clients
2. Subnetting when given the require number of n/w
3. Given on IP address and subnetting mask
4. VLSM most efficent one, there is no wastege in this mechanism

The Big Five FAQ In Design

1) How many subnet does the chosen subnet mask can produce
   2x where x is a number of masked host
   (1's in the new subnet mask)
2) How many host are available per subnet
   2n-2 where n is number of unmasked bits
   (0's in the new subnet mask)
3) What are the valid subnets
   256- subnet mask
4) What are the broad cast address for each subnet
   it is the number right before the next subnet so the BA for the 0 subnet is 64-1=63 for 64-127 f0r 128-191 for 192-255
5) What are the valid host addess range
   1-62, 65-126, 129-190.....

Example 1:- A service provider has given a class c networks 209.50.1.0 your company must break into many subnets as possible as long as there are 50 clients per subnet

1, 50= 00110010

6 bits to get number 50

2, 255.255.255.0
11111111.11111111.11111111.00000000

we must ensure that 6 of the client bits (0) remains asclients bit and save the host from the right to satsfiy the requirements

11111111.11111111.11111111.11000000

this is our increment

64

3, starting from the given add your increment to the subnetted octet

209.50.1.0-63

209.50.1.64-127

209.50.1.128-191

// Answer all the big FAQ questions

.

.

Example 2:- A service provider has given you the class c n/w range 216.21.5.0 then your company wants to break into 20 separet subnets

1) 20 =00010100 → 5 bits to get number 20

2) 255.255.255.0
11111111.11111111.11111111.00000000

here we are going to reserve the bit in subnet mask

11111111.11111111.11111111.11111000

8

3) 216.21.5.0 -7

.8-15

.16-23

.24

Great exception in doing subnetting

* 128,64, 32,16,8,4 these number throw off our calculation when we are doing baed on number of network
* 127,63,31,15,7,3 throw off our calaculation when we are doing based on the number of clients.

Thus rules to over come this problem

* Substract 1 when doing with n/w
* Add 1 when doing based on the number of clients

Example:- if one person ask us to do him for 7 host per each subnet....it will be 6 which is incorrect

IP= 192.168.10.0

need= 7

1) 00000111= 3 bits to get number 7

2) save the host bit

11111111.11111111.11111111.00000000

00001000= 8 is our increment

3) 192.168.10.0-7// b/n this there is only 6 which is incorrect

COMPUTER NETWORK SECURITY AND INTEGRITY

Chapter 5

Information, Computer and Network Security

Information security is the security of information. With the introduction of the computer, the need for automated tools for the protection of files, and other information stored on the computer has become evident. This is especially true for a shared system, such as a time sharing system, and the need is even more acute for systems that can be accessed over a public telephone network, data network or the internet. The generic name for the collection of tools designed to protect data and thwart hackers is **computer security.**

- Computer and network security measures go hand in hand.

Network Security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to be performed.

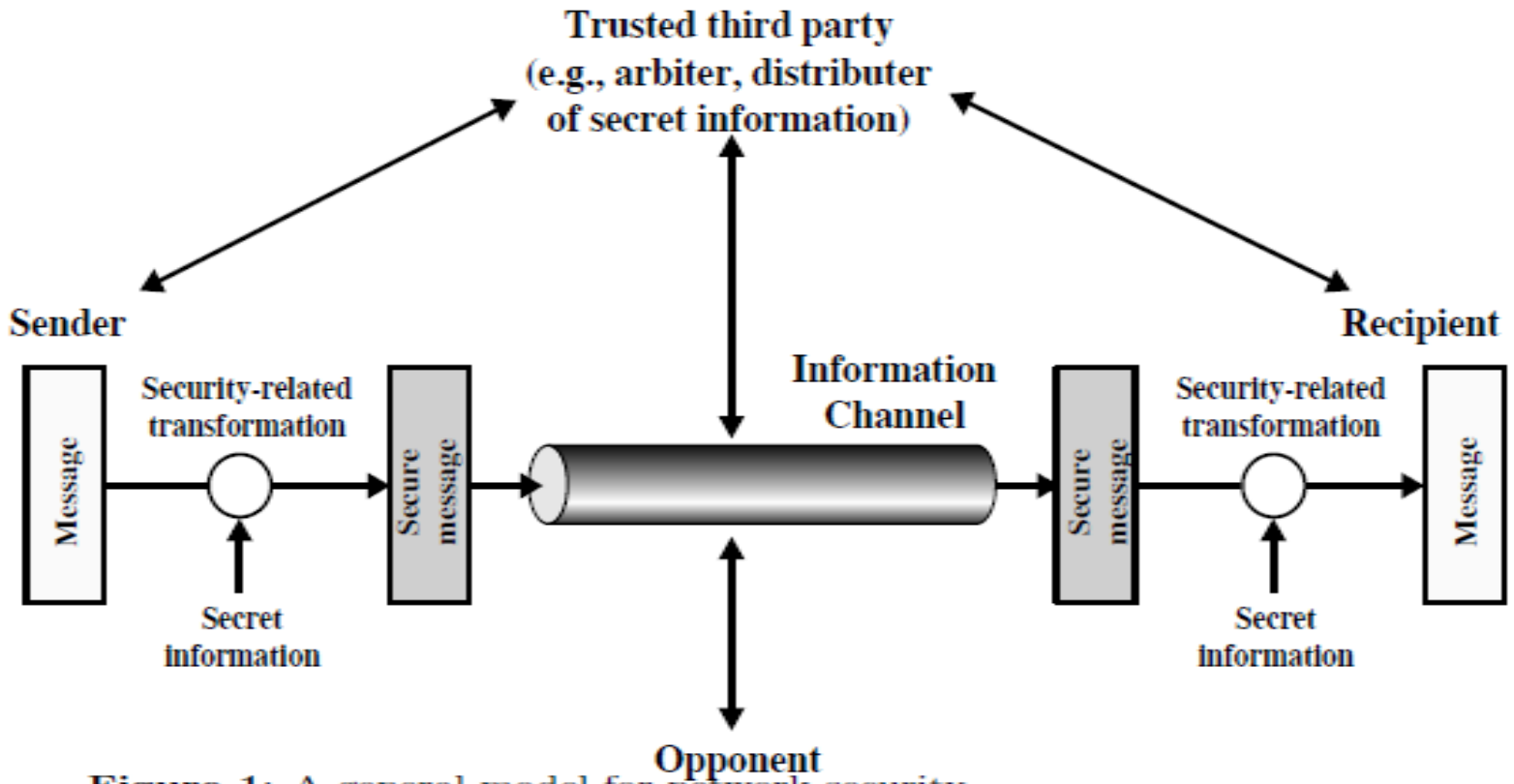


Figure 1: A general model for network security

We can also classify the attacks that compromise network security as passive attacks and active attacks.

1. Passive Attacks: These attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are **release of message contents** where an eavesdropper tries to learn the contents of what is being transmitted. This can be prevented by encryption (see model for cryptography below). A second type of passive attack is called **traffic analysis,** where the opponent tries to observe the pattern, frequency and length of messages being exchanged which could be used in guessing the nature of the communication that is taking place. Passive attacks are very difficult to detect since they do not involve the alteration of the data. The emphasis, therefore, is on prevention via a good encryption algorithm.

2. Active Attacks: Active attacks involve some modification of the data stream or the creation of a false stream. These attacks present the opposite characteristics of passive attacks. It is difficult to prevent active attacks absolutely because to do so would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Securing the Computer Network

- Creating security in the computer network model means creating a secure environments for a variety of resources.
- Ensuring the security of an object means protecting the object from unauthorized access both from within the object and externally. In short, we protect objects. System objects are either tangible or nontangible. In a computer network model, the tangible objects are the hardware resources in the system, and the intangible object is the information and data in the system, both in transition and static in storage.

