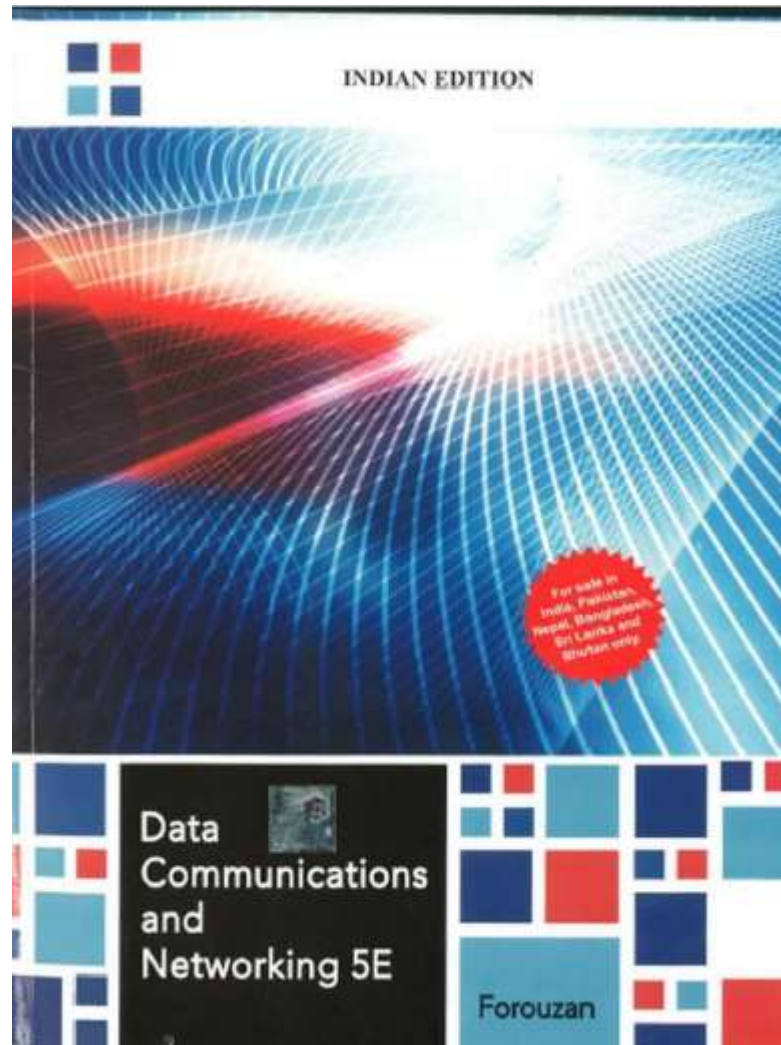


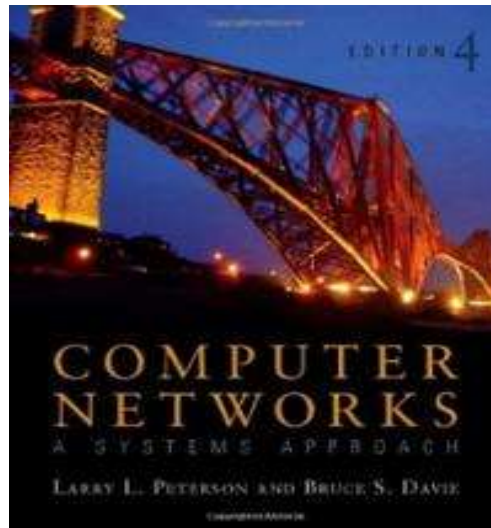
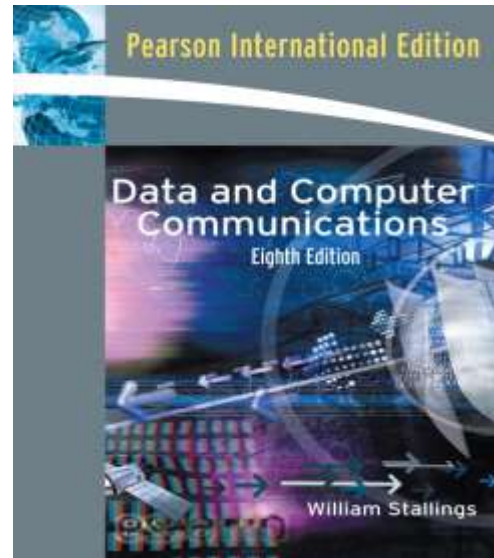
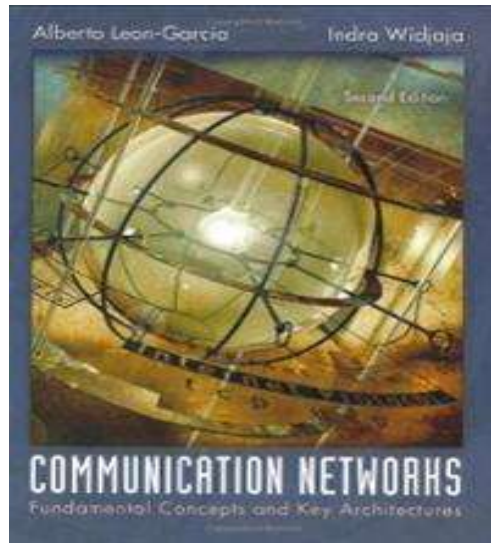
COMPUTER NETWORKS



TEXT BOOK



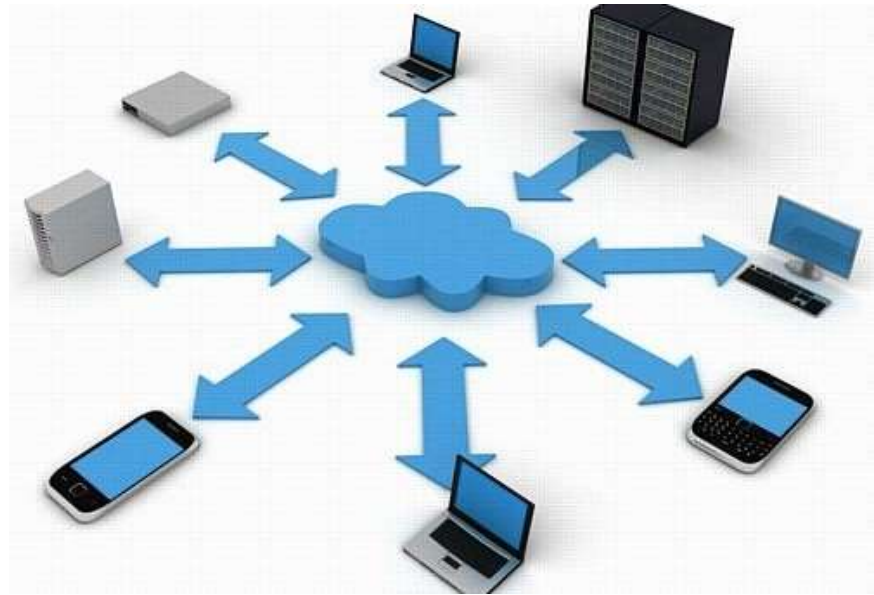
REFERENCE BOOKS



Chapter 1

Introduction

- *Data Communication*
- *Networks*
- *Network Types*
- *Internet History*
- *Standards and Administrations*

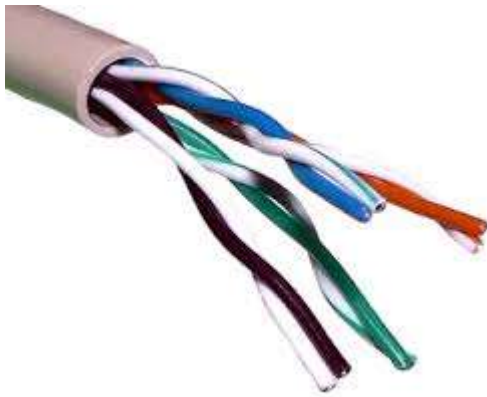


Data Communications

✚ Data communications and networking are changing today's world. Why wait for a week for some report from US to arrive by post where you can receive **instantaneously** through computer networks?

✚ Here we have to know how networks operate and what type of technologies are available.

■ *Data communications are the exchange of data between two devices via some form of **transmission medium** such as a wire cable.*



Characteristics

✚ *The four fundamental characteristics of data communications are:-*

■ **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and *only* by that device or user.



■ **Accuracy:** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

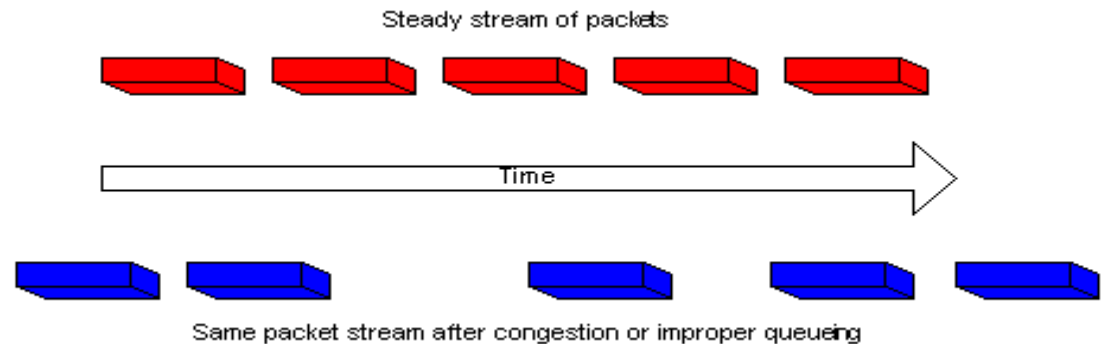


Characteristics

■ **Timeliness**: The system must deliver data in a **timely manner**. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay.



■ **Jitter**: Jitter refers to the **variation** in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.



Q.) What is data communication? What are its four important characteristics?

Q.) What is data communications? What are its characteristics?
Explain

**Dec 2010, 2011, 2013, 2014, 2015, 2016 June 2012, 2013, 2015 →
(06 Marks)**

Components

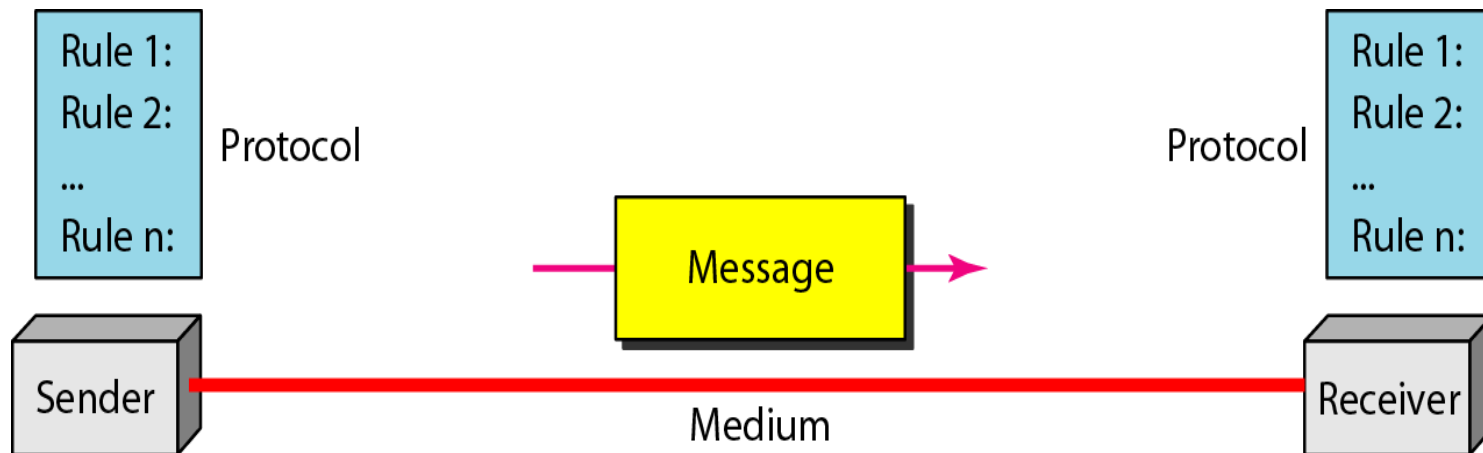


Figure: *Five components of data communication*



The five components of data communications are:

- **Message:** The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- **Sender:** The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, mobile, and so on.
- **Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- **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, fibre-optic cable, and radio waves.

■ **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.

