University of Technology
الجامعة التكنولوجية

Computer Science Department
قسم علوم الحاسوب

Principles of Networks
مبادئ الشبكات

Prof. Dr. Shaimaa Hameed
أ.د. شيماء حميد

cs.uotechnology.edu.iq

Principles of computer Networks

مبادئ شبكات الحاسوب

فرع ادارة شبكات الحاسوب/المرحلة الاولى/الفصل الدراسي الثاني

References:

1- COMPUTER NETWORKS ,Lecture Notes: DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING SHRI VISHNU ENGINEERING COLLEGE FOR WOMEN .

2- Data and Computer Communications.7th Edition, William Stallings.

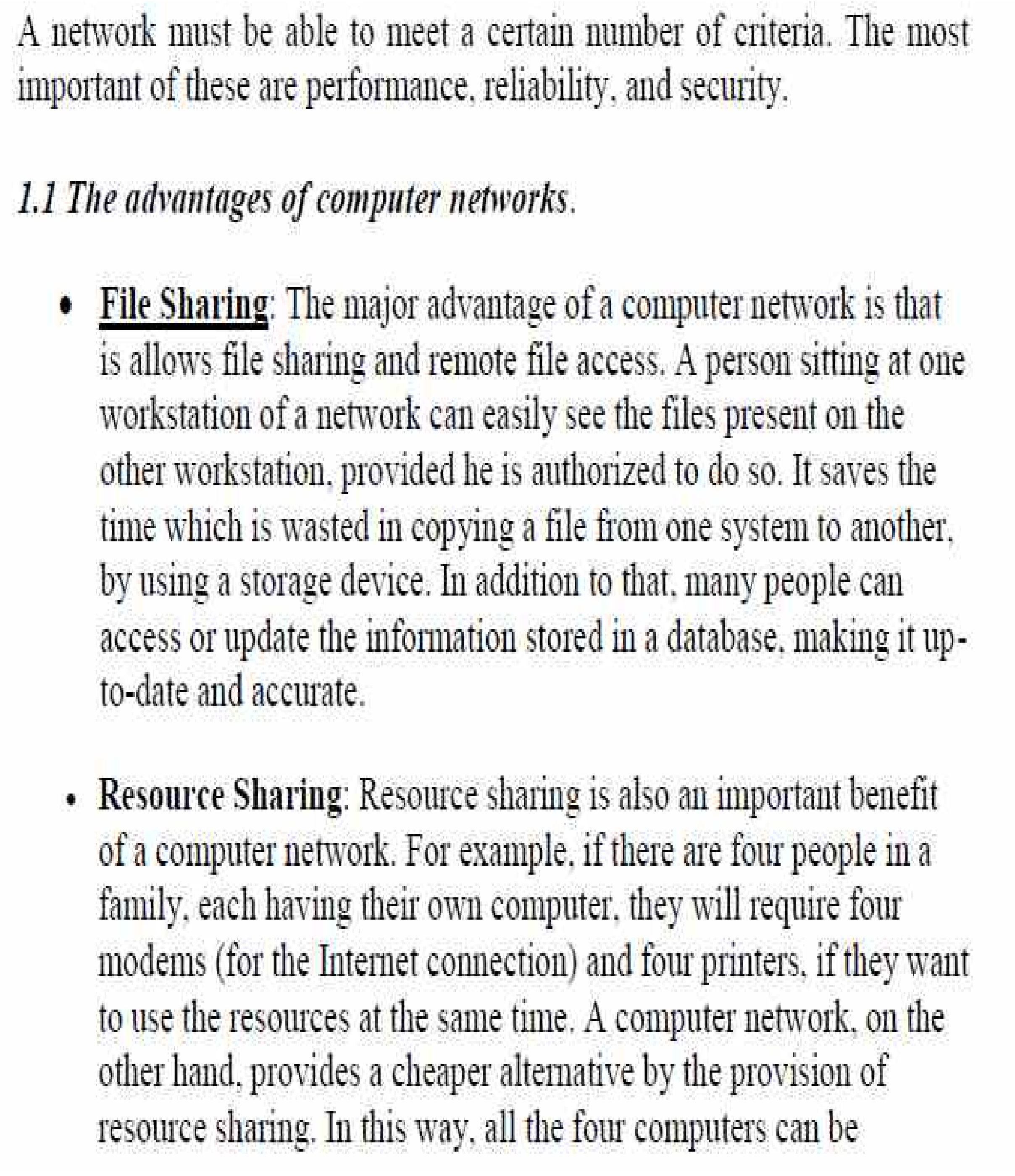
3- DATA COMMUNICATIONS AND NETWORKING: Fourth Edition,Behrouz A. Forouzan2007.

Chapter One

1. Introduction to Computer Networks:

Computer networks are defined as: "Interconnected collection of autonomous computers. Two computers are said to be interconnected if they are able to exchange information."**Or:** a network is simply a collection of intercommunicating computers and peripherals possibly having access to remote hosts and other computer networks. A network consists of a set of computers: hosts, connected via a communication subnet, the word 'host' refers to an individual computer connected to the computer, which can communicate with other hosts via the network.

A network is a set of devices (often referred to as *nodes)* connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

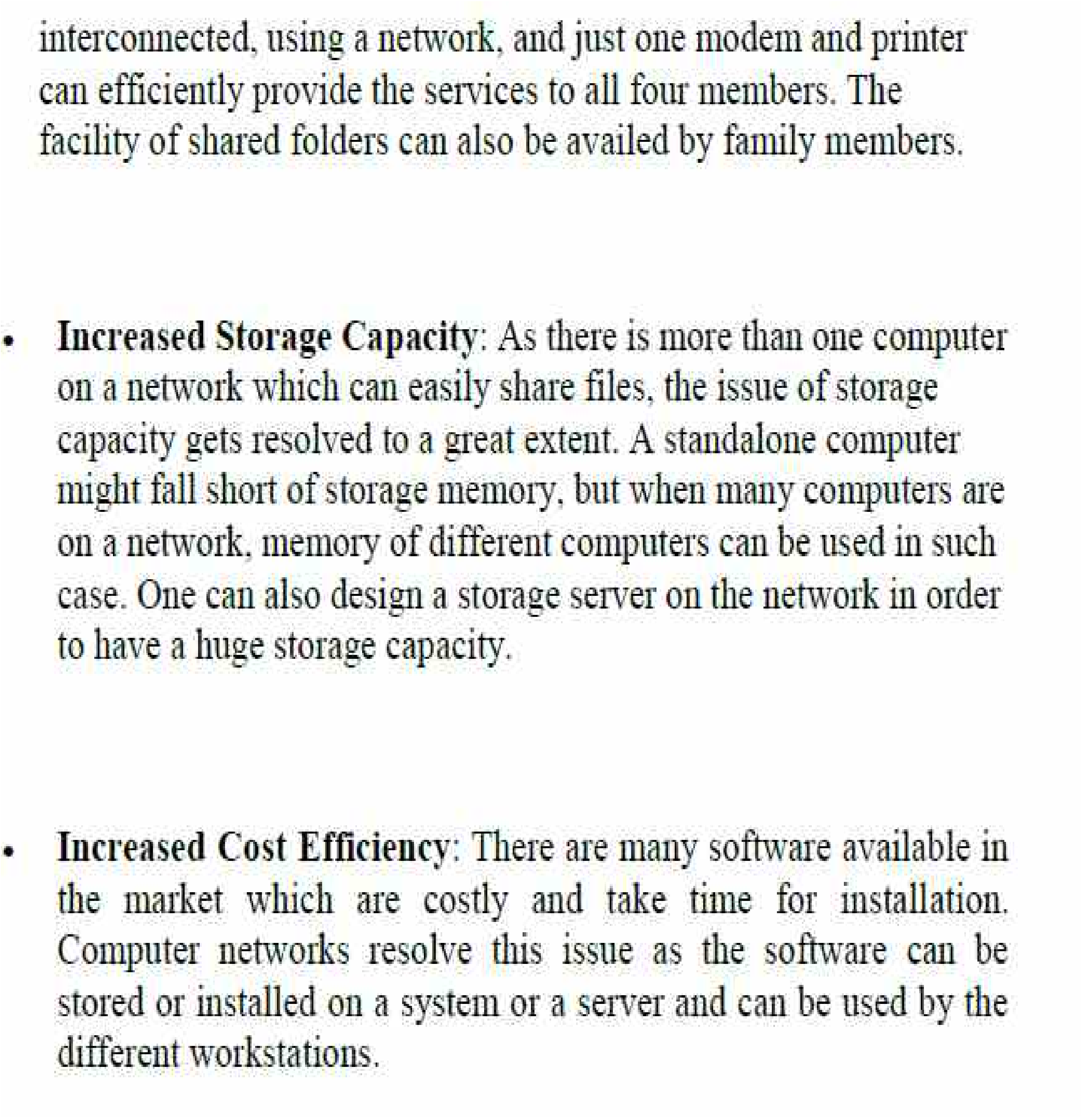


A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

1.1 The advantages of computer networks.

- **File Sharing**: The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation of a network can easily see the files present on the other workstation, provided he is authorized to do so. It saves the time which is wasted in copying a file from one system to another, by using a storage device. In addition to that, many people can access or update the information stored in a database, making it up-to-date and accurate.

- **Resource Sharing**: Resource sharing is also an important benefit of a computer network. For example, if there are four people in a family, each having their own computer, they will require four modems (for the Internet connection) and four printers, if they want to use the resources at the same time. A computer network, on the other hand, provides a cheaper alternative by the provision of resource sharing. In this way, all the four computers can be



interconnected, using a network, and just one modem and printer can efficiently provide the services to all four members. The facility of shared folders can also be availed by family members.

- **Increased Storage Capacity**: As there is more than one computer on a network which can easily share files, the issue of storage capacity gets resolved to a great extent. A standalone computer might fall short of storage memory, but when many computers are on a network, memory of different computers can be used in such case. One can also design a storage server on the network in order to have a huge storage capacity.

- **Increased Cost Efficiency**: There are many software available in the market which are costly and take time for installation. Computer networks resolve this issue as the software can be stored or installed on a system or a server and can be used by the different workstations.

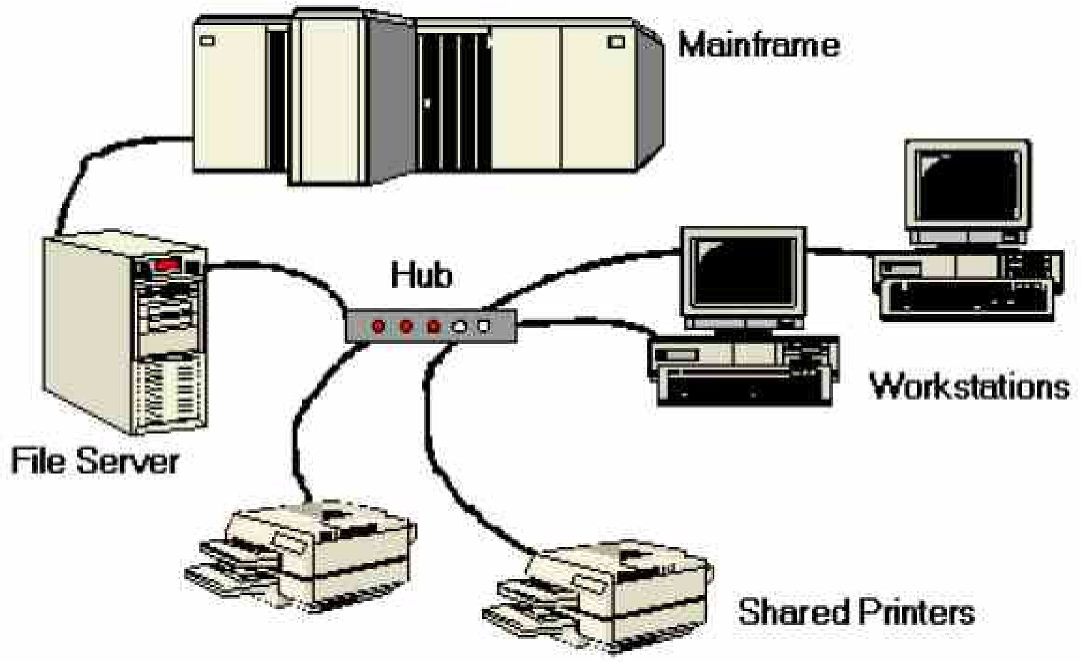
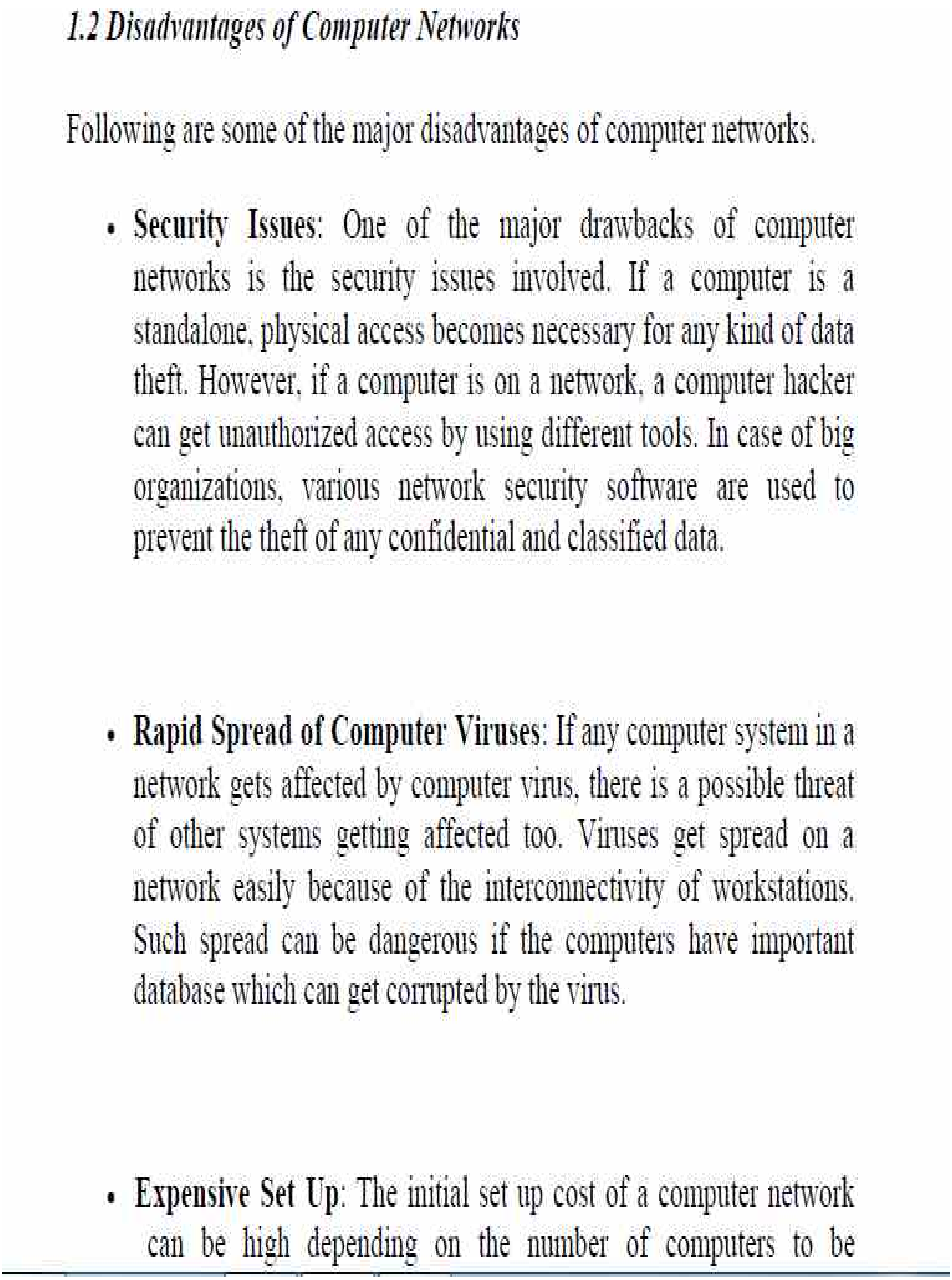


Figure 1-1: Modern networks can contain several components for allowing data and resource sharing.



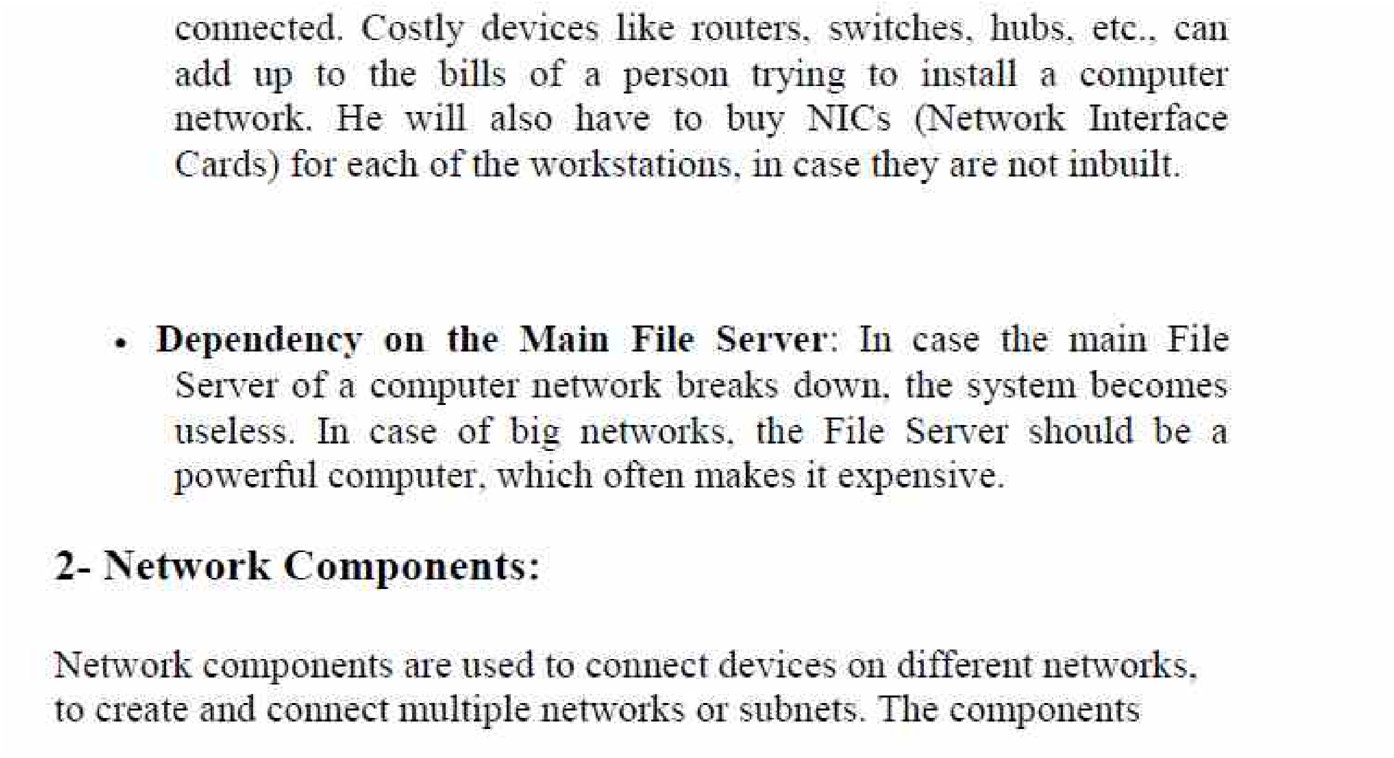
1.2 Disadvantages of Computer Networks

Following are some of the major disadvantages of computer networks.