Hardware

Protecting hardware resources include protecting:

- End-user objects that include the user interface hardware components such as all client system input components, including a keyboard, mouse, touch screen, light pens, and others
- Network objects like firewalls, hubs, switches, routers, and gateways which are vulnerable to hackers
- Network communication channels to prevent eavesdroppers from intercepting network communications

Software

Protecting software resources includes protecting hardware-based software, operating systems, server protocols, browsers, application software, and intellectual property stored on network storage disks and databases. It also involves protecting client software such as investment portfolios, financial data, real estate records, images or pictures, and other personal fi les commonly stored on home and business computers.

5.1 INTRODUCTION TO CRYPTOGRAPHY

- Security in networking is based on **cryptography.**
- Cryptography means the science and art of transforming messages to make them **secure** and **immune** to attack.
- An encryption algorithm transforms the plaintext into cipher text; a decryption algorithm transforms the cipher text back into plaintext.
- The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.
- Cryptography can provide several aspects of security related to the interchange of messages through networks. These aspects are **confidentiality, integrity, authentication, and non-repudiation.**

1. Confidentiality

The confidentiality service protects system data and information from unauthorized disclosure. When data leave one extreme of a system such as a client's computer in a network, it ventures out into a nonrusting environment. So, the recipient of that data may not fully trust that no third party like a cryptanalysis or a man-in-the middle has eavesdropped on the data. This service uses encryption algorithms to ensure that nothing of the sort happened while the data was in the wild. **Encryption protects the communications channel from sniffers.** Sniffers are programs written for and installed on the communication channels to eavesdrop on network traffic c, examining all traffic c on selected network segments. Sniffers are easy to write and install and difficult to detect. The encryption process uses an encryption algorithm and key to transform data at the source, called plaintext ; turn it into an encrypted form called cipher text , usually unintelligible form; and finally recover it at the sink. The encryption algorithm can either be symmetric or asymmetric .

2. Integrity

The integrity service protects data against active threats such as those that may alter it. Just like data confidentiality, data in transition between the sending and receiving parties is susceptible to many threats from hackers, eavesdroppers, and cryptanalysts whose goal is to intercept the data and alter it based on their motives. This service, through encryption and hashing algorithms , ensures that the integrity of the transient data is intact. A hash function takes an input message M and creates a code from it. The code is commonly referred to as a hash or a message digest. A one-way hash function is used to create a signature of the message – just like a human fingerprint. The hash function is, therefore, used to provide the message's integrity and authenticity. The signature is then attached to the message before it is sent by the sender to the recipient.

3. Authentication

Authentication is a service used to identify a user. User identity, especially of remote users, is difficult because many users, especially those intending to cause harm, may masquerade as the legitimate users when they actually are not. This service provides a system with the capability to verify that a user is the very one he or she claims to be based on what the user is, knows, and has. Physically, we can authenticate users or user surrogates based on checking one or more of the following user items

- **User name** (sometimes screen name)
- **Password**
- **Retinal images :** The user looks into an electronic device that maps his or her eye retina image; the system then compares this map with a similar map stored on the system.
- **Fingerprints :** The user presses on or sometimes inserts a particular finger into a device that makes a copy of the user fingerprint and then compares it with a similar image on the system user file.

- **Physical location :** The physical location of the system initiating an entry request is checked to ensure that a request is actually originating from a known and authorized location. In networks, to check the authenticity of a client's location a network or Internet protocol (IP) address of the client machine is compared with the one on the system user fi le. This method is used mostly in addition to other security measures because it alone cannot guarantee security. If used alone, it provides access to the requested system to anybody who has access to the client machine.

- **Identity cards :** Increasingly, cards are being used as authenticating documents. Whoever is the carrier of the card gains access to the requested system. As is the case with physical location authentication, card authentication is usually used as a second-level authentication tool because whoever has access to the card automatically can gain access to the requested system.

4. Nonrepudiation

This is a security service that provides proof of origin and delivery of service and/or information. In real life, it is possible that the sender may deny the ownership of the exchanged digital data that originated from him or her. This service, through digital signature and encryption algorithms, ensures that digital data may not be repudiated by providing proof of origin that is difficult to deny. A digital signature is a cryptographic mechanism that is the electronic equivalent of a written signature to authenticate a piece of data as to the identity of the sender.

5.1.1 Components of Cryptography

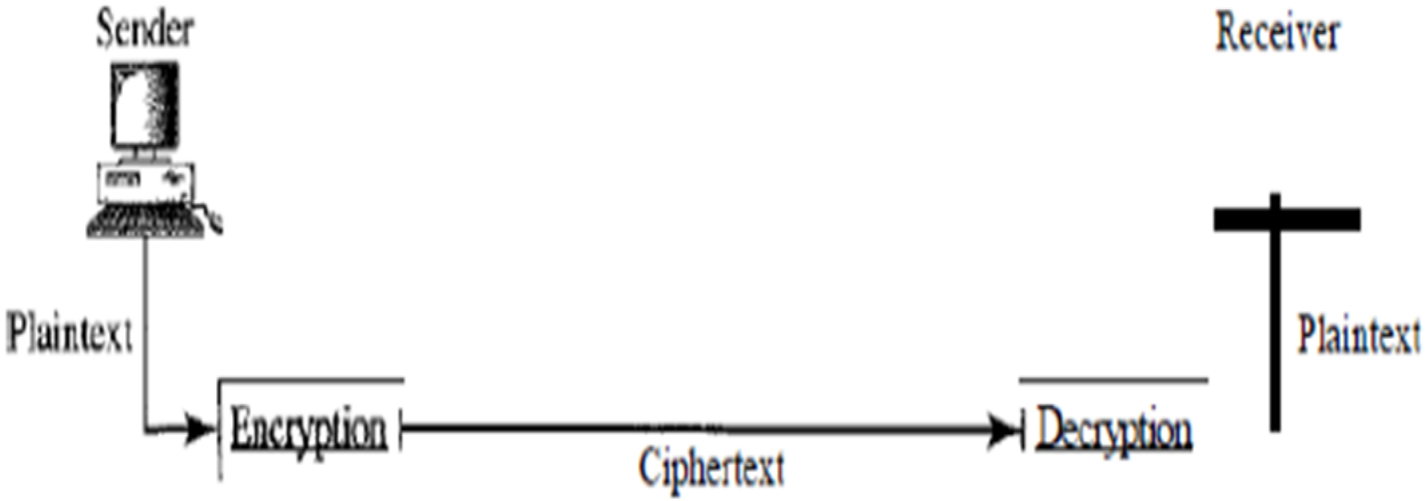


Fig. Cryptography Components

Plaintext: The original message, before being transformed, is called plain text.

Cipher text: After the message is transformed, it is called cipher text.

Encryption: A encryption means it transforms the plaintext into cipher text.

