COMPUTER NETWORKS

BCS502

Dr. Soumya J Bhat

Dept. of CSE

SMVITM, Bantakal

Textbook: 1. Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, Tata McGraw Hill,2013.

INTRODUCTION

What is computer network?

- A computer network is a system that connects two or more computing devices to share and transmit information. These devices can include mobile phones, servers, printers, and more. They can be connected using physical wires, like fiber optics, or wirelessly

Where is it used?

- Used for instantaneous information/data exchange. In business/personal applications

Can you compare computer network to any other existing system?

- It is very similar to postal system. Like how we write a letter, put it in an envelope, write the address, paste the stamp and send, here also many such similar tasks should be done before sending the information.
- After sending the letter, how it is transferred through multiple post offices before reaching the destination, here also it is transmitted through various routers before reaching the destination.

1.1 Data Communications

What is data?

- Data is information

What is data communication?

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

How do you measure the effectiveness of data communication?

-using 4 characteristics

1. Delivery – data must reach the correct destination. Others should not receive the data.
2. Accuracy – data should be received without errors
3. Timeliness – data must not be received late. Eg: during video call, or voice call, delayed data is useless
4. Jitter – Jitter means variation in the packet arrival time. There should not be variation in the delay. While watching youtube, If one video frame is received after 30ms delay, next video frame after 40ms delay, the video quality will be poor.

1.1.1 Components

Data communication system has 5 components.

Figure 1.1 *Five components of data communication*

Data communication system has 5 components.

1. Message – information such as text, video, audio that needs to be sent
2. Sender – device such as computer, video camera that sends the data/message
3. Receiver – device such as computer , tv that receives the data/message
4. Transmission medium – is the path used to send data such as fiber optics, radio waves
5. Protocol – rules used for communication or agreement between communicating devices. Eg: all must speak in English. If one speaks in kannada and one in tamil, they will be connected but no communication.

1.1.2 data representation -

These are the various data representations.

Text – sequence of bits. ASCII codes can be used to represent a character

Numbers – sequence of bits

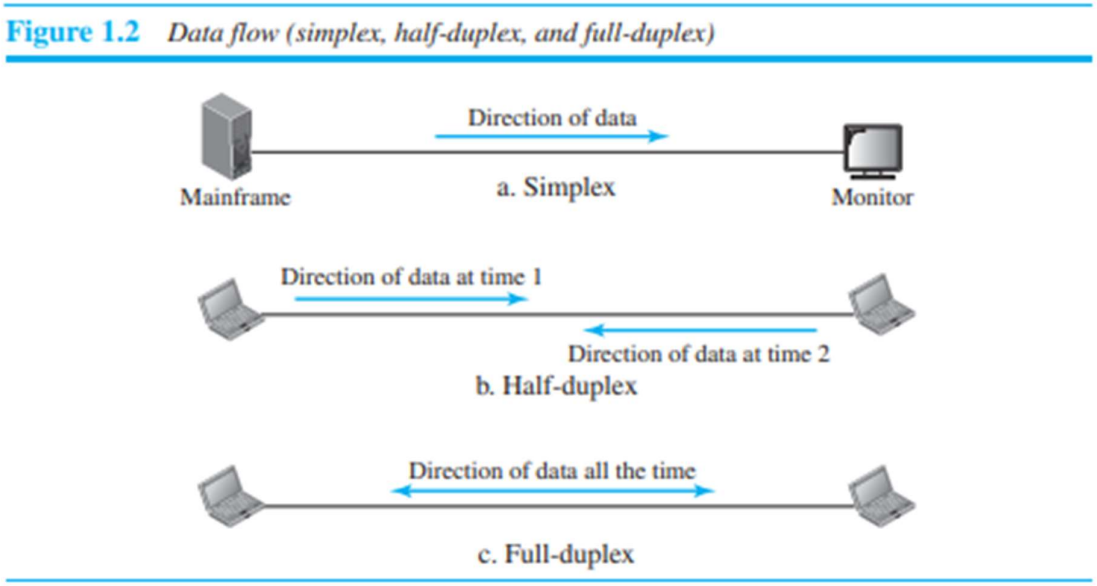
Images – it is a matrix of pixels. Each pixel is a dot. Size of the pixel depends on the resolution. An image can be divided into 1000 or 10000 pixels etc. 10000 pixels means higher resolution. After this, each pixel is represented as a sequence of bits. For black and white picture, 1 bit per pixel is enough.

For color image, RGB can be used. For each pixel, intensity of red, green and blue is measured and it is represented as a sequence of bits.

Audio, Video – continuous data. This should be converted into electric signal and then to discrete data

1.1.3 data flow

Two devices can exchange information in three modes – simplex, half-duplex or full duplex.



a.Simplex: one way communication. Eg: keyboard, monitor

b.Half duplex: each device either can transmit or receive, but not at the same time. When one device is sending, other device should listen. And Vice versa.

Eg: walkie talkie

c.Full duplex: Both devices can transmit and receive simultaneously.

Its like a 2 way street. Eg: telephone network

1.2 Networks

A network is the interconnection of a set of devices which can communicate with each other.

The devices in a network:

Computer, laptop, mobile phone – are called hosts

Routers, switches, modems etc.

Give an example for a small network and big network.

<u>1.2.1 Network Criteria – networks must meet some criteria</u>

There are 3 criteria – performance, reliability and security.

1*)Performance*:

a)Performance Can be measured using transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another device. Response time is the time taken between an inquiry and response.

b)Performance depends on number of users, type of transmission medium, hardware capacity, software efficiency

c)Performance can be measured using throughput and delay. We need more throughput and less delay.

2) *Reliability*

Is measured by the frequency of failure, time taken to recover from failure, how well network can perform in case of failures in some part of the network

3) *Security*

- Protecting data from unauthorized users, protecting data from damage, implementing procedures for recovering data when there is damage and unauthorized access.

1.2.2 Physical structures / network attributes

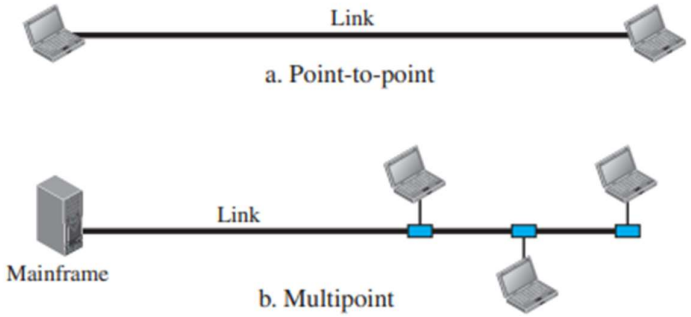
There are 2 attributes – type of connection and physical topology

1) ***Type of connection*:**

a) Point to point – a dedicated link for transmission of data between two devices.

b) Multipoint – a link is shared by more than two devices. Here capacity of the link is shared by many devices.

Figure 1.3 *Types of connections: point-to-point and multipoint*



2) Physical topology

Geometric representation of the devices and links in a network. There are 4 basic topologies:

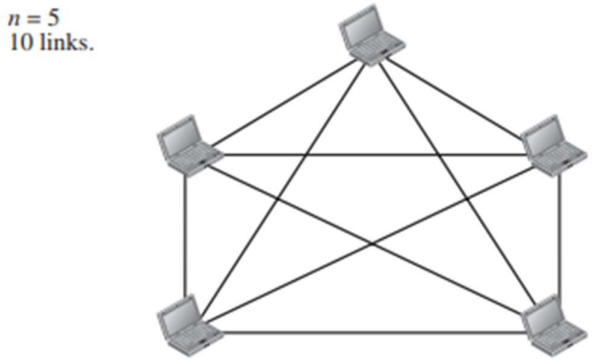
Mesh, star, bus and ring

a) Mesh topology – every device has a dedicated point to point link to every other device. The wire that connects two devices is a link. Dedicated means, this link is used to carry data between only those two device and no other devices use that link to carry data.
   How many links are required in a fully connected network with n nodes?
   Node 1 requires n-1 links to connect to other n-1 nodes
   Node 2 requires n-1 links to connect to other n-1 nodes
   ...
   Node n requires n-1 links to connect to other n-1 nodes
   Total (n-1)+(n-1)+....(n-1) = n(n-1) physical links.

   If one link allows communication in both directions, then **n(n-1)/2** duplex links are required.

Advantages of mesh topology – (a)traffic problems are eliminated as there is dedicated link between every device (b) if one link is damaged, other part of the network is not affected. Hence, it is robust . (c) because of dedicated links, there is privacy and security. (b) because of point to point links, fault detection and isolation is easy.

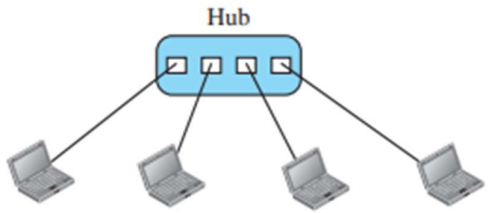
Figure 1.4 *A fully connected mesh topology (five devices)*



Disadvantages of mesh topology: because every device is connected to every other device, installation is difficult. Wiring required is more. Hardware required to connect each link to device is more.
Eg of mesh topology: telephone regional offices are connected with each other using mesh topology

b) Star topology:
Each device has a dedicated point to point link only to a central controller called a hub. Devices are not directly connected with each other. All the data should go to central controller and from there it can go to different devices. Device cannot send data to other device directly.

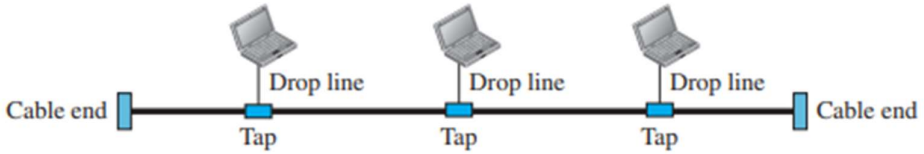
Figure 1.5 *A star topology connecting four stations*



Advantages of star topology – compared to mesh, less wiring, therefore installation is easy, hardware required is less. This is also robust because if one link is failed, other part of the network can function. Similar to mesh, here also fault identification is easy.
Disadvantage is: if the central controller, that is hub goes down, the whole network is dead.
Eg: local area network

c) Bus topology:
It is multipoint. One long cable is used to connect all the devices. Devices are connected to the bus through drop lines and taps.

Figure 1.6 *A bus topology connecting three stations*



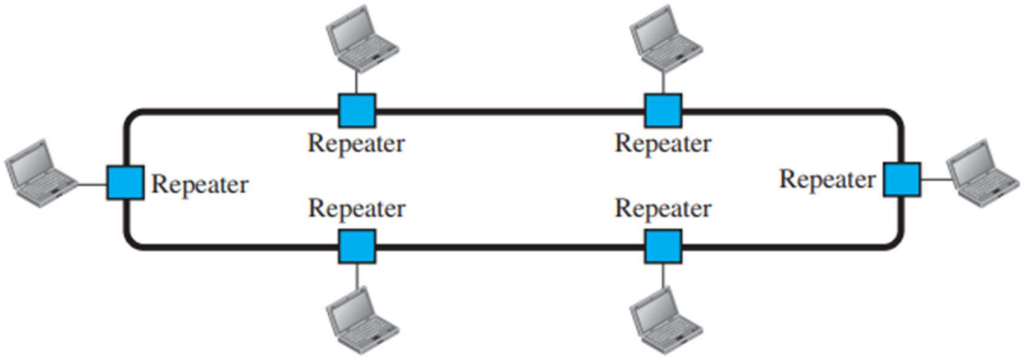
Advantage of bus topology – easy to install. First lay down the cable along the most efficient path, then connect the devices using drop lines and taps. Here, wiring required is less.
Disadvantages – difficult reconnection and fault identification. Quality of signal can get degraded if more number of devices and taps are used. Adding new devices is also difficult. If bus cable breaks, the entire transmission stops.

Transmission between the devices where there is no break in cable also stops because, signal gets reflected by the break in the line and affects all the devices.

LAN in older days were using this topology.

d) Ring topology:
Here each device has point to point connection with only two devices on its two sides. This forms a ring. Data is transferred only in one direction in this ring. There is repeater with each device. When device 1 sends message to device 3, the message first reaches device 2. Device 2's repeater regenerates the message and sends them to device 3.

Figure 1.7 *A ring topology connecting six stations*



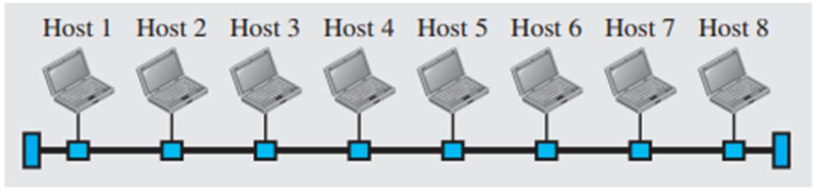
Advantages of ring topology: easy to install. Easy to add a new device or remove a device, only two connections should be changed. Fault detection is also easy.
Disadvantage: If one device fails, entire network stops working.
Used in olden types of LAN.