- **Security Issues**: One of the major drawbacks of computer networks is the security issues involved. If a computer is a standalone, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a computer hacker can get unauthorized access by using different tools. In case of big organizations, various network security software are used to prevent the theft of any confidential and classified data.

- **Rapid Spread of Computer Viruses**: If any computer system in a network gets affected by computer virus, there is a possible threat of other systems getting affected too. Viruses get spread on a network easily because of the interconnectivity of workstations. Such spread can be dangerous if the computers have important database which can get corrupted by the virus.

- **Expensive Set Up**: The initial set up cost of a computer network can be high depending on the number of computers to be



connected. Costly devices like routers, switches, hubs, etc., can add up to the bills of a person trying to install a computer network. He will also have to buy NICs (Network Interface Cards) for each of the workstations, in case they are not inbuilt.

- **Dependency on the Main File Server**: In case the main File Server of a computer network breaks down, the system becomes useless. In case of big networks, the File Server should be a powerful computer, which often makes it expensive.

2- Network Components:

Network components are used to connect devices on different networks, to create and connect multiple networks or subnets. The components include:

- **NIC**: (Network Interface Card) is used to enable a network device, such as a computer or other network equipment, to connect to a network.

- **Repeater**: A repeater is an inexpensive solution that is at the OSI physicallayer and enables a network to reach users in distant portions of a building.A repeater connects two or more cable segments and retransmits anyincoming signal to all other segments.

- **HUB**: A hub is a central network device that connects network nodes suchas workstation and servers in a star topology. A hub may also be referred toas a concentrator, which is a device that can have multiple inputs and outputs all active at one time.

- **Bridge**: A bridge is a network device that sends information between two LANs.

- **Router**: Routers are devices that direct traffic between hosts.

- **BRouter**: A BRouter is a network device that acts as a bridge in one Circumstance and as a router in another. A BRouter is used on networks that operate with several different protocols.

- **GATEWAY**: The term gateway is used in many contexts, but in general itrefers to a software or hardware interface that enables two different types ofnetworked systems or software to communicate.

3- Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.2

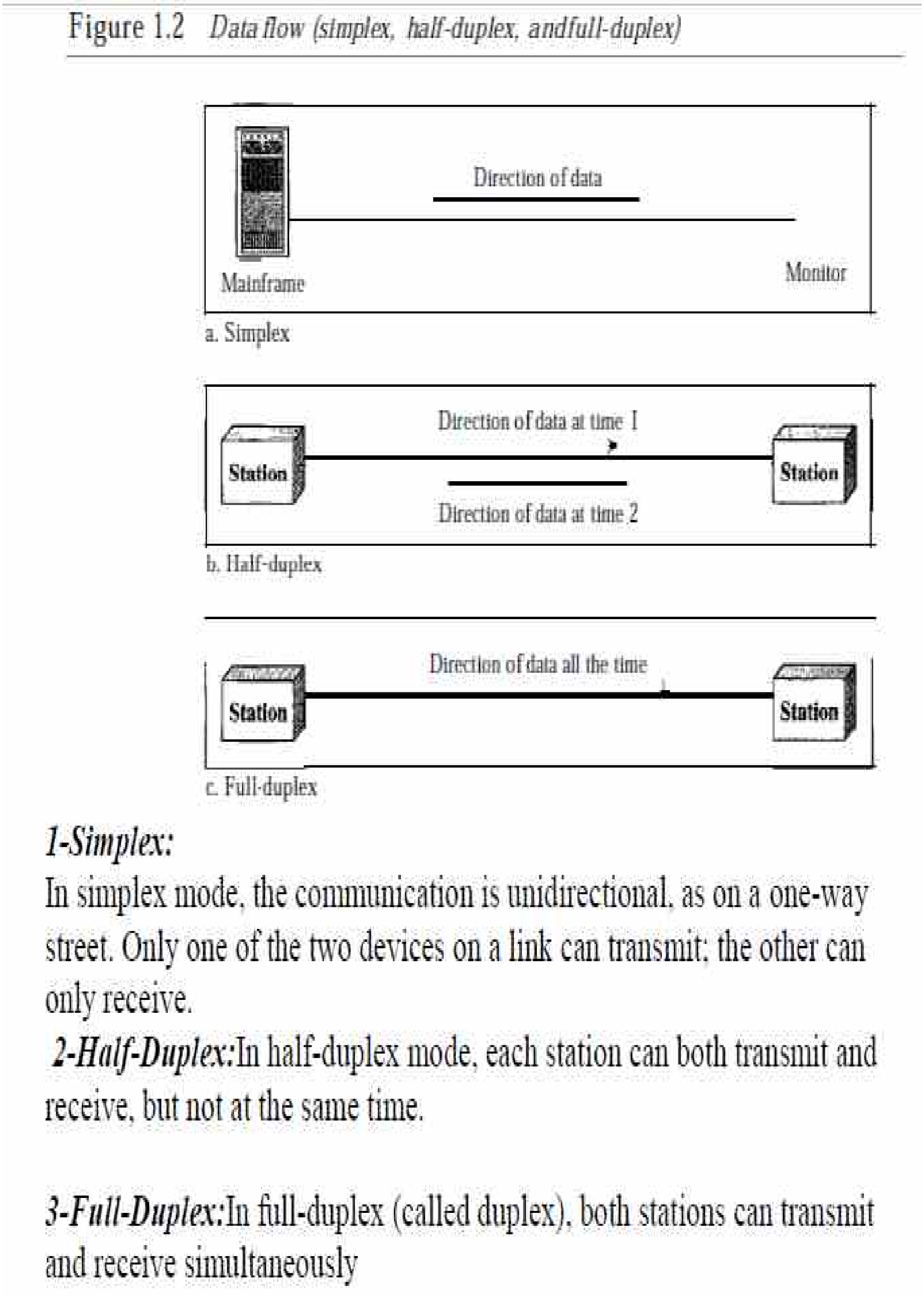


Figure 1.2 *Data flow (simplex, half-duplex, andfull-duplex)*

Direction of data
Mainframe
Monitor
a. Simplex
Direction of data at time 1
Station
Station
Direction of data at time 2
b. Half-duplex
Direction of data all the time
Station
Station
c. Full-duplex

1-Simplex:

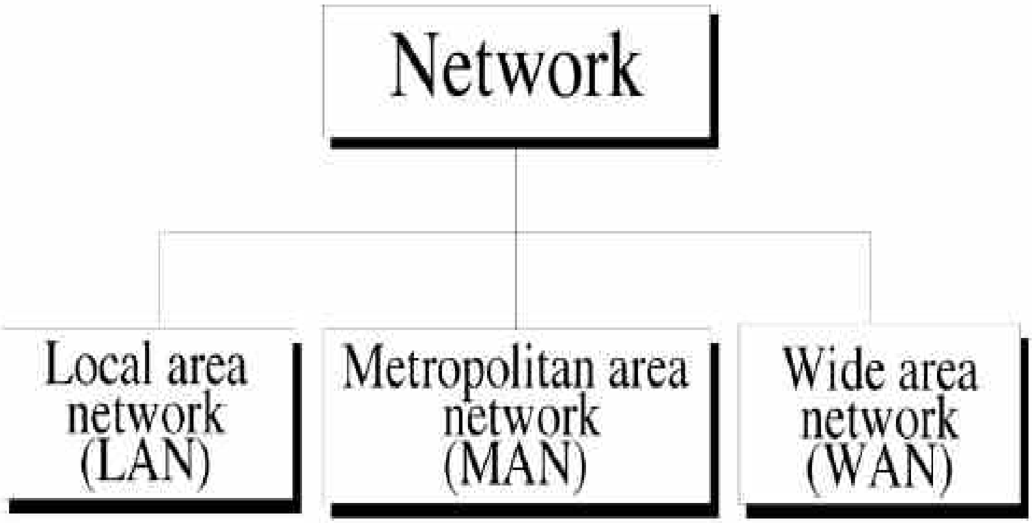
In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

2-Half-Duplex:In half-duplex mode, each station can both transmit and receive, but not at the same time.

3-Full-Duplex:In full-duplex (called duplex), both stations can transmit and receive simultaneously

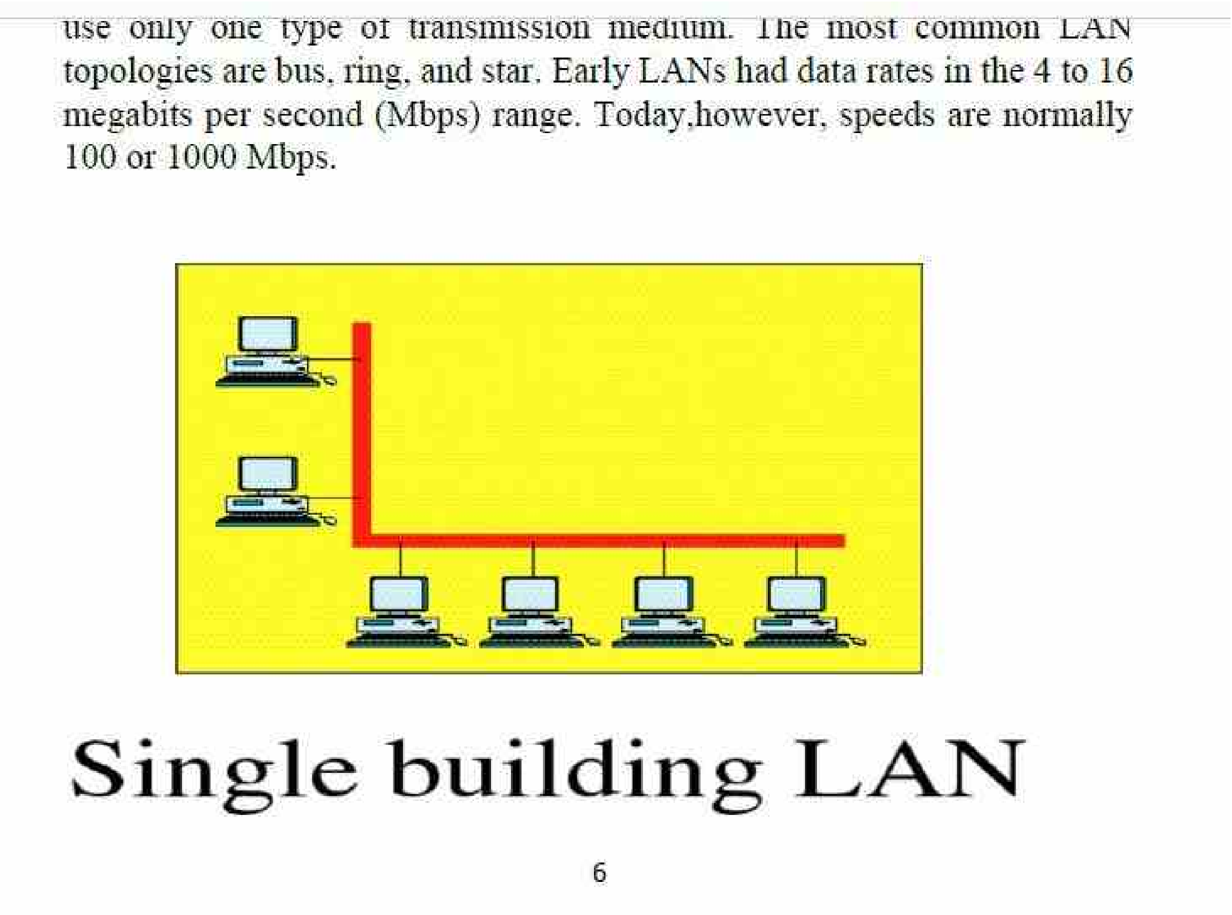
Chapter Two

2.1 Network classification



1-Local Area Network

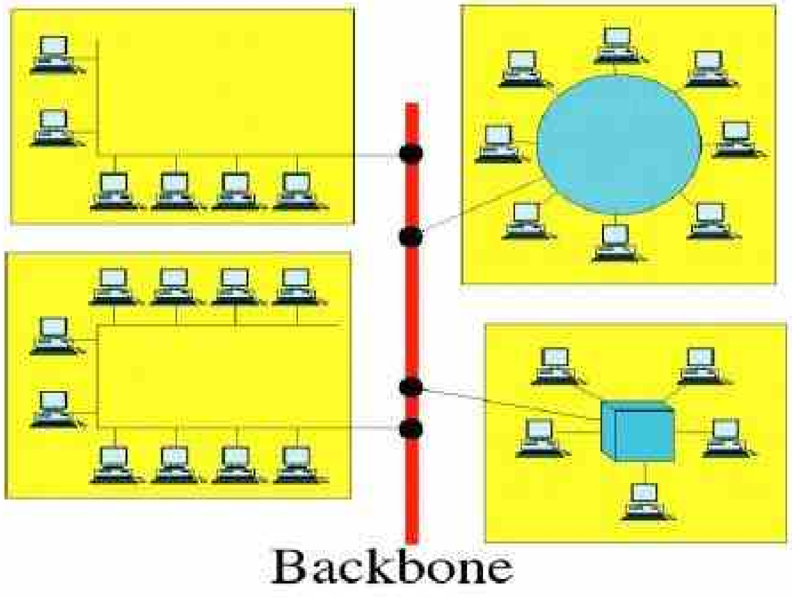
A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 1.10). Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16



use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today,however, speeds are normally 100 or 1000 Mbps.

Single building LAN

6



Multiple building LAN

1. Local Area Network (LAN):

LANs are privately owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other networks by three characteristics:

1. **Their size**: LANs are restricted in size, which means that the worst case transmission time is bounded and known in advance.
Knowing this make it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management.

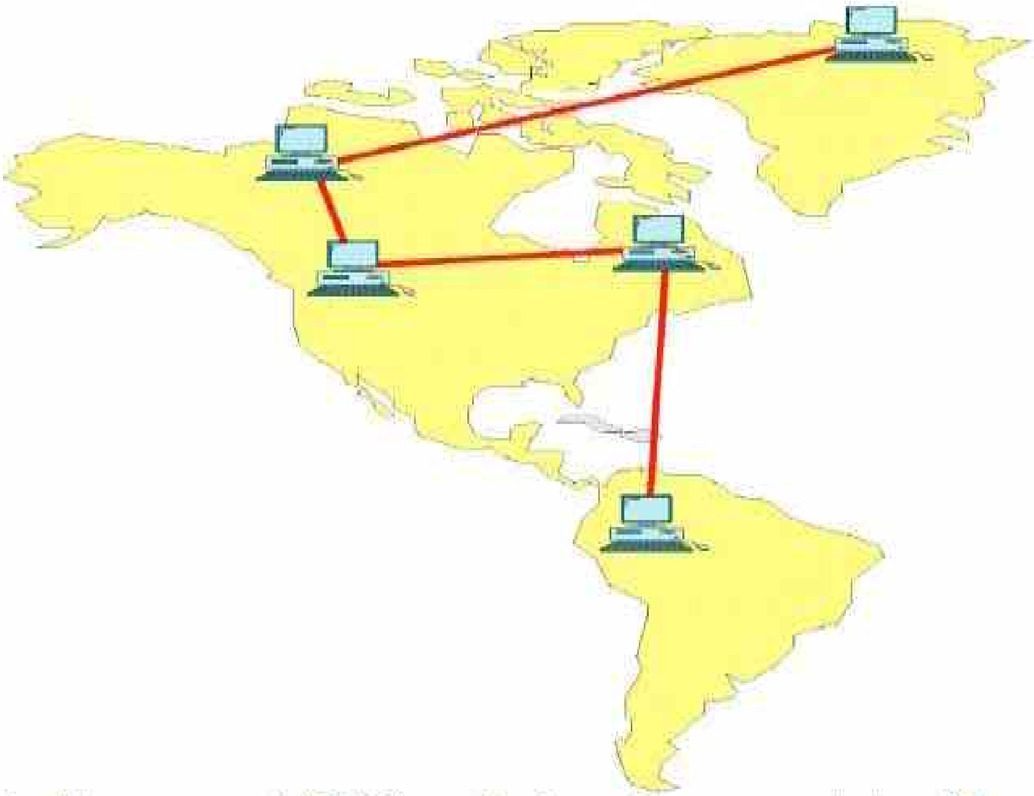
2. Their Transmission Technology: LANs often use a transmission technology consisting of a single cable to which all the machines are attached. LANs