Decryption: A decryption means it transforms the cipher text back into plain text. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm

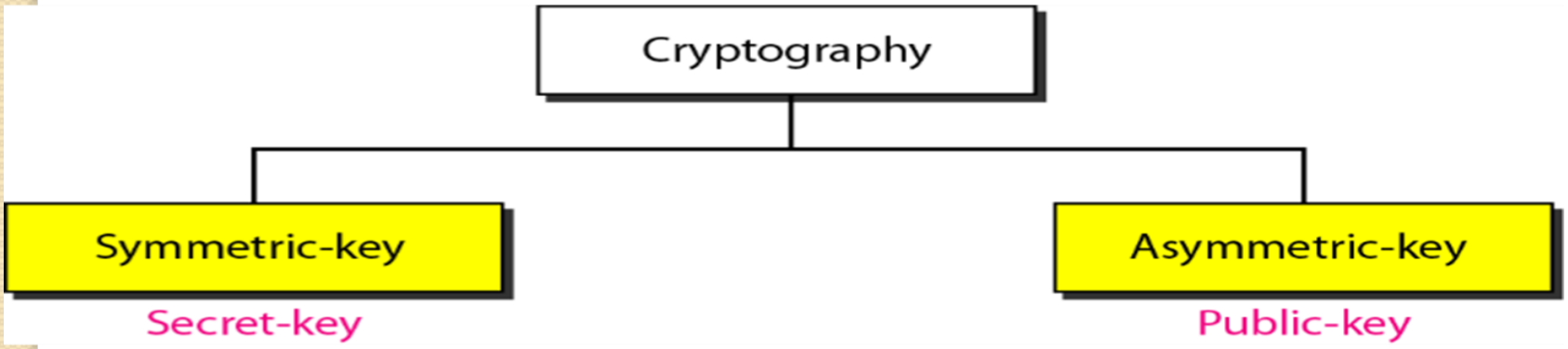
Security Services

Cryptography can provide five services. Four of these are related to the message exchange between

Alice and Bob. The fifth is related to the entity trying to access a system for using its resources.

- Message confidentiality means that the sender and the receiver expect privacy.
- Message integrity means that the data must arrive at the receiver exactly as sent.
- Message authentication means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
- Non-repudiation means that a sender must not be able to deny sending a message that he sent.
- Entity authentication means to prove the identity of the entity that tries to access the system's resources.

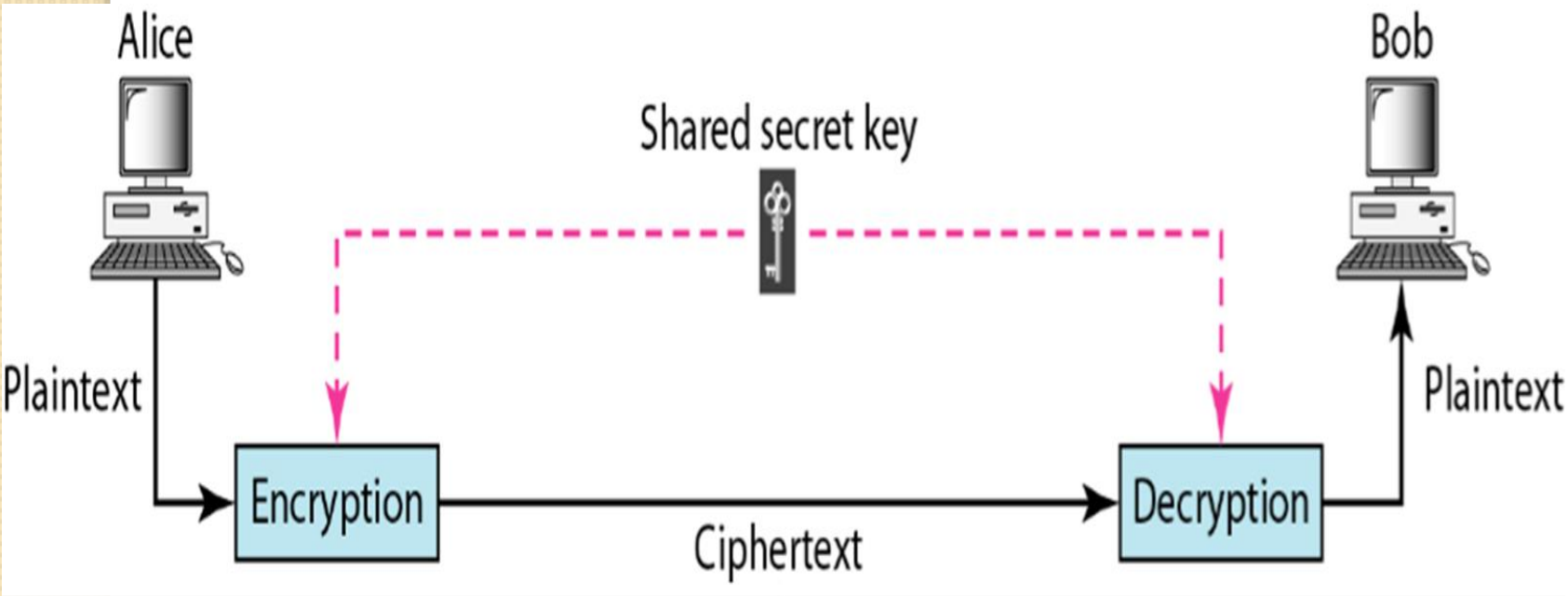
- A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on.
- To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext. These create the cipher text.
- To decrypt a message, we need a decryption algorithm, a decryption key, and the cipher text. These reveal the original plaintext.
- We can divide all the cryptography algorithms (ciphers) into two groups: symmetric-key (also called secret-key) cryptography algorithms and asymmetric (also called public-key) cryptography algorithms.



Symmetric-Key Cryptography

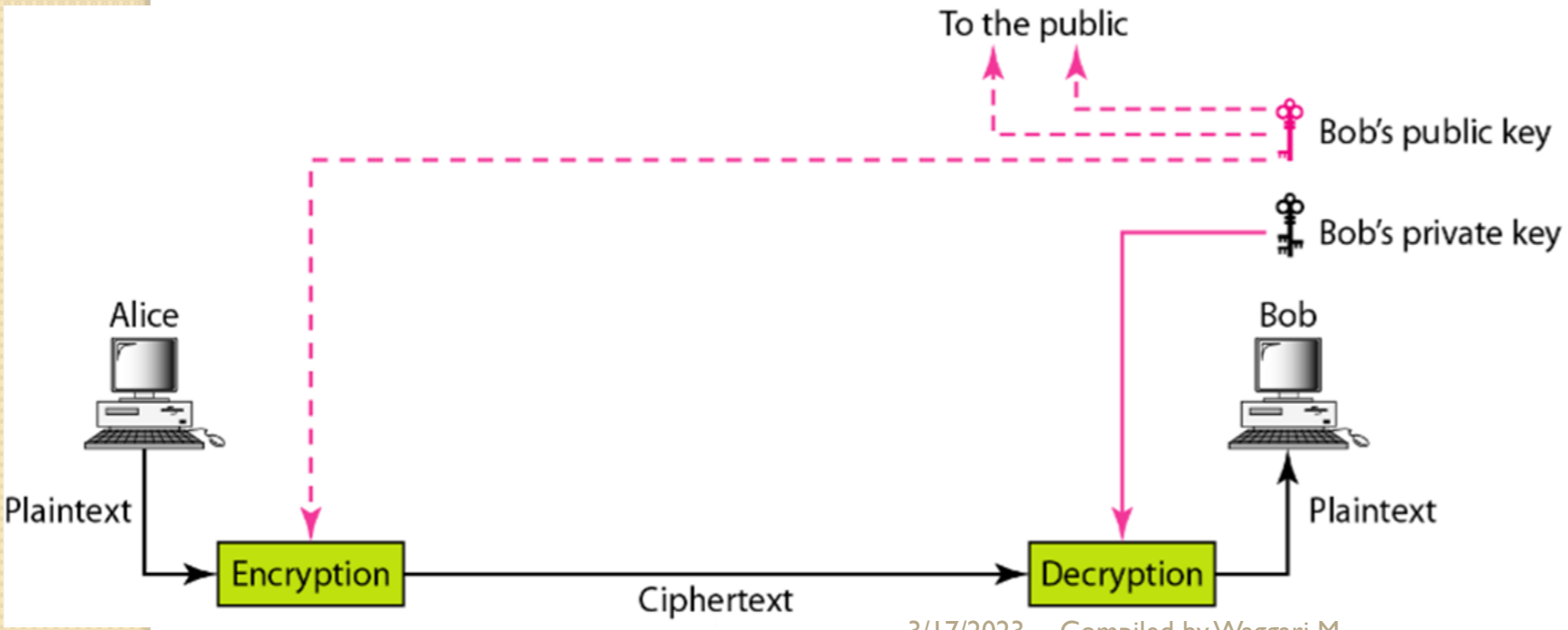
There two basic kinds of encryptions are symmetric (also called "secret key") and asymmetric(also called "public key"). It uses a common key and the same cryptographic algorithm to scramble and unscramble the message.