1.3 Network types:

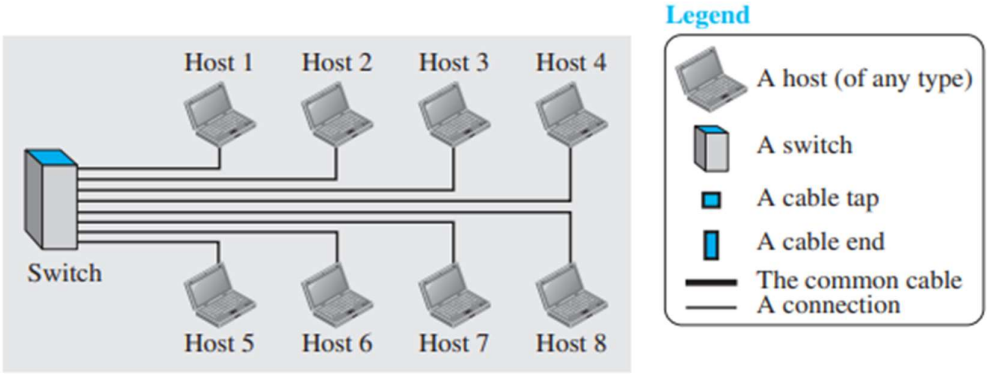
Different types of networks used today are discussed below

1.3.1 Local area network (LAN) – eg for a simple LAN is just one or two PCs and a printer at home office or the network in college. Each device in the LAN has an unique address. The message sent from one device to another will carry the source and destination device address.
In the past, all devices/hosts are connected through a common cable. Today LANs use a smart connecting switch.
LAN is normally limited in size, network within office, building or a campus.

Figure 1.8 *An isolated LAN in the past and today*



a. LAN with a common cable (past)



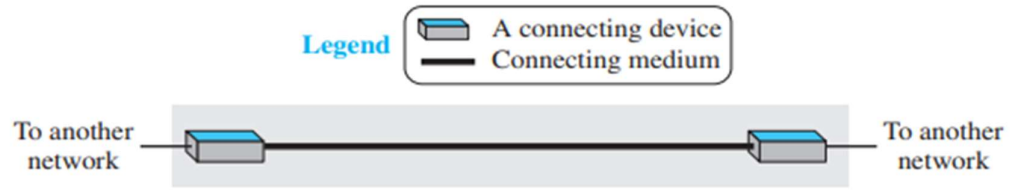
b. LAN with a switch (today)

1.3.2 – Wide area network

This is also an interconnection of devices. The network size is large compared to LAN. Networks span over a town, state, country or even world. There are two types of WANs.

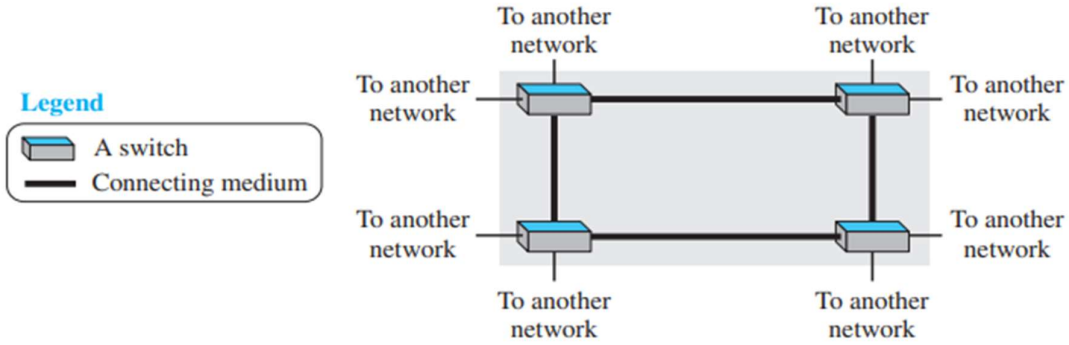
(a) Point to point WAN – is a network that connects two networks through a cable or air.

Figure 1.9 *A point-to-point WAN*



(b) Switched WAN – is a network that connects multiple networks.

Figure 1.10 *A switched WAN*

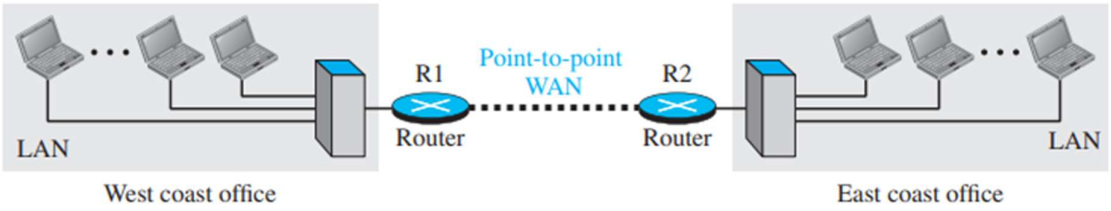


Internetwork:

Internetwork is an example for WAN. Largest internetwork is the Internet. It is a network with LANs and WANs connected together. Suppose, Infosys office in Bangalore has a LAN and Infosys office in USA has a LAN. To make the communication

between employees of these two offices possible, a point to point dedicated WAN from a service provider can be leased to connect these two LANs. This is called an internetwork or a private internet.

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

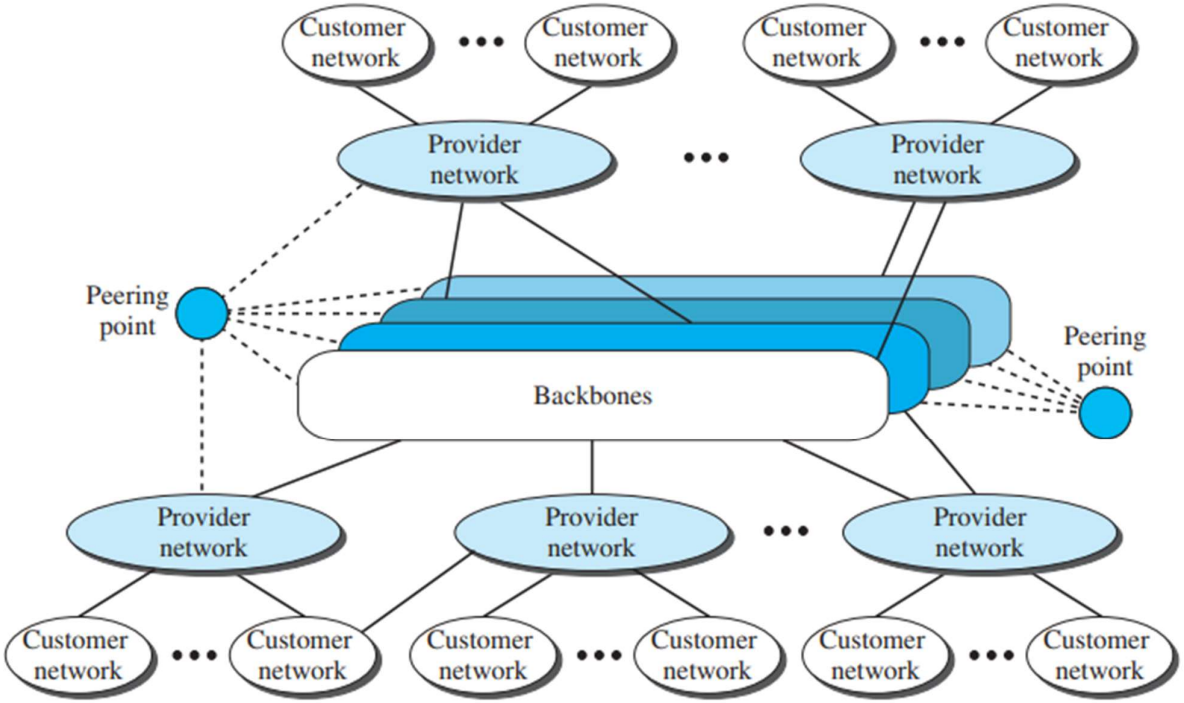


1.3.4 The Internet

This is the largest internetwork or internet.

Note: in this subject, internet means internetwork, many networks connected together. The Internet (with capital I) means our usual Internet. The Internet has many LAN, WAN and interconnected networks. Below fig shows a conceptual view of the Internet.

Figure 1.15 *The Internet today*



Backbones and provider networks are also called Internet Service Providers (ISPs). Eg: Airtel, Vodafone, etc

Accessing the Internet

a) Using Telephone Networks

b) Using Cable Networks

c) Using Wireless Networks

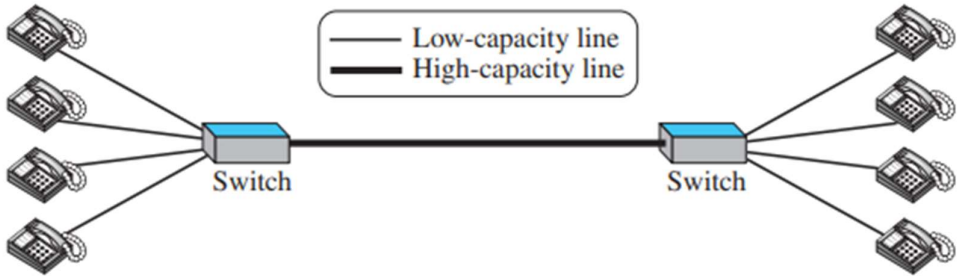
d) Direct Connection to the Internet

1.3.3 Switching

Internet is an eg for switched network. Here, switches are used to connect 2 networks. **Two common types of switched networks are circuit switched and packet switched network.**

(a) Circuit switched network: Here, between 2 end systems there is a dedicated connection. Each end system will have many devices like computer or phones etc. A switch is used to make the connection or break the connection.
Telephone networks in the past (landlines) used circuit switching.
In the example below, one end system has 4 telephones and other system has 4 lines. They are connected by a dedicated connection using 2 switches. Suppose user at phone 1 in first system wants to talk to user at phone 2 in second system, then, these 2 switches can make the connection.
Efficiency:
In this example, if the high capacity line has 4 times more capacity than low capacity line, then 4 people at one end can talk to 4 people at the other end. The high capacity line is efficiently utilized when 4 people at one end are talking to 4 people at other end. But, if only one person is talking, the high capacity line is not used efficiently. The capacity is wasted.

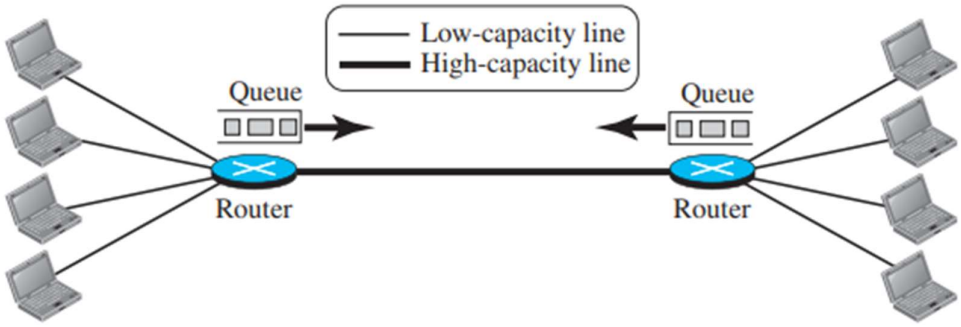
Figure 1.13 *A circuit-switched network*



(b) Packet switched network:
Here, the information from one computer in one system to the other computer in the other system is transmitted as blocks of data called **packets**. In this network, routers are used. Routers have a queue to store and forward the packets. In the below figure, if the high capacity line has 2 times more capacity than the low capacity lines, only 2 computers from one

side of the system can send data to 2 computers on the other system. If third computer sends data, that data will be stored in router. After the high capacity line becomes free, the router sends the packets waiting in its queue. But, in circuit switching network, this option to store data in switch is not there.

Figure 1.14 *A packet-switched network*



Network Models

2.1 PROTOCOL LAYERING

Protocols are rules that senders, receivers and all intermediate devices must follow for successful communication.

Communication between two devices in a network involves many tasks. Each task is handled by a separate layer. Each layer requires a protocol. (for eg, when you want to post a letter, you need to write the letter, put it in a envelop, write the address,

paste stamp and then put it in postbox. Similarly, in computer network also, there are many tasks to be done to send a data. Different layers handle different tasks.)

Advantage is: each layer can concentrate only on its tasks. If some functionality is not working, we need not debug every layer, only the responsible layer should be debugged.

