UNIT-I

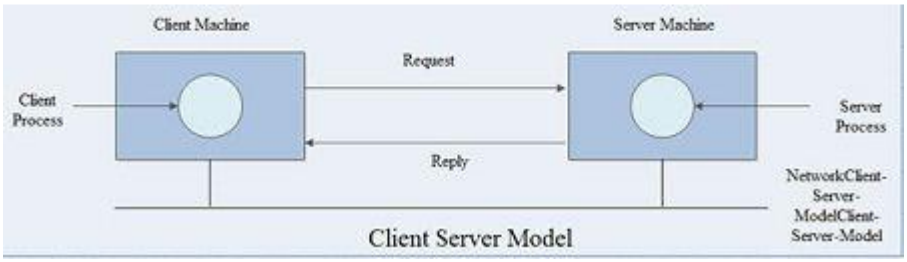
Definition: A large number of separate but interconnected computers are called as computer networks.

Uses of Computer Networks:

1. **Business Applications(Networks for companies) :**
   a) **Resource Sharing**: Many organizations have large number of substantial computers in operation often located far apart. Let us consider an example, a company having many factories situated at different locations. Initially each of these computers may have worked in isolation from each other, but at some point, the management may have decided to connect these computers to be able to extract and correlate the information of the entire company. It allows all programs, equipment's and data available to anyone on the network irrespective of the physical location of the resource and the user.

   b) **High Reliability**: The second goal or use of networking in companies is to high reliability by having alternative sources of supply. For example all the files can be replicated on two or more machines, so that in case one of them is not available (due to hardware failure), other copies can be used.

   c) **Saving Money**: The third goal is to save money. Small computers often have better price/performance ratio than the larger ones. Mainframe (room-size) computers are roughly ten faster than the personal computers, but are a thousand times costly. This imbalance caused the system designers to design a system consisting of personal computers, one per user, with data kept on one or more shared file server machines. In this model the user are called the clients and this whole arrangement is known as the **client-server model**.



Client Server Model

   d) **Communication medium**: A computer network provides a powerful communication medium among widely separated employees. Using network it is easy for two or more employees, who are separated by geographical locations to work on a report, document or R and D simultaneously i.e. on -line.

   e) **Scalability**: Scalability is the ability to increase the system performance gradually as the workload grows, by just adding more processors.

   f) **Electronic commerce**: Many companies are doing business electronically. It enables customers to inspect the on-line catalogues of thousands of companies. Some of the catalogues will soon provide the ability to get an instant video on any product by just clicking on the product’s name. Using computer networks, manufacturers can place orders electronically..

2. **Home Applications(Networks for people) :**

   a) **Access to Remote Information**:Access to remote information involves interaction· between a person and a remote database. Access to remote information comes in many forms like:

      (i) Home shopping, paying telephone, electricity bills, e-banking, on line share market etc.

      (ii) Newspaper is On-line and is personalized, digital library consisting of books, magazines, scientific journals etc.

      (iii) World Wide Web which contains information about the arts, business, cooking, government, health, history, hobbies, recreation, science, sports etc.

   b) **Person to person communication:**Electronic Mail popularly known as email is widely used by millions of people to send text messages, photographs audio as well as video to other people or group of people. Videoconferencing is also becoming popular these days. This technology makes it possible to have virtual meetings among far flung people.

   c) **Interactive Entertainment:**Interactive entertainment includes:

      (i) Multiperson real-time simulation games.

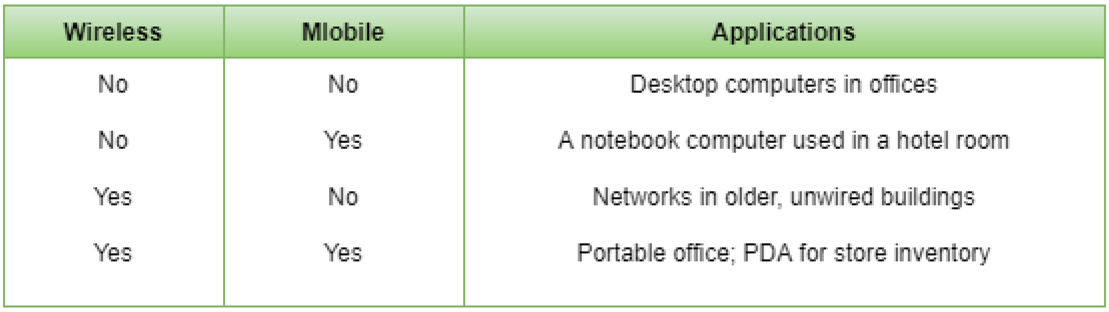
      (ii) Video on demand.