In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data



Asymmetric-Key Cryptography

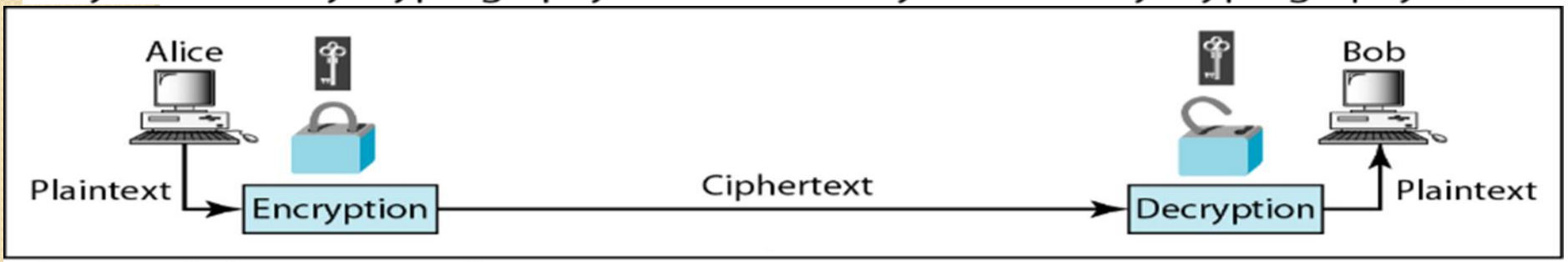
- Asymmetric encryption commonly known as public-key encryption uses two different keys: a public key known by all and a private key known by only the sender and the receiver. Both the sender and the receiver each has a pair of these keys, one public and one private. To encrypt a message, a sender uses the receiver's public key which was published. Upon receipt, the recipient of the message decrypts it with his or her private key.
- In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption. The public key is available to the public; the private key is available only to an individual.



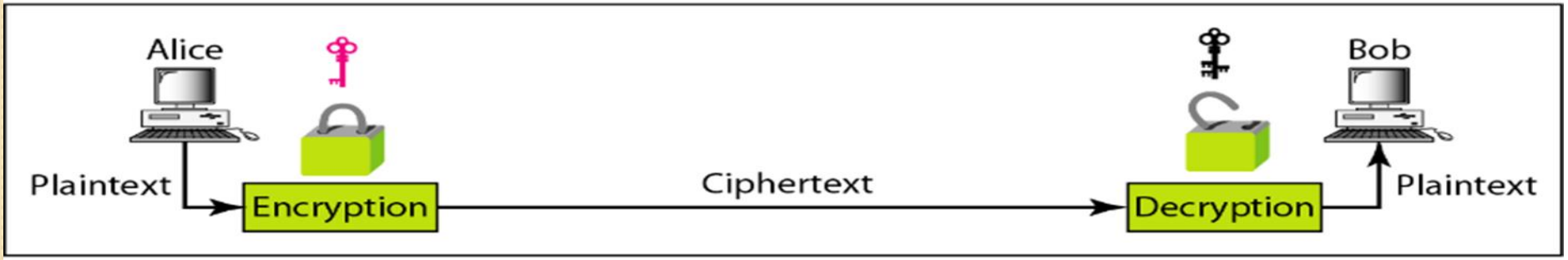
Keys used in cryptography

Symmetric-key cryptography

Asymmetric-key cryptography



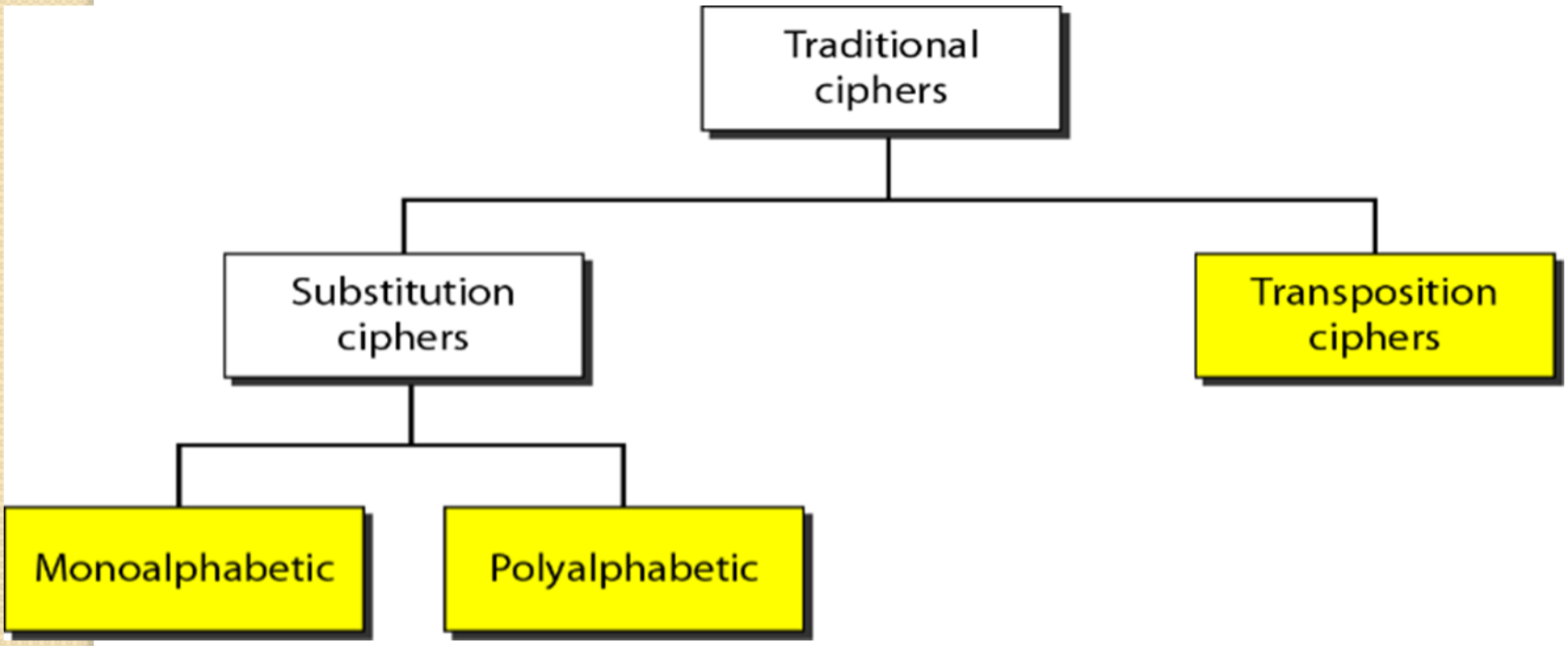
a. Symmetric-key cryptography



b. Asymmetric-key cryptography

SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war). We still mainly use symmetric-key cryptography in our network security.



A substitution cipher replaces one symbol with another.

Example:1

The following shows a plaintext and its corresponding cipher text. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: KHOOR

Solution

The cipher is probably monoalphabetic because both occurrences of L's are encrypted as O's.

Example 2

The following shows a plaintext and its corresponding cipher text. Is the cipher monoalphabetic?