Q.) What is data communication? What are its characteristics and components? Explain

(08 Marks)

■ **Information today comes in different forms such as :**

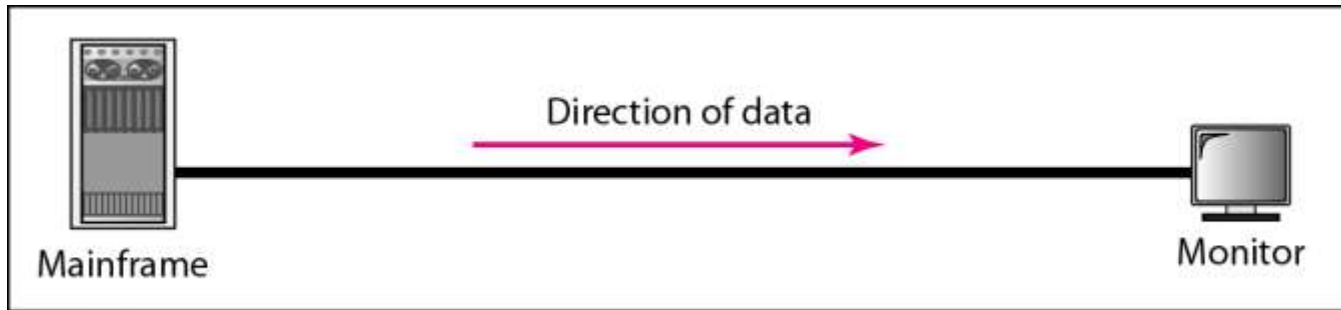
▶ Text

▶ Numbers

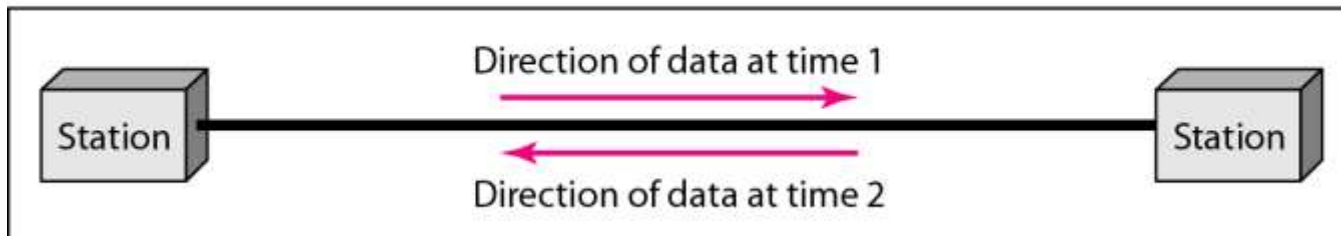
▶ Images

▶ Audio

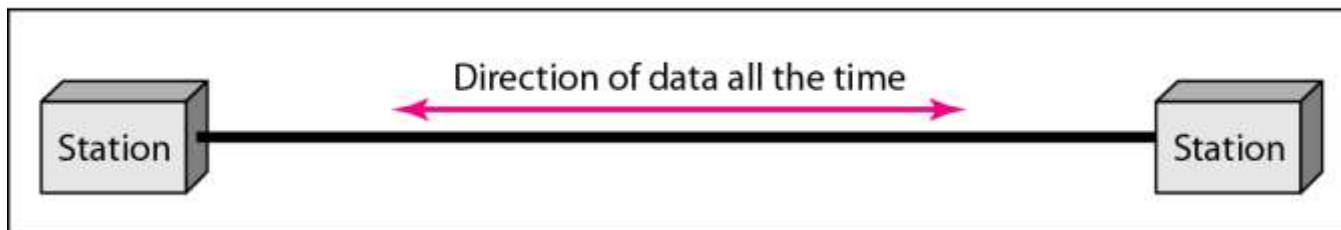
▶ Video



a. Simplex



b. Half-duplex



c. Full-duplex

Figure: *Data flow (simplex, half-duplex, and full-duplex)*

✚ Communication between two devices can be **simplex**, **half-duplex**, or **full-duplex** as shown in figure above.

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.

■ Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

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.

■ In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.

Example: Walkie-Talkie

Full-Duplex

■ In full-duplex mode (also called duplex), both stations can transmit and receive **simultaneously**.

■ In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction.

Example: Telephone

- “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 receiving data generated by other nodes on the network.
- When we connect two computers at home using a plug-and-play router, we have created a network, although very small.

Topics discussed in this section:

- Network Criteria
- Physical Structures
- Physical Topology

■ **Network Criteria** : A network must be able to meet a certain number of criteria. The most important of these are:

▶ **Performance**

▶ **Reliability**

▶ **Security**

Performance

■ Performance can be measured in many ways, including **transit time** and **response time**.

● **Transit time** is the amount of time required for a message to travel from one device to another.

● **Response time** is the elapsed time between an inquiry and a response.

■ The performance of a network depends on a number of factors, including the **number of users**, **the type of transmission medium**, **the capabilities of the connected hardware**, and **the efficiency of the software**.

■ Performance is often evaluated by two networking metrics: **throughput** and **delay**.

We often need **more throughput** and **less delay**.

➡ However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

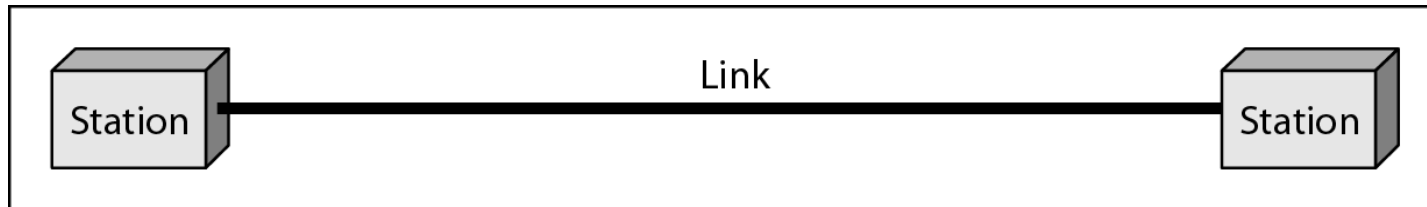
Reliability

- Network reliability is measured by the frequency of failure, that is the time it takes a link to **recover** from a failure.

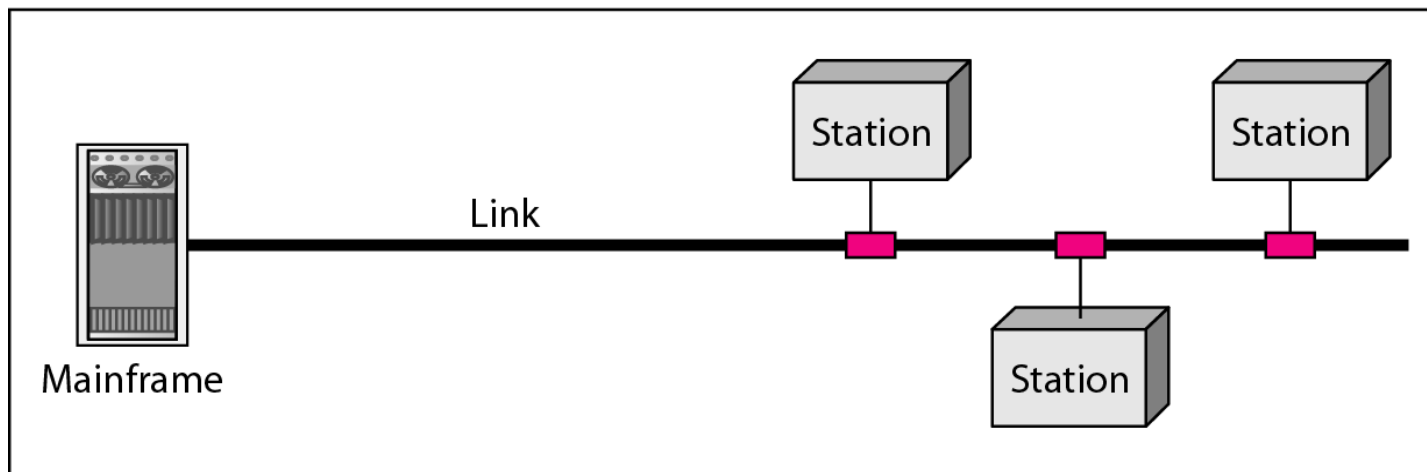
Security

- Network security deals with **protecting data** from unauthorized access.

■ Physical Structures



a. Point-to-point



b. Multipoint

Figure: *Types of connections: point-to-point and multipoint*

Type of Connection

➡ There are two possible types of connections: **Point-to-Point** and **Multipoint**.

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.

Multipoint

- Multipoint 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.
- It is a ***timeshared connection***.

- ❑ The term physical topology refers to the way in which a network is laid out physically.
- ❑ Two or more devices connect to a link; two or more links form a topology.

Definition

■ “The **topology** of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.”

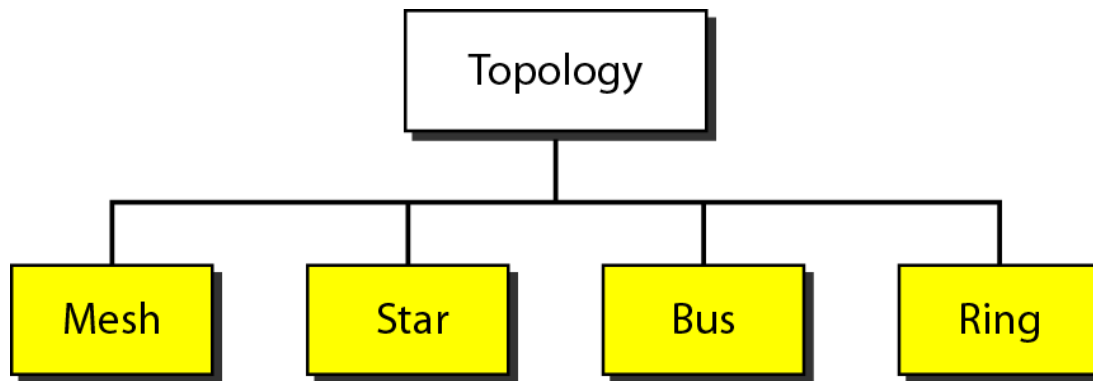


Figure : *Categories of topology*

Mesh Topology

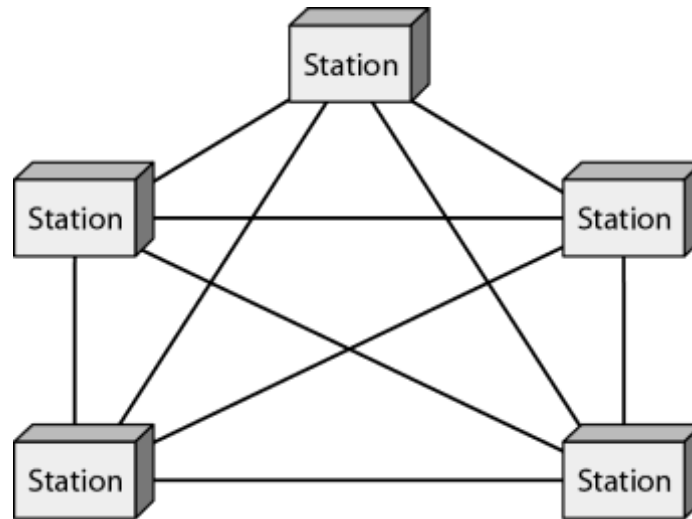


Figure : A fully connected mesh topology (five devices)

- 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 $n - 1$ 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 (duplex mode), 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.

Advantages

- The use of dedicated links guarantees that **each connection can carry its own data load**, thus eliminating the traffic problems that can occur when links must be shared by multiple 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. Physical boundaries prevent other users from gaining access to messages.
- Fault identification and fault isolation easy.

Dis-Advantages

- The main disadvantages of a mesh are related to the **amount of cabling and the number of I/O ports required.**
- Every device must be connected to every other device, **installation and reconnection are difficult.**
- The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star Topology

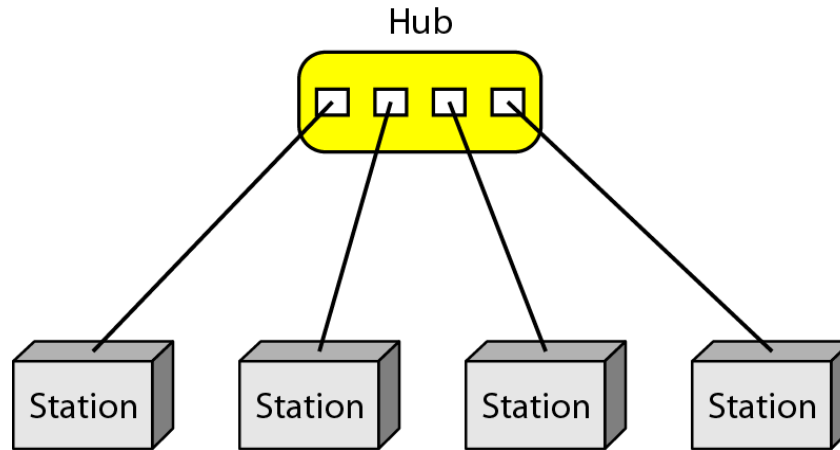


Figure : *A star topology connecting four stations*

- 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.
- 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 devices.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices.