2.1.2 Principles of Protocol Layering

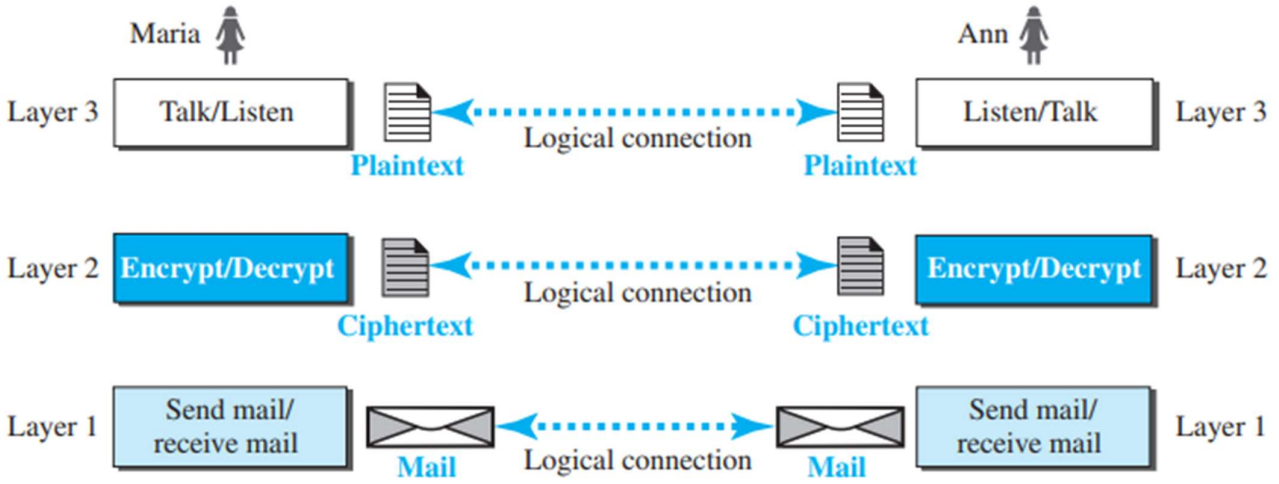
First principle - if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and talk (in the other direction).

Second Principle - two objects under each layer at both sites should be identical. If layer 2 at sender is responsible for address related work, layer 2 at receiver also should be responsible for address related work.

2.1.3 Logical Connections

There will be logical connection between each layer.

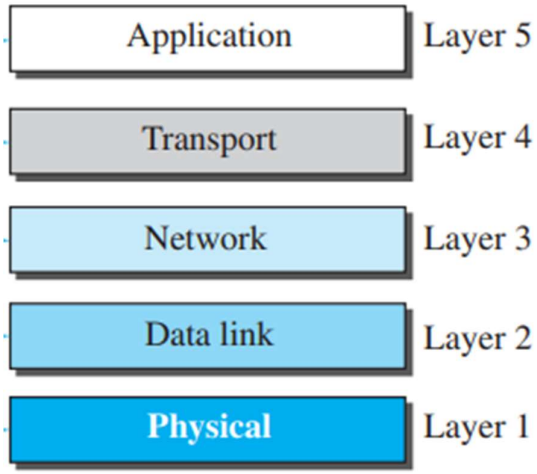
Figure 2.3 *Logical connection between peer layers*



TCP/IP, is a framework for organizing the set of communication protocols used in the Internet and similar computer networks

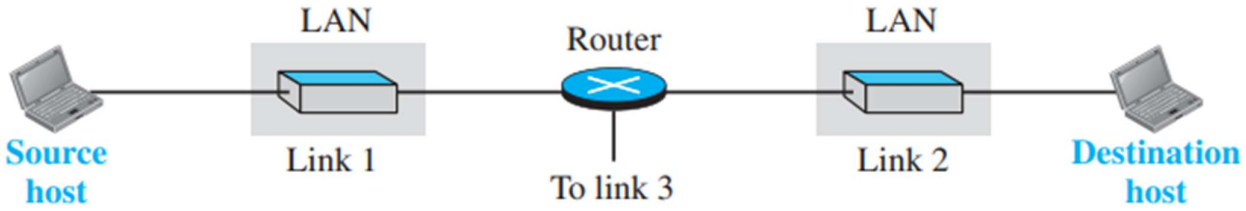
2.2 TCP/IP PROTOCOL SUITE - (Transmission Control Protocol/Internet Protocol).

This is a set of protocols for different layers. Here each lower level protocol provides service to upper level protocols. It has 5 layers.



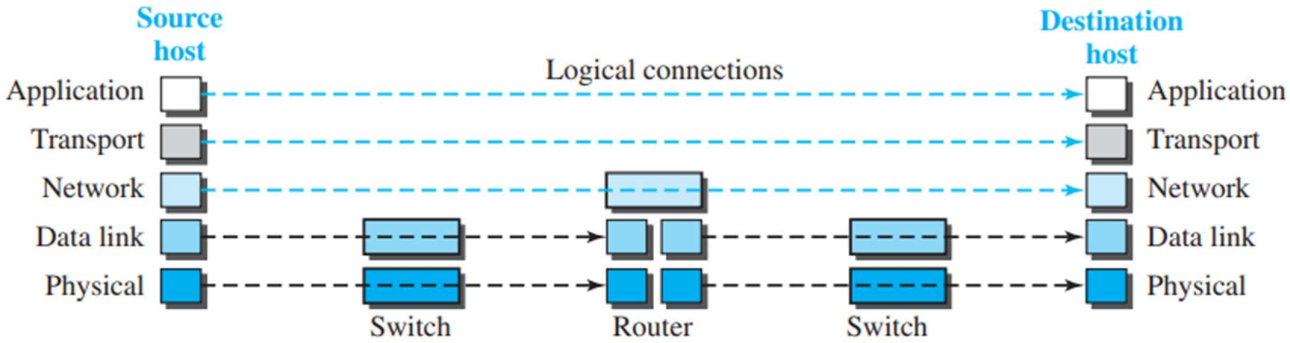
2.2.2 Layers in the TCP/IP Protocol Suite

Consider a simple network where A wants to communicate with B. Here there are 5 communicating devices in this network.



To better understand the duties of each layer, we need to think about the logical connections between layers. Figure 2.6 shows logical connections

Figure 2.6 *Logical connections between layers of the TCP/IP protocol suite*



Remember each layer is responsible for some tasks. Different communication devices have different set of layers based on their tasks. A router has no application and transport layer because router does not do those tasks. (for eg, while sending a letter using normal post, the task of pasting stamp is done only at the sender. The task is not repeated in post office again. Similarly, tasks of application layer and transport layer are not repeated again in router. But, tasks of data link layer is repeated in router, switch etc).

2.2.3 Description of Each Layer

What each layer does?

1. Application Layer
    - Communication at the application layer is between two processes (two programs running at this layer).
    - To communicate, a process sends a request to the other process and receives a response
    - The application layer in the Internet includes many protocols like Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Domain Name System (DNS) etc
2. Transport Layer

- This layer receives message from application layer
- This message is encapsulated in a transport layer packet (called a segment or a user datagram in different protocols)
- This layer gives services to application layer
- There are a few transport-layer protocols in the Internet
- The main protocol of this layer is Transmission Control Protocol (TCP).
    - This establishes a logical connection (like a pipe) for sending data from source machine to destination machine.
    - This protocol also provides flow control, error control and congestion control
    - (flow control: senders data rate and receivers data rate should match. Sender cannot send more data than what receiver can handle.
    - error control : to guarantee that the segments arrive at the destination without error and resending the corrupted ones
    - congestion control: if network is congested, sending further more traffic to network should be controlled.)
- User Datagram Protocol (UDP) is another main protocol of transport layer.
    - This is connectionless. This doesn't create logical connection before sending data. Each packet can take different route. It does not provide flow, error, or congestion control. Therefore small overhead. Useful to send short messages.

3. Network Layer
    - This is responsible for connection between source to destination (not at the link level).
    - The Internet uses Internet protocol (IP) at the network layer
    - The data forwarded by this layer is called a datagram.
    - This layer is responsible for the format and structure of addresses.
    - It is also responsible for routing (sending packets through best path) from source to destination. The path will have many routers. The data should pass through many routers and each router will choose the best path and forward the data to next router. Finally data must reach destination machine.
    - Network layer also has some additional protocols to help IP. The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet. The Internet Group Management Protocol (IGMP) is another

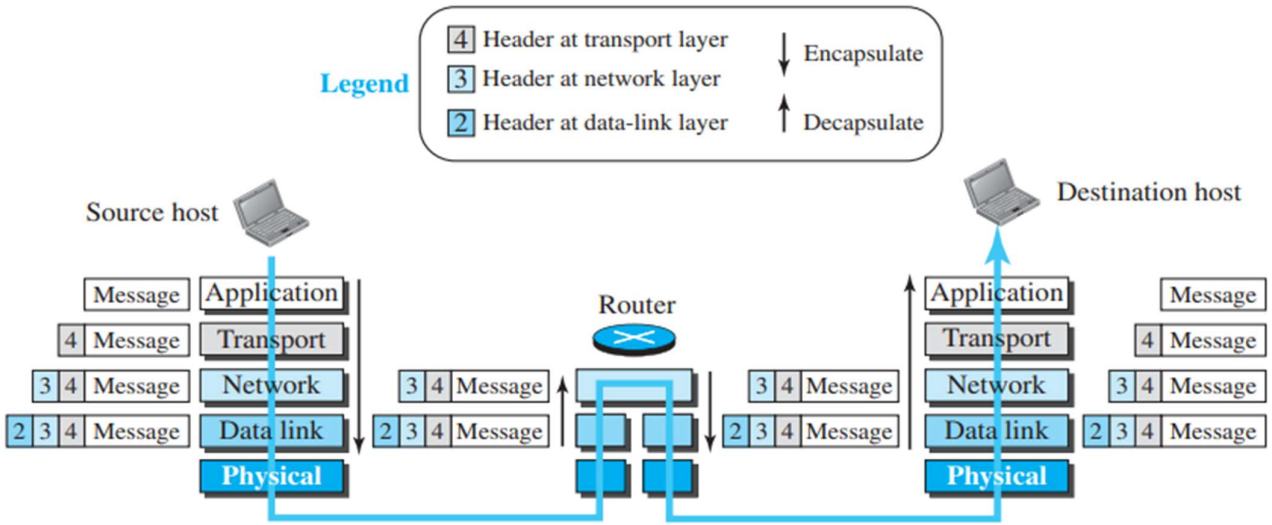
protocol that helps IP in multitasking. The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host. The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address.

- This layer gives service to transport layer

4. Data-link Layer:
    - This layer receives datagram from the network layer, encapsulates the received data in a packet called a frame.
    - TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols.
    - It works at the link level
    - This layer gives service to network layer
5. Physical layer:
    - Lowest level
    - Responsible for carrying **bits.**
    - transmission medium (cable or air) is below this layer. The bits are converted to electrical or optical signal and sent through the cable.
    - Data link layer is above physical layer. Data link layer sends frames to physical layer. Physical layer sends bits of frames through cables as electrical or optical signals.
    - This layer gives service to data link layer

2.2.4 Encapsulation and Decapsulation

Figure 2.8 *Encapsulation/Decapsulation*



Encapsulation at the Source Host:

At the source, we have only encapsulation.

At the **application layer**, the data to be exchanged is referred to as a **message**.

The message is passed to the transport layer.

The **transport layer** takes the message and adds the transport layer header such as **source and destination program id**, and some other information required for flow control and error control. This message from **application layer protocol + the added header is called the segment** (in TCP) and the **user datagram** (in UDP). The transport layer then passes the packet to the network layer.

The **network layer** takes the transport-layer packet and **adds** header such as **addresses of the source and destination** and some more information used for **error checking** of the header and so on. **Transport layer packet + header is called datagram**. The network layer then passes the datagram to the data-link layer.

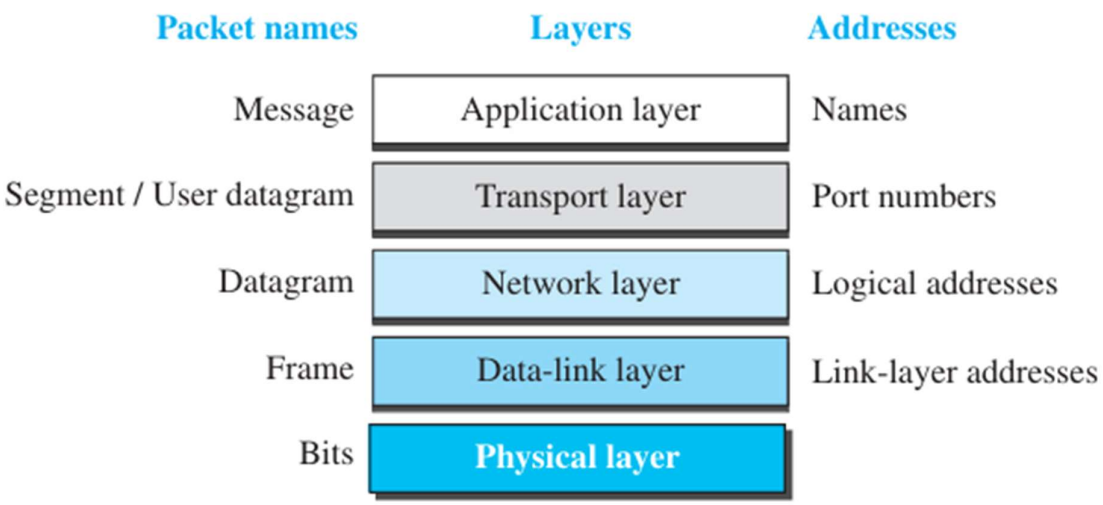
The **data-link layer** takes the network-layer packet , adds its header such as link-layer addresses of the host or **the next hop**. The **network layer packet + overhead** = **frame**. **Frame is sent to physical layer** for transmission.