      (iii) Participation in live TV programmes likes quiz, contest, discussions etc**.**

   d) **Ubiquitous computing** : Ubiquitous computing is one in which computing is embedded into everyday life .Many homes are already wired with security systems that include door and window sensors .Your electricity ,gas and water meters could also report usage over the network . Smoke detectors could call the fire department instead of making a big noise.

   e) Electronic commerce: Home shopping is already popular and enables users to inspect the on-line catalogues of thousands of companies. Some of the catalogues will soon provide the ability to get an instant video on any product by just clicking on the product’s name .Many people pay their bills, manage their bank accounts and handle their investments electronically**.**

3. **Mobile Users:** Mobile computers, such as notebook computers and Mobile phones, are one of the fastest-growing segments of the entire computer industry.Wi-Fi hotspots and 3G and 4G cellular provide wireless connectivity.Mobile users communicate, e.g., voice and texts, consumecontent, e.g., video and Web, and use sensors, e.g., GPS.Although wireless networking and mobile computing are often related, they are not identical, as the below figure shows.



Wireless	Mlobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

4. **Social issues:**The widespread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks is newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

- Network neutrality – no network restrictions
- Content ownership, e.g., Digital Millennium Copyright Act
- Privacy, e.g., Web tracking and profiling
- Theft, e.g., botnets and phishing

Network hardware: There is no generally accepted taxonomy into which all computer networks fit, but two dimensionsstand out as important: **transmission technology and scale.**

Classification of networks according to **transmission technology**:

- broadcast links,
- point-to-point links.

Broadcast networks are networks with single communication channel shared by all the machines. Short messages (packets) sent by any machine are received by all others. An address field within thepacket specifies for whom it is intended. Analogy: someone shout in the corridor with many rooms.

Broadcasting is a mode of operation in which a packet is sent to every machine using a special code in the address field.

Multicasting is sending a packet to a subset of the machines.

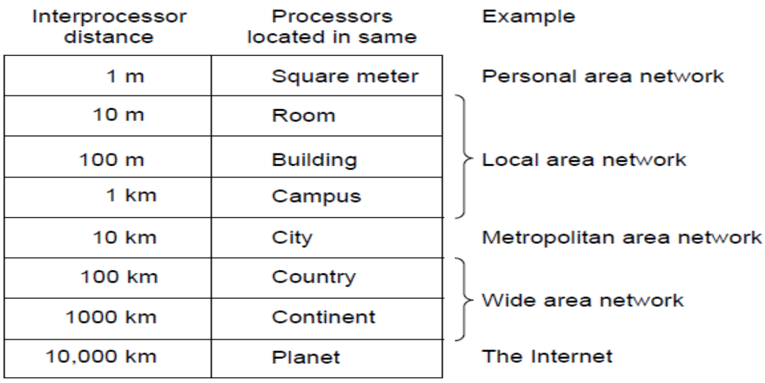
Point-to-point networks consist of many connections between individual pairs of machines. In these types of networks:

- A packet on its way from the source to the destination may go through intermediate machines.
- In general, multiple routes are possible - routing algorithms are necessary.

General rule (with many exceptions): smaller, geographically localized networks tends to use broadcasting, larger networks usually are point-to-point.

Classification of networks by**scale:**

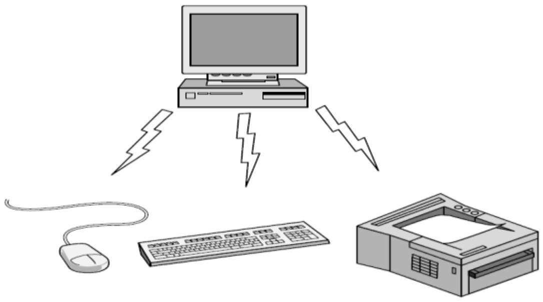
Distance is important as a classification metric because different technologies are used at different scales.At the top are the personal area networks, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitan, and wide area networks, each with increasing scale. Finally, the connection of two or more networks is called an internetwork. The worldwide Internet is certainly the best-known (but not the only) example of an internetwork.