Advantages

- A star topology is **less expensive** than a mesh topology.
- Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: **between that device and the hub.**
- If one link fails, only that link is affected. All other links remain active.
- Fault identification and fault isolation easy.

Dis-Advantages

- 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.**

Bus Topology

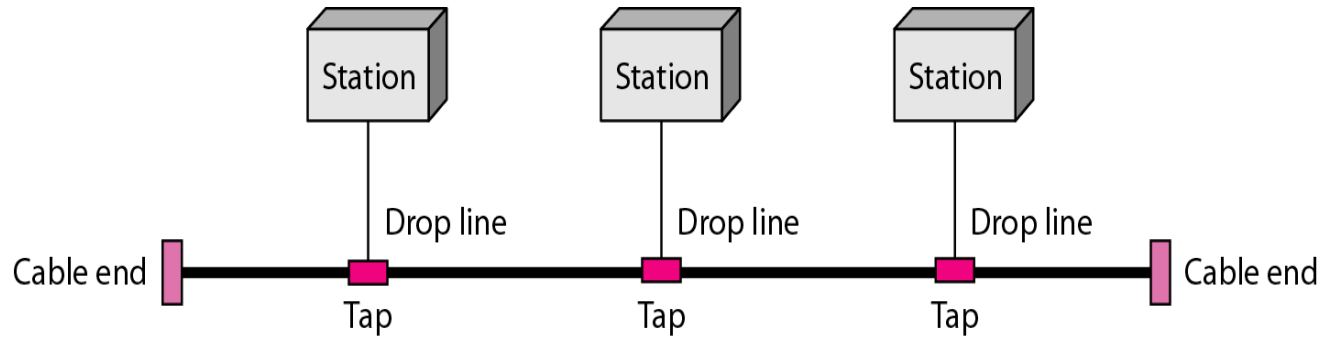


Figure : *A bus topology connecting three stations*

- The preceding topologies 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.
- Nodes are connected to the bus cable by **drop lines** and **taps**.
- A **drop line** is a connection running between the device and the main cable. A **tap** is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

Advantages

- Ease of installation. **Backbone cable can be laid along the most efficient path**, and then connected to the nodes by drop lines of various lengths.
- A bus uses less cabling than mesh or star topologies.

Dis-Advantages

- Difficult **reconnection** and fault isolation.
- Signal reflection at the taps can cause degradation in quality.
- **Adding new devices** may therefore require modification or replacement of the backbone.
- A **fault or break in the bus cable** stops all transmission.

Ring Topology

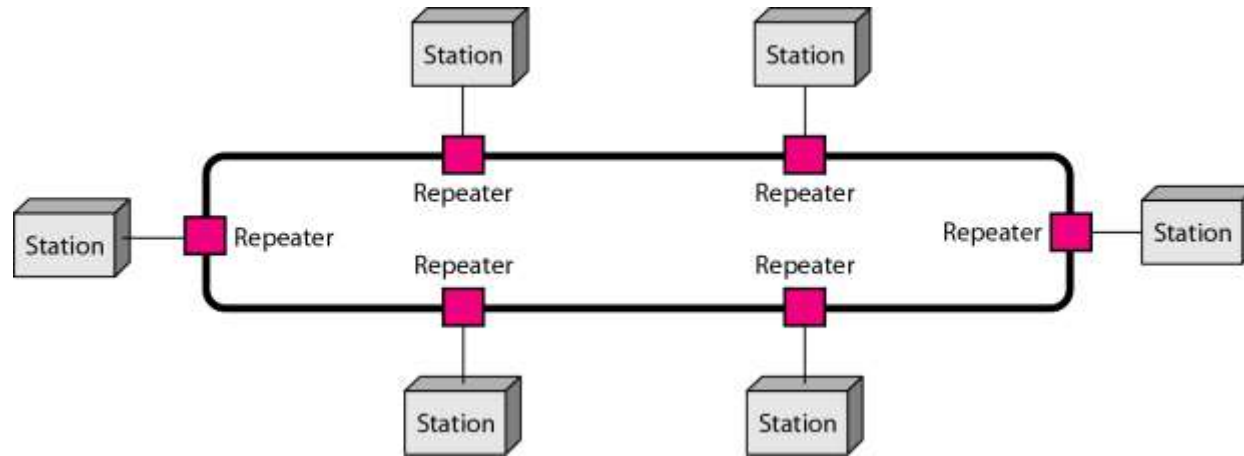


Figure : *A ring topology connecting six stations*

- 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.

Advantages

- A ring is relatively **easy to install and reconfigure**. Each device is linked to only its immediate neighbors.
- To add or delete a device **requires changing only two connections**.
- Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Dis-Advantages

- **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**. This weakness can be solved by using a dual ring.

Hybrid Topology

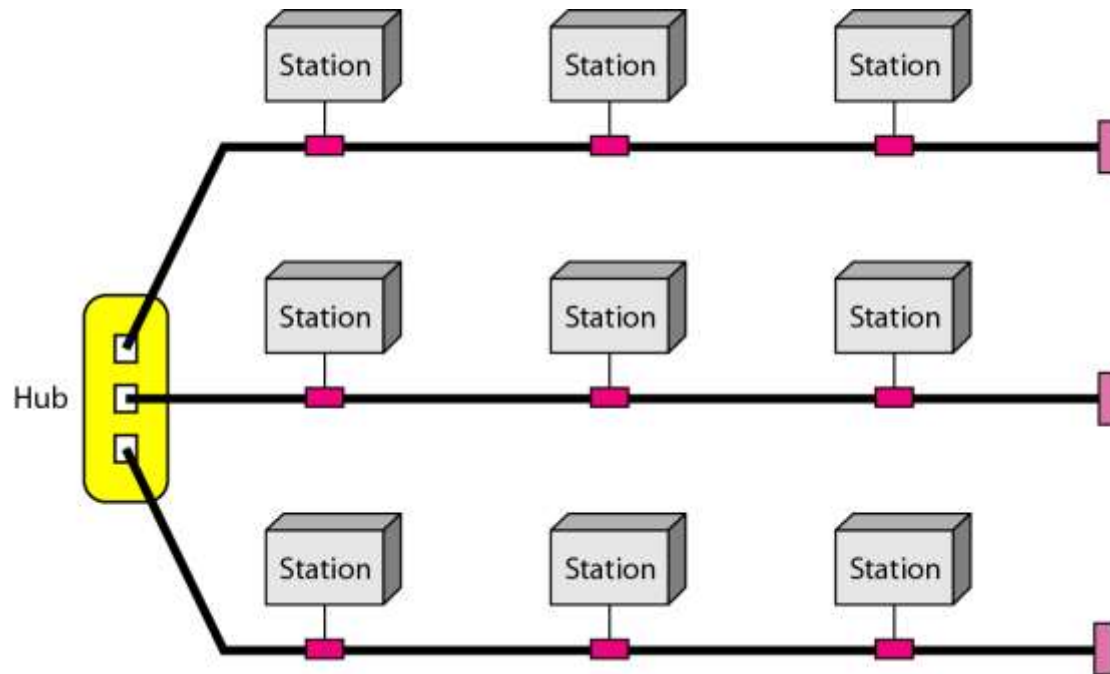
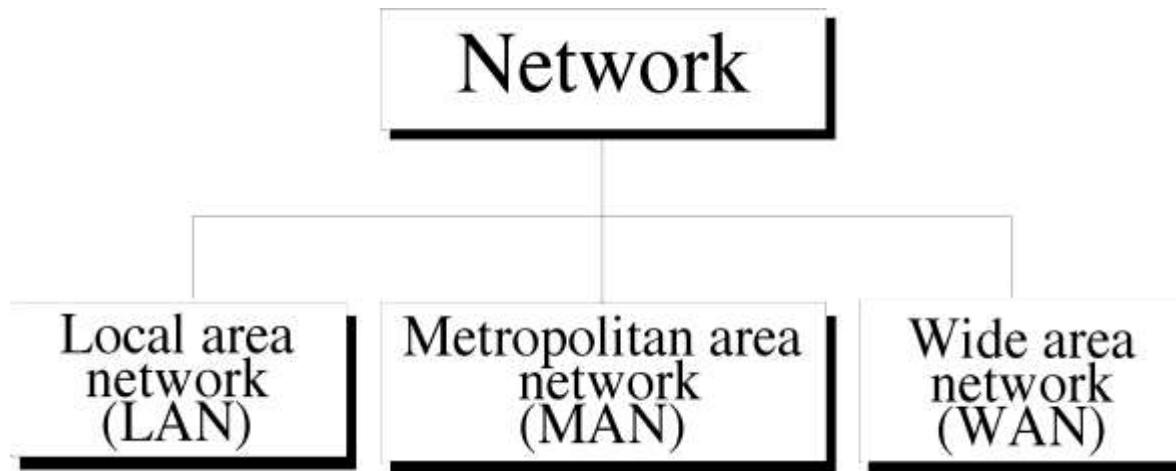


Figure : *A hybrid topology: a star backbone with three bus networks*

■ A network can be **hybrid**. For example, we can have a main star topology with each branch connecting several stations in a bus.

Network Types

■ Today when we speak of networks, we are generally referring to three primary categories: **LAN** , **MAN** and **WAN**.



■ The Category into which the network falls is determined by its size.

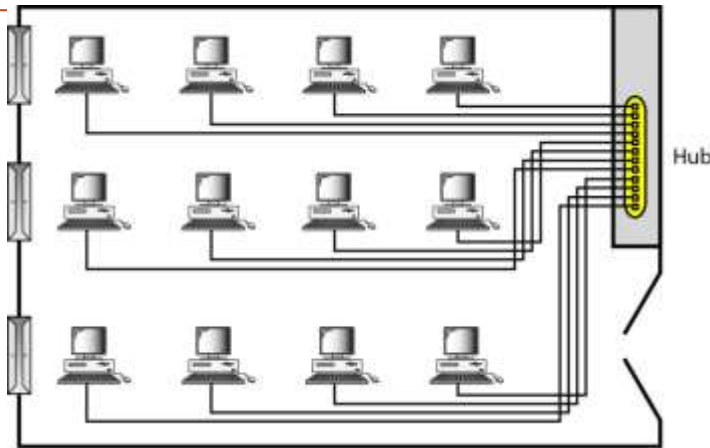
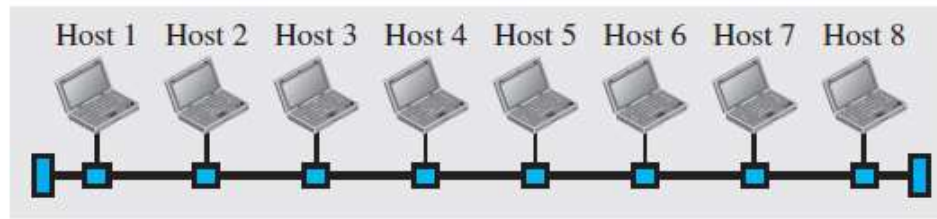
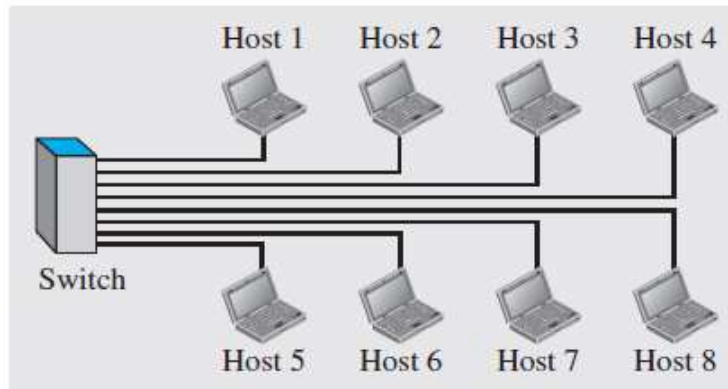


Figure : *An isolated LAN connecting 12 computers to a hub in a closet*

- A **local area network** (LAN) is usually privately owned and links the devices in a single office, building, or campus.
- 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.
- LANs are designed to allow resources to be shared between personal computers or workstations.
- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.

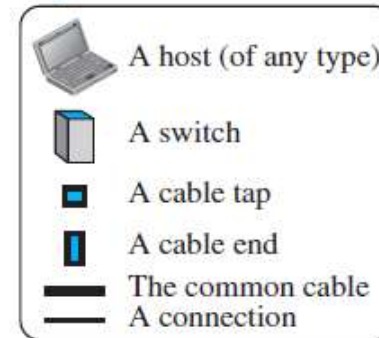


a. LAN with a common cable (past)



b. LAN with a switch (today)

Legend



In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet.