Plaintext: HELLO
Ciphertext: ABNZF

Solution

The cipher is not monoalphabetic because each occurrence of L is encrypted by a different character. The first L is encrypted as N; the second as Z.

The shift cipher is sometimes referred to as the Caesar cipher. In this cipher, the encryption algorithm is "shift key characters down," with key equal to some number. The decryption algorithm is "shift key characters up.“

Example:3

Use the shift cipher with key = 15 to encrypt the message “HELLO.”

Solution

We encrypt one character at a time. Each character is shifted 15 characters down. Letter H is encrypted to W. Letter E is encrypted to T. The first L is encrypted to A. The second L is also encrypted to A. And O is encrypted to D. The cipher text is WTAAD.

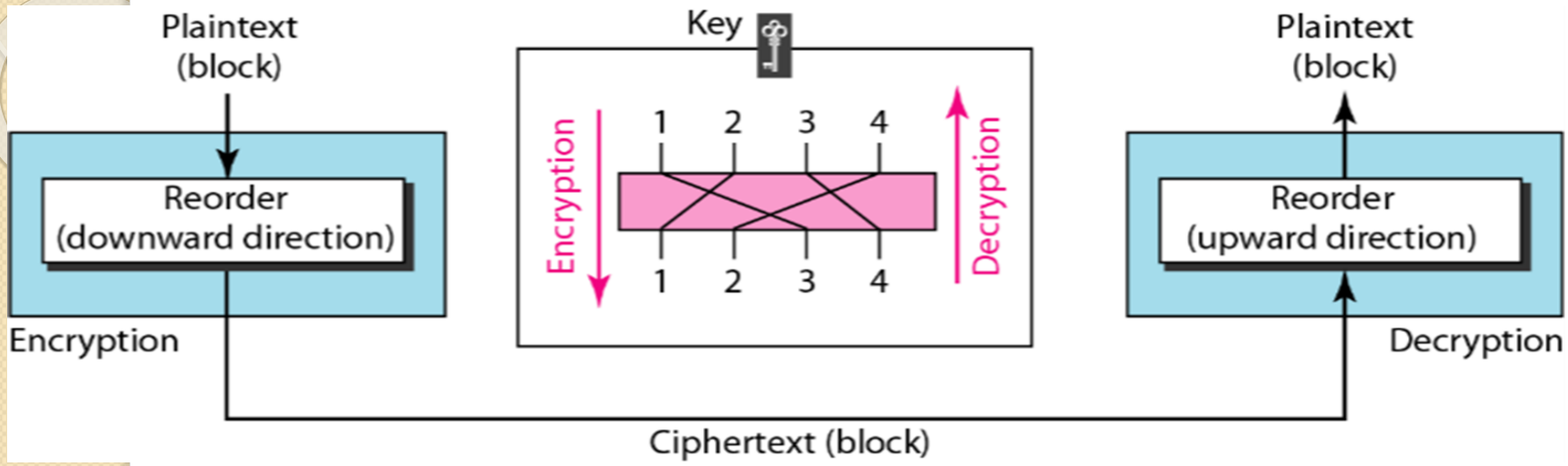
Example 2

Use the shift cipher with key = 15 to decrypt the message "WTAAD."

Solution

We decrypt one character at a time. Each character is shifted 15 characters up. Letter W is decrypted to H. Letter T is decrypted to E. The first A is decrypted to L. The second A is decrypted to L. And, finally, D is decrypted to O. The plaintext is HELLO.

A transposition cipher reorders (permutes) symbols in a block of symbols.



Encrypt the message “HELLO MY DEAR,” using the key shown in Figure above

Solution

We first remove the spaces in the message. We then divide the text into blocks of four characters. We add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ. We create a three-block cipher text ELHLMDOYAZER.

Basic Security Measures

The basic security measures for computer systems fall into the following categories:

1. External security
2. Operational security
3. Surveillance
4. Passwords/authentication
5. Auditing
6. Access rights
7. Standard system attacks
8. Viruses/worms and antivirus tools
9. Firewalls
10. Encryption and Decryption Techniques
11. Digital Signature
12. Security Policy

External Security

- Protection from environmental damage such as floods, earthquakes, and heat.
- Physical security such as locking rooms, locking down computers, keyboards, and other devices.
- Electrical protection from power surges.
- Noise protection from placing computers away from devices that generate electromagnetic interference.

Operational Security

- Deciding who has access to what.
- Limiting time of day access.
- Limiting day of week access.
- Limiting access from a location, such as not allowing a user to use a remote login during certain periods or any time.

Surveillance

- Proper placement of security cameras or CCTV can deter theft and vandalism.
- Cameras can also provide a record of activities.
- Intrusion detection is a field of study in which specialists try to prevent intrusion and try to determine if a computer system has been violated.

Passwords and ID Systems

Passwords are the most common form of security and the most abused.

Simple rules help support safe passwords, including:

- Change your password often.
- Pick a good, random password (minimum 8 characters, mixed symbols).
- Don’t share passwords or write them down.
- Don’t select names and familiar objects as passwords.

Authentication

Authentication is the process of reliably verifying the identity of someone (or something) by means of:

- A secret (password [one-time], ...)
- An object (smart card, ...)
- Physical characteristics (fingerprint, retina, ...)

Trust

Many new forms of "passwords" are emerging:

- Fingerprints
- Face prints
- Retina scans and iris scans
- Voice prints
- Ear prints

Auditing

- Creating a computer or paper audit can help detect wrongdoing.
- Auditing can also be used as a deterrent.
- Many network operating systems allow the administrator to audit most types of transactions.
- Many types of criminals have been caught because of computer-based audits.

Access Rights

Two basic questions to access right: who and how?

- Who do you give access right to? No one, group of users, entire set of users?
- How does a user or group of users have access? Read, write, delete, print, copy, execute?
- Most network operating systems have a powerful system for assigning access rights.

Computer virus and a Computer worm?

- **Viruses** are computer programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers.
- We send e-mail document attachments, trade programs on diskettes, or copy files to file servers. When the next unsuspecting user receives the infected file or disk, they spread the virus to their computer, and so on.
- **The computer worm** is a program that is designed to copy itself from one computer to another over a network (e.g. by using e-mail). The worm spreads itself to many computers over a network, and doesn't wait for a human being to help. This means that computer worms spread much more rapidly than computer viruses.

Standard System Attacks

Denial of service attacks, or distributed denial of service attacks, bombard a computer site with so many messages that the site is incapable of answering valid request.

e-mail bombing, a user sends an excessive amount of unwanted e-mail to someone.

Smurfing is a nasty technique in which a program attacks a network by exploiting IP broadcast addressing operations.

Ping storm is a condition in which the Internet Ping program is used to send a flood of packets to a server.

Spoofing is when a user creates a packet that appears to be something else or from someone else.

Trojan Horse is a malicious piece of code hidden inside a seemingly harmless piece of code.