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

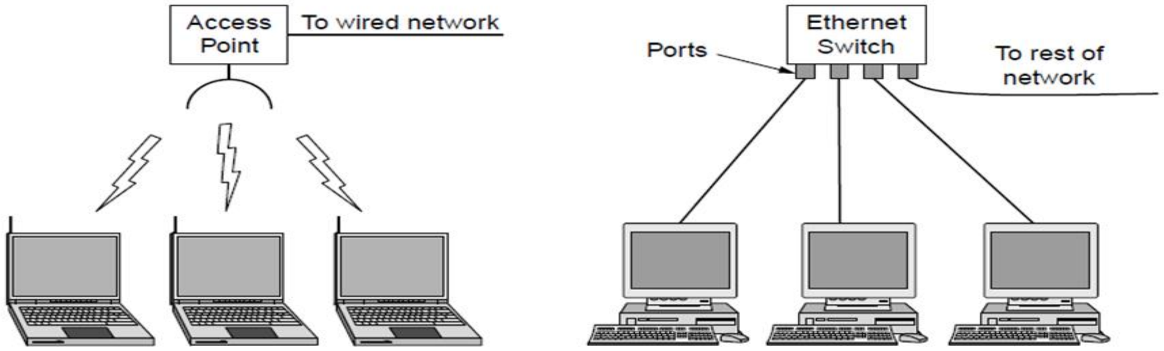
<u>Classification of interconnected processors by scale</u>

Personal Area Networks: PANs (Personal Area Networks) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer.A wireless network called Bluetooth is used to connect a short-range component without wires.A completely different kind of PAN is formed when an embedded medical device such as a pacemaker, insulin pump, or hearing aid talks to a user-operated remote control.



Local Area Networks: Local area networks (LANs) re privately-owned, within a single building or campus, of up to a few kilometres in size.LANs are restricted in size - the worst-case transmission time is known in advance, it makes possible to use certain kinds of design.LANs transmission technology often consists of a single cable to which all machines are attached. Traditional LANs run at speed of 10 to 100 Mbps. Newer LANs may operate at higher speeds.

Wireless LANs are very popular these days,in these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers. In most cases, each computer talks to a device in the ceilingcalled an AP (Access Point), wireless router, or base station, which relays packets between the wireless computers and also between them and the Internet. There is a standard for wireless LANs called IEEE 802.11, popularly known as Wi-Fi and standard for wired is 802.3, known as Ethernet

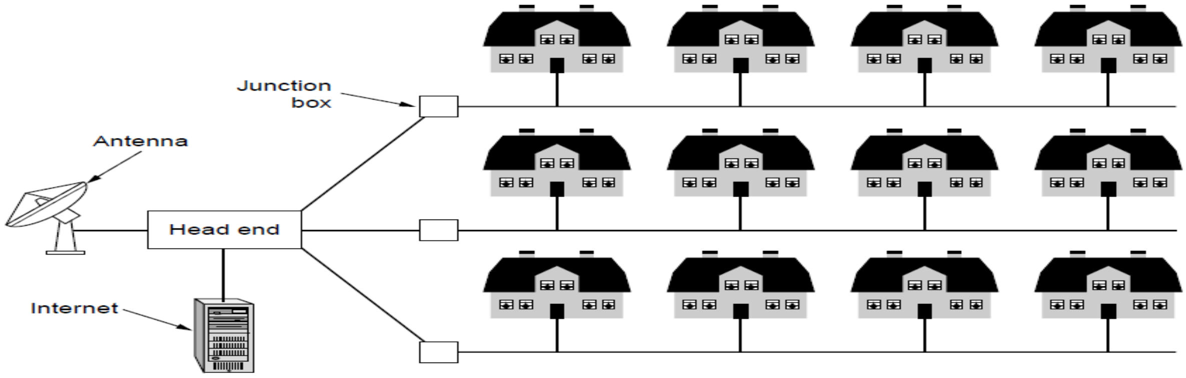


Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet

Both Broadcast networks can be, depending on how the channel is allocated, further divided into:

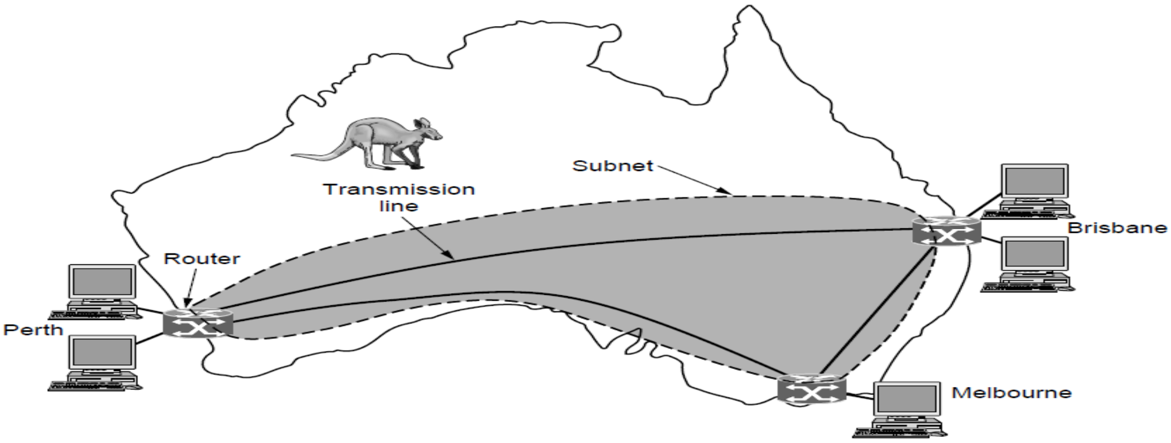
- Static - a typical would be a time division for the access to the channel and round-robin algorithms. It wastes channel capacity.
- Dynamic - on demand. Channel allocation could be centralized or decentralized.

Metropolitan Area Networks:MAN is basically a bigger version of a LAN and normally uses similar technology which covers a city.The best-known examples of MANs are the cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception.When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum. At that point both television signals and Internet being fed into the centralized cable head end for subsequent distribution to people’s homes.MAN has been standardized as IEEE 802.16 and is popularly known as WiMAX.



Wide Area Networks:A WAN (Wide Area Network) spans a large geographical area, often a country or continent.

- **Wired WANs**:The WAN in Figure is a network that connects offices in Perth, Melbourne, and Brisbane. Each of these offices contains computers intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts. The rest of the network that connects these hosts is then called thecommunication subnet, or just subnet for short. The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener. In most WANs, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fibre, or even radio links. Switching elements, or just switches, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.



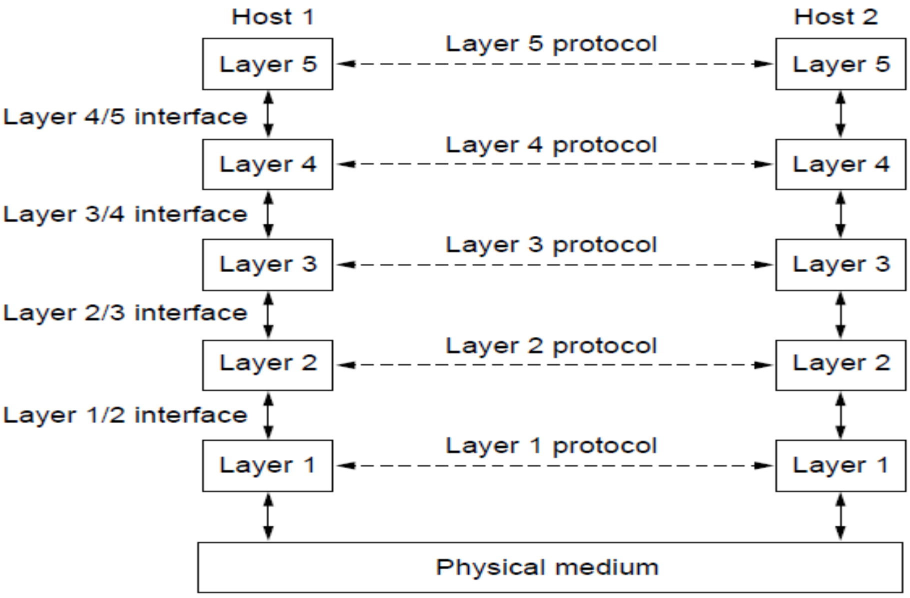
- **Wireless WAN’s:**In satellite systems, each computer on the ground has an antenna through which it can send data to and receive data from to a satellite in orbit. All computers can hear the output from the satellite, and in some cases they can also hear the upward transmissions of their fellow computers to the satellite as well. Satellite networks are inherently broadcast and are most useful when the broadcast property is important. The cellular telephone network is another example of a WAN that uses wireless technology.

Internetworks: Internetwork or internet is a collection of interconnected networks. A common form of internet is a collection of LAN connected by WAN. Connecting incompatible networks together requires using machines called gateways to provide the necessary translation. Internet (with uppercase I) means a specific worldwide internet.