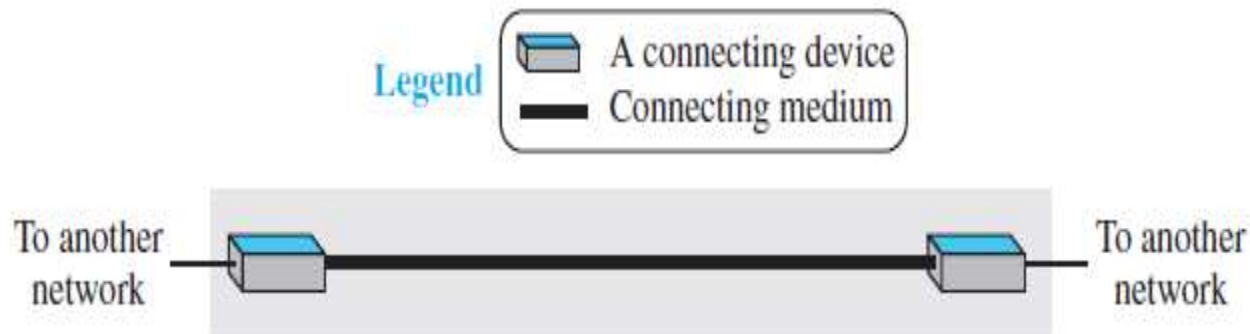
Today, most LANs use a **smart connecting switch**, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.

- A **wide area network (WAN)** is also an interconnection of devices capable of communication.
- However, there are some differences between a LAN and a WAN.

LAN	WAN
A LAN is normally limited in size, spanning an office, a building, or a campus;	A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.
A LAN interconnects hosts;	A WAN interconnects connecting devices such as switches, routers, or modems.
A LAN is normally privately owned by the organization that uses it;	A WAN is normally created and run by communication companies and leased by an organization that uses it.

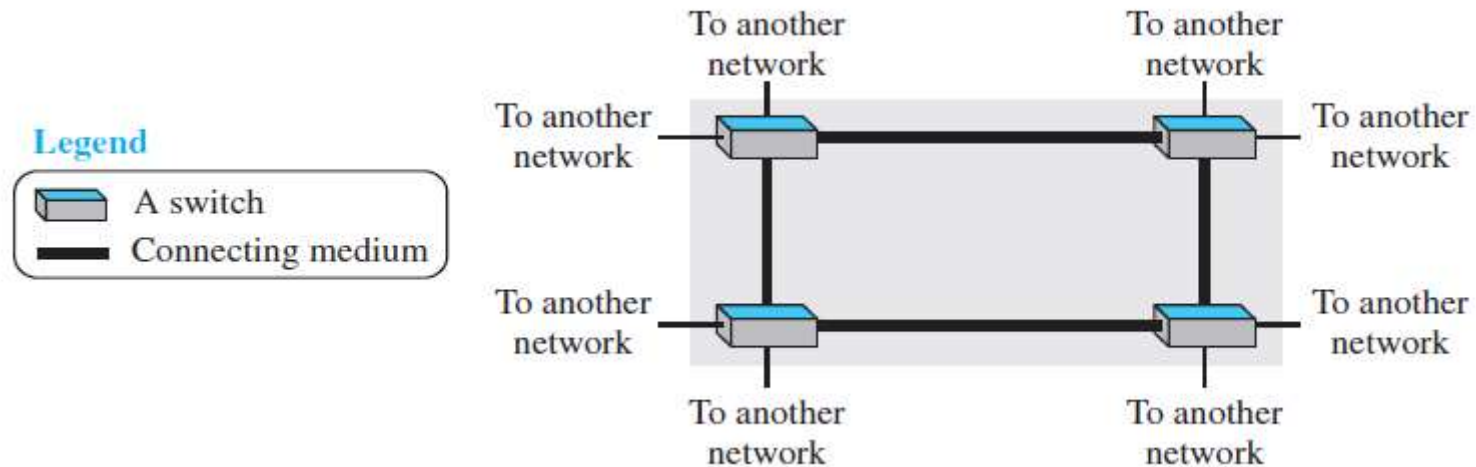
- We see two distinct examples of WANs today: **point-to-point WANs** and **switched WANs**.

Point-to-Point WAN



- A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).

Switched WAN

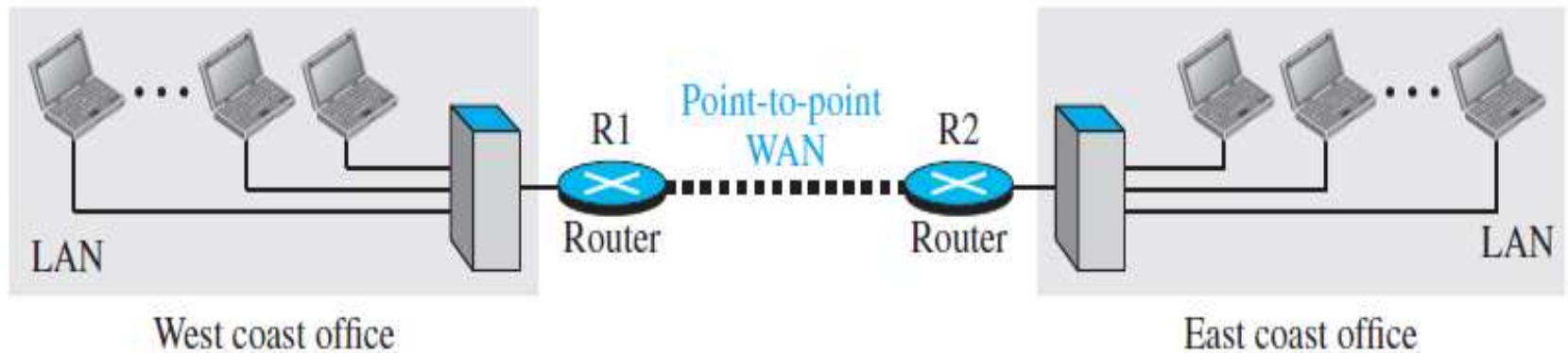


- ❑ A switched WAN is a network with more than two ends. A switched WAN, as we will see shortly, is used in the backbone of global communication today.
- ❑ We can say that a switched WAN is a **combination of several point-to-point WANs** that are connected by switches.

Internetwork

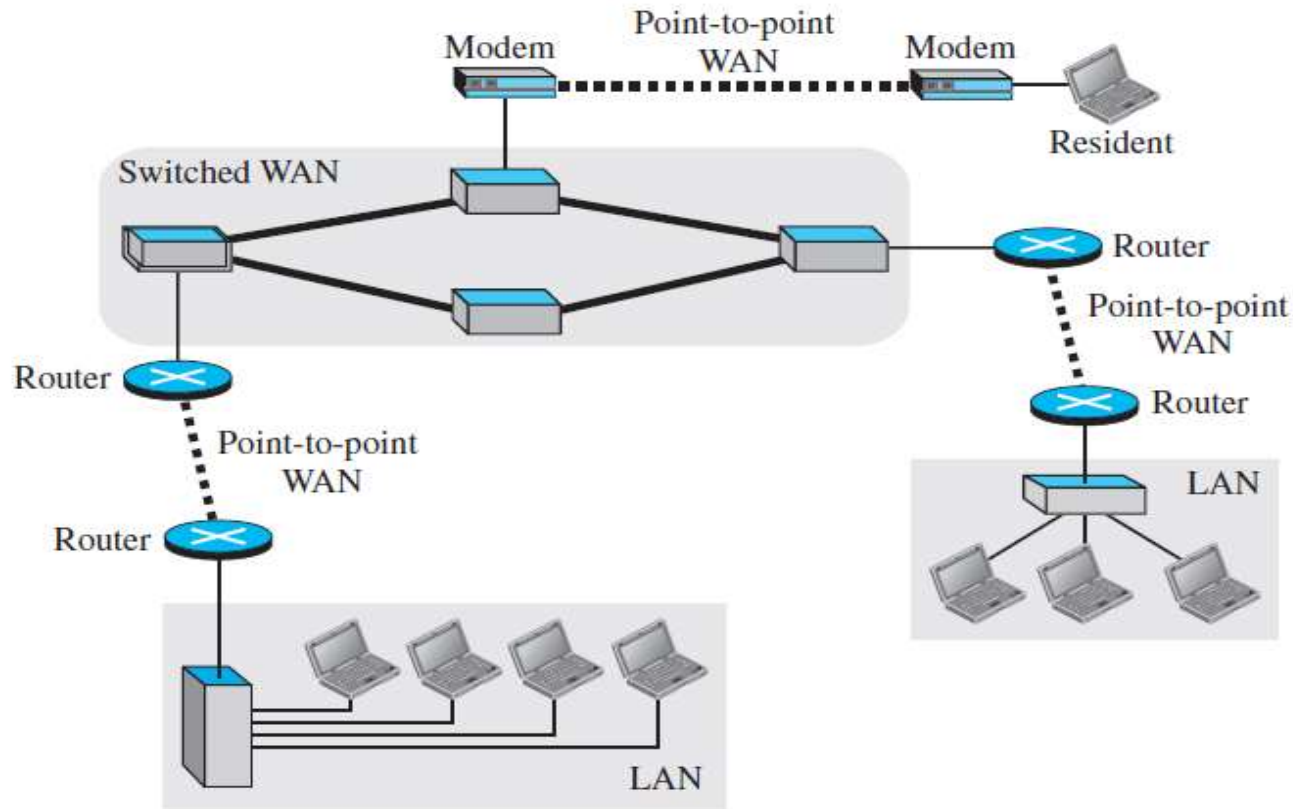
- Today, it is very rare to see a LAN or a WAN in isolation; they are connected to one another. When two or more networks are connected, they make an **internetwork**, or **internet**.

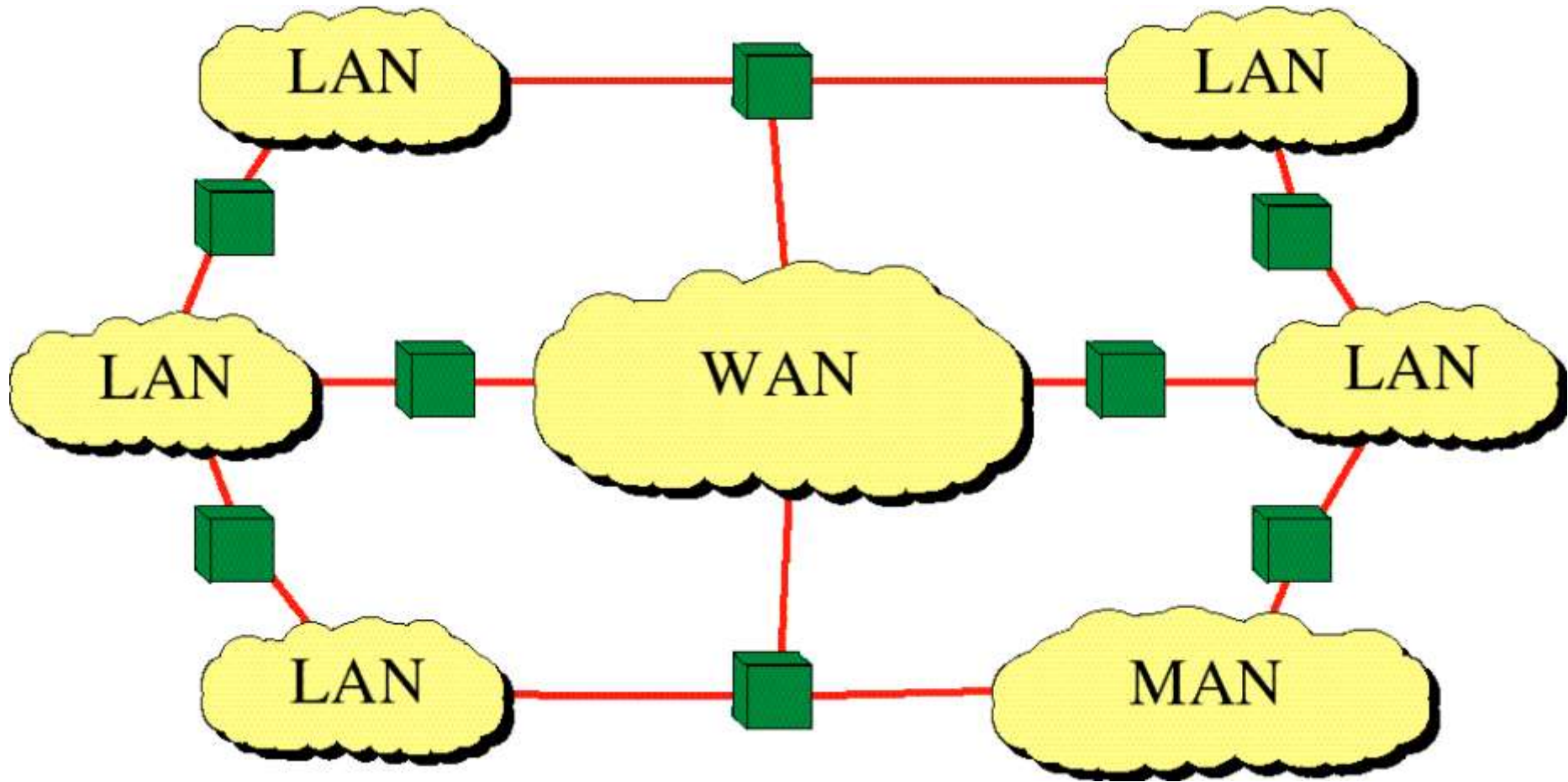
Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*



- ❑ This shows another internet with several LANs and WANs connected. One of the WANs is a switched WAN with four switches.