Decapsulation and Encapsulation at the Router:
At the router, we have both decapsulation and encapsulation.
Router has only 3 layers.
Physical layer receives data from source machine. Physical layer **removes its header** and passes the frame to data link layer. Data link layer removes its header and passes the data to network layer. Network layer removes its header. The header will have source and destination address. Based on this, **it identifies the next router** where the packet should be sent. It **adds new header** with this new information. Sends the data to data link layer. Data link layer adds its header and sends data to physical layer. Physical layer adds its header and sends the data to next router or destination machine.

Decapsulation at the Destination Host
Finally at the destination machine, each layer removes its header and passes the data to the next higher layer. Finally, application layer receives the required message.

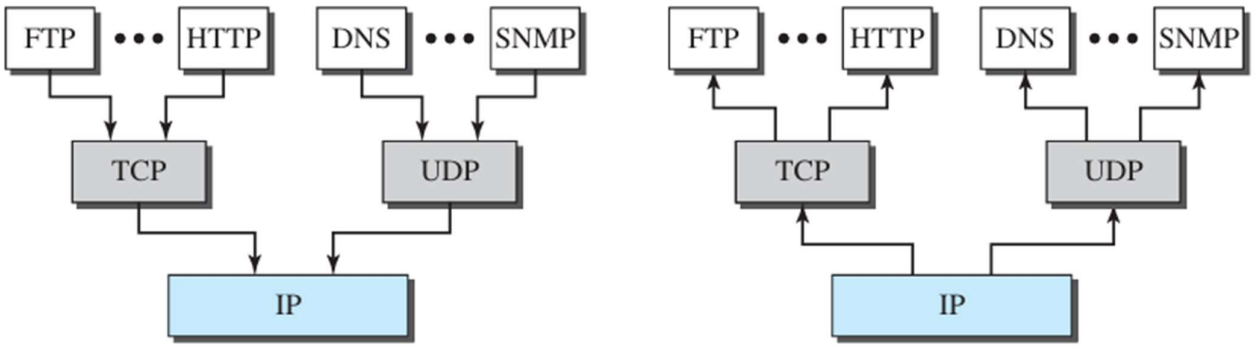
2.2.5 Addressing
For sending a data from source to destination, we require source address and destination address. Each layer requires different types of address. For eg, in application layer, the address is in the form of website name or email address. Transport layer uses port number as address. (Port numbers are local addresses that distinguish between several programs running at the same time). Network layer uses IP address that is unique to the whole Internet. Link layer uses MAC address, which is local to LAN or WAN.

Figure 2.9 *Addressing in the TCP/IP protocol suite*



2.2.6 Multiplexing and Demultiplexing (one to many and many to one)

Figure 2.10 *Multiplexing and demultiplexing*



a. Multiplexing at source

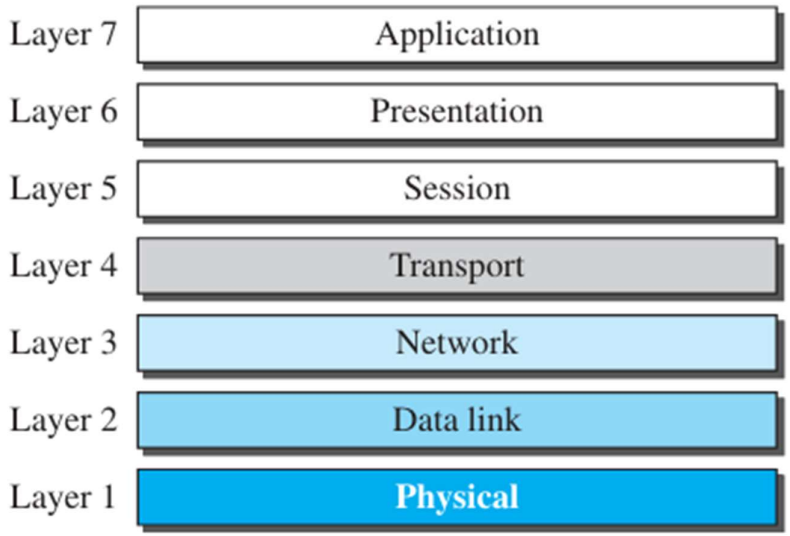
b. Demultiplexing at destination

As there are many protocols at some layers, a lower layer should be able to encapsulate a packet from several next-higher layer protocols (one at a time); demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).

2.3 THE OSI MODEL

This is another protocol suite similar to TCP/IP.
Open Systems Interconnection (OSI) model was first introduced in the late 1970s.
It has 7 layers.

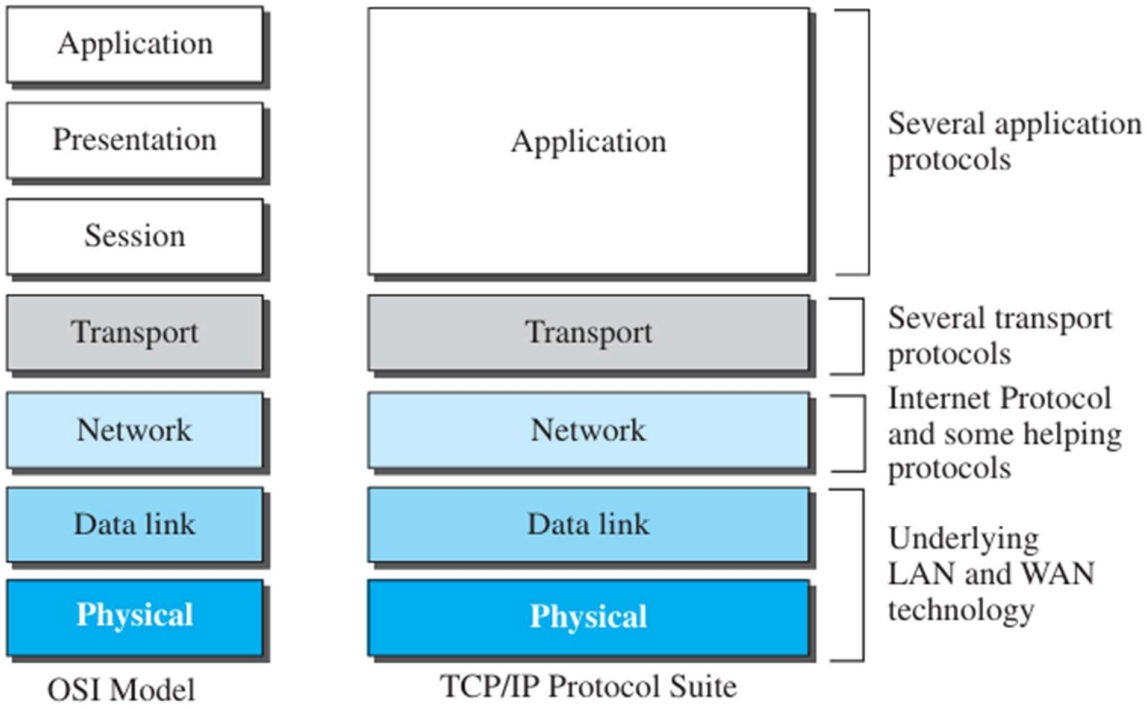
Figure 2.11 *The OSI model*



2.3.1 OSI versus TCP/IP

The application layer in TCP/IP is the combination of three layers in the OSI model

Figure 2.12 *TCP/IP and OSI model*



2.3.2 Lack of OSI Model's Success

The OSI model appeared after the TCP/IP protocol suite. Everyone thought that the TCP/IP protocol would be fully replaced by the OSI model. This did not happen for the below reasons

1. All were already using TCP/IP. Changing again would be costly
2. Some layers like session and presentation layers are not fully defined
3. When 1-2 organizations tried implementing OSI model, they did not see much high performance improvement

Introduction to Physical Layer

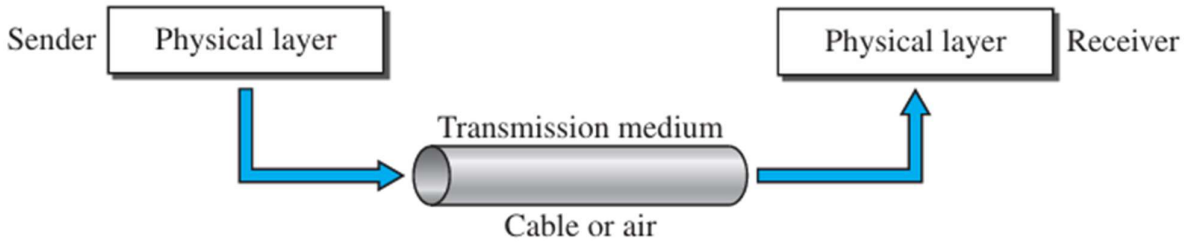
The **Physical Layer** in the **TCP/IP** model corresponds to the lowest layer responsible for the actual transmission of raw data bits over a physical medium, such as cables, wireless signals, or fibre optics.

Transmission Media

7.1 INTRODUCTION

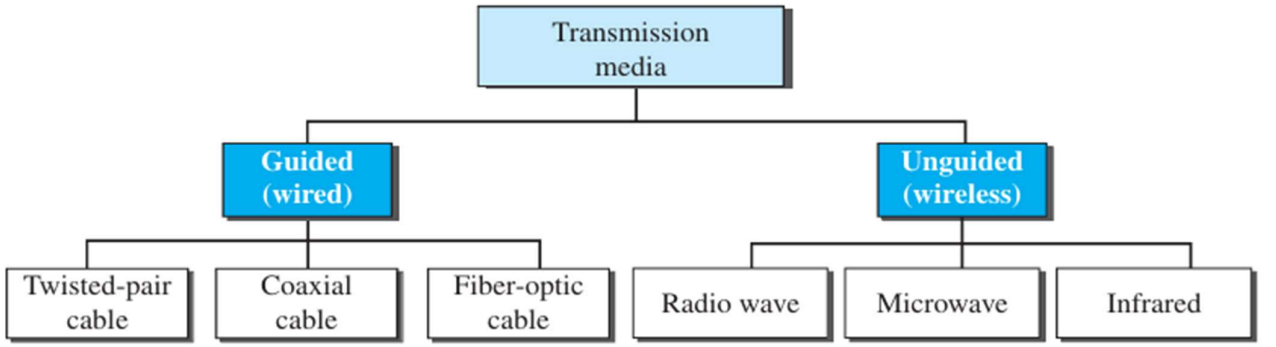
Transmission media is the actual media such as air or optical cable that is used to send the data. This lies below the physical layer.

Figure 7.1 *Transmission medium and physical layer*



transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

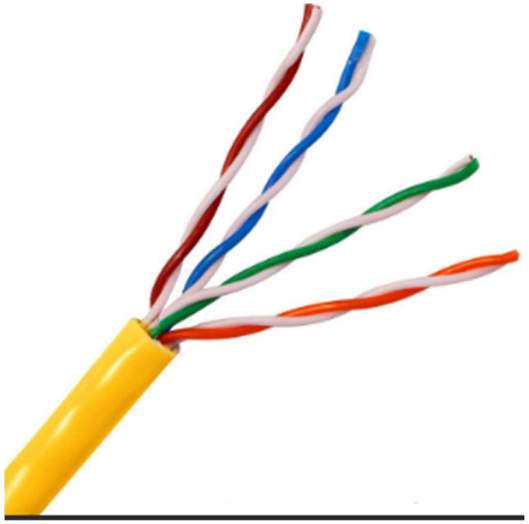
Figure 7.2 *Classes of transmission media*



7.2 GUIDED MEDIA

Eg for guided media - twisted-pair cable, coaxial cable, and fiber-optic cable

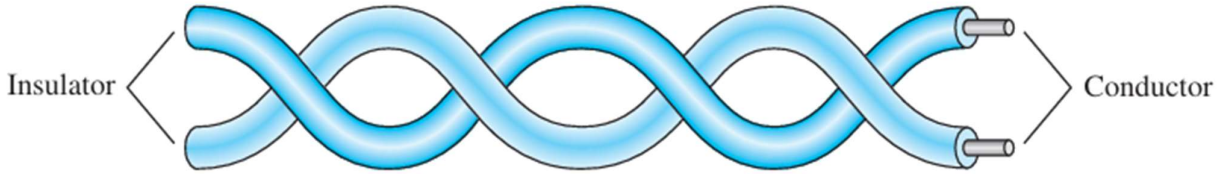
7.2.1 Twisted-Pair Cable



A twisted pair consists of two copper conductors (wires), each with its own plastic insulation, twisted together.