Subnets, networks and internetworks are often confused.Subnet makes the most sense in the context of a wide area network, where it refers to the collectionof routers and communication lines. The combination of a subnet and its hosts forms a network. An internetwork is formed when distinct networks are connected together.

NETWORK SOFTWARE: The first computer networks were designed with the hardware as the main concern and the software as an afterthought. This strategy no longer works. Network software is now highly structured.The following are the software structuring technique

1. **Protocol Hierarchies:**To reduce their design complexity, most networks are organized as a series of layers or levels, each one built upon the one below it. The actual structure of layers differs from network to network. Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are known as layer n protocol.



- Data between layers n on different machines are not transferred directly. Each layer passes data and control information to the layer directly below it until the lowest layer is reached. Below layer 1 there is a physical medium through which actual communication occurs.
- Between each pair of adjacent layers there is an interface. The **interface** defines which primitive operations and services the lower layer offers to the upper one.
- A set of layers and protocols is called **network architecture**. A list of protocols used by a certain system, one protocol per layer, is called a **protocol stack**.
- The peer process abstraction is crucial to all network design. Using it, the unmanageable task of designing the complete network can be broken into several smaller, manageable, design problems, namely the design of the individual layers.
- Lower layers of the protocol hierarchy are frequently implemented in hardware or firmware

2. **Design Issues for the Layers:**The following are the design issues for the layers:

- **Reliability**: It is a design issue of making a network that operates correctly even when it is made up of unreliable components.
- **Error Control**: It is an important issue because physical communication circuits are not perfect. Many error detecting and error correcting codes are available. Both sending and receiving ends must agree to use any one code.

- **Routing**: When there are multiple paths between source and destination, only one route must be chosen. This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination
- **Addressing**: There are multiple processes running on one machine. Every layer needs a mechanism to identify senders and receivers
- **Scalability:** When network gets large, new problem arises. Thus scalability is important so that network can continue to work well when it gets large.
- **Flow Control**: If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on. Some process will not be in position to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and the reassembling messages.
- **Multiplexing and De-multiplexing**: If the data has to be transmitted on transmission media separately, it is inconvenient or expensive to setup separate connection for each pair of communicating processes. So, multiplexing is needed in the physical layer at sender end and de-multiplexing is need at the receiver end.
- **Confidentiality and Integrity**: Network security is the most important factor. Mechanisms that provide confidentiality defend against threats like eavesdropping. Mechanisms for integrity prevent faulty changes to messages.

3. **Connection-Oriented Versus Connectionless Service:**Layers can offer two different types of service to the layers above them:
    - Connection-oriented and
    - Connectionless.

    Connection-oriented service (modelled after the telephone system): to use it, the service user firstestablishes a connection, uses the connection, and then releases the connection. The essential aspectof a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and thereceiver takes them out in the same order at the other end.

    Connectionless service (modelled after the postal system): Each message carries the full destinationaddress, and each one is routed through the system independent of all the others.

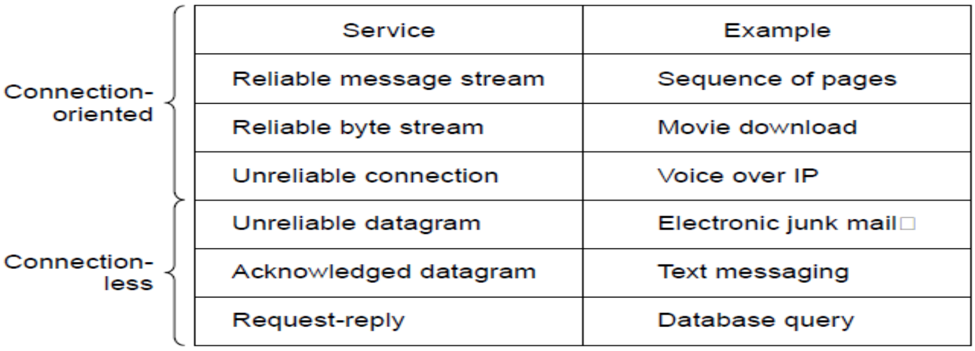
    Quality of service - some services are reliable in the sense that they never lose data. Reliability is usually implemented by having the receiver acknowledge the receipt of each message. Theacknowledgment process is often worth but introduces sometimes undesirable overheads and delays.