Figure 1.12 *A heterogeneous network made of four WANs and three LANs*

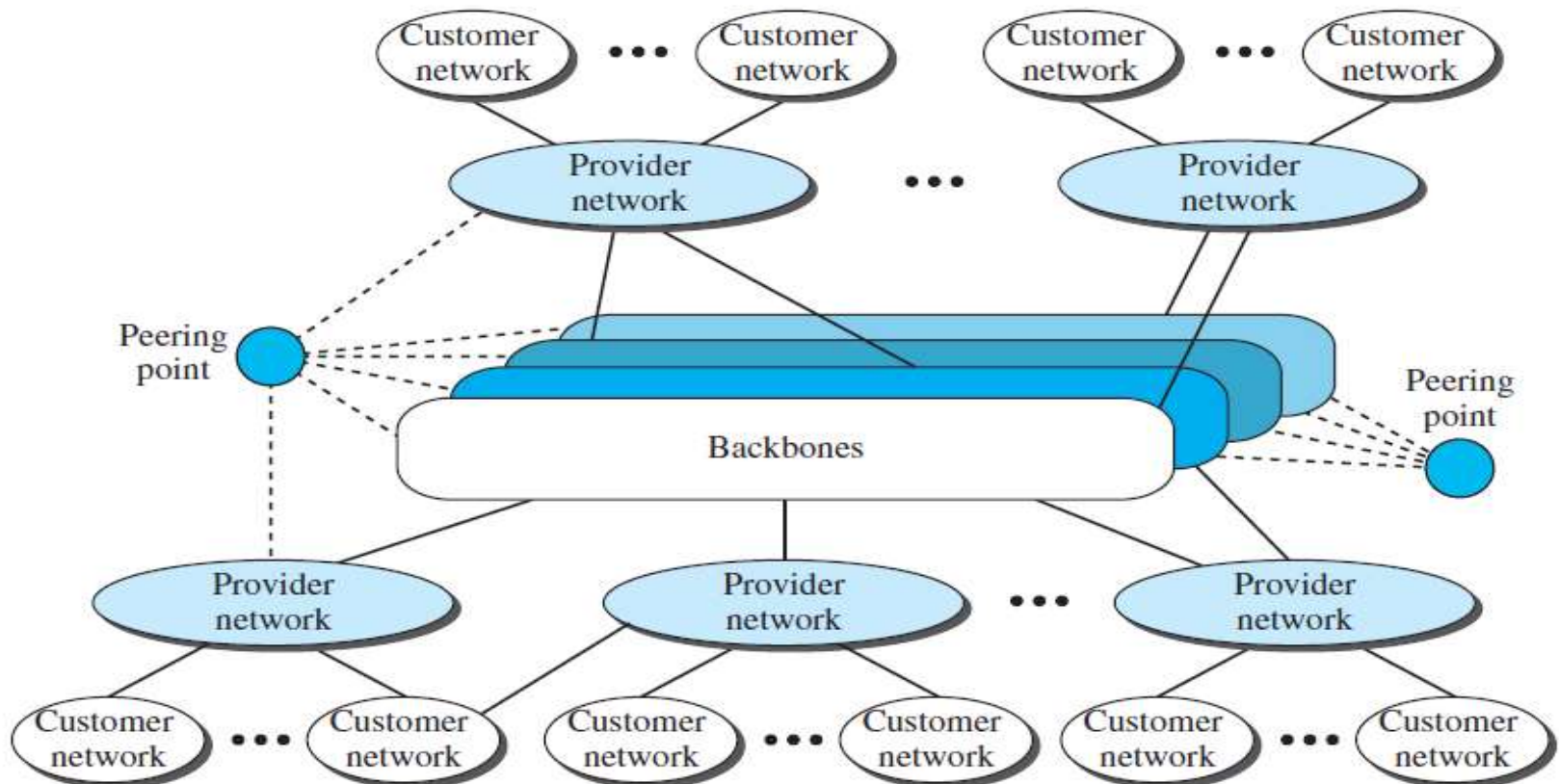




The Internet

- ❑ An **internet** is two or more networks that can communicate with each other and is composed of thousands of interconnected networks.

Figure 1.15 *The Internet today*



- ❑ The figure above shows the Internet as several backbones, provider networks, and customer networks.
- ❑ At the top level, **the backbones** are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT.
- ❑ The backbone networks are connected through some complex switching systems, called **peering points**.
- ❑ At the second level, there are smaller networks, called **provider networks**, that use the services of the backbones for a fee.
- ❑ The provider networks are connected to backbones and sometimes to other provider networks.
- ❑ The **customer networks** are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.

- ❑ Backbones and provider networks are also called **Internet Service Providers (ISPs)**.
- ❑ The backbones are often referred to as *international ISPs*.
- ❑ The provider networks are often referred to as *national* or *regional ISPs*.

Accessing the Internet

✚ The Internet today is an internetwork that allows any user to become part of it.

Using Telephone Networks

✓ Today most residences and small businesses have telephone service, which means they are connected to a telephone network.

❑ Dial-up service: The first solution is to add to the telephone line a modem that converts data to voice. The software installed on the computer dials the ISP and imitates making a telephone connection. Unfortunately, the dial-up service is very slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection. It is only useful for small residences.

❑ DSL Service: Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide higher speed Internet services to residences or small businesses. The DSL service also allows the line to be used simultaneously for voice and data communication.

- ❑ **Using Cable Networks:** More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet.
- ❑ **Using Wireless Networks:** Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet.
- ❑ **Direct Connection to the Internet:** A large organization or a large corporation can itself become a local ISP and be connected to the Internet.

✚ Now that we have given an overview of the Internet, let us give a brief history of the Internet.

❑ Early History

There were some communication networks, such as telegraph and telephone networks, before 1960. These networks were suitable for constant-rate communication at that time, which means that after a connection was made between two users, the encoded message (telegraphy) or voice (telephony) could be exchanged.

❑ *Birth of Packet-Switched Networks*

The theory of packet switching for bursty traffic was first presented by Leonard Kleinrock in 1961 at MIT. At the same time, two other researchers, Paul Baran at Rand Institute and Donald Davies at National Physical Laboratory in England, published some papers about packet-switched networks.

❑ ARPANET

In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency (ARPA)** in the Department of Defense (DOD) was interested in finding a way to connect computers.

In 1967, ARPA presented its ideas for the **Advanced Research Projects Agency Network (ARPANET)**, a small network of connected computers. The idea was that each host computer would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Software called the **Network Control Protocol** (NCP) provided communication between the hosts.

Birth of the Internet

✚ In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Project*. They wanted to link dissimilar networks so that a host on one network could communicate with a host on another.

□ TCP/IP

Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

Shortly thereafter, authorities made a decision to split TCP into two protocols: **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**. IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The new combination became known as TCP/IP.

❑ MILNET

In 1983, ARPANET split into two networks: **Military Network (MILNET)** for military users and ARPANET for nonmilitary users.

❑ CSNET

Another milestone in Internet history was the creation of CSNET in 1981. **Computer Science Network (CSNET)** was a network sponsored by the National Science Foundation (NSF). The network was conceived by universities that were ineligible to join ARPANET due to an absence of ties to the Department of Defense. CSNET was a less expensive network; there were no redundant links and the transmission rate was slower.

❑ NSFNET

With the success of CSNET, the NSF in 1986 sponsored the **National Science Foundation Network (NSFNET)**, a backbone that connected five supercomputer centers located throughout the United States.

❑ ANSNET

In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and Verizon, filled the void by forming a nonprofit organization called Advanced Network & Services (ANS) to build a new, high-speed Internet backbone called **Advanced Network Services Network (ANSNET)**.

Internet Today

✚ Today, we witness a rapid growth both in the infrastructure and new applications. What has made the Internet so popular is the invention of new applications.

❑ World Wide Web

The 1990s saw the explosion of Internet applications due to the emergence of the World Wide Web (WWW).

❑ Multimedia

Recent developments in the multimedia applications such as voice over IP (telephony), video over IP (Skype), view sharing (YouTube), and television over IP (PPLive) has increased the number of users and the amount of time each user spends on the network.

❑ Peer-to-Peer Applications

Peer-to-peer networking is also a new area of communication with a lot of potential.

Internet Standards

- ❑ An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet.
- ❑ It is a formalized rules & regulation that must be followed.
- ❑ A specification begins as an Internet draft. An **Internet draft** is a working document (a work in progress) with no official status and a six-month lifetime.
- ❑ Upon recommendation from the Internet authorities, a draft may be published as a **Request for Comment (RFC)**.
- ❑ Each RFC is edited, assigned a number, and made available to all interested parties.
- ❑ RFCs go through **maturity levels** and are categorized according to their **requirement level**.

Maturity Levels

An RFC, during its lifetime, falls into one of five *maturity levels*:

- ❑ **Proposed Standard:** A proposed standard is a specification that is **stable**, **well understood**, and of sufficient interest to the Internet community
- ❑ **Draft Standard:** A proposed standard is elevated to draft standard status after at least two **successful independent and interoperable** implementations.
- ❑ **Internet Standard:** A draft standard reaches Internet standard status after **demonstrations of successful** implementation.
- ❑ **Experimental:** An RFC classified as experimental describes work related to an experimental situation that **does not affect the operation of the Internet**.
- ❑ **Informational:** An RFC classified as informational contains **general, historical, or tutorial information** related to the Internet.

Requirement Levels

RFCs are classified into five *requirement levels*:

- ❑ **Required:** An RFC is labeled *required* if it must be implemented by all Internet systems to achieve minimum conformance. For example, IP and ICMP.
- ❑ **Recommended:** An RFC labeled recommended is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP and TELNET
- ❑ **Elective:** An RFC labeled elective is not required and not recommended. However, a system can use it for its own benefit.
- ❑ **Limited Use:** An RFC labeled limited use should be used only in limited situations. Most of the experimental RFCs fall under this category.
- ❑ **Not Recommended:** An RFC labeled not recommended is inappropriate for general use.

✚ Following are the few administrations that coordinate internet issues and have guided the growth and development of internet:

ISOC:

- ❑ The **Internet Society (ISOC)** is an international organization formed in 1992 to provide support for the Internet standards process.
- ❑ ISOC accomplishes this through maintaining and supporting other Internet administrative bodies such as IAB, IETF, IRTF, and IANA.
- ❑ ISOC also promotes research and other scholarly activities relating to the Internet.

IAB:

- ❑ The **Internet Architecture Board (IAB)** is the technical advisor to the ISOC.
- ❑ The main purposes of the IAB are to oversee the continuing development of the TCP/IP Protocol Suite.

IETF:

- ❑ The **Internet Engineering Task Force (IETF)** is a forum of working groups.
- ❑ IETF is responsible for identifying operational problems and proposing solutions to these problems.
- ❑ IETF also develops and reviews specifications intended as Internet standards.

IRTF:

- ❑ The **Internet Research Task Force (IRTF)** is a forum of working groups.
- ❑ IRTF focuses on long-term research topics related to Internet protocols, applications, architecture, and technology.

Overall Summary of Chapter-1

- Data communication is the transfer of data from one device to another via some form of transmission medium.
- A data communications system must transmit data to the correct destination in an accurate and timely manner.
- The five components that make up a data communications system are the message, sender, receiver, medium, and protocol.
- Text, numbers, images, audio, and video are different forms of information.
- Data flow between two devices can occur in one of three ways: simplex, half-duplex, or full-duplex.
- A network is a set of communication devices connected by media links.

-
- A network can be categorized as a local area network (LAN), a metropolitan-area network (MAN), or a wide area network (WAN).
 - A LAN is a data communication system within a building, plant, or campus, or between nearby buildings.
 - A MAN is a data communication system covering an area the size of a town or city.
 - A WAN is a data communication system spanning states, countries, or the whole world.
 - An internet is a network of networks.
 - The Internet is a collection of many separate networks.
 - There are local, regional, national, and international Internet service providers (ISPs).

-
- In a point-to-point connection, two and only two devices are connected by a dedicated link. In a multipoint connection, three or more devices share a link.
 - Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology.
 - A protocol is a set of rules that governs data communication; the key elements of a protocol are syntax, semantics, and timing.
 - Standards are necessary to ensure that products from different manufacturers can work together as expected.