They are used in telephone lines.

Figure 7.3 *Twisted-pair cable*

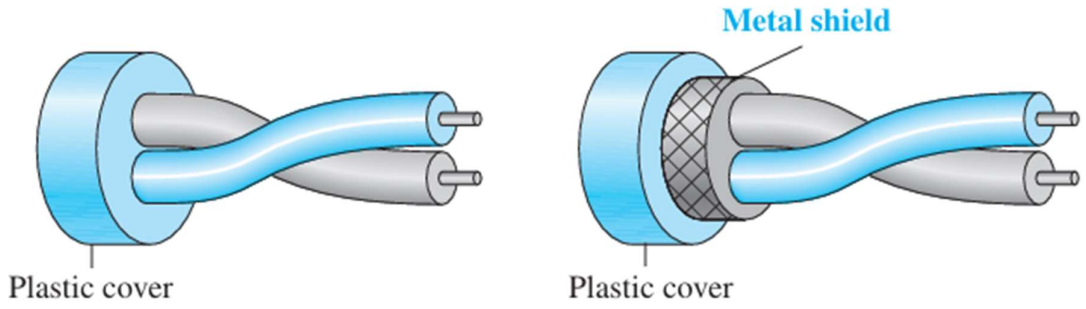


Here data is carried in terms of electric current. One wire carries data as electric signal and other is a ground reference
Wires are twisted to balance the noise (twisted so that each wire will have same noise level)
Receiver calculates the difference between the wire with the signal and ground. With equal noise, the noise gets cancelled out.
Quality depends on the number of twists per unit of length

Unshielded Versus Shielded Twisted-Pair Cable

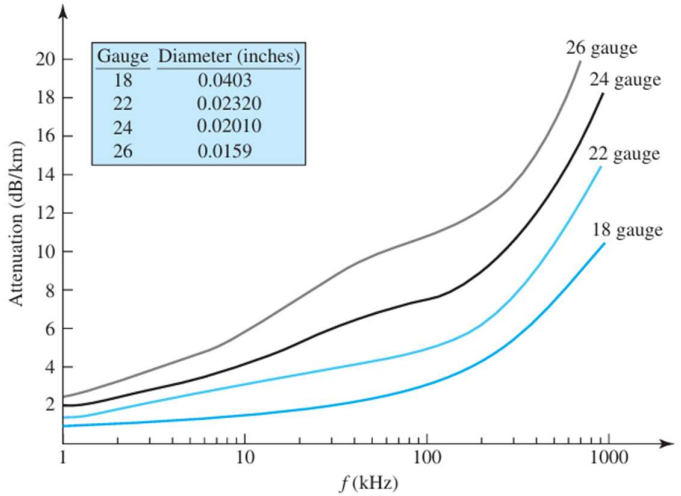
shielded twisted-pair has a metal foil or braided mesh covering for each pair of insulated conductors. This metal casing improves the quality but it increases the cable size and expensive.

Figure 7.4 *UTP and STP cables*



Unshielded twisted pair cables can be classified into 7 categories based on cable quality. Category 1 is lowest quality, 7 is highest.
UTP uses RJ45 connector .
Performance of UTP can be measured as attenuation at different frequencies.
As shown in below fig, with increase in frequency, attenuation increases. The increase is very sharp after 100kHz.

Figure 7.6 *UTP performance*

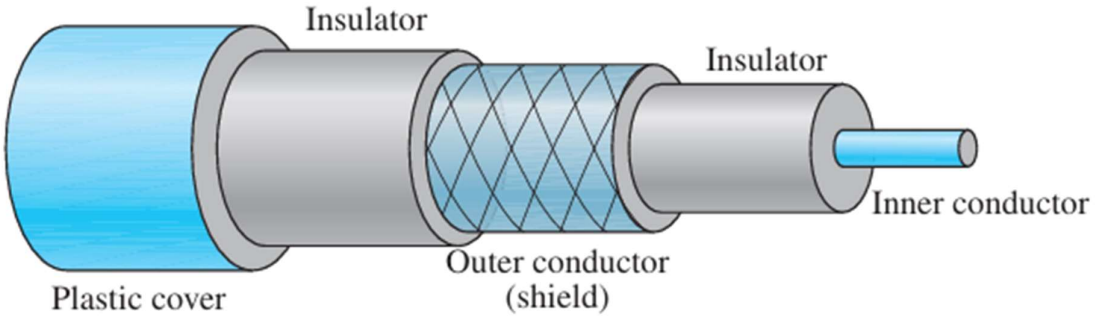


Note that gauge is a measure of the thickness of the wire.

7.2.2 Coaxial Cable

Coaxial cables can carry higher frequency signals.
Coaxial cable has a central core (inner conductor), enclosed in an insulator, which is enclosed in an outer conductor. The outer conductor provides protection against noise. This outer conductor has another insulator cover and the whole cable is protected by a plastic cover.

Figure 7.7 *Coaxial cable*



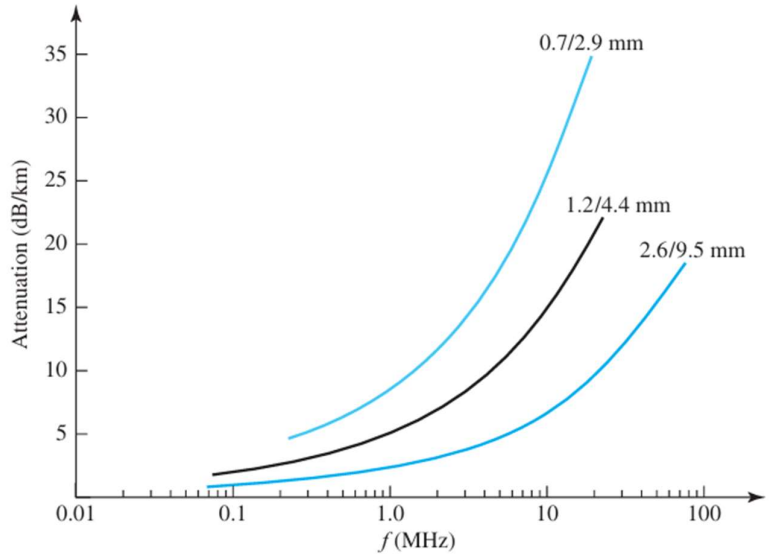
Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes the wire gauge of the inner conductor, thickness and type of inner insulator, etc.

Table 7.2 *Categories of coaxial cables*

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

To connect coaxial cable to devices Bayonet Neill-Concelman (BNC) connectors are used.
Performance can be measured as attenuation at different frequencies.

Figure 7.9 *Coaxial cable performance*



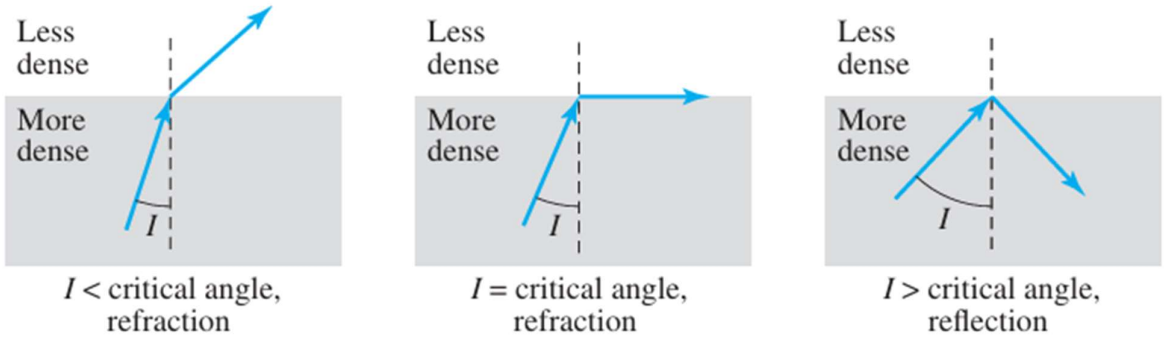
From the above figure we can see that, attenuation is low at lower frequencies. Attenuation increases rapidly with increase in frequency. In that case repeaters should be used.

Coaxial cables were used in analog telephone networks and digital telephone networks. In Analog telephone networks, one cable could carry 10000 voice signals and in digital network, one cable could carry 600Mbps. However, now its being replaced by optical fibres.
Ethernet LAN and cable TV networks also used coaxial cables.

7.2.3 Fiber-Optic Cable

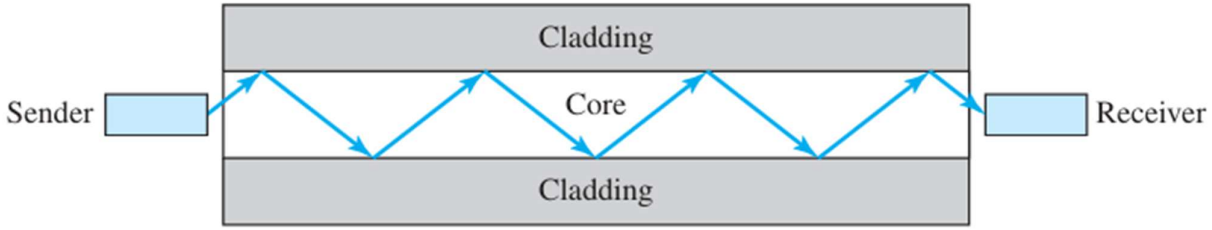
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. The ray reflects or refracts based on the angle of incidence.

Figure 7.10 *Bending of light ray*



Optical fibres use reflection property as in below fig. The fibres will have glass or plastic core which is surrounded by cladding. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Figure 7.11 *Optical fiber*

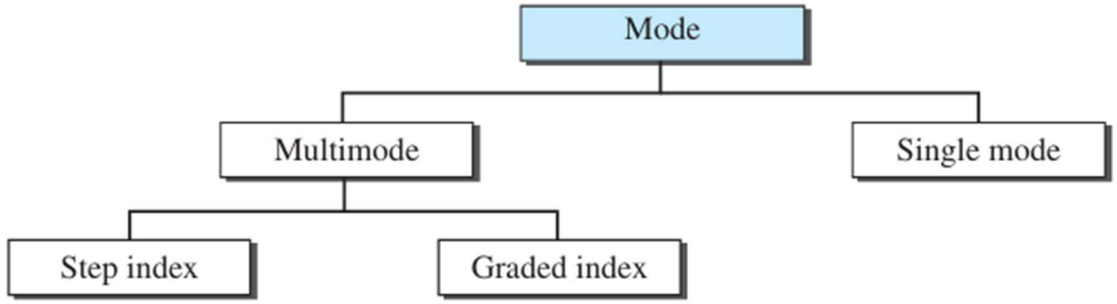


Propagation Modes

multimode and single mode

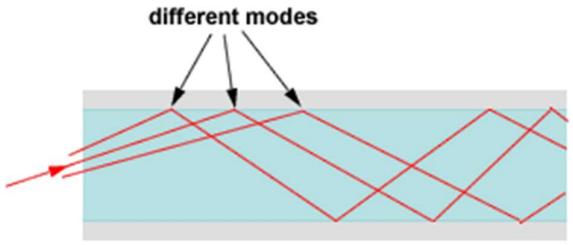
Multi mode can be implemented in two forms: step-index or graded-index

Figure 7.12 *Propagation modes*

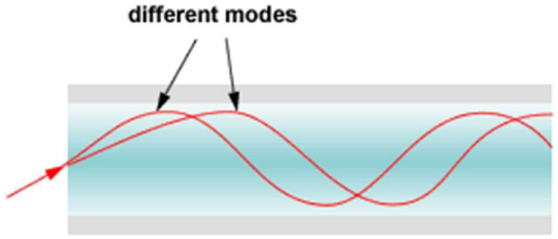


multimode step-index fiber: the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion.

multimode graded-index fiber: Density is highest at the center of the core and decreases gradually to its lowest at the edge.