Stealing, guessing, and intercepting passwords is also a tried and true form of attack

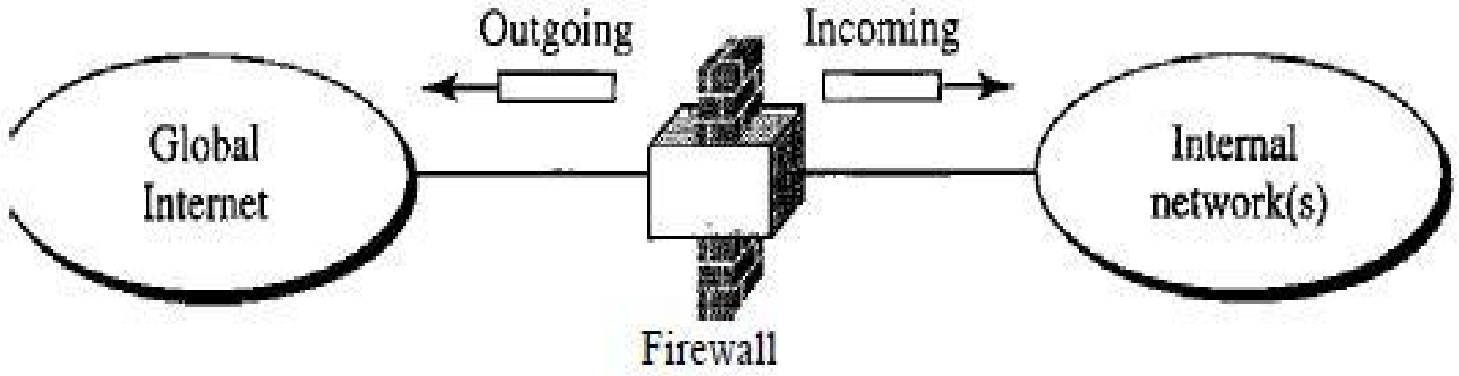
Digital Signatures

- A digital signature is much like a hand signature in that it provides proof that you are the originator of the message (Authentication); assigns a code to a document.
- Used to bound the message originator with the exact contents of the message through the use of key pairs. This allows for the feature of non-repudiation to be achieved - this is crucial for electronic commerce.
- Non-repudiation is a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action related to data.
- The private key of the sender is used to compute a message digest.

Firewalls

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.

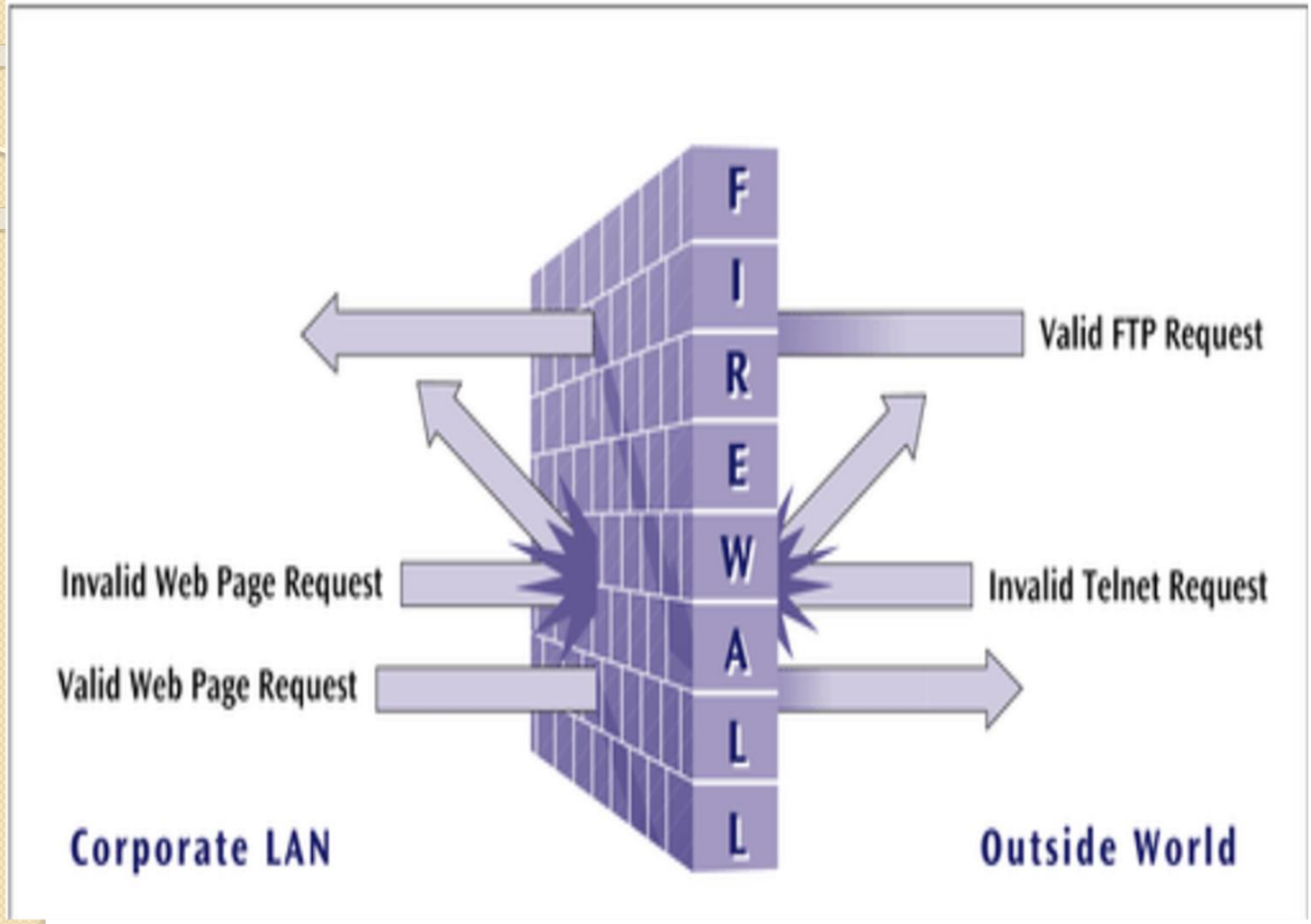
- A system or combination of systems that supports an access control policy between two networks.
- A firewall can limit the types of transactions that enter a system, as well as the types of transactions that leave a system.
- Firewalls can be programmed to stop certain types or ranges of IP addresses, as well as certain types of TCP port numbers (applications such as ftp, telnet, etc.)



For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization.

A firewall is usually classified as a packet-filter firewall and a proxy-based firewall.

A firewall as it stops certain internet and external transactions

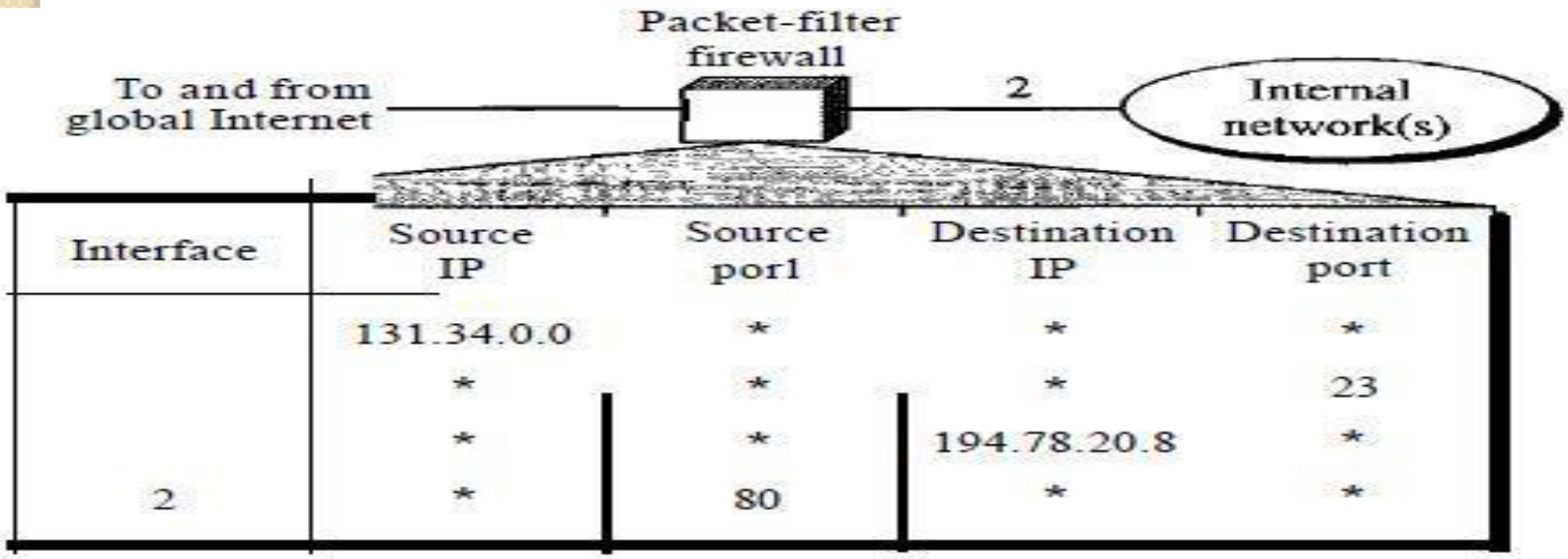


1. Packet-Filter Firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information

In the network layer and transport layer headers: source and destination IP addresses, source and Destination port addresses, and type of protocol (TCP or UDP).