END of *Chapter 1*


Connecting Devices




Network Interface Card

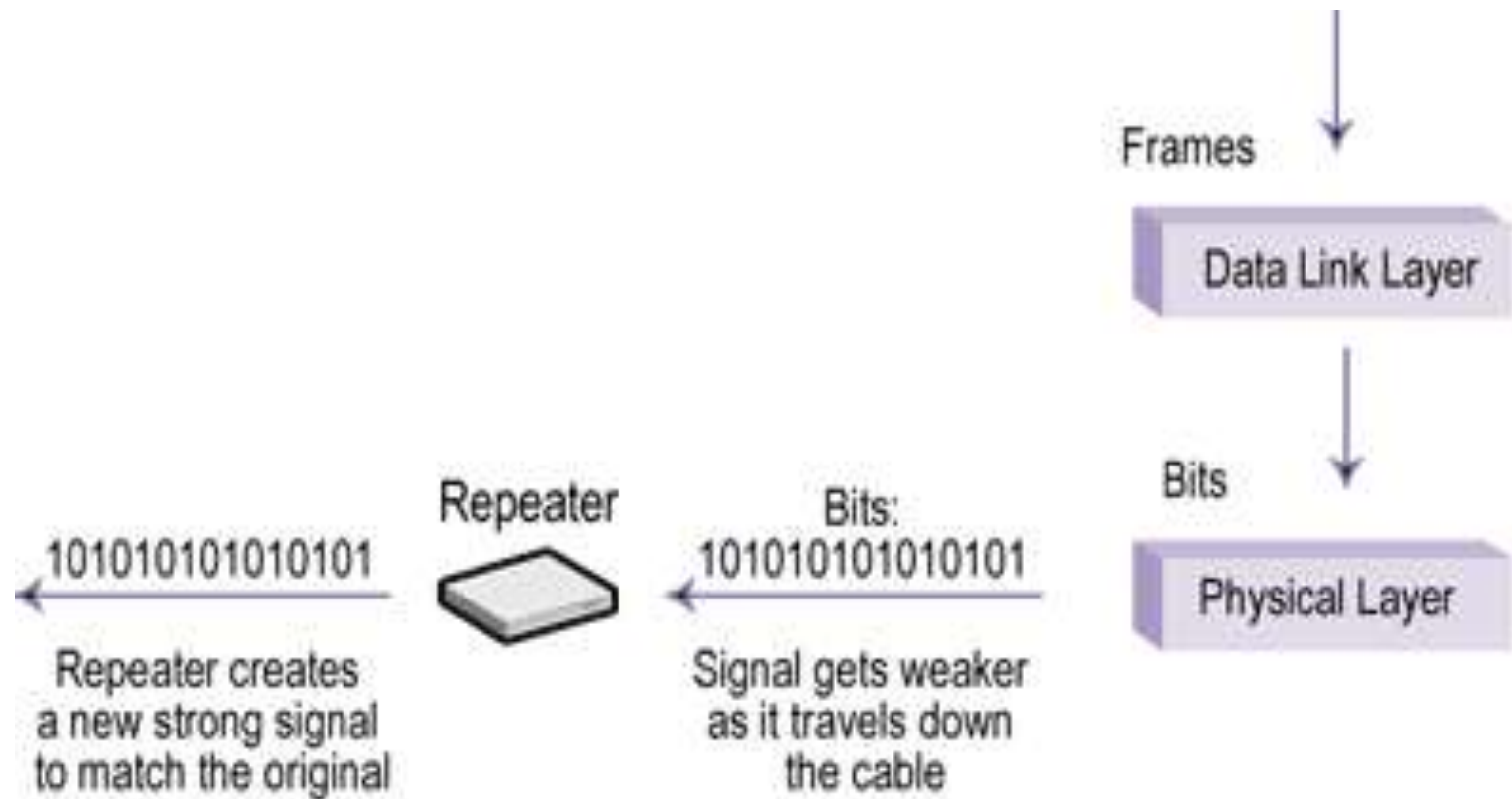


NIC (Cont.)

- ▶ The Network Interface Card links the computer to the Computer Network.
 - ▶ It serves as the input /output device transferring data in and out of the computer.
 - ▶ The function of a NIC is to connect a host device to the network medium. NICs are considered Layer 2 devices because each NIC carries a unique code called a MAC address (48 Bit address) .
- 

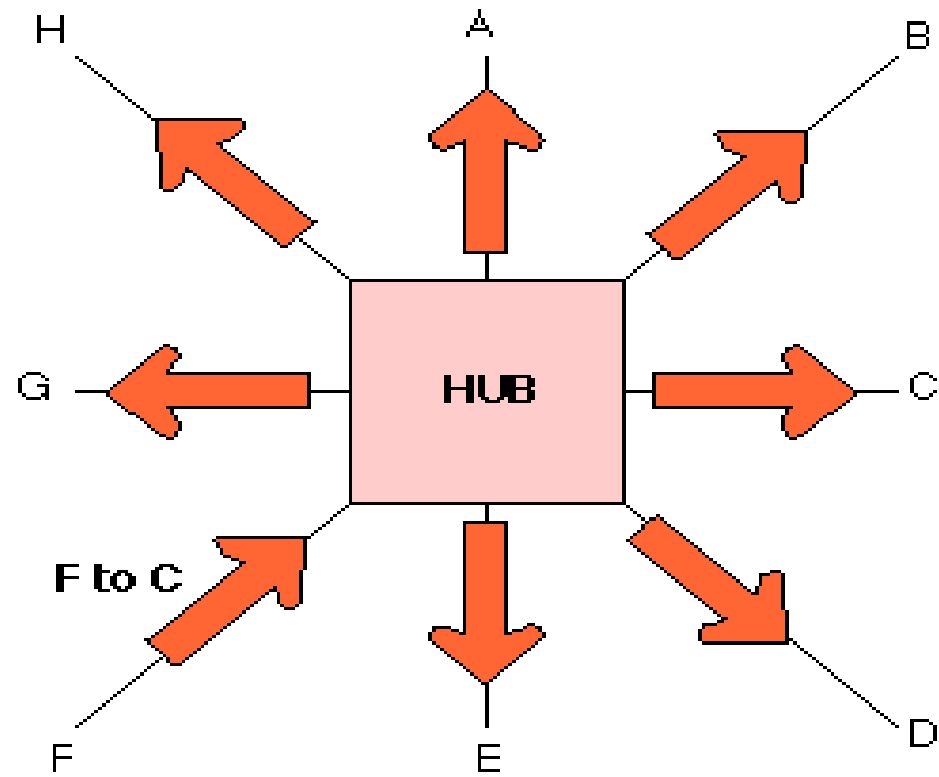
Repeaters

- ▶ Repeaters and hubs are Physical Layer devices (Layer 1 device)
 - ▶ These devices are simple,
 - ▶ They transmit bits, but do not evaluate them
 - ▶ They add power to the signal as they actively retransmit it.
 - ▶ Repeaters operate on bits and extend the length of a physical medium.
- 




Hub


- ▶ To increase the number of devices connected to a network, we use a device called a "hub".
- ▶ Hubs provide a central point of connectivity for networking devices.
- ▶ A hub is sometimes called a "wiring concentrator". or "multi-port repeaters"
- ▶ Logically functions as a shared bus or multi-port repeater.
- ▶ All devices connected to a hub receive frames transmitted by any other device on that hub.




Bridges

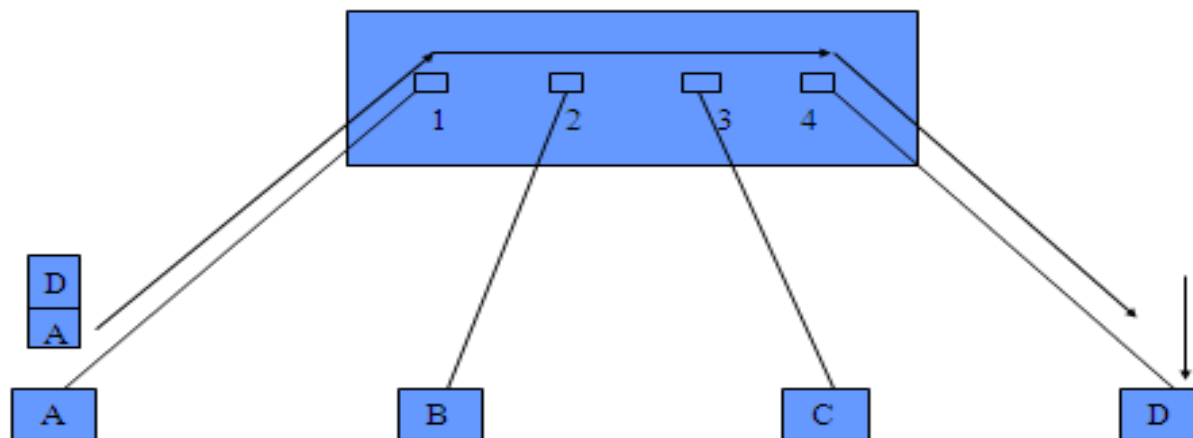
- ▶ This connects two LANs that use same networks. Bridges operate at the Data Link Layer of the OSI model. Sometimes they are called "Layer 2 devices" or "Link Layer devices".
 - ▶ These devices are used to increase the overall performance of a network by isolating traffic within network segments.
- 

Switch

- ▶ Switches are Data Link Layer (Layer 2) devices used to increase performance in LANs
 - ▶ Like a bridge, a switch isolates traffic and creates separate collision domains by forwarding, filtering and flooding the frames.
 - ▶ Bridge, which shares the LAN bandwidth among all of its ports
- 


- ▶ Switch dedicates the entire LAN media bandwidth, such as 10-Mbps Ethernet, to each port-to-port frame transmission.
 - ▶ That is a switch multiplies the bandwidth between each port
 - ▶ Like bridge , hub is also shared(divide) the bandwidth between each ports
- 

Switched Network



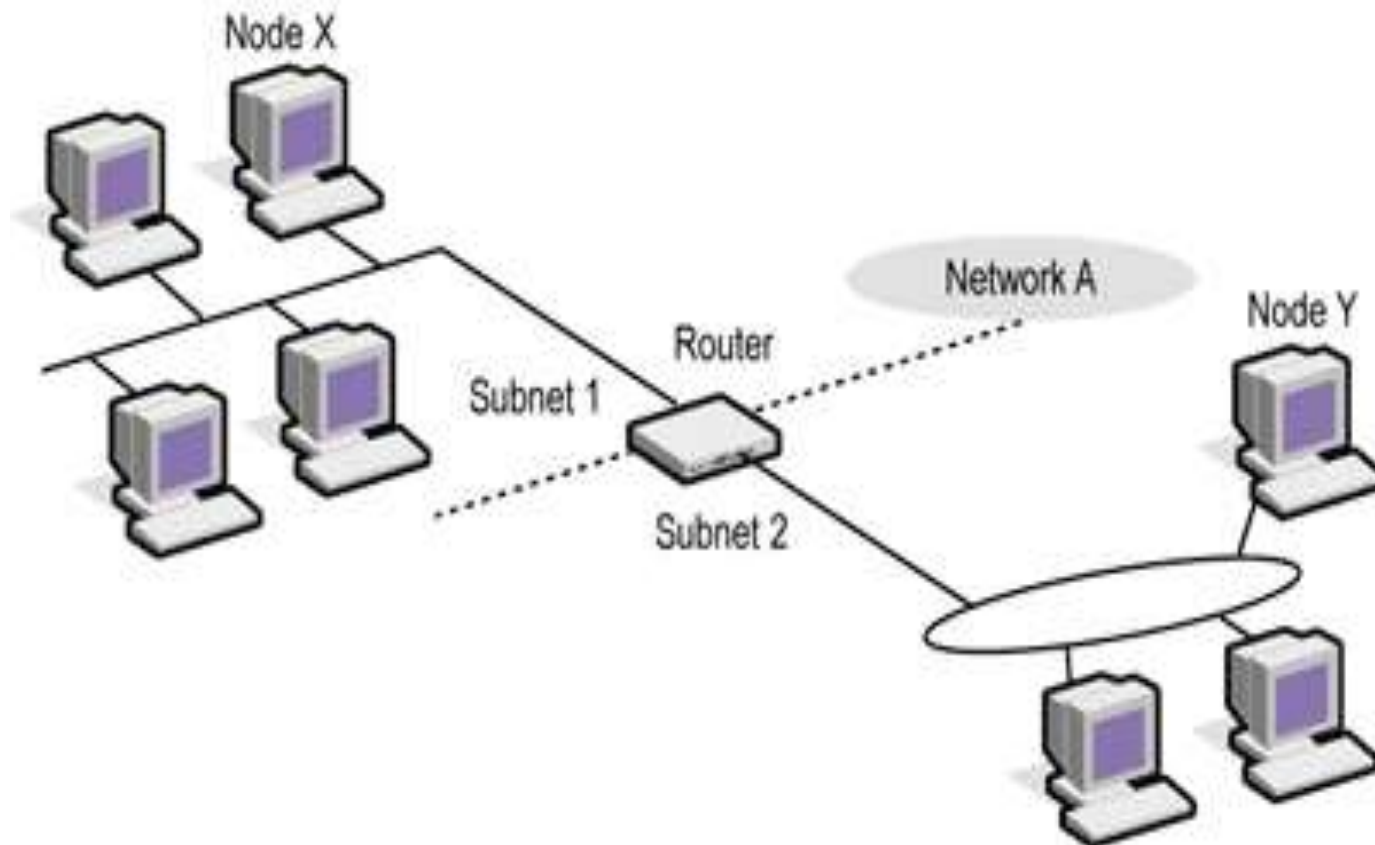
PORT	MAC address
1	A
2	B
3	C
4	D

Router

- ▶ Router connects multiple networks. It is a internetworking device
 - ▶ A router operates at the Network Layer of the OSI reference model.
 - ▶ It makes intelligent packet-forwarding decisions based on each packet's network address (IP address / logical Address)
- 

- ▶ Routers use packet addresses (IP address) to route information between networks.
- ▶ Each port of a router connects to a different network or subnet.