1. Run at speed of 10 to 100 Mbps.
2. Make very few errors.
3. Have low delay (tens of microseconds).

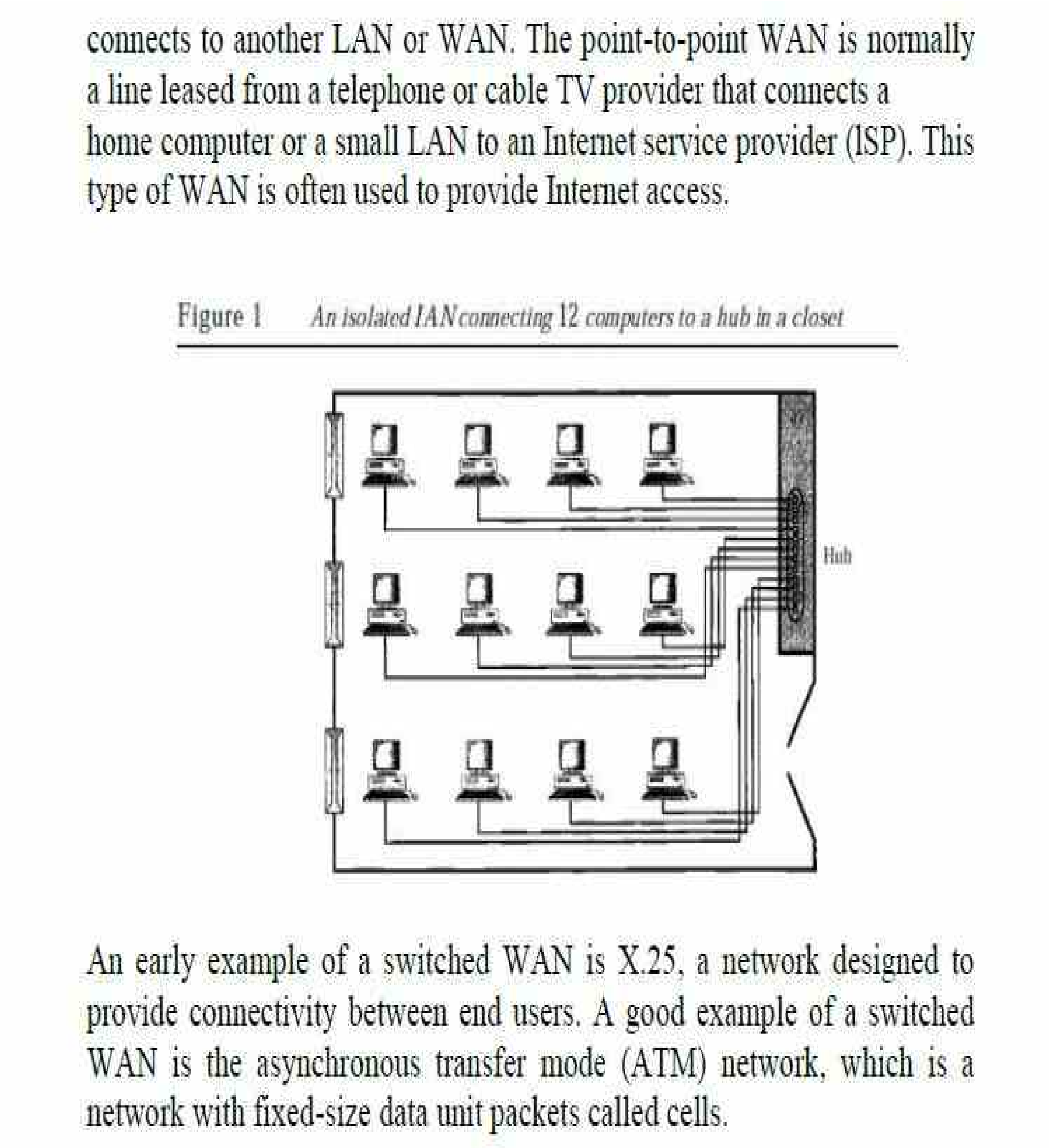
The new LAN operate at higher speed, up to hundred of megabits/sec.

3. Their topology: Various topologies are possible for broadcast LAN which are bus and ring.

2- Wide Area Network



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. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN (Figure 1).The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that



connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access.

Figure 1 *An isolated IAN connecting 12 computers to a hub in a closet*

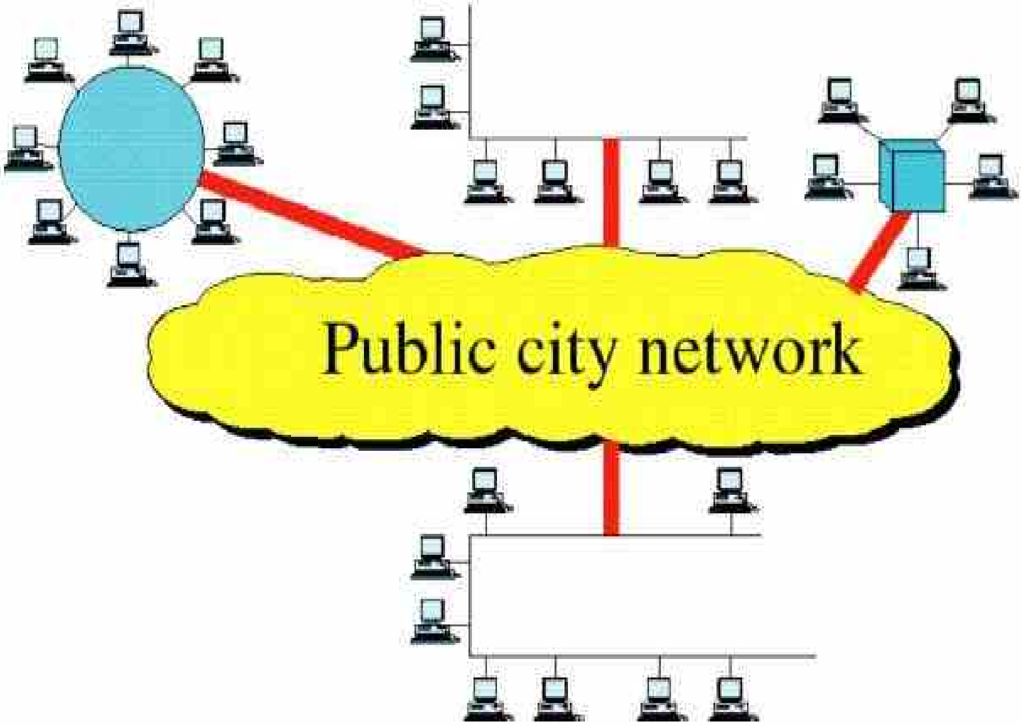
An early example of a switched WAN is X.25, a network designed to provide connectivity between end users. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells.

2. Metropolitan Area Network (MAN):

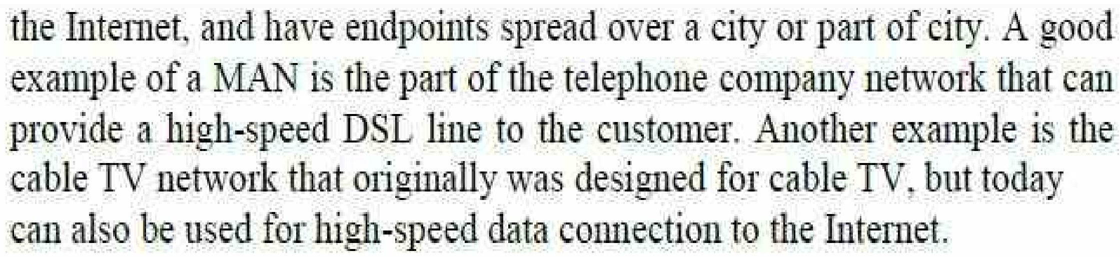
Is basically a bigger version of a LAN and normally uses similar technology it might cover a group of nearby corporate offices or a city and might be either private or public. A MAN might be related to the local cable television network.

A MAN just has one or two cables. And the main reason for even distinguishing MAN as a special category is called DQDB (Distributed Queue Dual Bus). DQBD consists of two unidirectional buses (cables) to which all the computers are connected. Each bus has a head-end, a device that initiates transmission activity. Traffic that is destined for a computer to the right of the sender uses the upper bus. Traffic to the left uses the lower one.

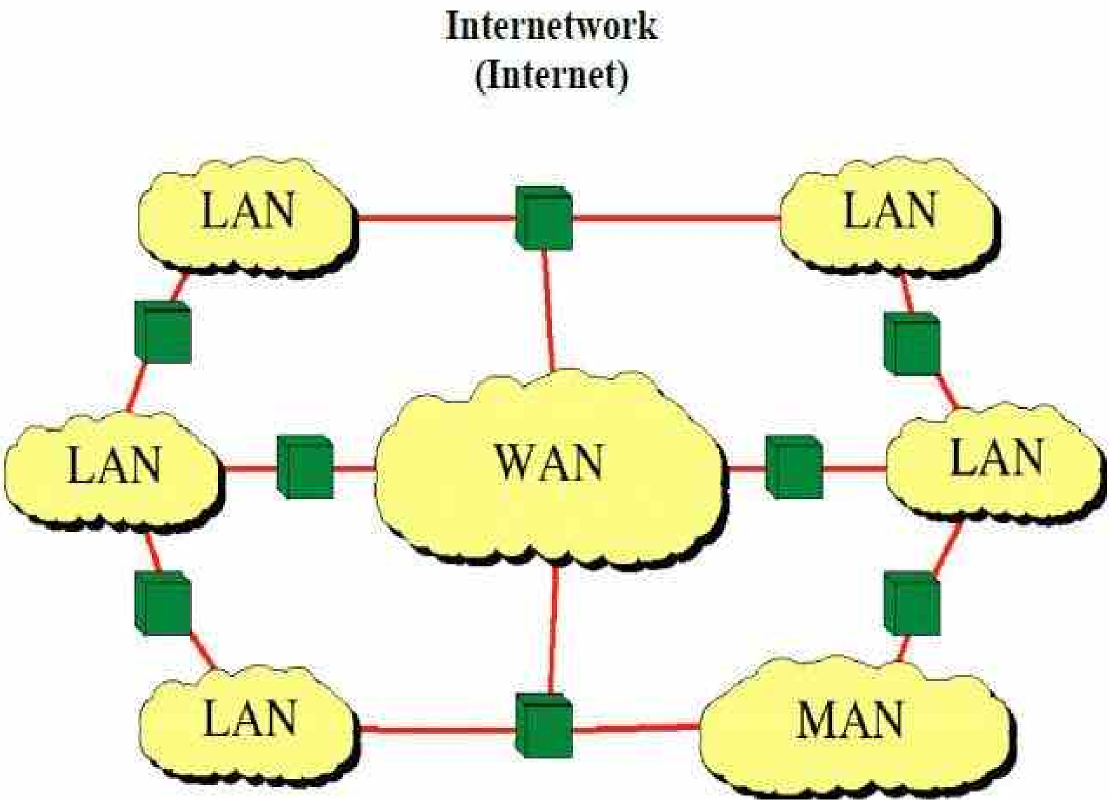
3-Metropolitan Area Networks



A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to



the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.



3. Wide Area Network (WAN):

A WAN spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs. We will refer to these machines by hosts. The hosts are connected by a communication subnet, the job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Transmission lines (also called circuits, channels, or trunks) move bits between machines. The switching elements are specialized computers used to connect two or more transmission lines.

Wireless Network

Mobile computers, such as notebook computers and personal digital assistants (PADs). Are the fastest-growing segment of the computer industry. Many of the owners of these computers have desktop machines on LANs and WANs back at the office and want to be connected to their home base even when away from home. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless network. Wireless networks have many uses which are:

1. A Common one is the portable office. People on the road often want to use their portable electronic equipment to send and receive telephone calls, fax, and electronic mail, read remote files, and so on, and do this from anywhere on land, sea, or air.

2. Another use is for rescue workers at disaster site (fires, floods, earthquakes, etc.) where the telephone system has been destroyed. Wireless LANs are easy to install also have some disadvantages are:

1.They have capacity of 1 - 2 Mbps, which is much slower than Wired LANs.

2.The error rates are often much higher.

3.The transmission from different computers can interfere with one another.

Internetwork (Internet):

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. This desire requires connecting together different, and frequently incompatible networks, sometimes by using machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnection networks is called an internetwork or just Internet.

A common form of internet is a collection of LANs connected by WAN. In fact, if we were to replace the label "subnet" by " WAN", Nothing else in the figure would have change . The only real distinction between a subnet and a WAN in this case is whether or not hosts are present. If the system with in the closed curve contains only routers, it is a subnet. If it contains both routers and hosts with their own users, it is a WAN.

Protocol Hierarchies

To reduce their design complexity, most networks are organized as a series of **layers or levels,** each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. In all networks, the purpose of each layer is to offer certain services to the higher layers.

Layer n on one machine carries on a conversation with layers on another machine. The rules and conventions used in this conversation are collectively known as, the **layer n protocol** .Basically, a protocol is an agreement between the communicating parties on how communication is to proceed. Violating the protocol will make communication more difficult, if not impossible.

The entities comprising the corresponding layers on different machines are called **peers.** In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each- layer passes- data and control information to the layer immediately below it, until the lowest layer is reached. Between each pair of adjacent layers there is an **Interface.** The interface defines which primitive operations and services the lower layer offers to the upper. A set of layers and protocols are called **network architecture.** The specification of an architecture must contain enough information to allow an implementer to write the program or build the Hardware for each layer so that it will correctly obey the appropriate protocol. Neither the details of the implementation nor the specification of the interfaces are part of the architecture because these are hidden away inside the machines and not visible from the outside. **It** is not even necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols.

A list of protocols used by a certain system, one protocol peer layer is called a **protocol stack.** Note that each protocol is completely independent of the other ones as long as the interfaces are not changed.

How to provide communication to the top layer of the five-layer network:

1. Message, **M,** is produced by an application process running **layer 5** and given to **layer 4** for transmission.

2. **Layer 4** puts a header in front of the message to identify the message and parses the result to **layer** 3.

3. The header includes control information, such as sequence numbers, to allow **layer 4** on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence. In some layers, headers also contain size, times, and other control fields.

4. There is-no limit to the size of messages transmitted in the **layer4** protocol, but there is nearly always a limit imposed by the **layer 3** protocol. Consequently **layer 3** must break up the incoming messages into smaller units, packets, adding a layer header to each packet.

5. Layer2 adds not only a header to each piece, but also a trailer, and gives the resulting unit to **layer 1** for physical transmission.

6. At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses. None of the headers for **layers below n** are passed up to **layer n.**

Design Issues For The Layers:

1. Every layer needs a mechanism for identifying senders and receivers. Since a network, normally has many computers, some of which have multiple processes, a means is needed for a process on one machine to specify with whom it wants to talk.

2. Rules for data transfer: In some systems, data only travel in one direction **(simplex communication).** In others they can travel in either direction, but not simultaneously **(half-duplex communication).** In others they travel in both directions at once **(full-duplex communication).**

3. Error control is an important issue because physical communication circuits are not perfect. The receiver must have some way to telling the sender which messages have been correctly received and which have not.

4. Not all communication channels preserve the order of messages sent on them. The solution is to number the pieces.

5. How to keep a fast sender from swamping a slow receiver, with data Some of them involve some kind of feedback from the receiver to the sender, either directly or indirectly, about the receiver's current situation.

6. The inability of all processes to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting, and then reassembling messages.

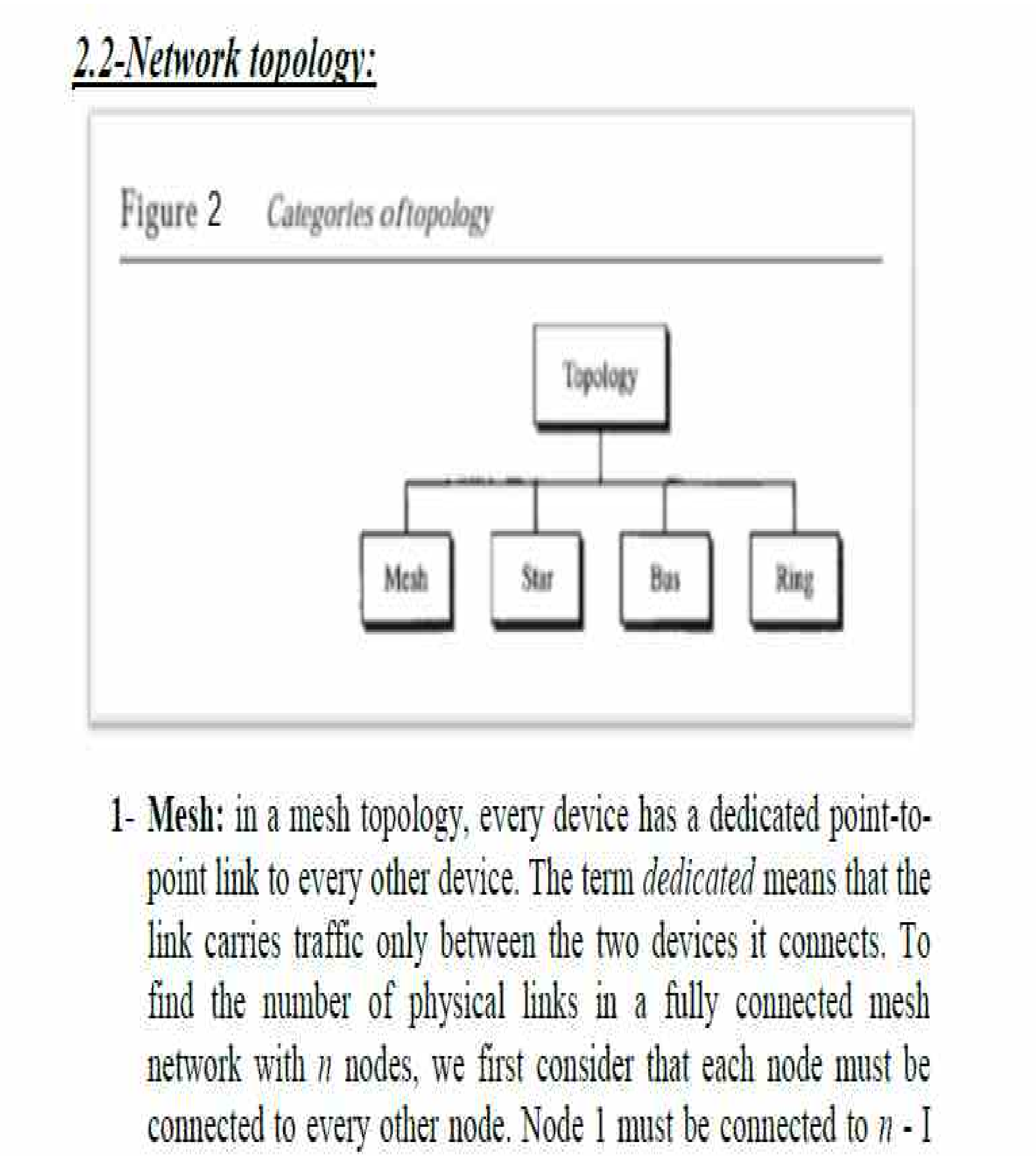
The Relationship of Services to Protocols

Services and protocols are distinct concepts, although they are frequently confused. This distinction is:

A **service** is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

A **Protocol** is a set of rules governing the format and meaning of the frames, packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols in order to implement their service definitions.