A packet-filter firewall is a router that uses a filtering table to decide which packets must be Discarded (not forwarded). The following figure shows an example of a filtering table for this kind of a firewall.



Interface	Source IP	Source port	Destination IP	Destination port
	131.34.0.0	*	*	*
	*	*	*	23
	*	*	194.78.20.8	*
2	*	80	*	*

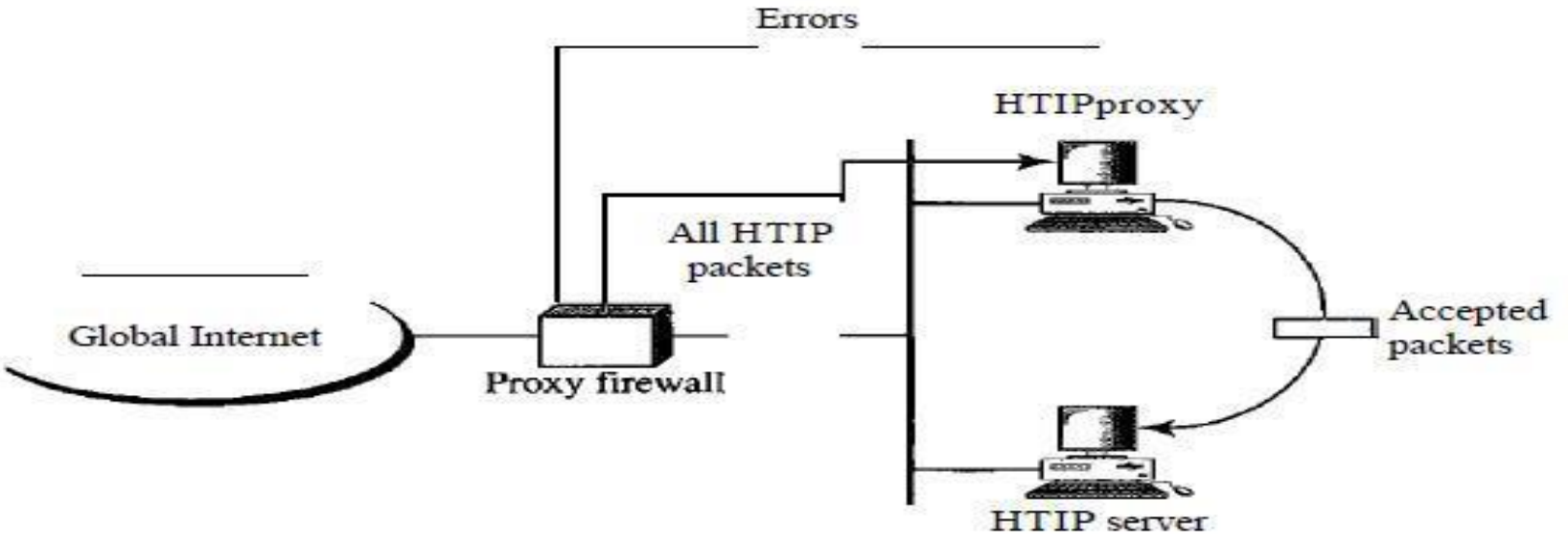
According to the figure, the following packets are filtered:

1. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the *
(asterisk) means "any."
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants
this host for internal use only.
4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not
want employees to browse the Internet.

2. Proxy Firewall

A proxy server is a more advanced firewall that acts as a doorman into a corporate network. Any external transaction that request something from the corporate network must enter through the proxy server. Proxy servers are more advanced but make external accesses slower.

The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCPIUDP). However, sometimes we need to filter a message based on the information available in the message itself (at the application layer).



When the user client process sends a message, the proxy firewall runs a server process to receive the request. The server opens the packet at the application level and finds out if the request is legitimate. If it is, the server acts as a client process and sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user.
In this way, the requests of the external users are filtered based on the contents at the application layer..

Firewall Functions

- Protect the system from the hackers from logging into machines on network.
- Provide a single access point from where security and audit can be imposed.
- Act as an effective tracing tool.
- Provide an important logging and auditing function
- Provide information about the nature of traffic and the number of attempts made to break into it.

Security Policy Design Issues

- What is the company's desired level of security?
- How much money is the company willing to invest in security?
- If the company is serious about restricting access through an Internet link, what about restricting access through all other entry ways?
- The company must have a well-designed security policy

Achieving Privacy

To achieve privacy, organizations can use one of three strategies: **private networks, hybrid networks, and virtual private networks.**

Private Networks: An organization that needs privacy when routing information inside the Organization can use a private network as discussed previously. A small organization with one single site can use an isolated LAN. People inside the organization can send data to one another that totally remain inside the organization, secure from outsiders. A larger organization with several sites can create a private internet. The LANs at different sites can be connected to each other by using routers and leased lines. In other words, an internet can be made out of private LANs and private WANs. The following figure shows such a situation for an organization with two sites. The LANs are connected to each other by routers and one leased line.

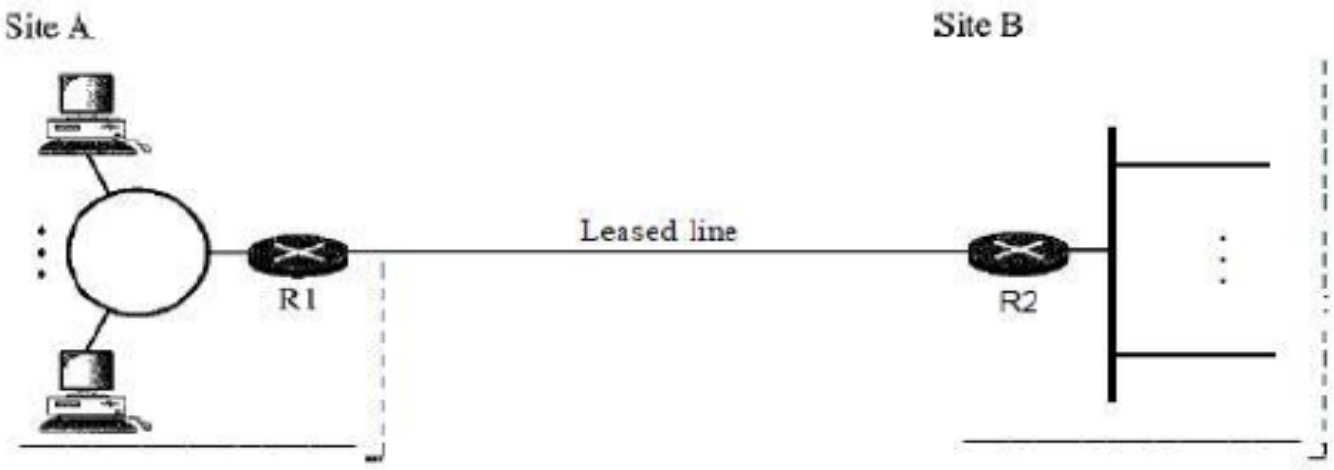


Fig. Private Network

Hybrid Networks: Today, most organizations need to have privacy in intra-organization data exchange, but, at the same time, they need to be connected to the global Internet for data exchange with other organizations. One solution is the use of a hybrid network. A hybrid network allows an organization to have its own private internet and, at the same time, access to the global Internet. Intra-organization data are routed through the private internet; inter-organization data are routed through the global Internet.