Step-Index Multimode Fiber



Graded-Index Multimode Fiber

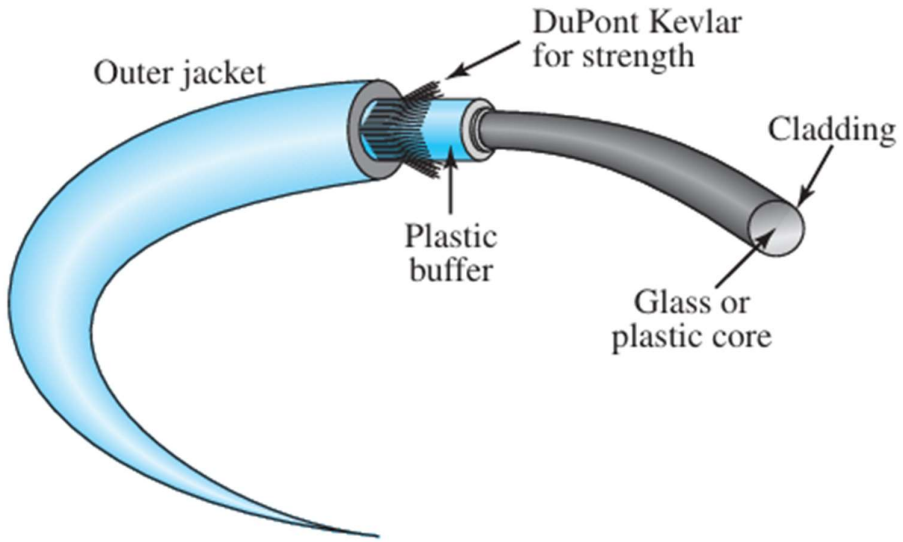
Single-Mode: **If the fiber's diameter is reduced** to a few wavelengths of light the fiber acts like a wave guide and the light can propagate only in a straight line, without bouncing, yielding a **single-mode fiber**. **Single-mode fibers are more expensive** but are widely used for longer distances.

Fiber Sizes 195 Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding

Table 7.3 *Fiber types*

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

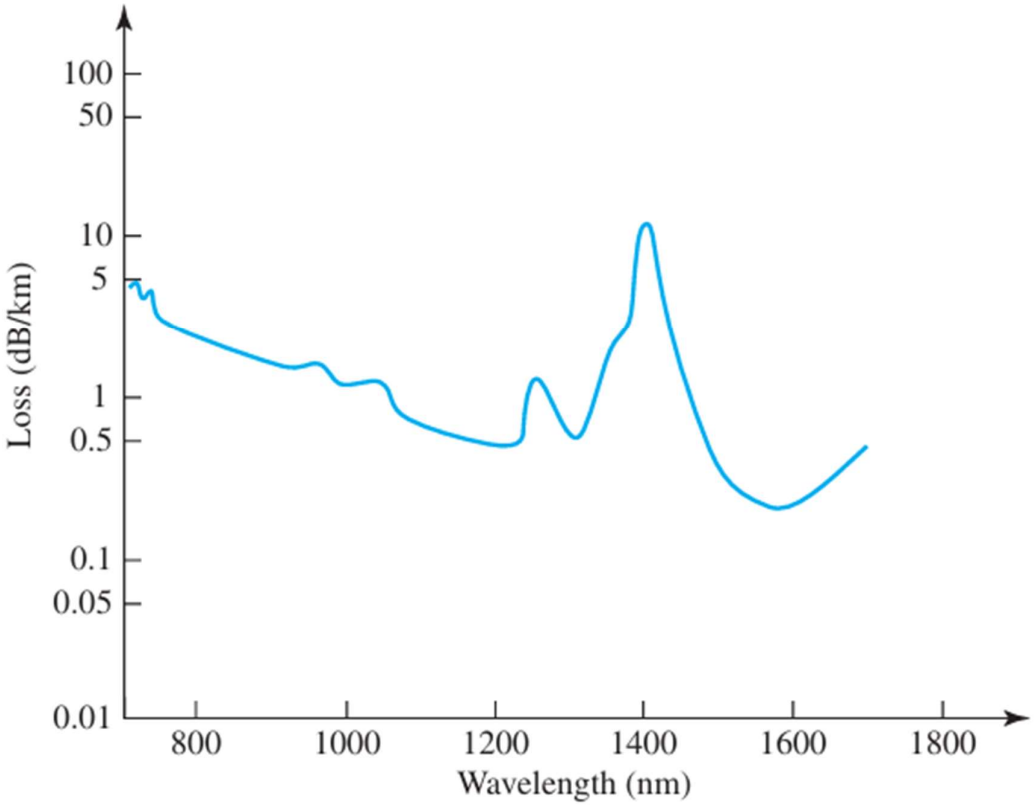
Figure 7.14 *Fiber construction*



Fiber-Optic Cable Connectors :
There are three types of connectors
subscriber channel (SC) connector, straight-tip (ST) connector and MT-RJ

Performance of fiber optics is shown below. It can be observed that, attenuation in fiber optics is less than twisted pair and coaxial

Figure 7.16 *Optical fiber performance*



Application – cable TV, internet, LAN

Advantages:

Higher bandwidth. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable.

Less signal attenuation. Fiber-optic transmission distance is significantly greater than that of other guided media.

Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.

Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.
Light weight. Fiber-optic cables are much lighter than copper cables.
Greater immunity to tapping. Fiber-optic cables are more immune to tapping than copper cables.

Disadvantages :
Installation and maintenance. Fiber optics are sensitive and require specific handling techniques to prevent damage.
Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
Cost. The cable and the interfaces are relatively more expensive than those of other guided media.

7.3 UNGUIDED MEDIA:
WIRELESS communication:

Audio or data signals are typically low-frequency signals that cannot travel long distances in free space (The frequency range of the human voice typically falls between **85 Hz** and **255 Hz**).

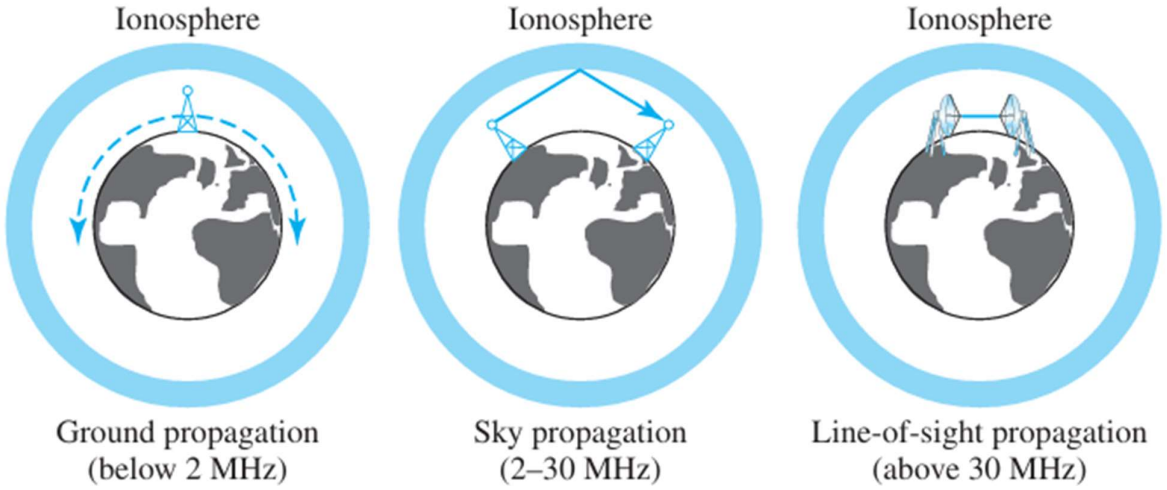
> **Modulating** these low-frequency signals onto a high-frequency carrier wave allows the signals to travel much farther and more efficiently through the atmosphere. Modulation in wireless communication is the process of varying one or more properties of a **carrier signal** (such as amplitude, frequency, or phase) in order to transmit information, typically in the form of data, voice, or video. The carrier signal is a high-frequency signal that can be easily transmitted over the air, while the information signal is typically a lower-frequency signal that contains the actual message or data.
> Modulation allows the information to be transmitted over long distances, makes more efficient use of the available frequency spectrum, and helps overcome interference and noise.

Electromagnetic (EM) waves are used as carrier signals for wireless communication because they possess several properties that make them ideal for transmitting information over long distances, across various environments, and through different media. Electromagnetic waves from 3 kHz to 900 THz are used for sending data
Different frequency ranges are used in different applications.
Eg: 300 kHz–3 MHz – AM Radio, 3–30 MHz – aircraft, 30–300 MHz – TV and FM Radio, 300 MHz–3 GHz – cellular phones

Signals are normally broadcast through free space/air and thus are available to anyone

Unguided signals can travel from the source to the destination in several ways: ground propagation, sky propagation, and line-of-sight propagation

Figure 7.18 *Propagation methods*



In ground propagation, low frequency radio waves (below 2MHz) from antenna travel through the lowest portion of the atmosphere, hugging the earth. Here, the radio waves follow the Earth's contour rather than dispersing into space. Distance depends on the amount of power in the signal. Ground propagation is commonly used for AM radio broadcasting, and some military applications. **Sea water** is highly conductive and allows ground waves to travel farther (up to 500 to 2,000 km). Over land, the typical range for ground wave propagation is **50 to 300 km**. AM radio stations, operating in the frequency range of 500 kHz to 1.6 MHz, can typically achieve **ground wave ranges of 100 to 300 km** over land, and much farther over water (up to 1,000 km or more).

In sky propagation, higher-frequency radio waves (typically between 3 MHz and 30 MHz) are radiated upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances. Radio waves can undergo multiple reflections between the ionosphere and the Earth's surface, allowing them to cover thousands of kilometers in a "hopping" manner. Each reflection is referred to as a "hop." With enough hops, signals can travel halfway around the world. Skywave propagation is frequency-dependent. Frequencies that are too low can be absorbed by the ionosphere, while frequencies that are too high may pass through the ionosphere and not reflect back to Earth. The optimal frequency range for skywave propagation is typically in the HF band (3 to 30 MHz). **Shortwave Radio**: This is widely used for international broadcasting, allowing radio stations to reach global audiences.

In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and tall so that communication is not affected by the curvature of the earth. **Line of Sight (LOS) propagation** is a method of radio wave transmission in which the signal travels directly from the transmitter to the receiver in a straight line, without any significant obstructions such as buildings, hills, or the curvature of the Earth. This type of propagation is essential for high-frequency signals, especially those used in microwave, satellite, television, and cellular communications.

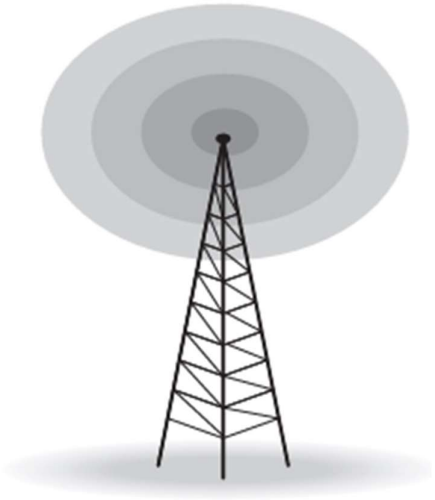
We can divide wireless transmission into three broad groups: radio waves, micro waves, and infrared waves.

Radio waves:

- electromagnetic waves ranging in frequencies between **3 kHz and 1 GHz** are normally called radio waves;
- Radio waves, for the most part, are **omnidirectional**. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- But, The omnidirectional property has a disadvantage. The radio waves transmitted by one antenna are susceptible **to interference by another antenna that may send signals using the same frequency** or band.
- radio waves are a good candidate for long-distance broadcasting such as AM and FM radio, television, cordless phones, and paging.

- Radio waves **can penetrate walls**. Because of this property, we can receive AM radio inside the building. But disadvantage is, we cannot isolate a communication to just inside or outside a building.
- Radio waves use omnidirectional antennas that send out signals in all directions.

Omnidirectional antenna



-

7.3.2 Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves. **Microwaves are unidirectional. When an antenna transmits microwaves, the sending and receiving antennas need to be aligned.**

Advantage is – because they are directional, they don't interfere with other transmissions

characteristics of microwave propagation:

Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. If not, the curvature of the earth and other blocking obstacles block the communication.

Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.

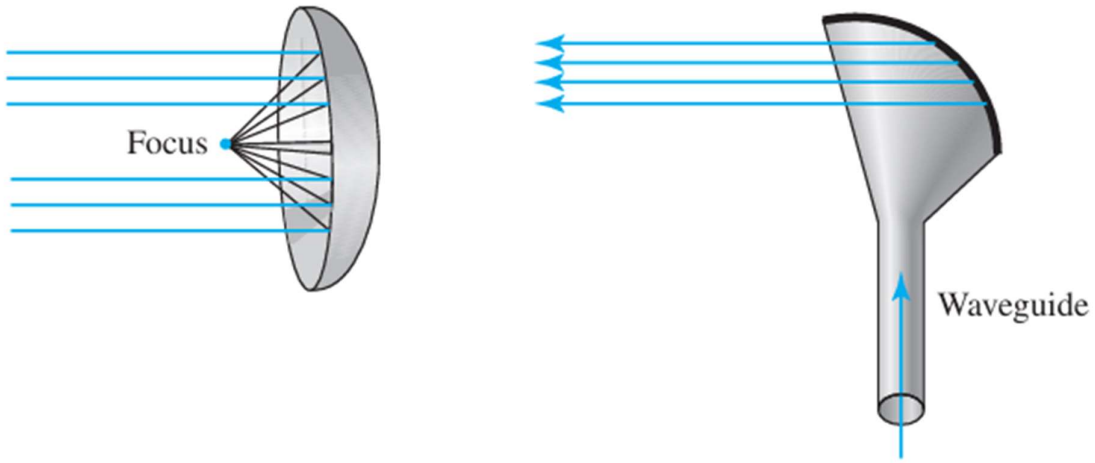
The microwave band is relatively wide, almost 299 GHz. Therefore high data rate is possible.