They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocols are completely decoupled.



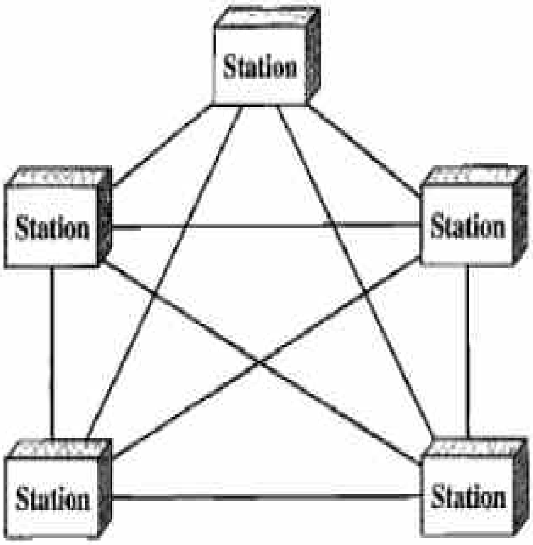
2.2-Network topology:

Figure 2 *Categories of topology*

Topology
Mesh
Star
Bus
Ring

1- **Mesh:** in a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to n - 1 nodes. We need $n(n - 1)$ physical links. However, if each physical link allows communication in both directions (duplexmode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need $n(n - 1) /2$ duplex-mode links.To accommodate that many links, every device on the network must have $n - 1$ input/output *(VO)* ports (see Figure 1.5) to be connected to the other n - 1 stations.

Figure3 *A fully connected mesh topology (five devices)*



The advantages of this topology :

1. the use of dedicated links guarantees that each connection can carry its own data load, thus eliminatingthe traffic problems that can occur when links must be shared by multiple devices.

can occur when links must be shared by multiple devices.

2. a mesh topology is robust
3. the advantage of privacy or security
4. point-to-point links make fault identification and fault isolation easy.

The disadvantages of this topology related to the amount of cabling and the number of I/O ports required:

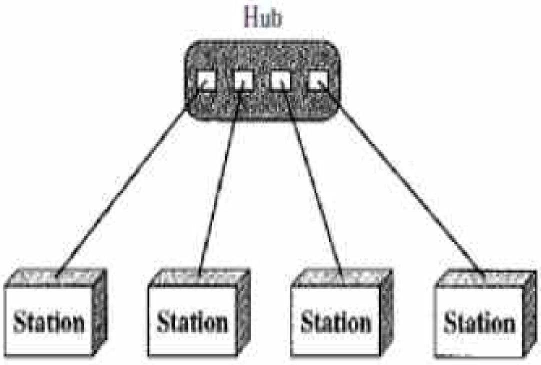
1. every device must be connected to every other device, installation and reconnection are difficult.
2. the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
3. the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

2- **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 (see Figure 1.6) .

Figure 4 *A star topology connecting four stations*

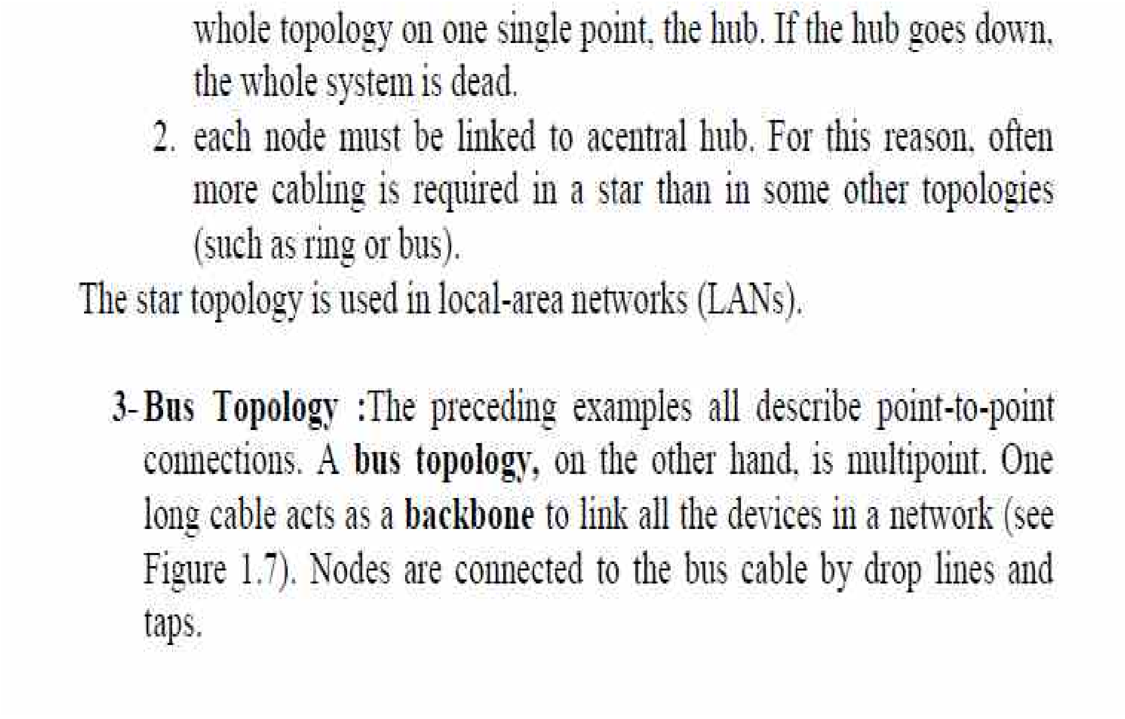


The advantages of this topology :

1. A star topology is less expensive than a mesh topology
2. it easy to install and reconfigure
3. include robustness. If one link fails, only that link is affected. Allother links remain active.
4. easy fault identification and fault isolation

The disadvantages of this topology

1. One big disadvantage of a star topology is the dependency of the



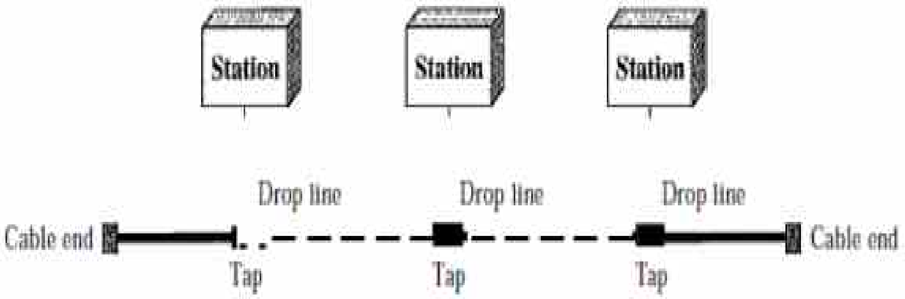
whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

2. each node must be linked to acentral hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

The star topology is used in local-area networks (LANs).

3- **Bus Topology :**The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network (see Figure 1.7). Nodes are connected to the bus cable by drop lines and taps.

Figure 5 *A bus topology connecting three stations*



The advantages of this topology:

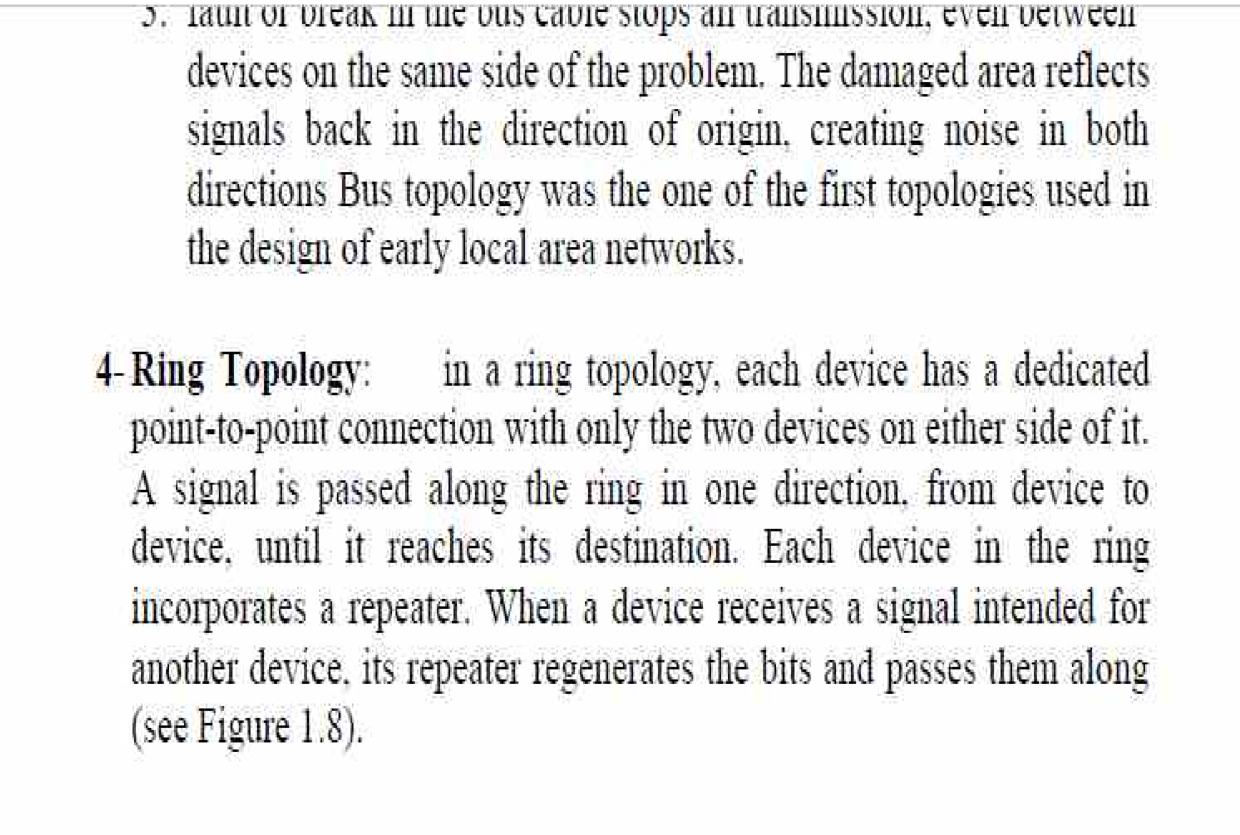
1. ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
2. In this way, a bus uses less cabling than mesh or star topologies.

The disadvantages of this topology

1. include difficult reconnection and fault isolation

fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the

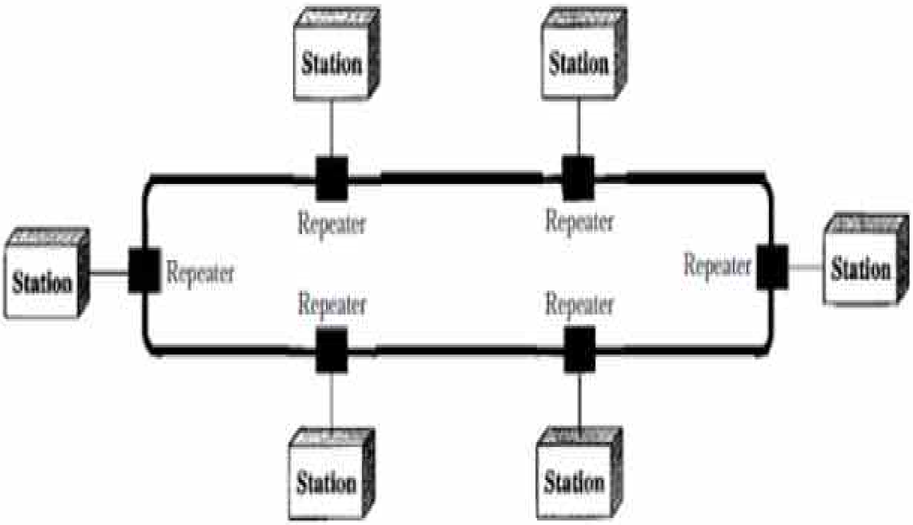
1. direction of origin, creating noise in both directions.
2. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable
3. fault or break in the bus cable stops all transmission, even between



3. fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions Bus topology was the one of the first topologies used in the design of early local area networks.

4- **Ring Topology**: in a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure 1.8).

Figure 6 *A ring topology connecting six stations*



The advantages of this topology:

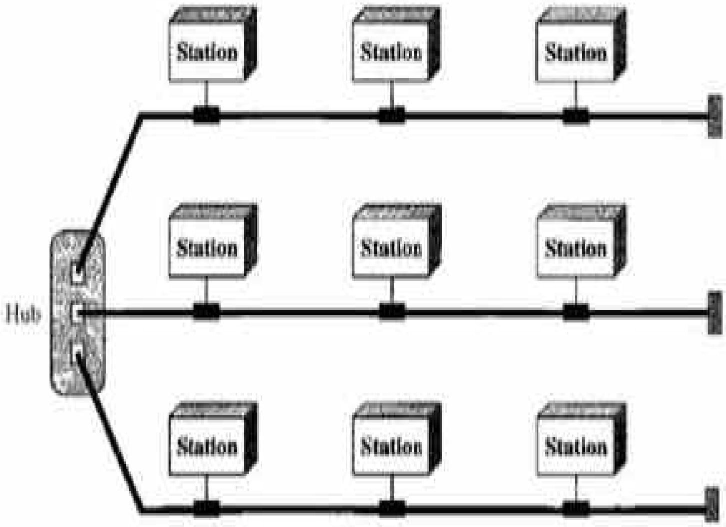
1. easy to install and reconfigure.
2. To add or delete a device requires changing only two connections.
3. fault isolation is simplified.

The disadvantages of this topology

1. 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.

Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure 1.9.

Figure 7 A *hybrid topology: a star backbone with three bus networks*

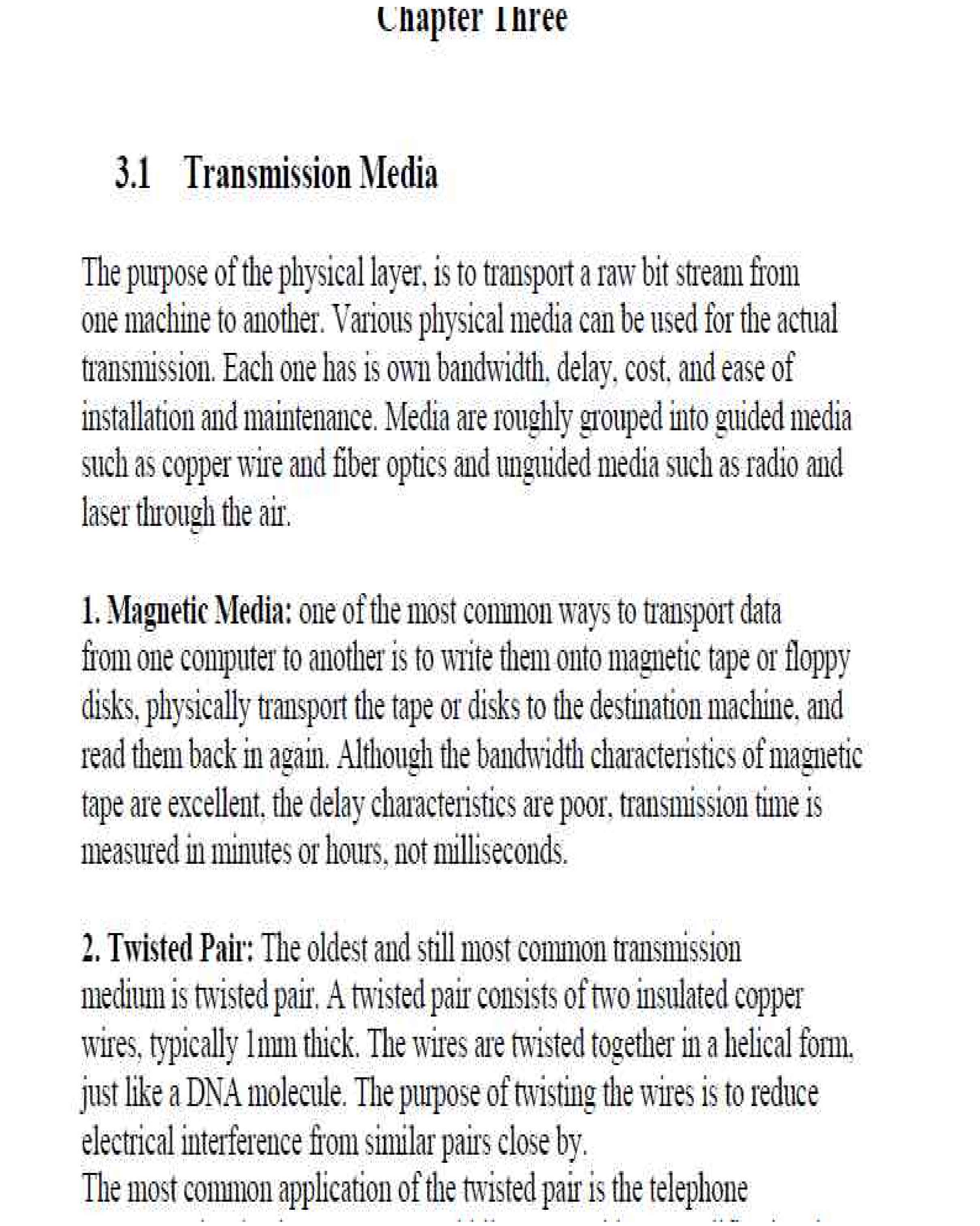


Note : the reference(Ch1&Ch2) :

'DATA COMMUNICATIONS ANDNETWORKING"

Fourth Edition,Behrouz A. Forouzan,DeAnza College

With,Sophia Chung Fegan,PDF.2007.