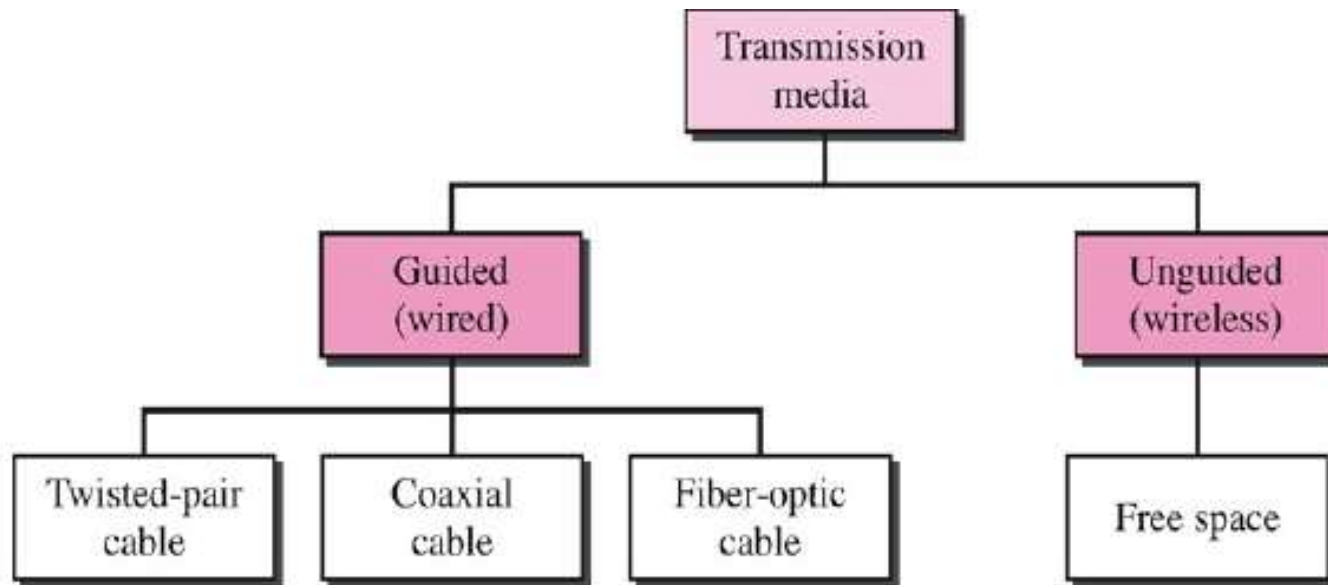
Router Vs Switch

Router	Switch
Basically, a router is used to connect <u>computers belonging to one network with those belonging to another or other networks.</u> <u>Thus, a router connects two or more different networks.</u>	A switch on the other hand, connects different <u>computers within one network.</u>
As per the OSI model, a router is a Network Layer device, i.e. it <u>operates at Layer 3.</u>	a network switch <u>operates at Layer 2 (Data Link Layer).</u>
Routers are much more sophisticated and intelligent network devices, as compared to switches.	In comparison with routers, switches are less sophisticated and less intelligent.
A router works on the principle of <u>IP addresses.</u> <u>Logical Address / Internet Address</u>	A switch works on the basis of <u>MAC addresses/ Physical Address / NIC Address/ Hardware Address</u>
A router's inbuilt hardware makes use of routing algorithms to compute the best possible path for routing data packets across different computer networks.	A switch does not perform any such activities.
Routers have their own inbuilt operating systems and they need to be configured before use.	Most switches do not require any prior configuration and are usually 'ready-to-use'.

TRANSMISSION MEDIA

- ▶ Transmission medium is the physical path between the transmitter and receiver.
- ▶ It is the transmission medium through which information usually moves from one network device to another.
- ▶ In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types.

Types of Media



Primary Cable Types

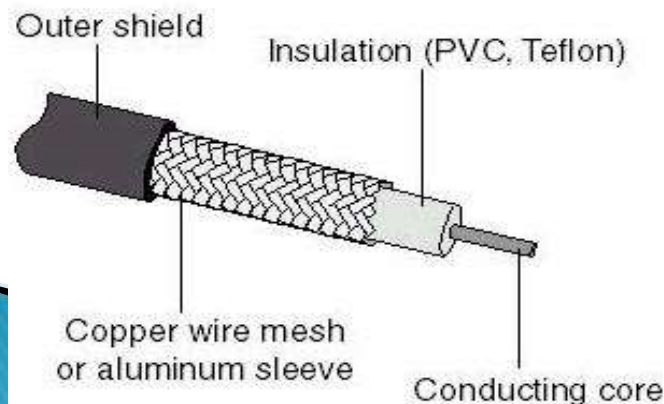
The networks are connected by some sort of wiring or cabling that acts as a network transmission medium that carries signals between computers.

Three major groups of cabling connect the majority of networks:

- Coaxial cable
- Twisted-pair (unshielded and shielded) cable (UTP/STP)
- Fiber-optic cable

Coaxial Cable

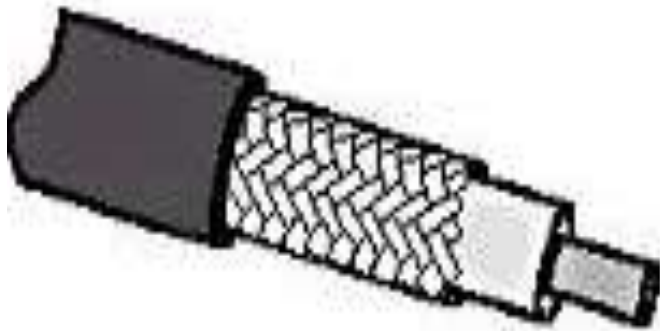
- In its simplest form, coaxial cable consists of a core of copper wire surrounded by insulation, a metal **shielding**, and an outer cover.
 - The core of a coaxial cable carries the electronic signals that make up the data.
 - This wire core is usually copper.
 - Surrounding the core is a dielectric insulating layer that separates it from the wire mesh.
 - The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk.
- (Crosstalk is signal overflow from an adjacent wire.)



Types of Coaxial Cable

There are two types of coaxial cable:

- Thinnet cable
- Thicknet cable



Thicknet core



Thinnet core

Twisted-Pair Cable

Twisted-pair cable consists of two insulated strands of copper wire twisted around each other.

Two types of twisted-pair cable: **unshielded twisted-pair (UTP)** and **shielded twisted-pair (STP) cable**.

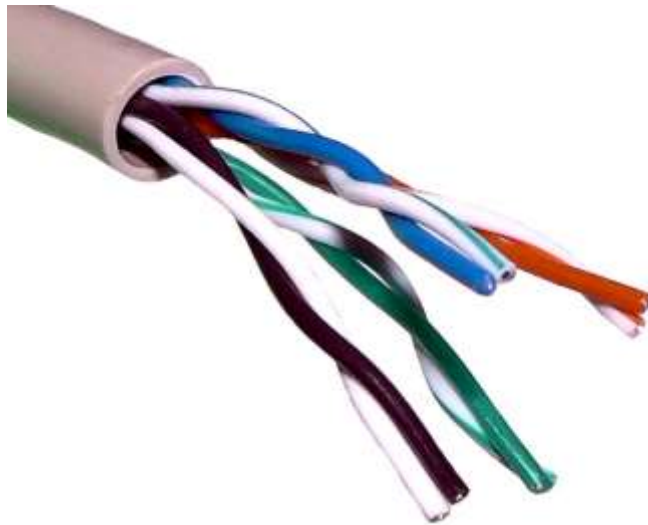


A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays, and transformers.

a) Unshielded Twisted-Pair (UTP) Cable

UTP, using the 10BaseT specification, is the most popular type of twisted-pair cable .

The maximum cable length segment is 100 meters. Traditional UTP cable consists of two insulated copper wires.



Categories of UTP cable

Category 1 this can carry voice but not data transmissions

Category 2 UTP cable for data transmissions up to 4 Mbps

Category 3 UTP cable for data transmissions up to 16 Mbps

Category 4 UTP cable for data transmissions up to 20 Mbps

Category 5 UTP cable for data transmissions up to 100 Mbps

Category 6 UTP cable for data transmissions up to 155 Mbps

Category 7 UTP cable for data transmissions up to 1000 Mbps

b) Shielded Twisted–Pair (STP) Cable

STP also uses a foil wrap around each of the wire pairs.

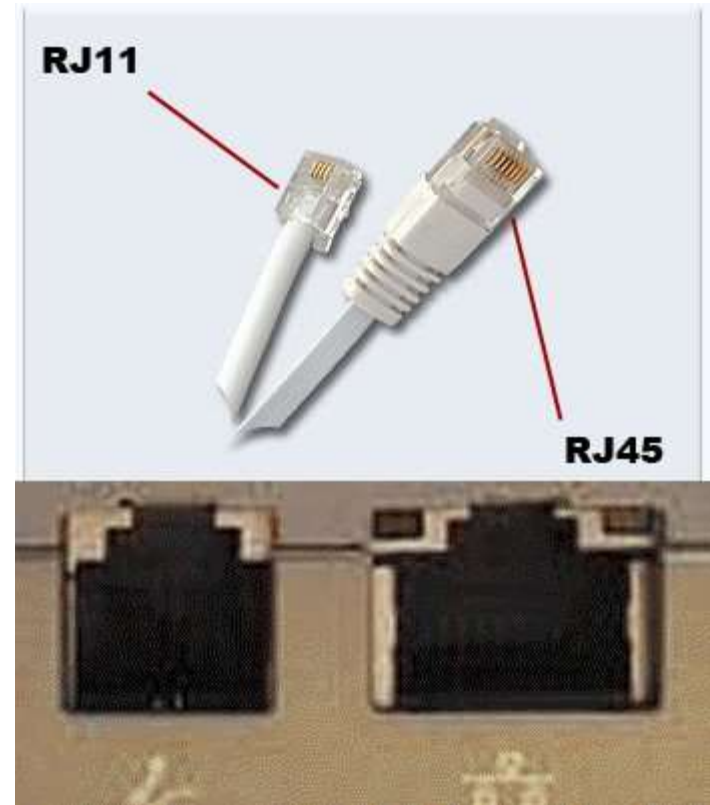
This gives STP excellent shielding to protect the transmitted data from outside interference, which allows higher transmission rates over longer distances than UTP.