Use of certain portions of the band requires permission from authorities

Unidirectional Antenna:

Two types of antennas are used for microwave communications: the parabolic dish and the horn

Figure 7.20 *Unidirectional antennas*



a. Parabolic dish antenna b. Horn antenna

Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

7.3.3 Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for **short-range communication**.

Infrared communication generally requires a **line-of-sight** path between the transmitter and receiver

Infrared waves **cannot penetrate walls**. Therefore, when we use our infrared remote control, we do not interfere with the use of the remote by our neighbors.

However, because of this, infrared signals are useless for long-range communication.

In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Application: remote control, for communication between devices such as keyboards, mice, PCs, and printers.

(For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC. the IrDA port on the keyboard needs to point to the PC for transmission to occur)

8.3 PACKET SWITCHING

Packet switching is a type of data communication method. Here, the data is divided into small packets and sent through packet switched network. In packet switching, there is no resource allocation, or reserved bandwidth or reserved path for data communication.

Resources are allocated on demand.

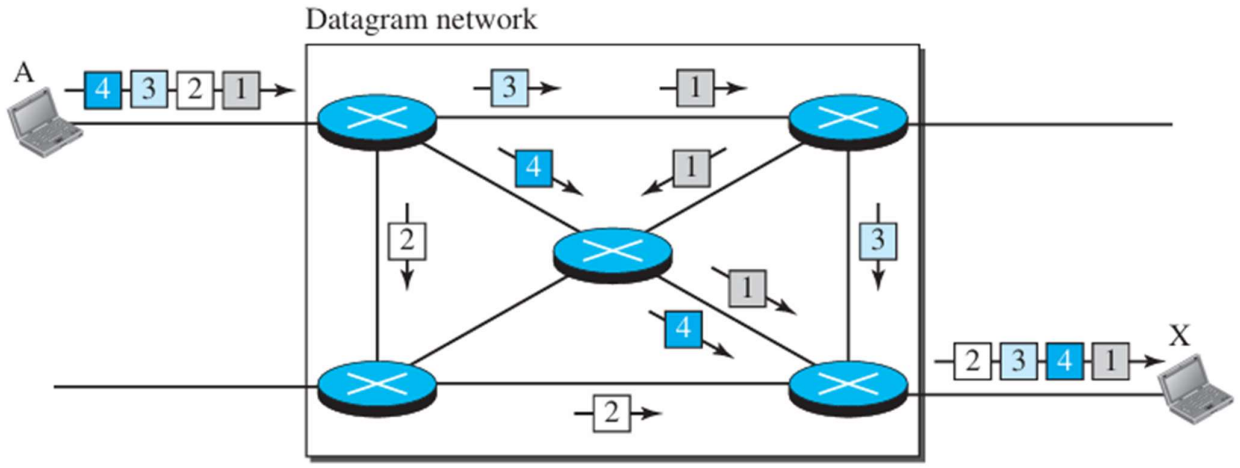
The allocation is done on a first come, first-served basis. When a switch receives a packet, no matter what the source or destination is, the packet must wait if there are other packets being processed.

two types of packet-switched networks: datagram networks and virtual circuit networks.

8.3.1 Datagram Networks- Here, each packet is treated independently. If a single message is broken down into small packets, each packet is treated as an independent packet.

Packets in this type of method are referred to as datagrams.

Figure 8.7 *A datagram network with four switches (routers)*



In the above figure, one big message is divided into 4 small packets. These packets take different routes based on the availability of resources. If there is not enough resource, the packet is sent through different path where there are resources. Therefore, packets may be received at different order in the receiver. If there are not enough resources, packets may be dropped also. It is the responsibility of the upper layers to rearrange them in correct order.

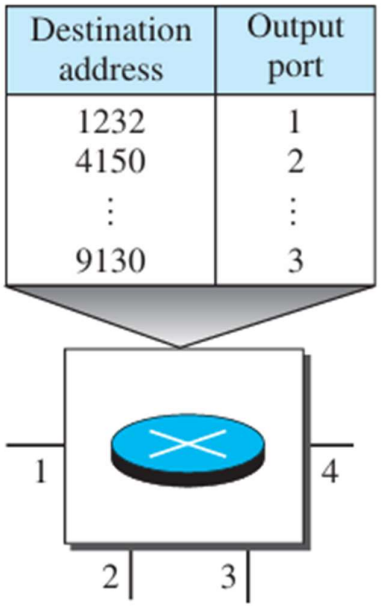
The datagram networks are sometimes referred to as connectionless networks.

Routing Table –

If there is no fixed path, how the packets know where to go?

Here, each switch/router will have a routing table. The table will have list of destination addresses and the corresponding forwarding port numbers. The tables are updated periodically.

Figure 8.8 *Routing table in a datagram network*

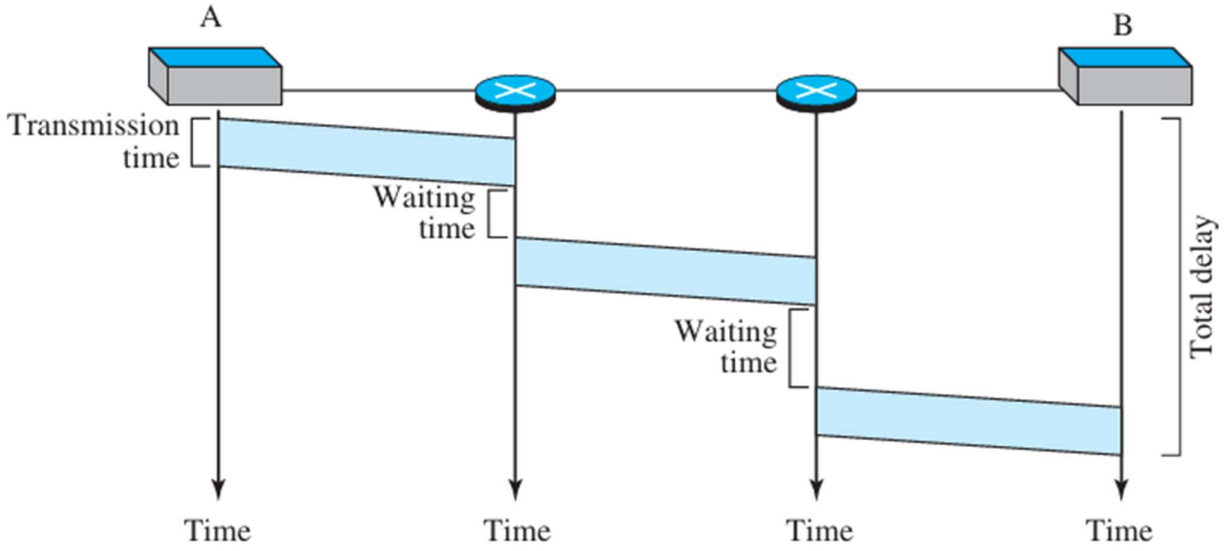


Every packet in the datagram carries an additional header field with few important information such as destination address. When the packet arrives at the switch, its destination address is checked. The routing table will have details like if the destination address is 4150, the packet should be forwarded to port 2. Based on the destination address, the packet is forwarded to corresponding port as mentioned in the routing table.

Efficiency of datagram network is better because resources are not reserved for any packet. Resources are allocated only when a packet arrives. If a source sends a packet and there is a delay before sending the next packet, the network can be used for sending data from other sources.

Delay in a datagram network is high, because each packet may experience a delay at the switch. Also, since different packets are transmitted through different routes, each packet experiences a different delay.

Figure 8.9 *Delay in a datagram network*



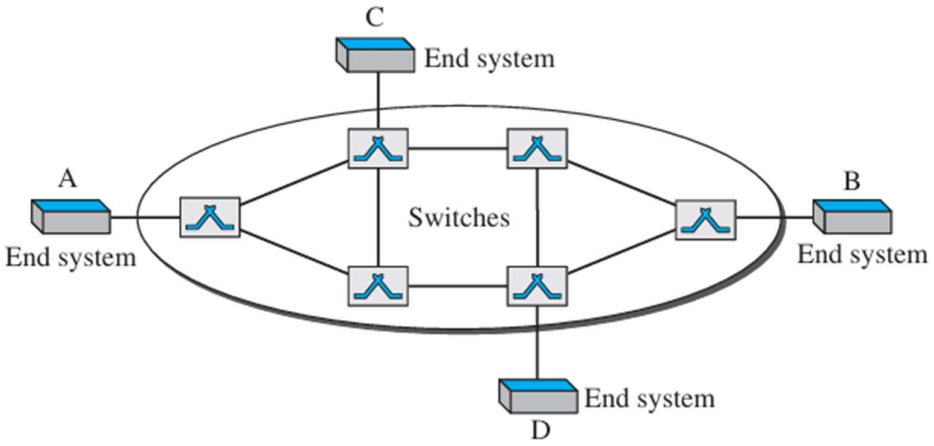
Total delay = 3T + 3τ + w1 + w2, where T is transmission time, τ is propagation delay, w1 and w2 are waiting times.

8.3.2 Virtual-Circuit Networks

Characteristics:

1. It has 3 phases. Setup, data transfer and teardown.
2. Resources can be allocated in the setup phase or on demand during data transfer.
3. All packets follow the same path established during the connection
4. Similar to datagram network, the message is converted into packets and each packet carries destination address. However, the destination address is only a local address.

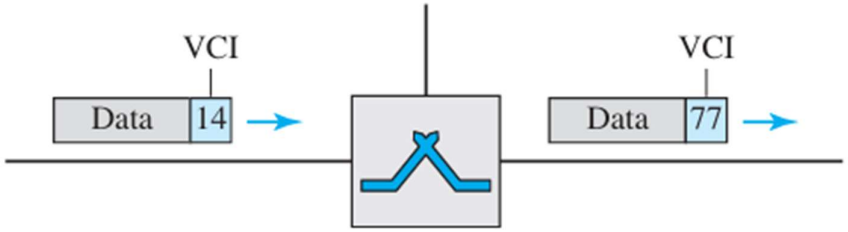
Figure 8.10 *Virtual-circuit network*



In a virtual-circuit network, two types of addressing are involved: global and local
Global addressing: address that can be unique in the scope of the network or internationally if the network is part of an international network. Source or destination needs to have a global address

Local addressing (Virtual-Circuit Identifier): It is a small number that has only switch scope; When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.

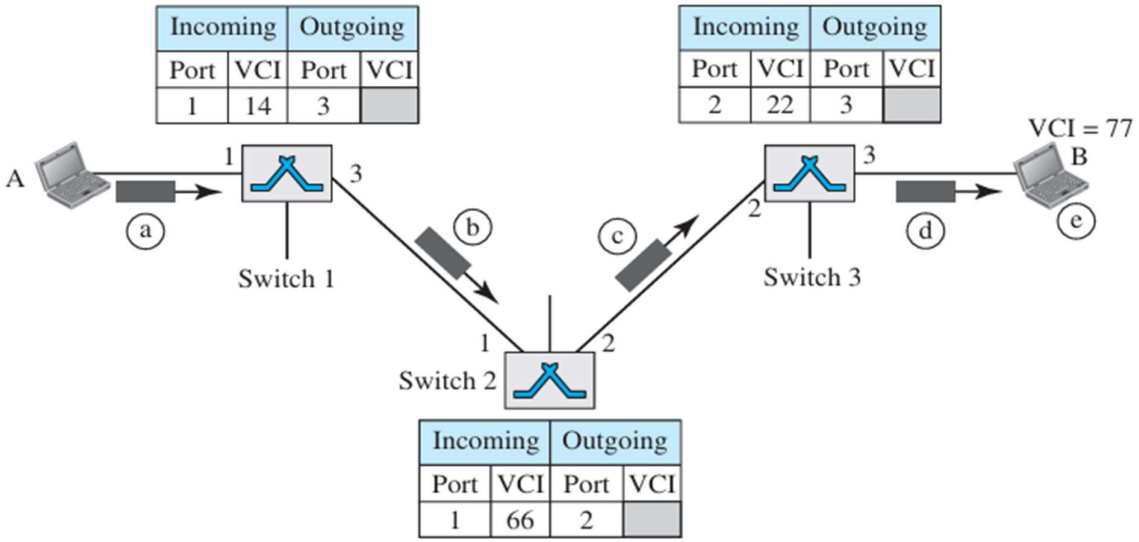
Figure 8.11 *Virtual-circuit identifier*



Three Phases

1. **Setup phase:**
   suppose source A needs to send data to Source B, Two steps are required in setup phase: the setup request and the acknowledgment.
   Setup request:
   A setup request frame is sent from the source to the destination. Figure 8.14 shows the process.