Chapter Three

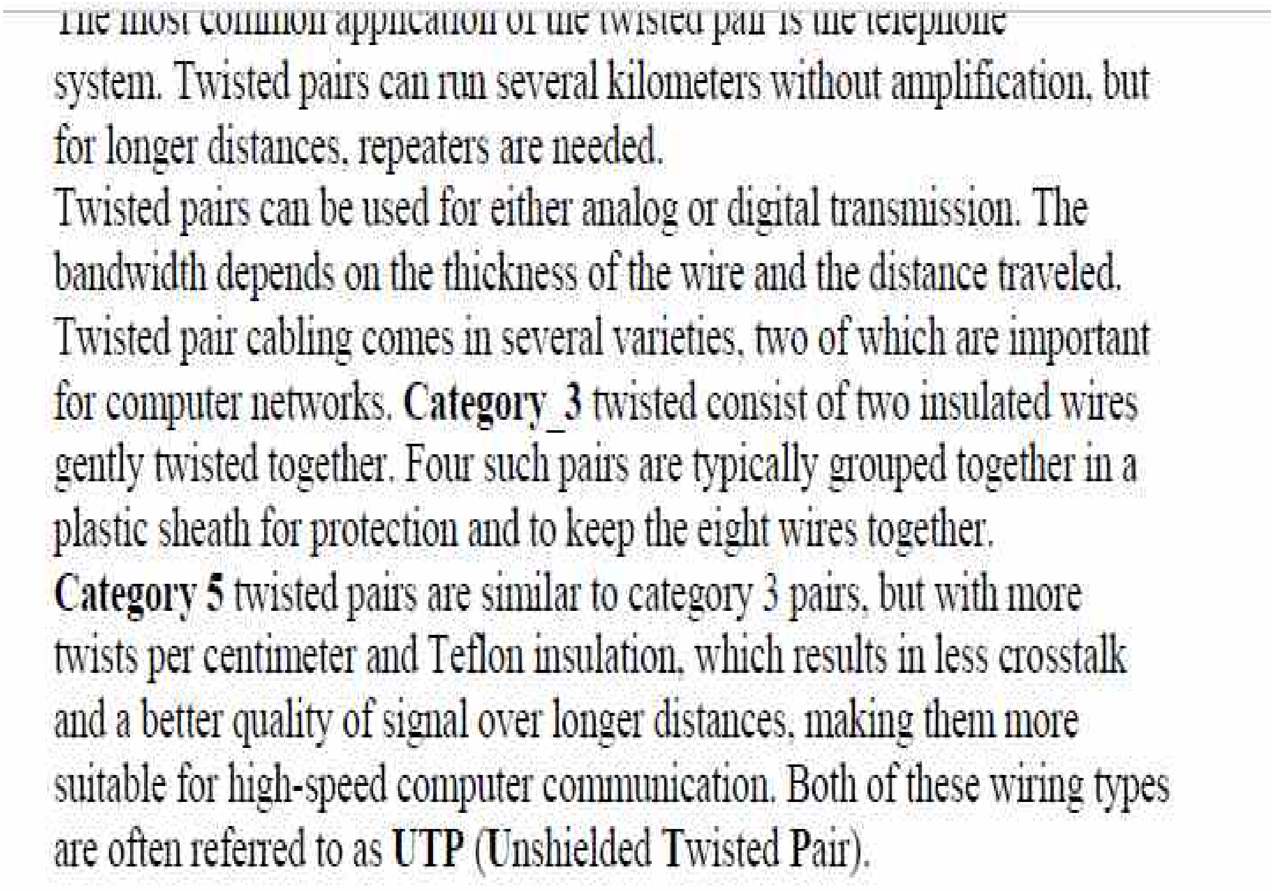
3.1 Transmission Media

The purpose of the physical layer, is to transport a raw bit stream from one machine to another. Various physical media can be used for the actual transmission. Each one has is own bandwidth, delay, cost, and ease of installation and maintenance. Media are roughly grouped into guided media such as copper wire and fiber optics and unguided media such as radio and laser through the air.

1. Magnetic Media: one of the most common ways to transport data from one computer to another is to write them onto magnetic tape or floppy disks, physically transport the tape or disks to the destination machine, and read them back in again. Although the bandwidth characteristics of magnetic tape are excellent, the delay characteristics are poor, transmission time is measured in minutes or hours, not milliseconds.

2. Twisted Pair: The oldest and still most common transmission medium is twisted pair. A twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form, just like a DNA molecule. The purpose of twisting the wires is to reduce electrical interference from similar pairs close by.

The most common application of the twisted pair is the telephone



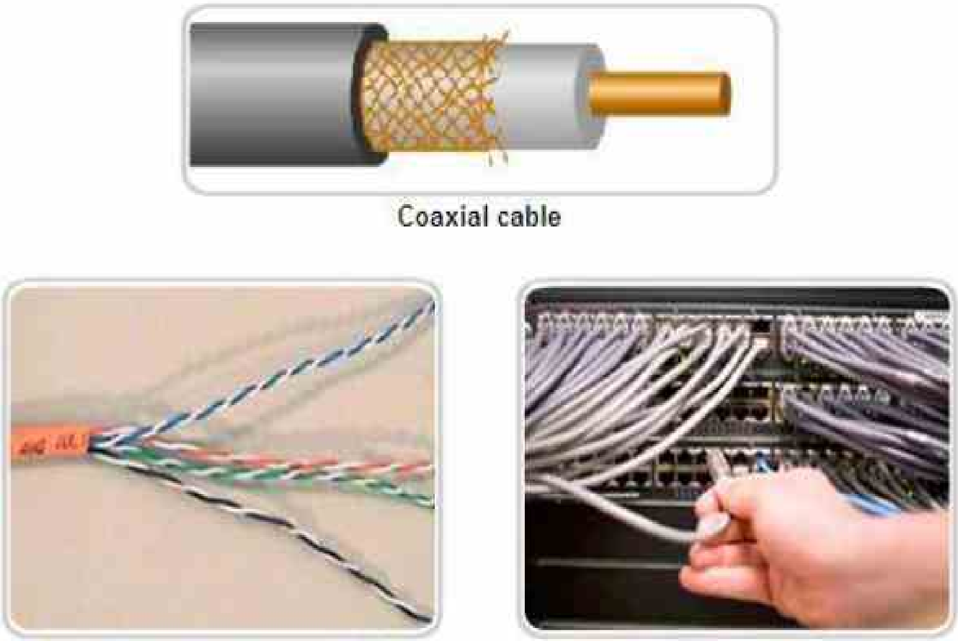
The most common application of the twisted pair is the telephone system. Twisted pairs can run several kilometers without amplification, but for longer distances, repeaters are needed.

Twisted pairs can be used for either analog or digital transmission. The bandwidth depends on the thickness of the wire and the distance traveled.

Twisted pair cabling comes in several varieties, two of which are important for computer networks. **Category_3** twisted consist of two insulated wires gently twisted together. Four such pairs are typically grouped together in a plastic sheath for protection and to keep the eight wires together.

Category 5 twisted pairs are similar to category 3 pairs, but with more twists per centimeter and Teflon insulation, which results in less crosstalk and a better quality of signal over longer distances, making them more suitable for high-speed computer communication. Both of these wiring types are often referred to as **UTP** (**U**nshielded **T**wisted **P**air).

Copper Media

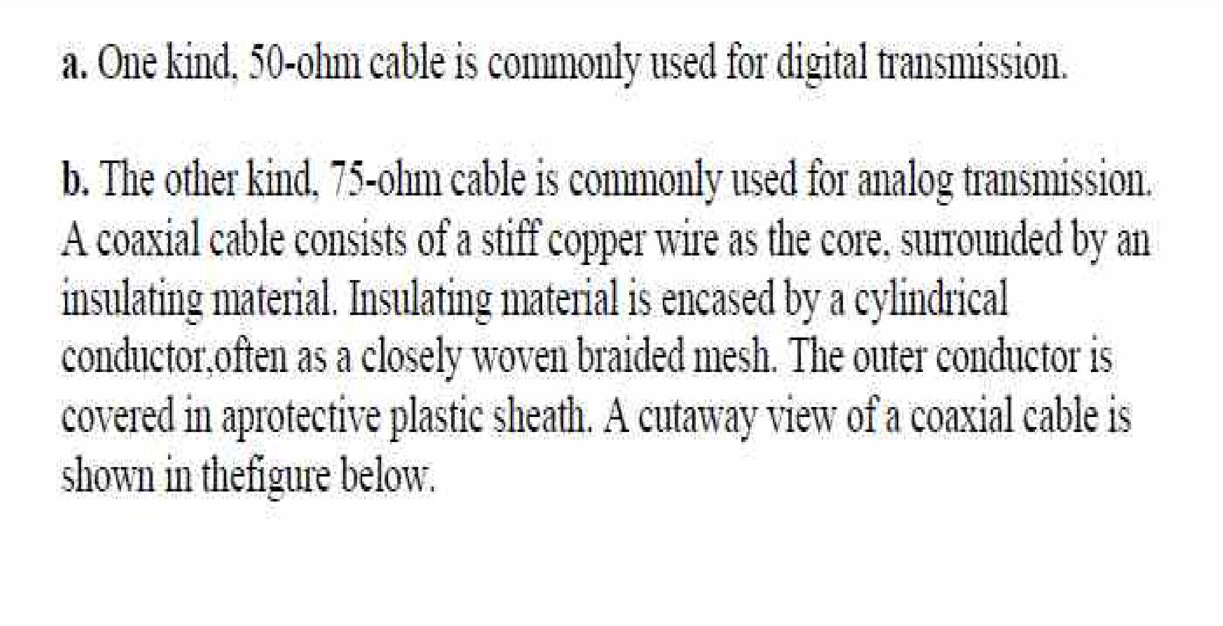


Coaxial cable

Unshielded twisted-pair cable

RJ-45 connections

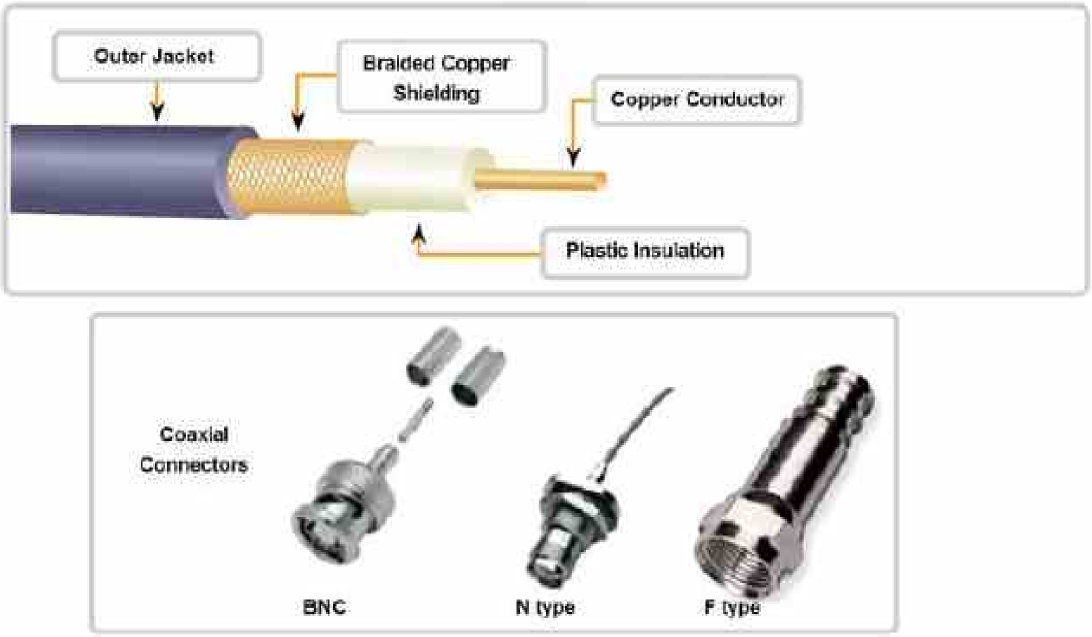
3. Baseband Coaxial Cable: Another common transmission medium is the coaxial cable (known as coax), it has better shielding than twisted pair, so it can span longer distances at higher speeds. Two kinds of coaxial cables are widely used:



a. One kind, 50-ohm cable is commonly used for digital transmission.

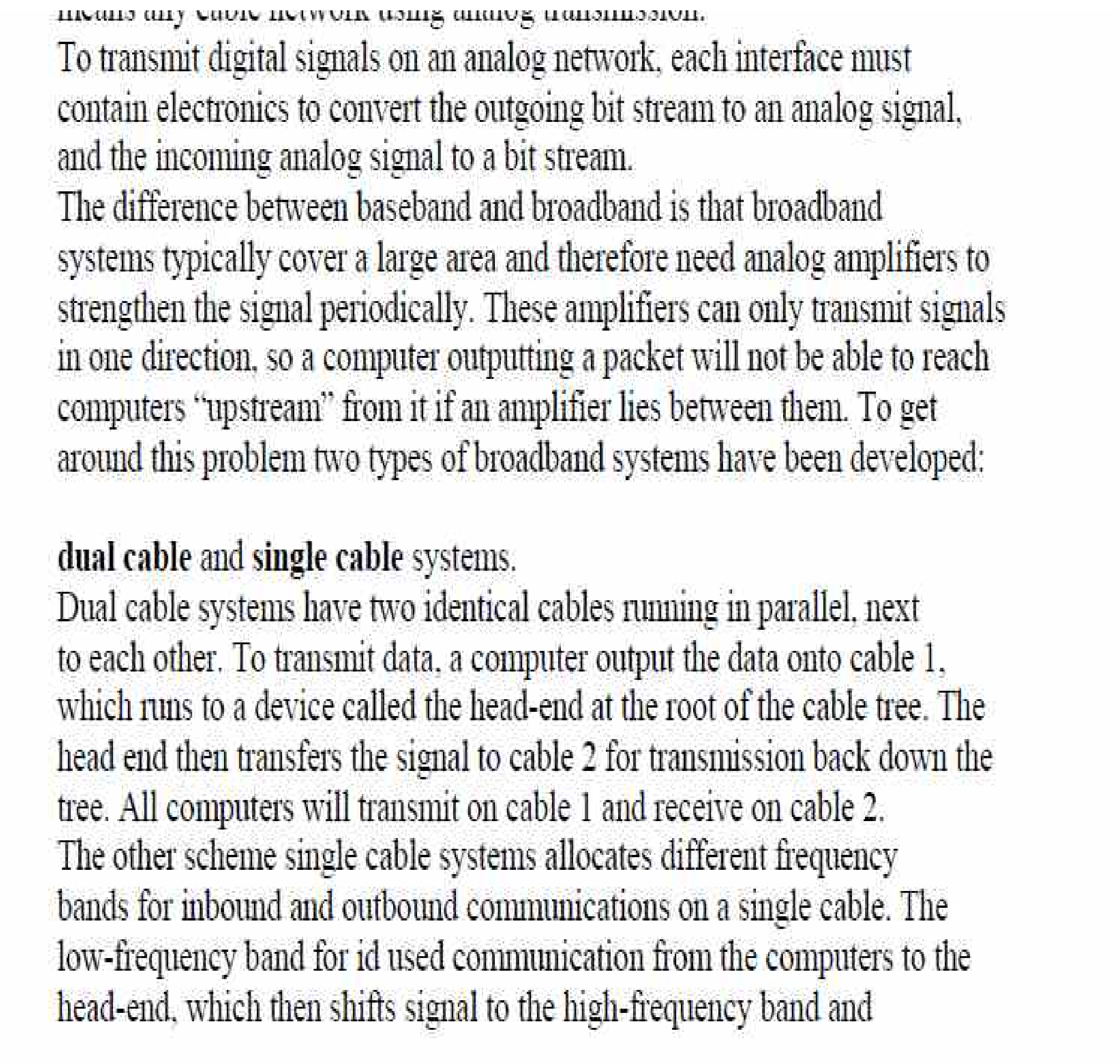
b. The other kind, 75-ohm cable is commonly used for analog transmission. A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. Insulating material is encased by a cylindrical conductor,often as a closely woven braided mesh. The outer conductor is covered in aprotective plastic sheath. A cutaway view of a coaxial cable is shown in thefigure below.

Coaxial Cable Design



The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable length. Coax is still widely used for cable television and some local area networks.

Broadband Coaxial Cable: The other kind of coaxial cable systems uses analog transmission on standard cable television cabling. It is called broadband. The term "broadband cable" in the computer networking world means any cable network using analog transmission.
To transmit digital signals on an analog network, each interface must



means any cable network using analog transmission.