An organization with two sites uses routers Rl and R2 to connect the two sites privately through a leased line; it uses routers R3 and R4 to connect the two sites to the rest of the world. The organization uses global IP addresses for both types of communication. However, packets destined for internal recipients are routed only through routers Rl and R2. Routers R3 and R4 route the packets destined for outsiders.

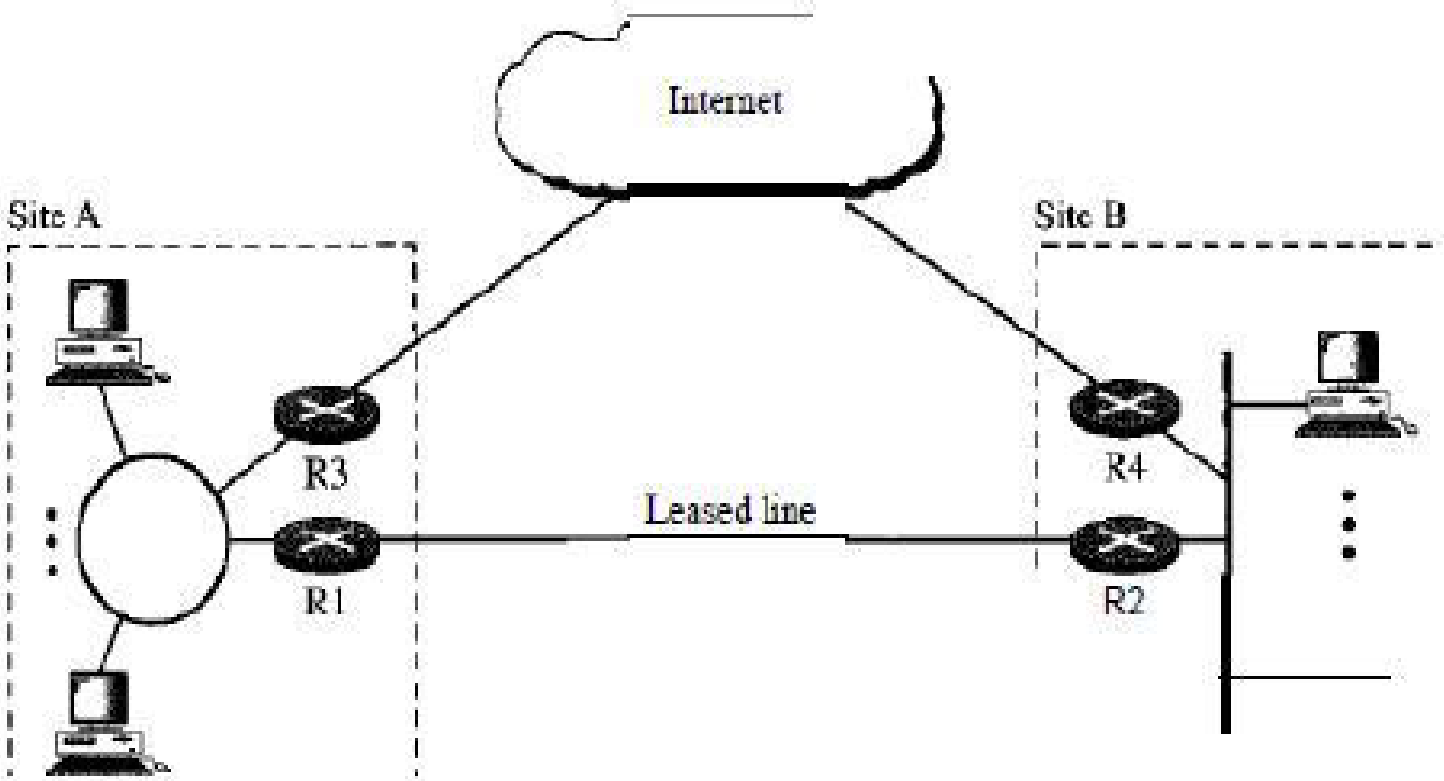


Fig. Hybrid Network

Virtual Private Networks: Both private and hybrid networks have a major drawback: cost.

Private wide-area networks (WANs) are expensive. To connect several sites, an organization

Needs several leased lines, which means a high monthly fee. One solution is to use the global Internet for both private and public communications. A technology called **virtual private network** allows organizations to use the global Internet for both purposes for both public and private networks.

VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

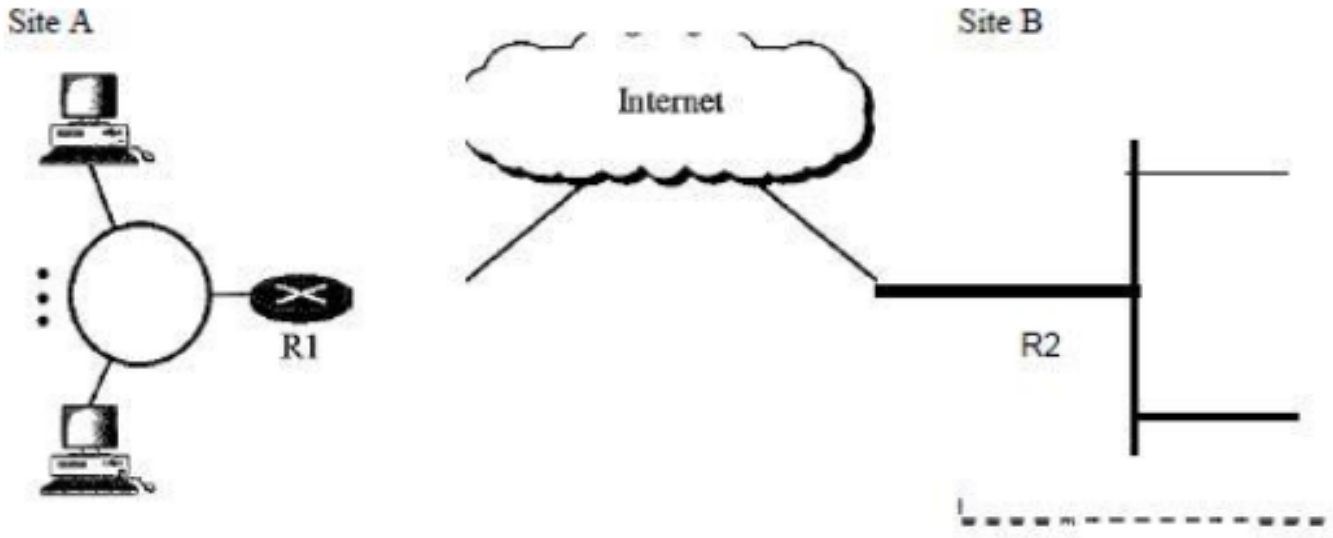


Fig. Virtual Private Network

10 Tips for Computer Network Security

1. Use a good anti-virus program.
2. Make sure your virus definitions are up-to-date.
3. Run regular virus scans.
4. Update your operating system regularly.
5. Configure and use a firewall.
6. Use your Web browser's security features.
7. Enable your router's security features.
8. Install an anti-spyware program.
9. Use strong, varied passwords.
10. Consider a computer network security suite and policy. .