Hardware connection and UTP cable Termination

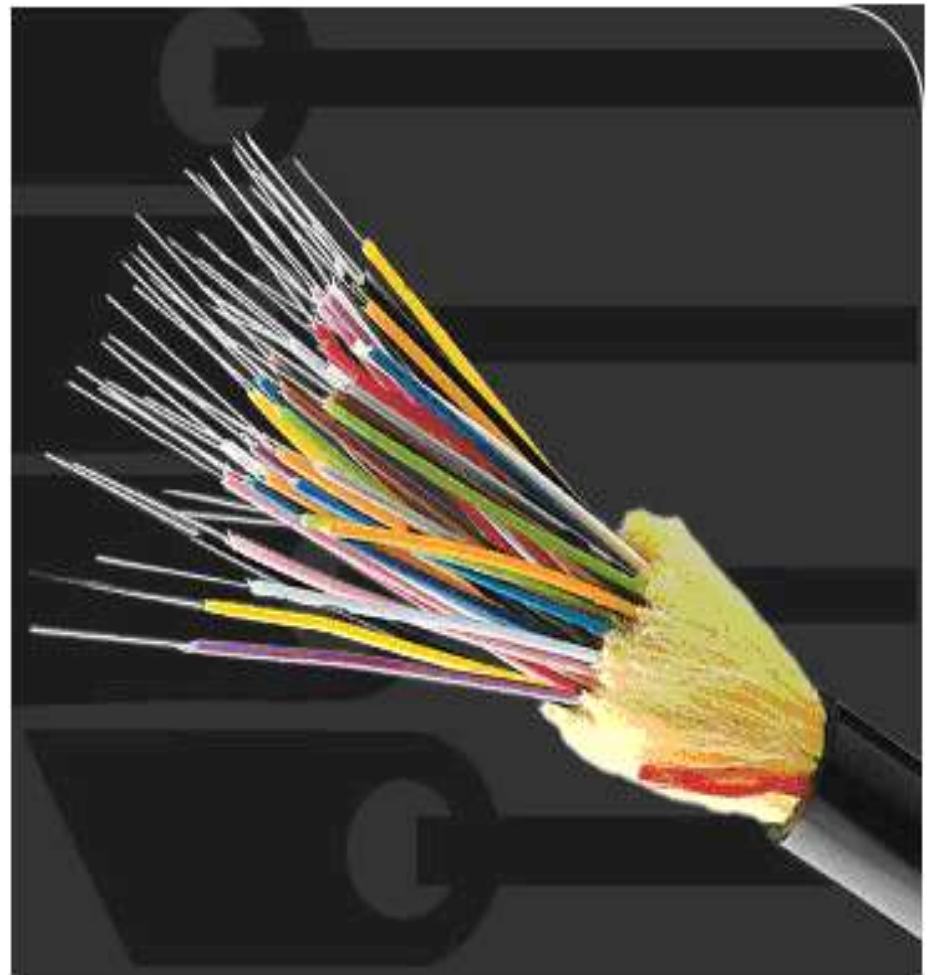
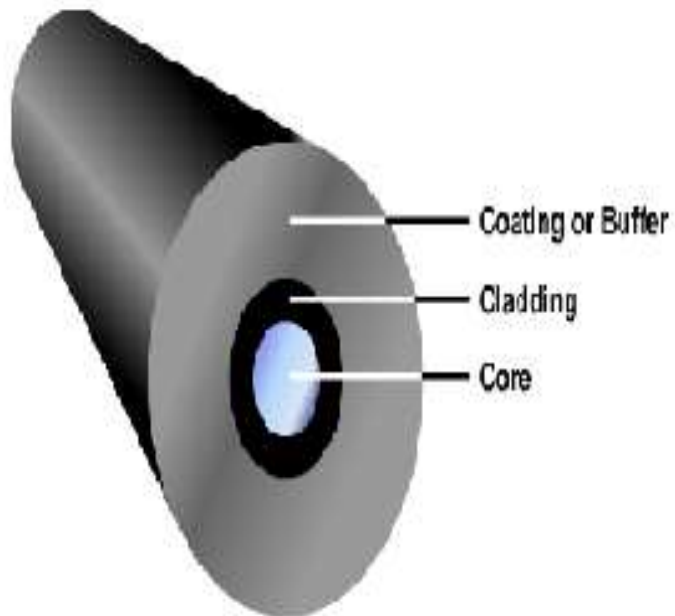
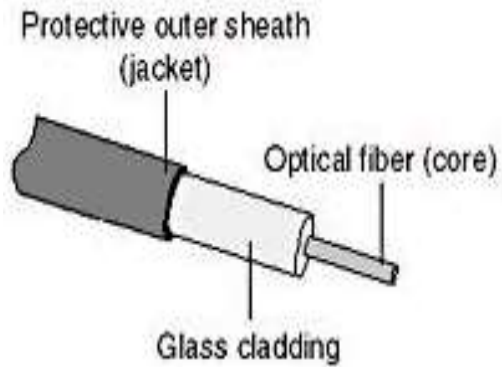
Two-pair (four-wire) UTP used for **telephone** use is normally terminated in an **RJ-11** connector.

Four-pair (eight-wire) UTP used for data use is normally terminated in an **RJ-45** connector



Fiber-Optic Cable

- In fiber-optic cable, **optical fibers carry digital data signals** in the form of **modulated pulses of light**.
- This is a relatively safe way to send because fiber **optic cable cannot be tapped**, and its data **cannot be stolen**.
- Fiber-optic cable is good for **very high-speed, high-capacity data transmission** because of the purity of the signal and lack of signal attenuation.



Types of Optical Fiber

- Single-mode fiber
- Multi-mode fiber

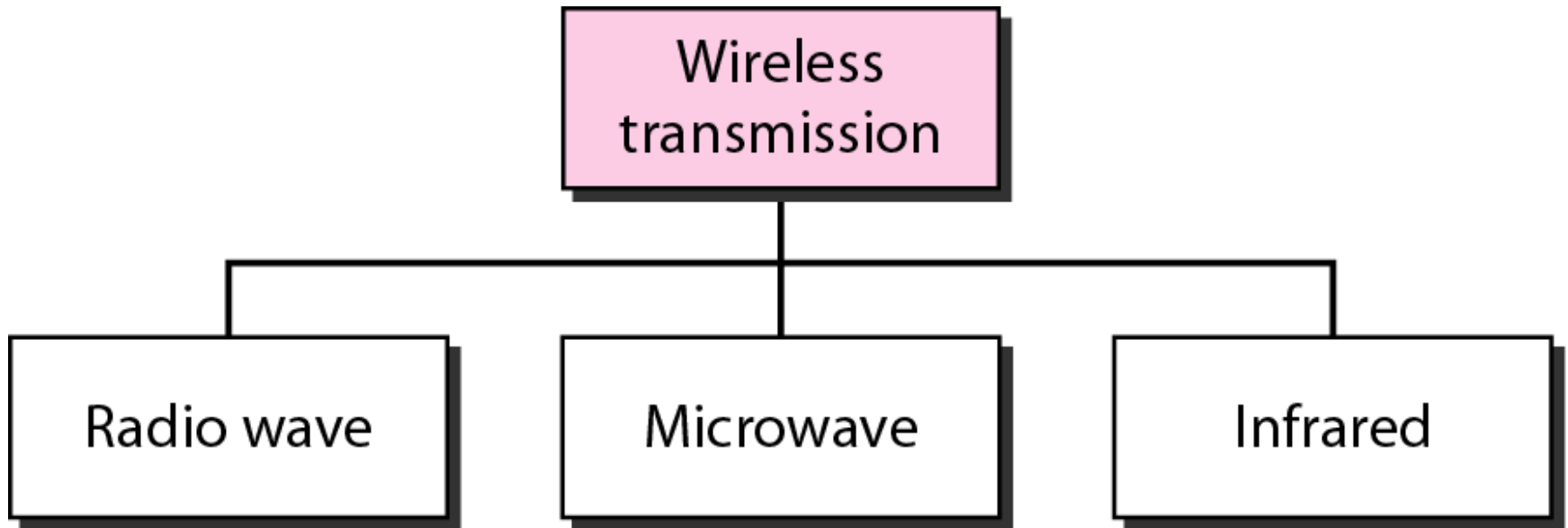
Cable Comparison Table

Characteristics	Thinnet Coaxial (10Base2) Cable	Thicknet Coaxial (10Base5) Cable	Twisted-Pair (10BaseT) Cable	Fiber-Optic Cable
Cable length	185 meters (about 607 feet)	500 meters (about 1640 feet)	UTP and STP: 100 meters (about 328 feet)	2 kilometers (6562 feet)
Transmission rates	4-100 Mbps	4-100 Mbps	UTP: 4-100 Mbps STP: 16-500 Mbps	100 Mbps or more (> 1Gbps)
Ease of installation	Easy to install	Moderately easy to install	UTP: Very easy; STP: Moderately easy	Difficult to install
Susceptibility to interference	Good resistance to interference	Good resistance to interference	UTP: Very susceptible STP: Good resistance	Not susceptible to interference
Preferred uses	Medium to large sites with high security needs	Linking thinnet networks	UTP: smaller sites on budget. STP: Token Ring in any size	Any size installation requiring speed and high data security and integrity

Unguided Media

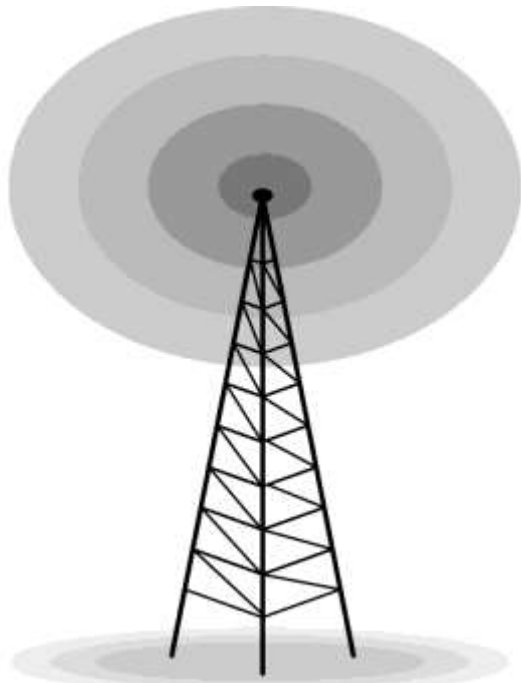
- ▶ Free space (Wireless) media carry electromagnetic signals at radio and microwave frequencies that represent the binary digits of data communications.
- ▶ As a networking medium, wireless is not restricted to conductors or pathways, as are copper and fiber media.
- ▶ Free space as the medium has the main advantage that the receiver can be fixed or mobile.
- ▶ Free space is called an unguided medium because the electromagnetic waves can travel freely in all directions.

Wireless transmission waves



Radio wave

Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls. Highly regulated. Use omni directional antennas

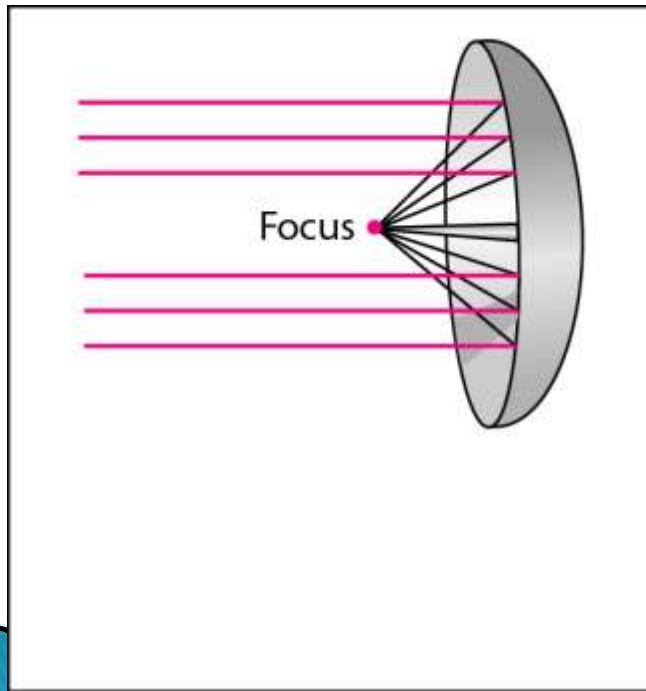


Omnidirectional antenna

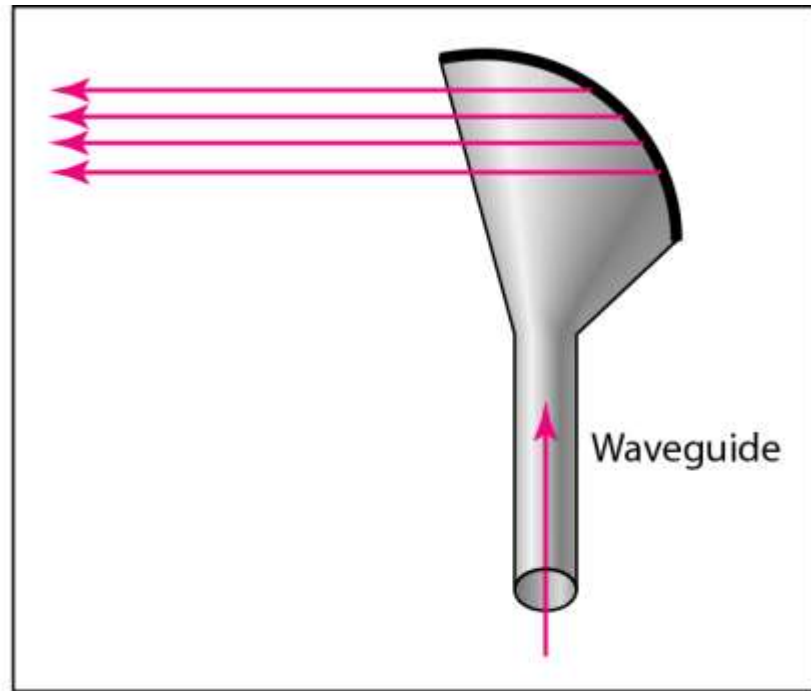
Microwaves

Microwaves are used for unicast communication such as cellular telephones, satellite networks and wireless LANs. Higher frequency ranges cannot penetrate walls. Use directional antennas – point to point line of sight communications.

Unidirectional antennas



a. Dish antenna



b. Horn antenna