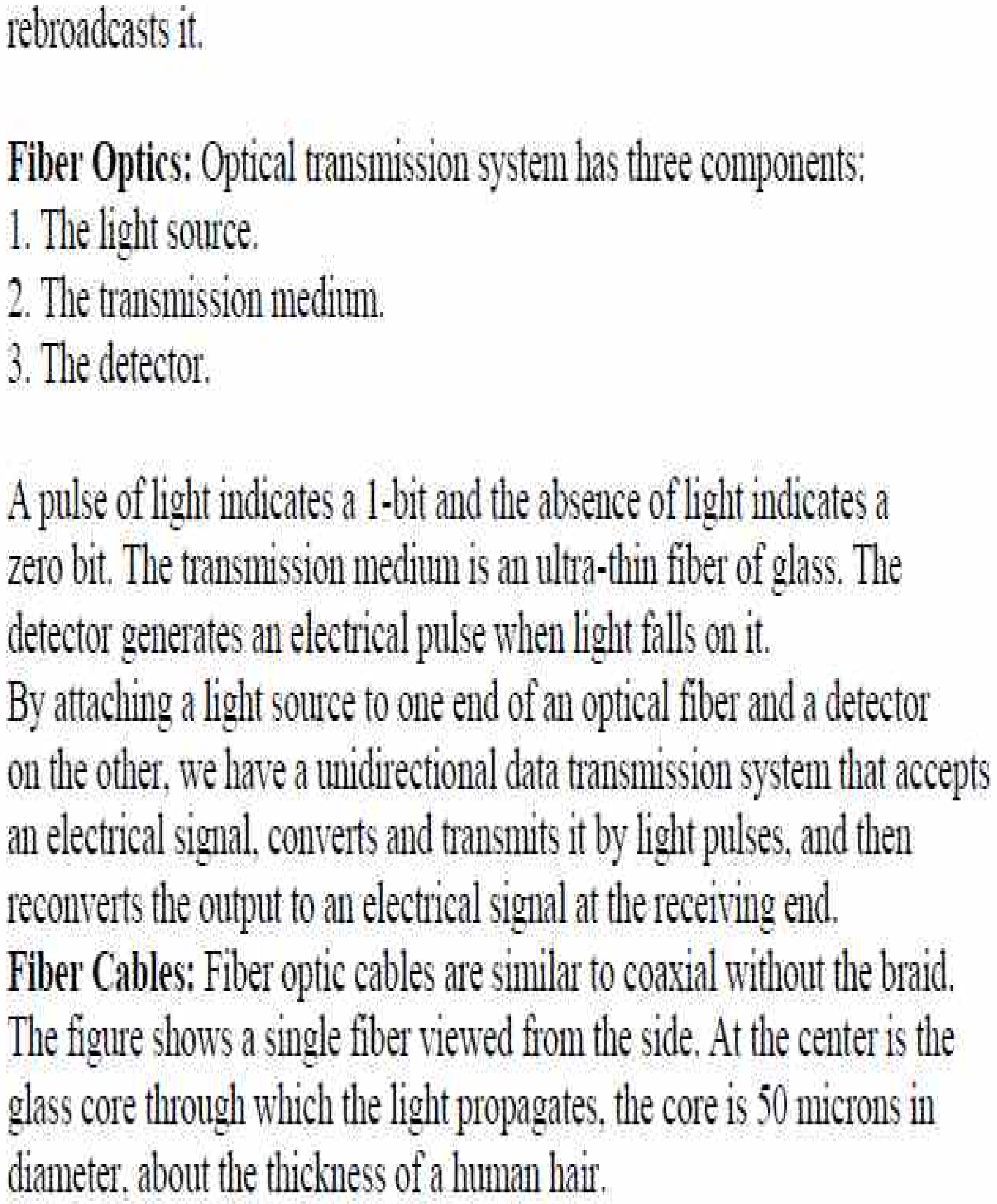
To transmit digital signals on an analog network, each interface must contain electronics to convert the outgoing bit stream to an analog signal, and the incoming analog signal to a bit stream.

The difference between baseband and broadband is that broadband systems typically cover a large area and therefore need analog amplifiers to strengthen the signal periodically. These amplifiers can only transmit signals in one direction, so a computer outputting a packet will not be able to reach computers “upstream” from it if an amplifier lies between them. To get around this problem two types of broadband systems have been developed:

dual cable and **single cable** systems.

Dual cable systems have two identical cables running in parallel, next to each other. To transmit data, a computer output the data onto cable 1, which runs to a device called the head-end at the root of the cable tree. The head end then transfers the signal to cable 2 for transmission back down the tree. All computers will transmit on cable 1 and receive on cable 2.

The other scheme single cable systems allocates different frequency bands for inbound and outbound communications on a single cable. The low-frequency band for id used communication from the computers to the head-end, which then shifts signal to the high-frequency band and



rebroadcasts it.

Fiber Optics: Optical transmission system has three components:

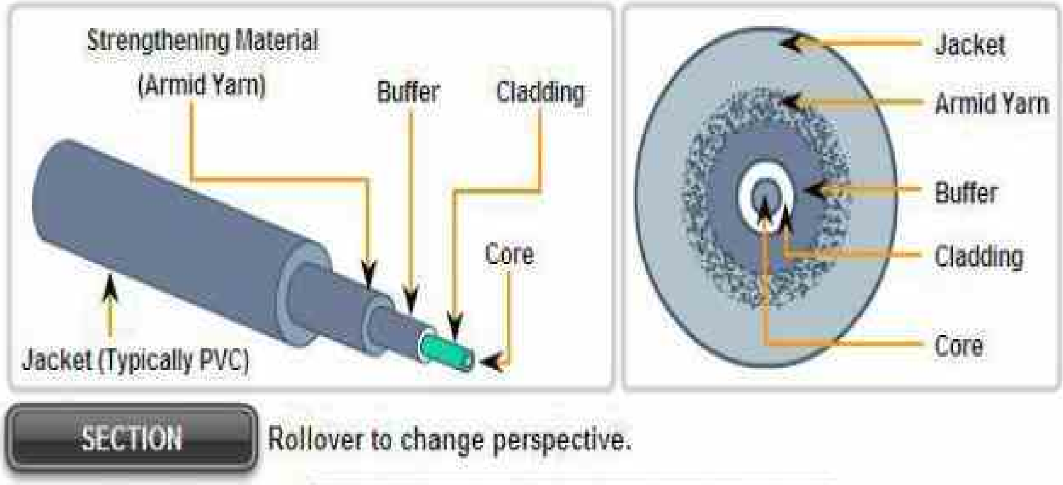
1. The light source.
2. The transmission medium.
3. The detector.

A pulse of light indicates a 1-bit and the absence of light indicates a zero bit. The transmission medium is an ultra-thin fiber of glass. The detector generates an electrical pulse when light falls on it.

By attaching a light source to one end of an optical fiber and a detector on the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.

Fiber Cables: Fiber optic cables are similar to coaxial without the braid. The figure shows a single fiber viewed from the side. At the center is the glass core through which the light propagates, the core is 50 microns in diameter, about the thickness of a human hair.

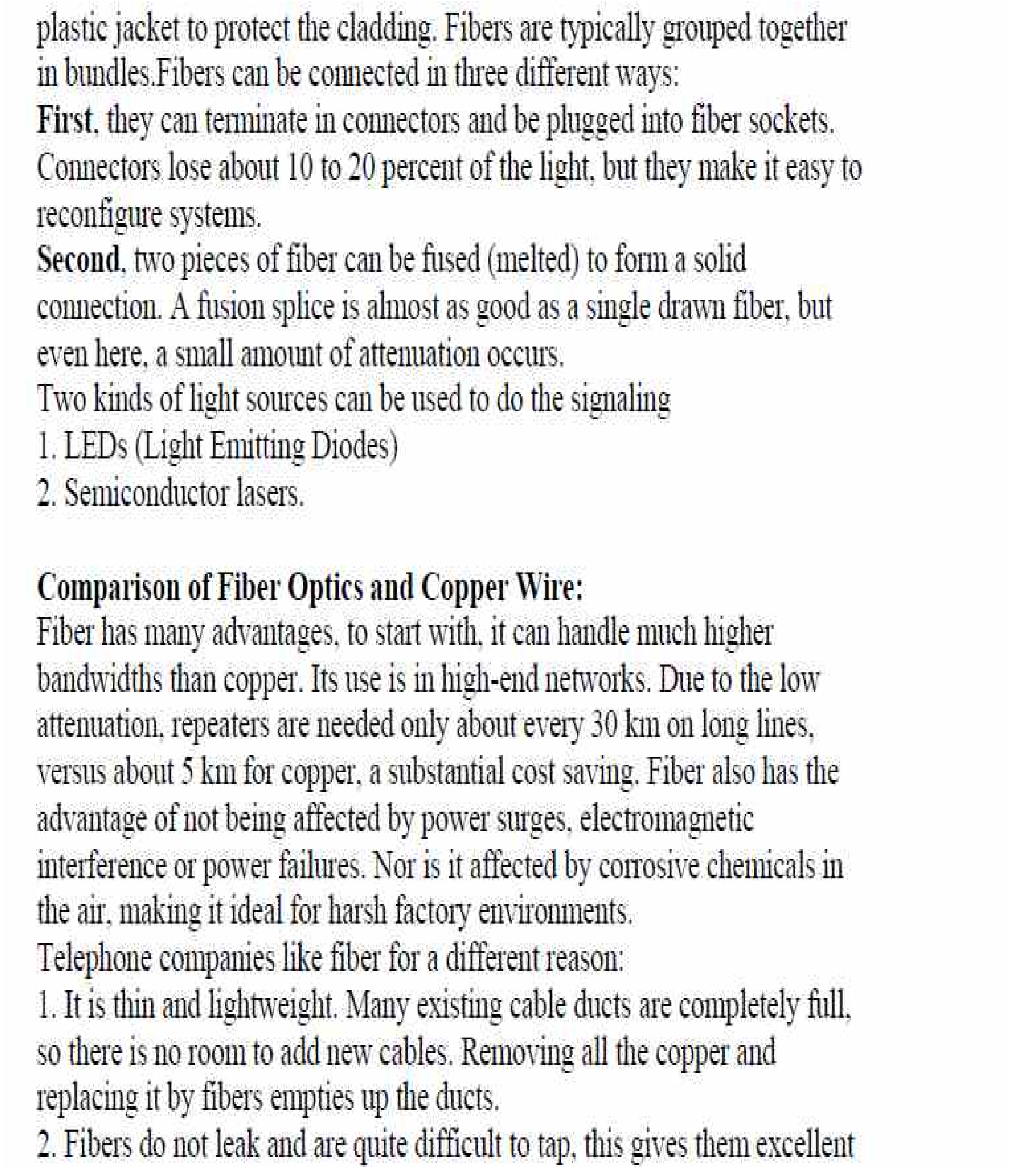
Fiber Media Cable Design



Rollover to change perspective.

Fiber Connectors

The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all light in the core. Next comes a thin



plastic jacket to protect the cladding. Fibers are typically grouped together in bundles.Fibers can be connected in three different ways:

First, they can terminate in connectors and be plugged into fiber sockets. Connectors lose about 10 to 20 percent of the light, but they make it easy to reconfigure systems.

Second, two pieces of fiber can be fused (melted) to form a solid connection. A fusion splice is almost as good as a single drawn fiber, but even here, a small amount of attenuation occurs.

Two kinds of light sources can be used to do the signaling

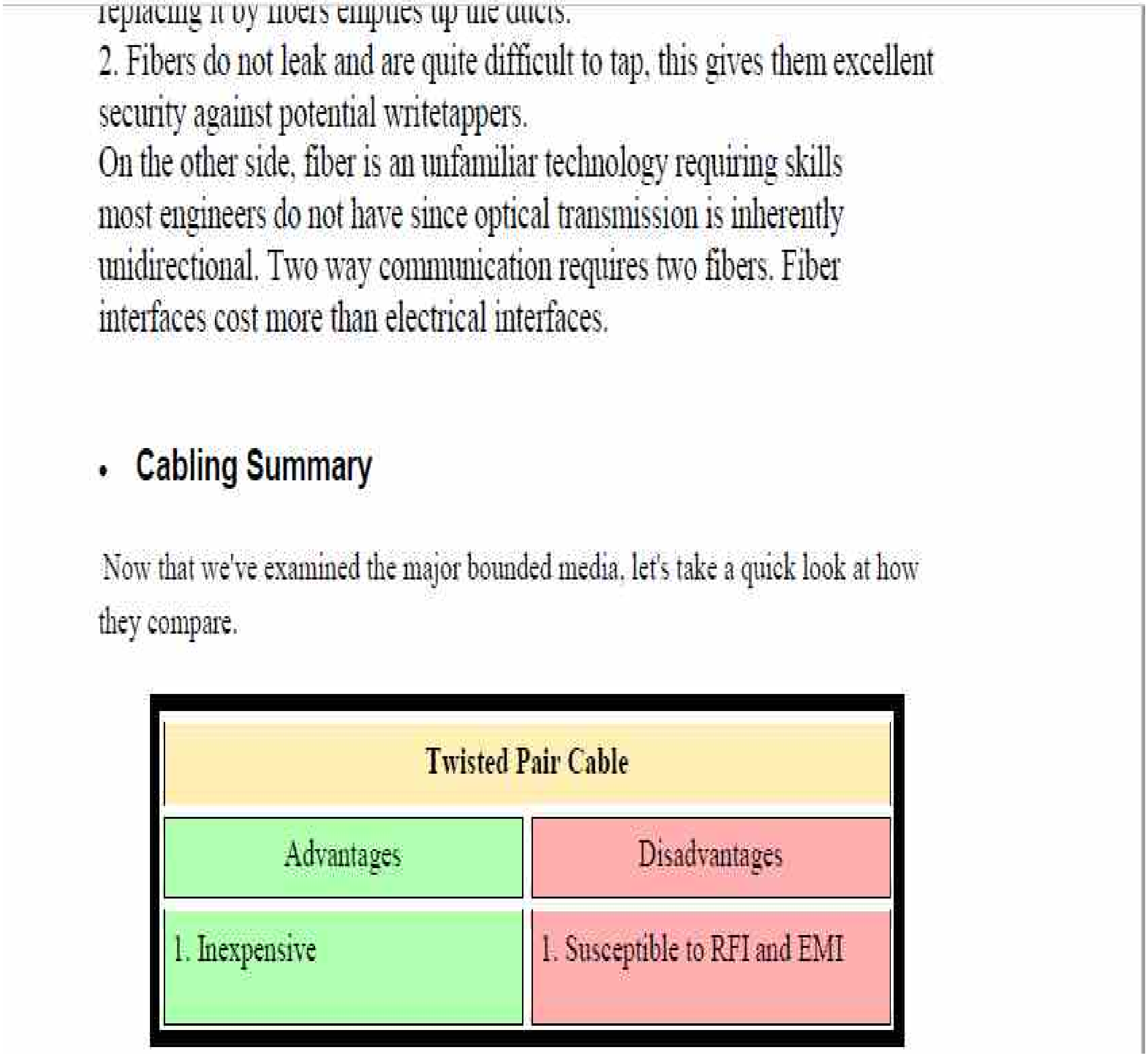
1. LEDs (Light Emitting Diodes)
2. Semiconductor lasers.

Comparison of Fiber Optics and Copper Wire:

Fiber has many advantages, to start with, it can handle much higher bandwidths than copper. Its use is in high-end networks. Due to the low attenuation, repeaters are needed only about every 30 km on long lines, versus about 5 km for copper, a substantial cost saving. Fiber also has the advantage of not being affected by power surges, electromagnetic interference or power failures. Nor is it affected by corrosive chemicals in the air, making it ideal for harsh factory environments.

Telephone companies like fiber for a different reason:

1. It is thin and lightweight. Many existing cable ducts are completely full, so there is no room to add new cables. Removing all the copper and replacing it by fibers empties up the ducts.
2. Fibers do not leak and are quite difficult to tap, this gives them excellent

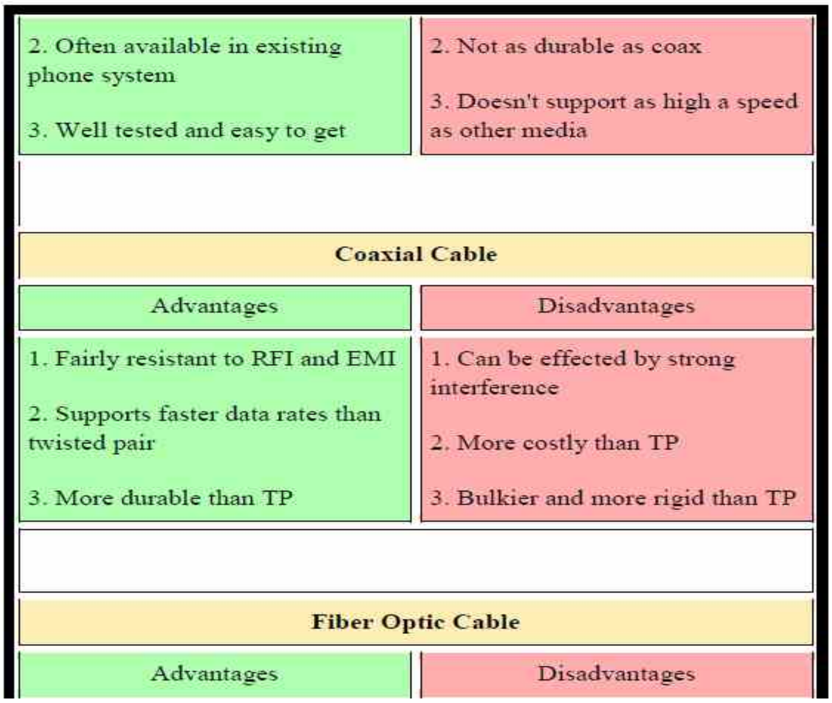


replacing it by fibers empties up the ducts.
2. Fibers do not leak and are quite difficult to tap, this gives them excellent security against potential writetappers.
On the other side, fiber is an unfamiliar technology requiring skills most engineers do not have since optical transmission is inherently unidirectional. Two way communication requires two fibers. Fiber interfaces cost more than electrical interfaces.

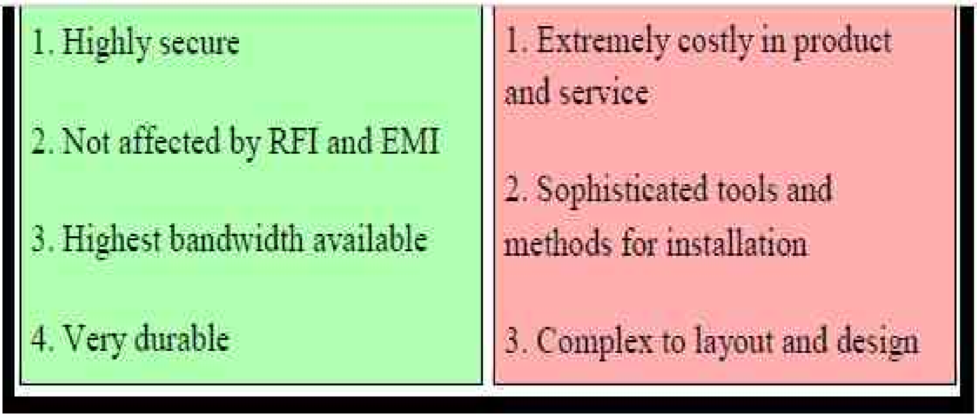
- **Cabling Summary**

Now that we've examined the major bounded media, let's take a quick look at how they compare.