Figure 8.14 *Setup request in a virtual-circuit network*

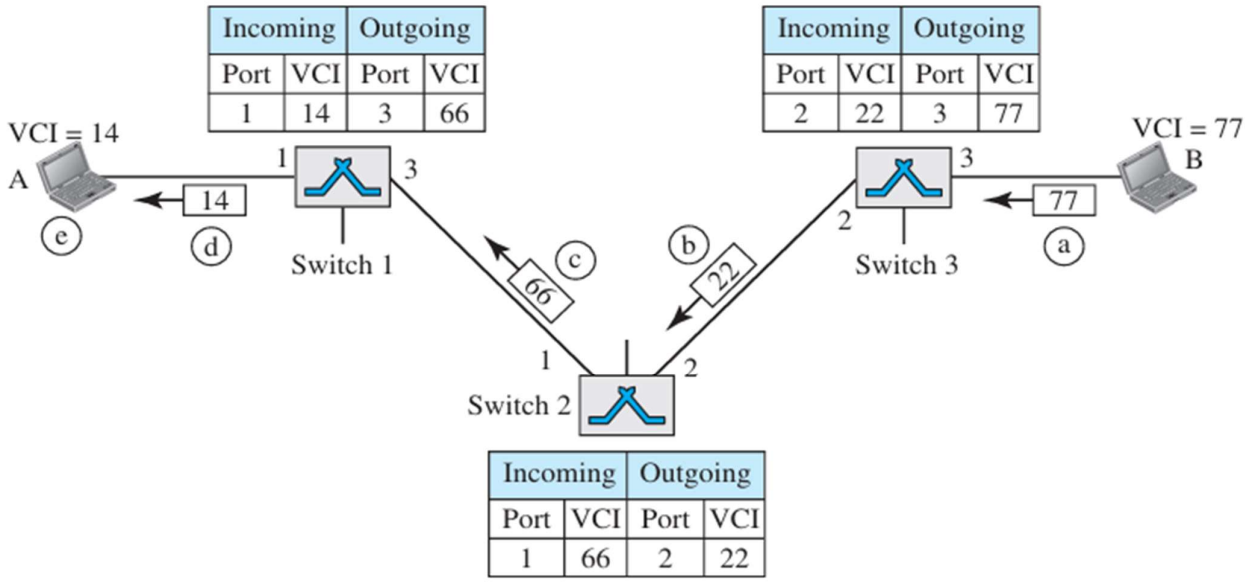


- Source A sends a setup frame to switch 1.
- Switch 1 receives the setup request frame. It knows that a frame going from A to B goes out through port 3. The switch creates an entry in its table for this virtual circuit, but it is only able to fill three of the four columns. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found dur ing the acknowledgment step.
- Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (1), incoming VCI (66), and outgoing port (2).
- Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).
- Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77.

Acknowledgment : A special frame, called the acknowledgment frame, completes the entries in

the switching tables.

Figure 8.15 *Setup acknowledgment in a virtual-circuit network*



a. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77. Switch 3 uses this VCI to complete the outgoing VCI column for this entry.
b. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table
c. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table
d. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table
e. The source uses this as the outgoing VCI for the data frames to be sent to destination B.

Data-Transfer Phase: To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns.

Figure 8.12 *Switch and tables in a virtual-circuit network*

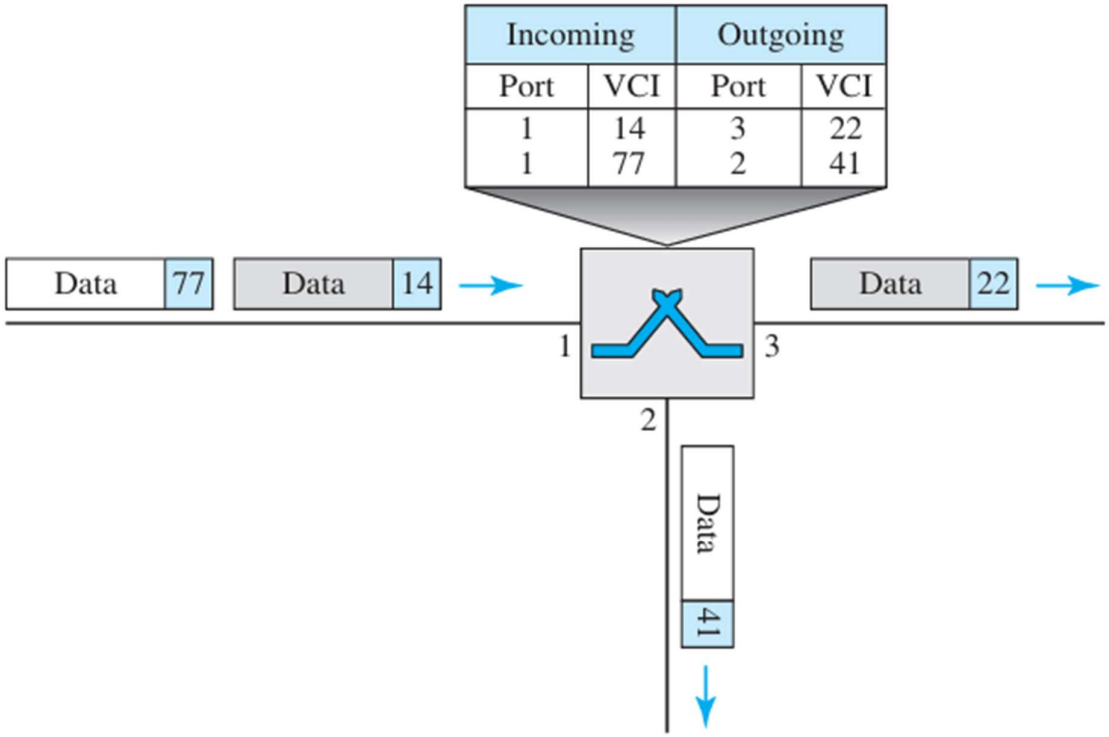


Figure 8.12 shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3.

Figure 8.13 *Source-to-destination data transfer in a virtual-circuit network*

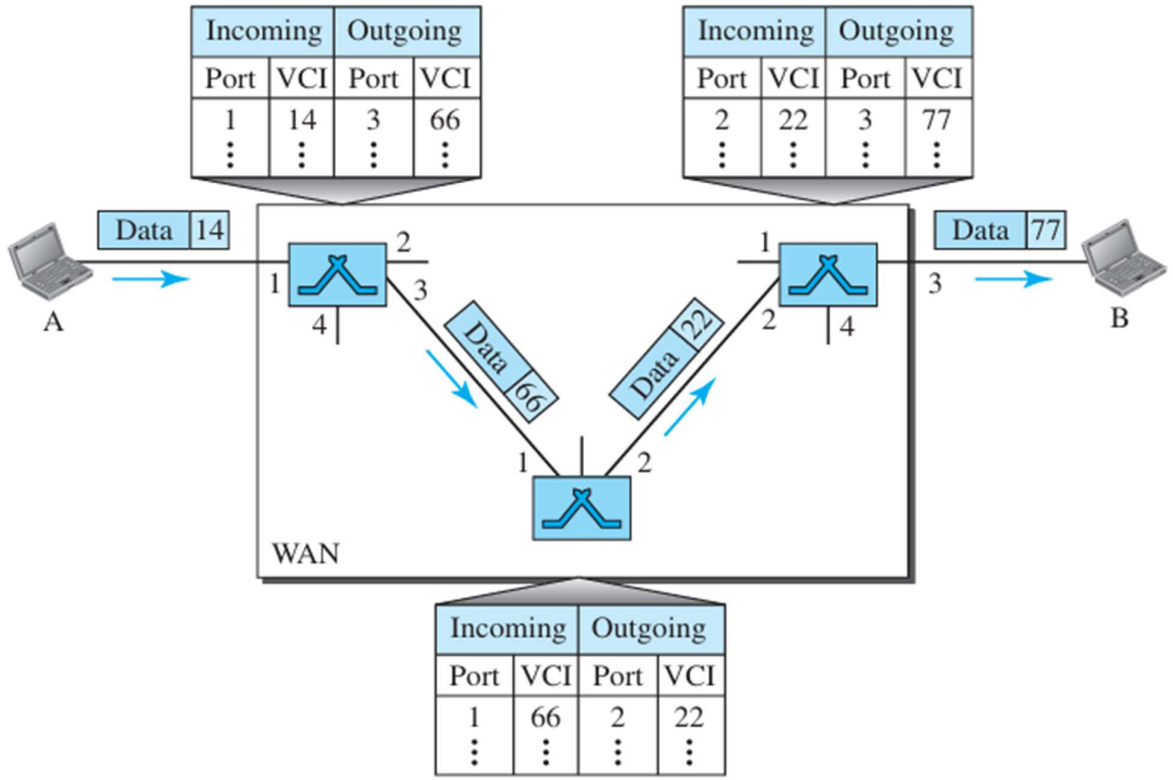


Figure 8.13 shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame.

Teardown Phase : In this phase, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Efficiency:

resource reservation in a virtual-circuit network can be done in two ways.

1. Resource reservation is made during the setup phase.

In the first case, the delay for each packet is the same;

2. Resource reservation is made on demand during the data-transfer phase

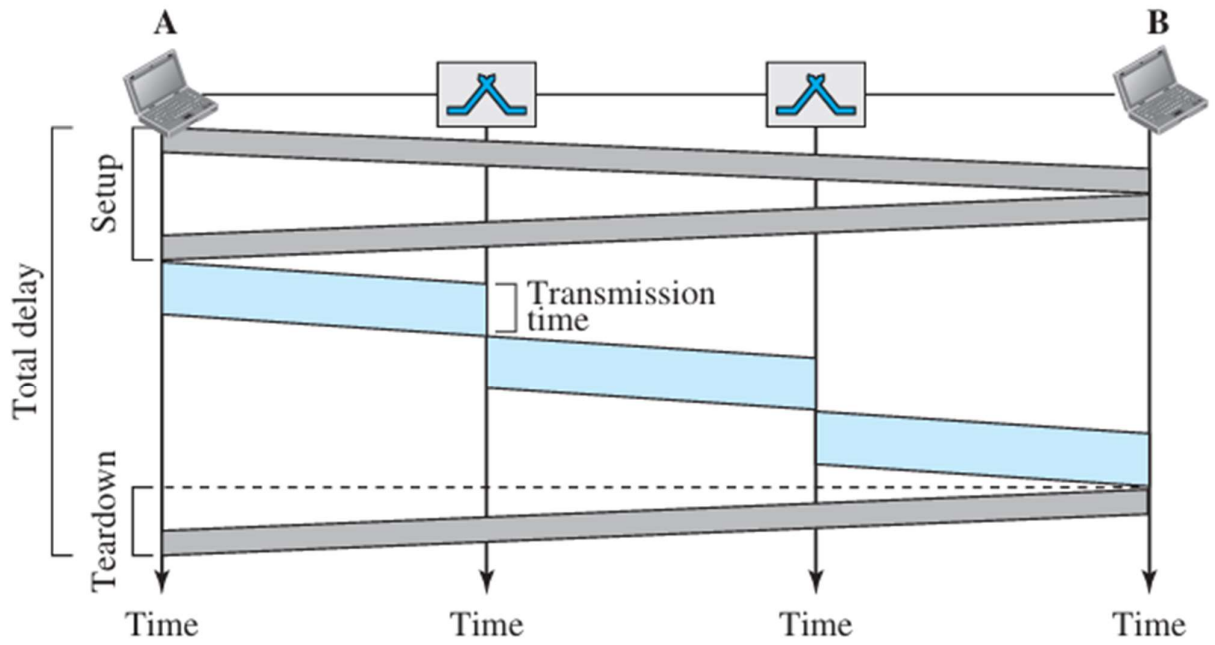
in the second case, each packet may encounter different delays. Here, The source can check the availability of the resources, without actually reserving it.

In virtual-circuit switching, all packets belonging to the same source and destination travel the same path, but the packets may arrive at the destination with different delays if resource allocation is on demand.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. There are three transmission times (3T), three propagation times (3τ), data transfer depicted by the sloping lines, a setup delay and a teardown delay.

Figure 8.16 *Delay in a virtual-circuit network*



The total delay time is = 3T + 3τ + setup delay + teardown delay