Twisted Pair Cable	
Advantages	Disadvantages
1. Inexpensive	1. Susceptible to RFI and EMI



2. Often available in existing phone system 3. Well tested and easy to get	2. Not as durable as coax 3. Doesn't support as high a speed as other media
Coaxial Cable	
Advantages	Disadvantages
1. Fairly resistant to RFI and EMI 2. Supports faster data rates than twisted pair 3. More durable than TP	1. Can be effected by strong interference 2. More costly than TP 3. Bulkier and more rigid than TP
Fiber Optic Cable	
Advantages	Disadvantages

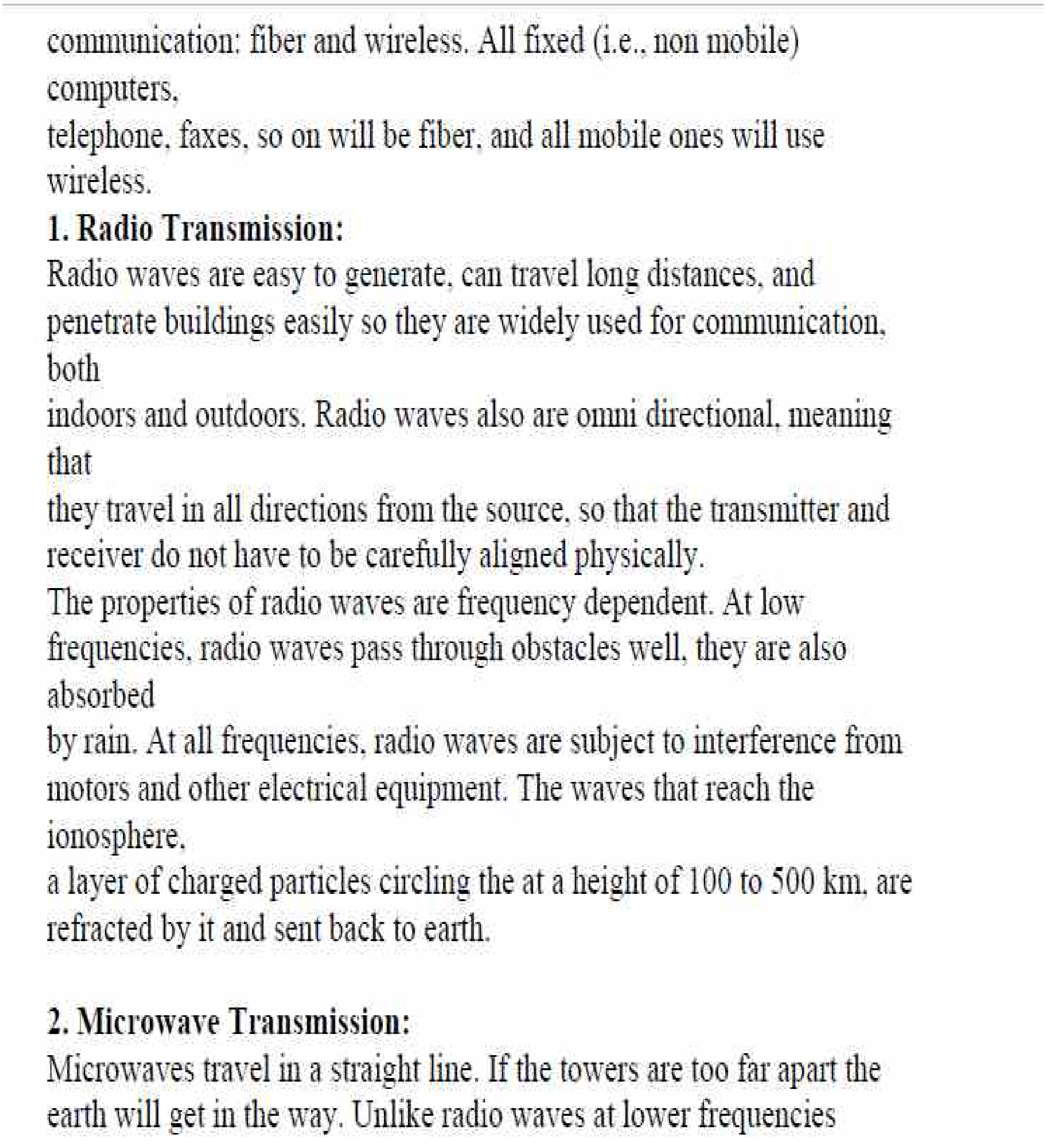


1. Highly secure 2. Not affected by RFI and EMI 3. Highest bandwidth available 4. Very durable	1. Extremely costly in product and service 2. Sophisticated tools and methods for installation 3. Complex to layout and design

3.2 Wireless Transmission:

People who need to be on-line all the time need mobile service, and for these mobile users twisted pair, coaxial, and fiber optic are of no use. They
need to get to their data from their laptops and notebooks without being tethered to the terrestrial communication infrastructure. For these users wireless communication is the answer.

Some people even believe that the future holds only two kinds of



communication: fiber and wireless. All fixed (i.e., non mobile) computers, telephone, faxes, so on will be fiber, and all mobile ones will use wireless.

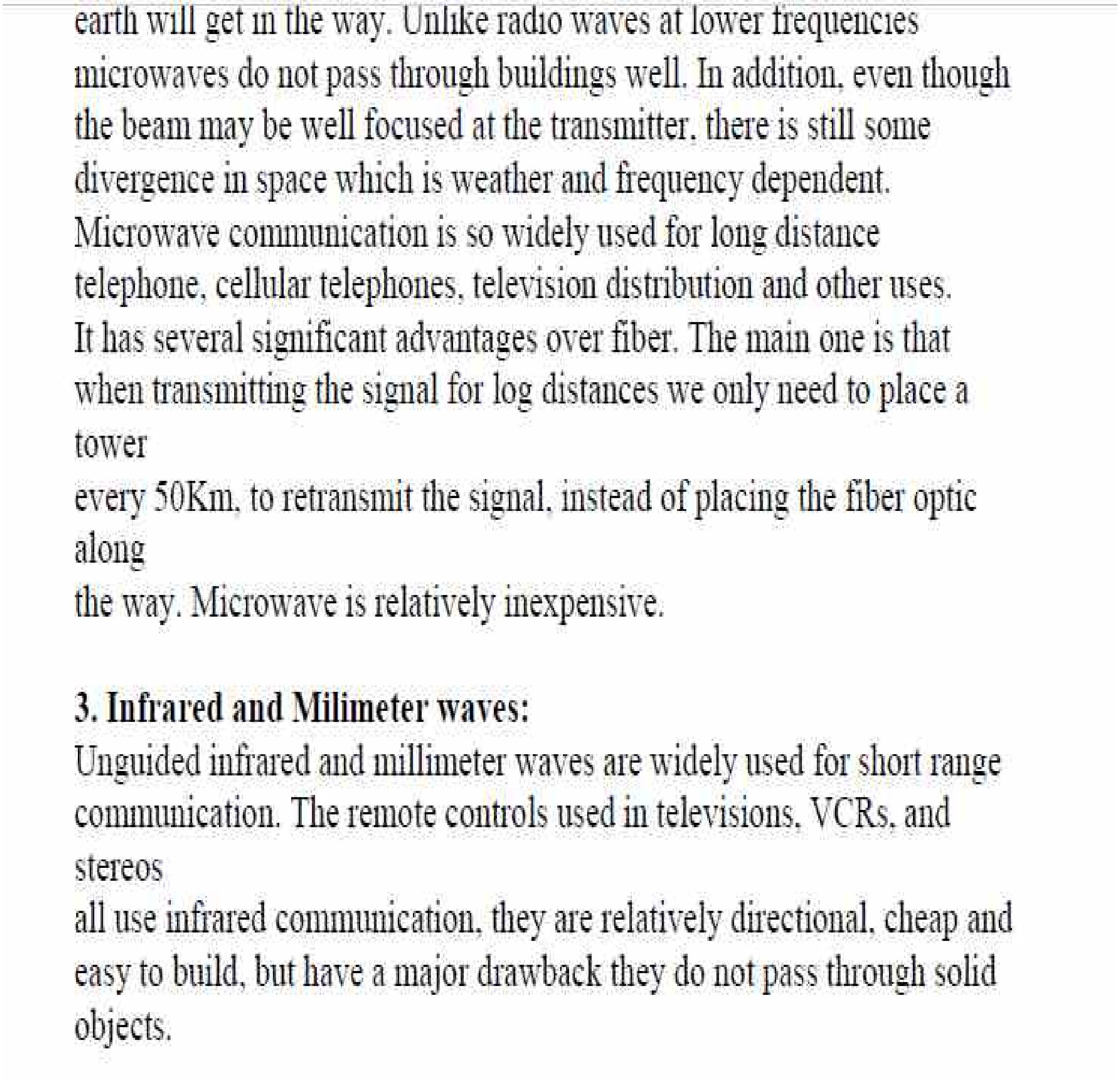
1. Radio Transmission:

Radio waves are easy to generate, can travel long distances, and penetrate buildings easily so they are widely used for communication, both indoors and outdoors. Radio waves also are omni directional, meaning that they travel in all directions from the source, so that the transmitter and receiver do not have to be carefully aligned physically.

The properties of radio waves are frequency dependent. At low frequencies, radio waves pass through obstacles well, they are also absorbed by rain. At all frequencies, radio waves are subject to interference from motors and other electrical equipment. The waves that reach the ionosphere, a layer of charged particles circling the at a height of 100 to 500 km, are refracted by it and sent back to earth.

2. Microwave Transmission:

Microwaves travel in a straight line. If the towers are too far apart the earth will get in the way. Unlike radio waves at lower frequencies

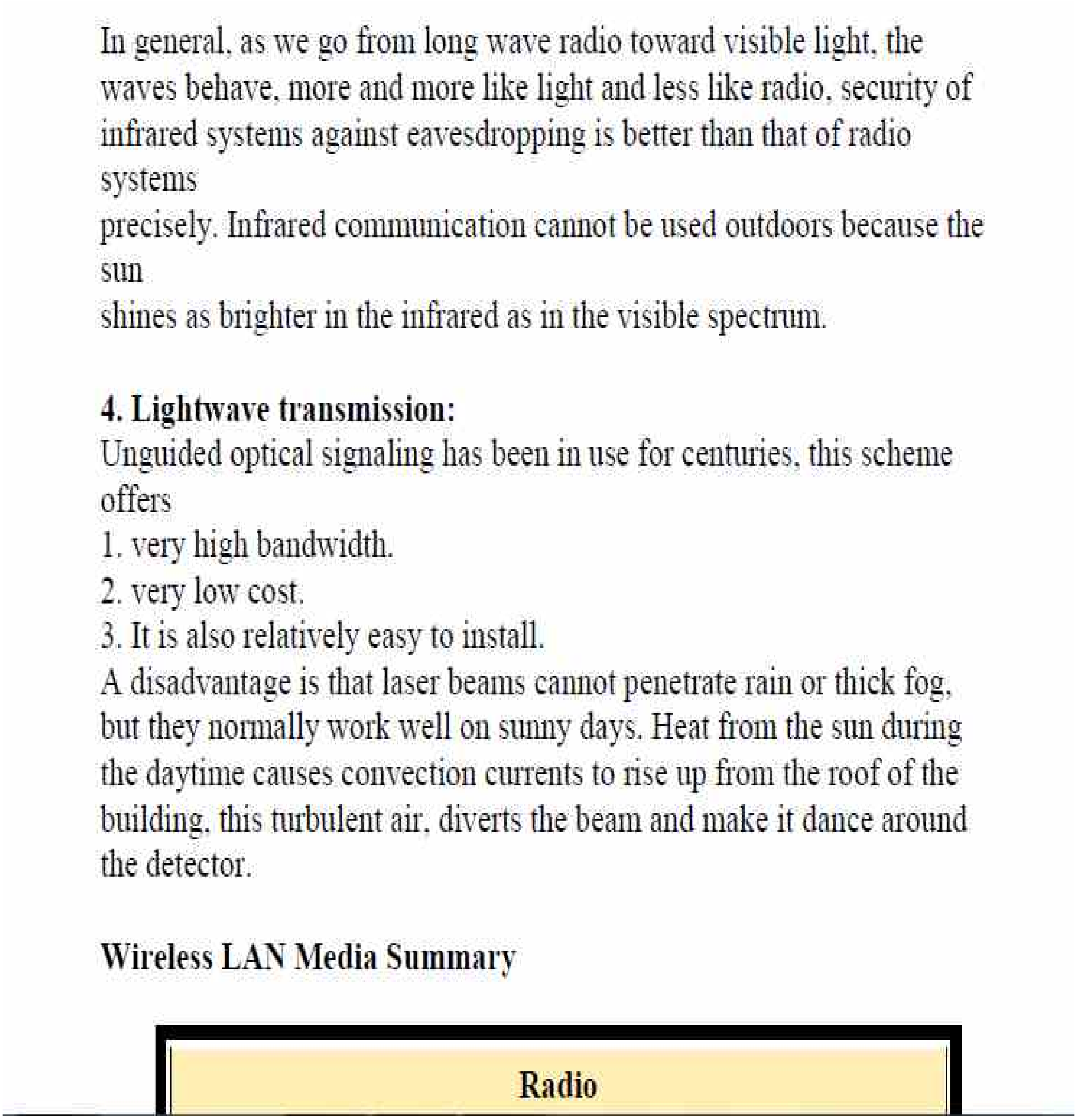


earth will get in the way. Unlike radio waves at lower frequencies microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space which is weather and frequency dependent.

Microwave communication is so widely used for long distance telephone, cellular telephones, television distribution and other uses. It has several significant advantages over fiber. The main one is that when transmitting the signal for log distances we only need to place a tower every 50Km, to retransmit the signal, instead of placing the fiber optic along the way. Microwave is relatively inexpensive.

3. Infrared and Milimeter waves:

Unguided infrared and millimeter waves are widely used for short range communication. The remote controls used in televisions, VCRs, 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 objects.



In general, as we go from long wave radio toward visible light, the waves behave, more and more like light and less like radio. security of infrared systems against eavesdropping is better than that of radio systems
precisely. Infrared communication cannot be used outdoors because the sun
shines as brighter in the infrared as in the visible spectrum.

4. Lightwave transmission:

Unguided optical signaling has been in use for centuries, this scheme offers

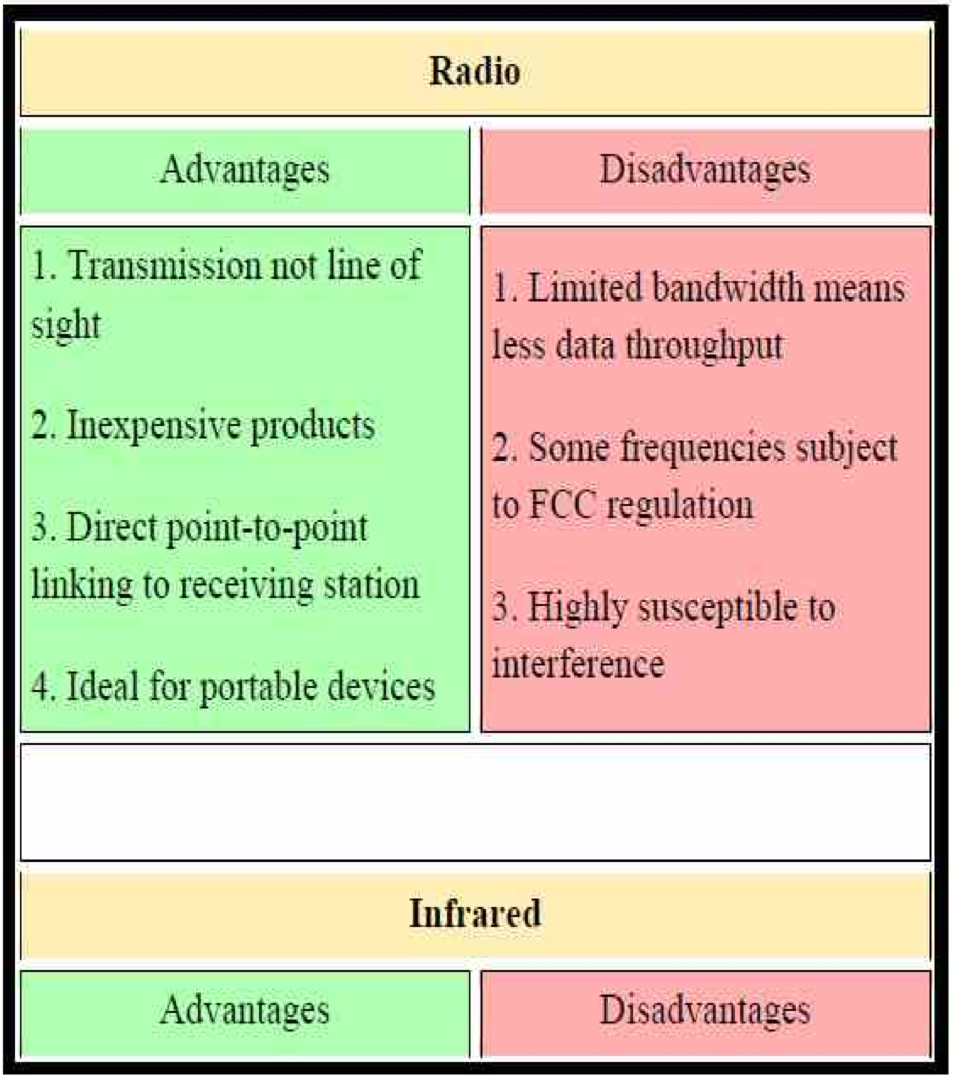
1. very high bandwidth.
2. very low cost.
3. It is also relatively easy to install.

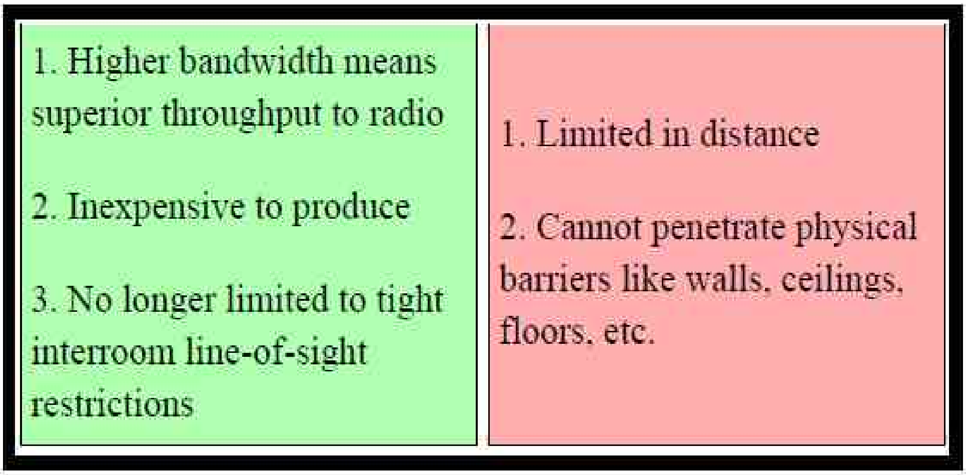
A disadvantage is that laser beams cannot penetrate rain or thick fog, but they normally work well on sunny days. Heat from the sun during the daytime causes convection currents to rise up from the roof of the building, this turbulent air, diverts the beam and make it dance around the detector.

Wireless LAN Media Summary

Radio

Wireless LAN Media Summary





Radio	
Advantages	Disadvantages
1. Transmission not line of sight 2. Inexpensive products 3. Direct point-to-point linking to receiving station 4. Ideal for portable devices	1. Limited bandwidth means less data throughput 2. Some frequencies subject to FCC regulation 3. Highly susceptible to interference
Infrared	
Advantages	Disadvantages
1. Higher bandwidth means superior throughput to radio 2. Inexpensive to produce 3. No longer limited to tight interroom line-of-sight restrictions	1. Limited in distance 2. Cannot penetrate physical barriers like walls, ceilings, floors, etc.

Chapter Four
Reference Model

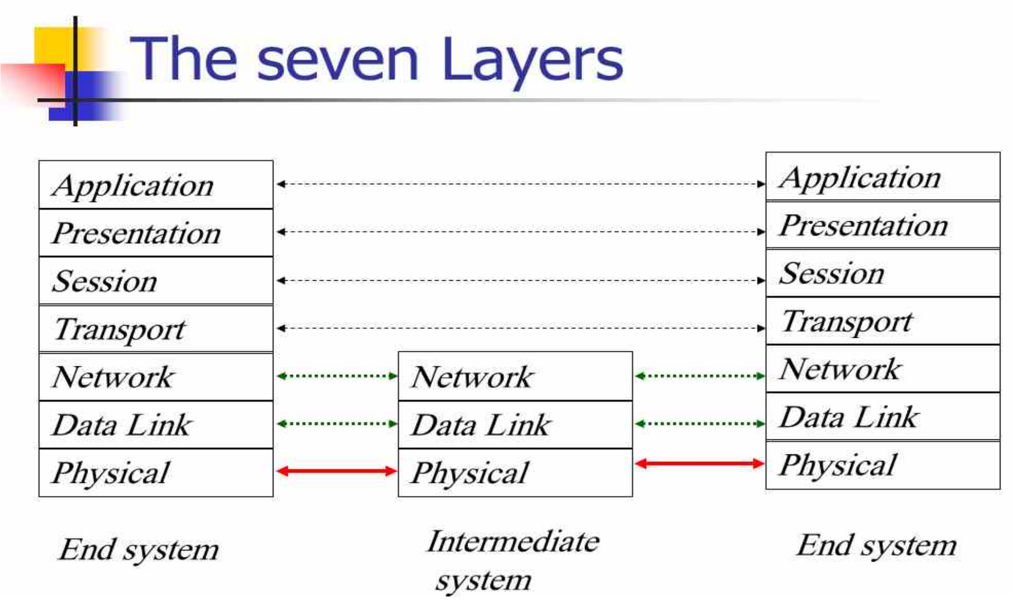
We have discussed layered networks; it is time to look at some examples. In the next two sections we will discuss two important network architectures, the OSI reference model and the TCP/IP reference model.

1. The OSI Reference model

The OSI model is shown in the coming Figure This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers.

The model is called the ISO OSI (Open system Interconnection Reference Model because it deals with connecting open systems - that is, systems : open for communication with other systems. we will usually just call it the OSI model for short. The OSI model has seven layers. The principles that were applied to arrive at the seven layers are as follows:

1. Each layer should perform a well defined function.
2. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
3. The layer boundaries should be chosen to minimize the information flow across the interfaces.
4. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.



The seven Layers

The Physical Layer:

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are how many volts should be used to represent a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how many pins the network connector has and what each pin is used for. The design issues here largely deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium,which lies below the physical layer.

The Data Link Layer:

The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer. The sender break the input data up into data frames (typically a few hundred or a few thousand bytes), transmit the frames equentially, and process the acknowledgement frames sent back by the receiver.

It is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. A noise burst on the line can destroy a frame completely. **In** this case, the data link layer software on the source machine can retransmit the frame. Multiple transmissions of the same frame introduce the possibility of duplicate frames. A duplicate frame could be sent if the acknowledgement frame from the receiver back to the sender were lost.

The data link layer may coffer several different service classes to the network layer, each of a different quality and with a different price. Another issue that arises in the data link layer is how to keep a fast transmitter from drowning a slow receiver in data. If the line can be used to transmit data in both directions, this introduces a new complication that the data link layer software must deal with. The problem is that the acknowledgement frames for A to B traffic compete for the use of the line with data frames for the B to A traffic.

The Network Layer

The network layer is concerned with controlling the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on:

1. Static tables that are "wired into" the network and rarely.
2. They can also be determined at the start of each conversation.

3. Finally, they can be highly dynamic.

If too many packets are present in the subnet at the same time, they will get in each other's way forming bottlenecks. The control of such congestion also belongs to the network layer.

When a packet has to travel from one network to another to get to its destination many problems can arise:

1. The addressing used by the second network may be different from the first one.
2. The second one may not accept the packet at all because it is too large.
3. The protocols may differ, and so on. It is up to the network laver to overcome all these problems to allow heterogeneous networks to-be interconnected.

The Transport Layer

The basic function of the transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. The transport layer creates a distinct network connection for each transport connection required by the session layer. If the transport connection requires a high throughput, however, the transport layer might create multiple network connections, dividing the data among the network connections to improve throughput. Creating or maintaining a network connection is expensive. The transport layer also determines what type of service to provide the session layer, and ultimately, the users of the network.

The most popular type of transport connection is an error-free pointto- point channel that delivers messages or bytes in the order in which they were sent.

The Session Layer

The session layer allows users on different machines to establish sessions between them. A session allows ordinary data transport, as does the transport layer, but it also provides enhanced services-useful in some applications. A session might be used to allow a user to log into a remote timesharing system or to transfer a file between two machines. One of the services of the session layer is to manage dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time.

The Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information transmitted. Most user programs do not exchange random binary bit strings. They exchange things such as people's names, dates, amounts of money, and Invoices. These items are represented as character strings, integers, floating-point numbers, and data structures composed of several simpler items. Different computers have different codes for representing character strings (e.g., ASCII and Unicode), integers (e.g., one's complement and two's complement), and so on. In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way along; with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and converts from the representation used inside the computer to the network standard representation and back.

The Application Layer

The application layer contains a variety of protocols that are commonly needed. For example, there are hundreds of incompatible terminal types in the world. each with different screen layouts, escape sequences for inserting and deleting text, moving the cursor, etc.

One way to solve this problem is to define an abstract network virtual terminal that editors and other programs can be written to deal with. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example, when the editor moves the virtual terminal's cursor to the upper left-hand comer of the screen, this software must issue the proper command sequence to the real terminal to get its cursor there too. All the virtual, terminal software is in the application layer. Another application layer function is file transfer. Different file systems have different file naming conventions, different ways of representing text lines, and so on.

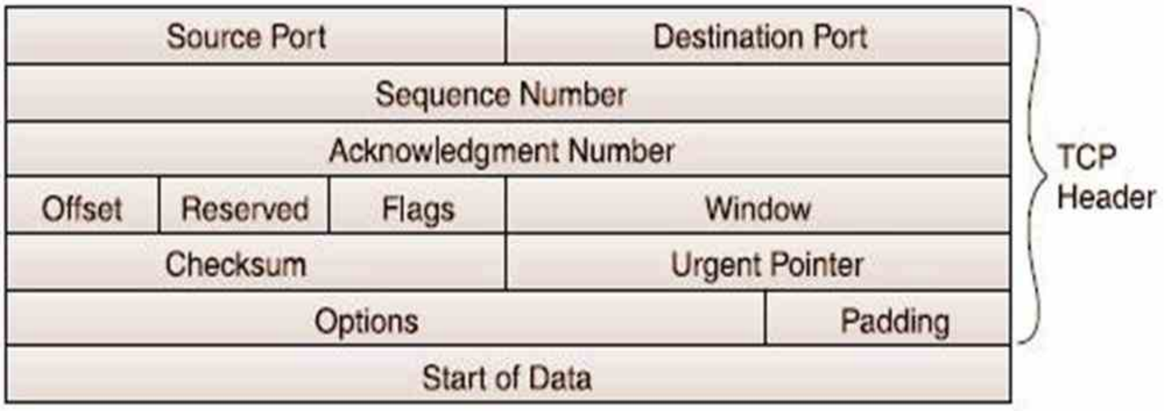
Data Transmission in the OSI Model

The figure shows an example of how data can be transmitted using the OSI model. The sending process has some data it wants to send to the receiving process it gives the data to the application layer, which then attaches the application header to the front of it and gives the resulting item to the presentation layer.

The presentation layer may transform this item in various ways and possibly add a header to the front, giving the result to the Session layer. This process is repeated until the data reach the physical layer.

The TCP/IP Reference Model

Let us now turn from the OSI model to the reference model used in the grandparent of all computer networks, the ARPANET, and its successor, the worldwide Internet. This architecture later became known as the ***TCP/IP*** Reference Model.



Source Port | Destination Port

Sequence Number

Acknowledgment Number

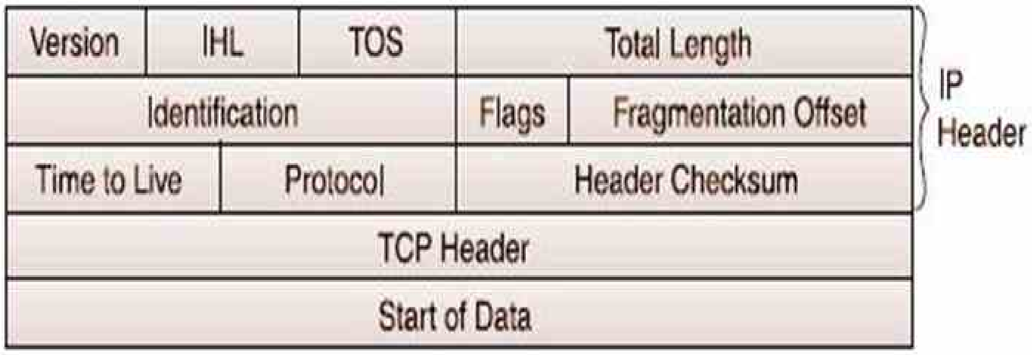
Offset | Reserved | Flags | Window

Checksum | Urgent Pointer

Options | Padding

Start of Data

TCP Header



Version | IHL | TOS | Total Length

Identification | Flags | Fragmentation Offset

Time to Live | Protocol | Header Checksum

TCP Header

Start of Data

IP Header

The Application Layer:

The TCP/IP model does not have session or presentation layers. No need for them was perceived, so they were not included. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones include virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). The virtual terminal protocol allows a user on one machine to log into a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another.

The Transport Layer:

The layer above the internet layer in the TCP/IP model is called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, the same as in the OSI transport layer. Two end-to-end protocols have been defined here. The first one, **TCP (Transmission Control Protocol)** is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. The second protocol in this layer, **UDP (User Datagram Protocol),** is an unreliable, connectionless protocol. It is also widely used for one-shot .client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery.

The Internet Layer:

This layer, called the internet layer, its job is to permit hosts to inject packets into any network and have them travel independently to the destination, (potentially on a different network). They may even arrive in a different order than they were sent. A person can drop a sequence of international Letters into a mail box in one country and most of them will be delivered to the correct address in the destination country. The internet layer defines an official packet format and protocol called **IP** (Internet Protocol). The job of the internet layer is to deliver **IP** packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the *TCP/IP* internet layer is very similar in functionality to the OSI network layer.

The Host-To-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send **IP** packets over it. This protocol is not defined and varies from host to host and network to network.

A Comparison of the OSI and TCP Reference Models:

The OSI and TCP/IP reference models have much similarity which are:

1. Both are based on the concept of a stack of independent protocols.

2. Also the Functionality of the layers is roughly similar. For example, in both models the layers up through and Including the Transport layer are there to provide an end-to-end network-independent transport service to processes wishing to communicate.

And the Differences are:

1. Three concepts are central to the OSI model:

A. Services.

B. Interfaces.

C. Protocols .

OSI model make the distinction between these three concepts explicit. Each layer performs some services for the layer above it. The TCP/IP model did not originally clearly distinguished between services, interfaces, and protocols.

2. As a consequence, the protocols in me OSI model are better hidden than TCP/IP model.

3. OSI reference model was devised before the protocols were invented. This ordering means that the model was not biased toward one. With the TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model. They fit perfectly.

4. Another difference is in the area of connectionless versus connection oriented communication. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer. The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer.

5. TCP/IP has four layers where OSI have seven layers.

The Network Layer

The Network layer, or OSI Layer 3, provides services to exchange the individual pieces of data over the network between identified end devices. To accomplish this end-to-end transport, Layer 3 uses four basic processes:
1. Addressing: First, the Network layer must provide a mechanism for addressing the end devices. In an IPv4 network, when this address is added to a device, the device is then referred to as a host.
2. Encapsulation : addition of source address and destination addresses.
3. Routing : Intermediary devices that connect the networks are called routers. The role of the router is to select paths for and direct packets toward their destination. This process is known as routing.
4. Decapsulation: The removal of source address and destination addresses.

Network Layer Protocols
1. Internet Protocol version 4 (IPv4).
2. Internet Protocol version 6 (IPv6).
3. Novell Internetwork Packet Exchange (IPX).
4. AppleTalk.

5. Connectionless Network Service (CLNS/DECNet).

The Network layer services implemented by the TCP/IP protocol suite are the Internet Protocol (IP) Version 4 of IP (IPv4) is currently the most widely-used version of IP. It is the only Layer 3 protocol that is used to carry user data over the Internet. IP version 6 (IPv6) is developed and being implemented in some areas. IPv6 will operate alongside IPv4 and may replace it in the future.

The services provided by IP, as well as the packet header structure and contents, are specified by either IPv4 protocol or IPv6 protocol. The Internet Protocol was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks. The protocol was not designed to track and manage the flow of packets. Layer 3 uses connectionless communication that is sending a letter to someone without notifying the recipient in advance. Connectionless data communications works on the same principle. IP packets are sent without notifying the end host that they are coming.

Connection-oriented protocols, such as TCP, require that control data be exchanged to establish the connection as well as additional fields in the PDU header. Because IP is connectionless, it requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded, nor does it require additional fields in the PDU header to maintain this connection. This process greatly reduces the overhead of IP.

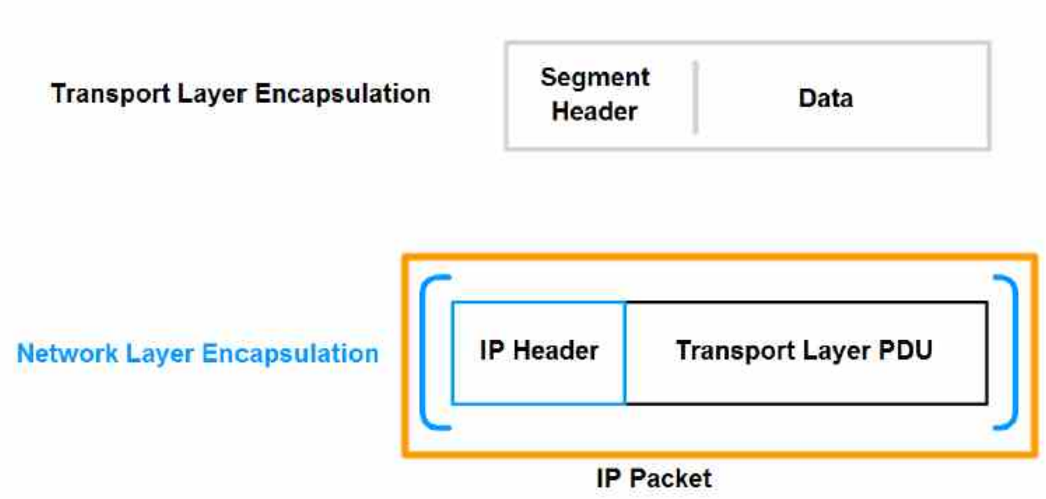
Connectionless packet delivery may, however, result in packets arriving at the destination out of sequence. If out-of-order or missing packets create problems for the application using the data, then upper layer services will have to resolve these issues.

The IP protocol does not burden the IP service with providing reliability. Compared to a reliable protocol, the IP header is smaller. Transporting these smaller headers requires less overhead. Less overhead means less delay in delivery. This characteristic is desirable for a Layer 3 protocol. The mission of Layer 3 is to transport the packets between the hosts while placing as little burden on the network as possible. IP is often referred to as an unreliable protocol. Unreliable means simply that IP does not have the capability to manage, and recover from, undelivered or corrupt packets. The header of an IP packet does not include fields required for reliable data delivery. There are no acknowledgments of packet delivery. There is no error control for data. Nor is there any form of packet tracking; therefore, the is no possibility for packet retransmissions.

The Network layer is also not burdened with the characteristics of the media on which packets will be transported. IPv4 and IPv6 operate independently of the media that carry the data at lower layers of the protocol stack. Part of the control communication between the Data Link layer and the Network layer is the establishment of a maximum size for the packet. This characteristic is referred to as the Maximum Transmission Unit (MTU). The Data Link layer passes the MTU upward to the Network layer. The Network layer then determines how large to create the packets. In some cases, an intermediary device - usually a router - will need to split up a packet when forwarding it from one media to a media with a smaller MTU. This process is called fragmenting the packet or fragmentation.

The process of encapsulating data by layer enables the services at the different layers to develop and scale without affecting other layers. This means that transport layer segments can be readily packaged by existing Network layer protocols, such as IPv4 and IPv6 or by any new protocol that might be developed in the future. Routers can implement these different Network layer protocols to operate concurrently over a network to and from the same or different hosts. The routing performed by these intermediary devices only Considers the contents of the packet header that encapsulates the segment. In all cases, the data portion of the packet - that is, the encapsulated Transport layer PDU - remains unchanged during the Network layer processes.

Generating IP Packets



In TCP/IP based networks, the Network layer PDU is the IP packet.