    Reliable connection-oriented service has two minor variations:
    - Message sequences - the message boundaries are preserved.
    - Byte streams - the connection is simply a stream of bytes, with no message boundaries.

    Applications where delays introduced by acknowledgment are unacceptable:
    - digitized voice traffic,
    - Video film transmission.

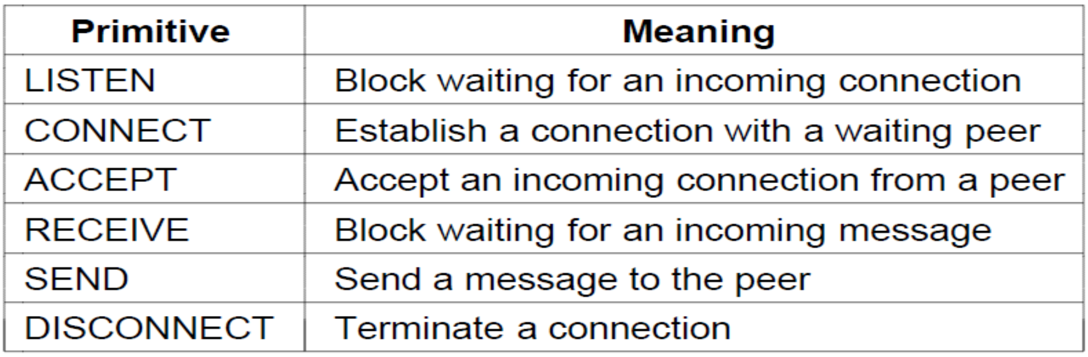
The use of connectionless services:

- electronic junk mail (third class mail as advertisements) - this service is moreover unreliable (meaning not acknowledged). Such connectionless services are often called datagramservices.
- acknowledged datagram services - connectionless datagram services with acknowledgment.
- request-reply service - the sender transmits a single datagram containing a request. The reply contains the answer. Request-reply is commonly used to implement communication in the client-server model.



	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail□
	Acknowledged datagram	Text messaging
	Request-reply	Database query

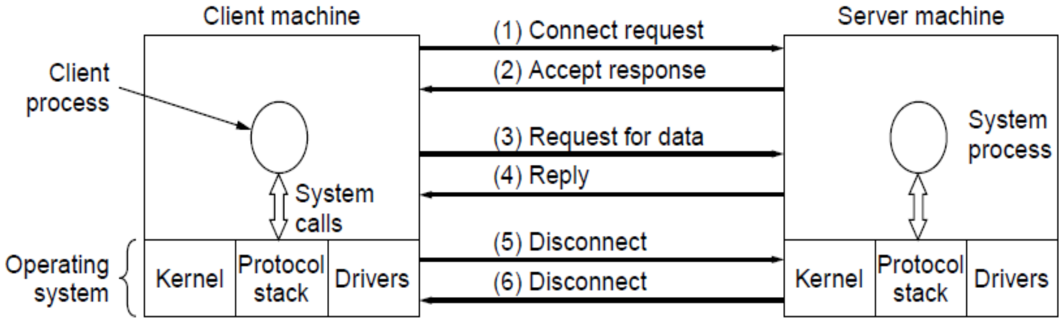
4. **Service Primitives:**A service is formally specified by a set of primitives (operations) available touser processes to access the service. These primitives tell the service to performsome action or report on an action taken by a peer entity.The set of primitives available depends on the nature of the service being provided.The primitives for connection-oriented service are different from those ofconnectionless service



Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Six service primitives that provide a simple connection-oriented service

These primitives might be used for a request-reply interaction in a client-server environment as shown in the figure below



First, the server executes LISTEN to indicate that it is prepared to accept incoming connections.Next, the client process executes CONNECT to establish a connection with the server. The operating system then typically sends a packet to the peer asking it to connect. The server process can then establish the connection with the ACCEPT call.The next step is for the server to execute RECEIVE to prepare to accept the first request.Then the client executes SEND to transmit its request followed by the execution of RECEIVE to get the reply.When the client is done, it executes DISCONNECT to terminate the connection.

OSI REFERENCE MODEL: The OSI model (minus the physical medium) is based on a proposal develop by ISO as a first step toward international standardization of the protocols used in the various layers. The model is called ISO OSI (Open Systems Interconnection) Reference Model.

Open system is a system open for communication with other systems.

The OSI model has 7 layers .The principles that were applied to arrive at the seven layers are as follows:

1. A layer should be created where a different level of abstraction is needed.

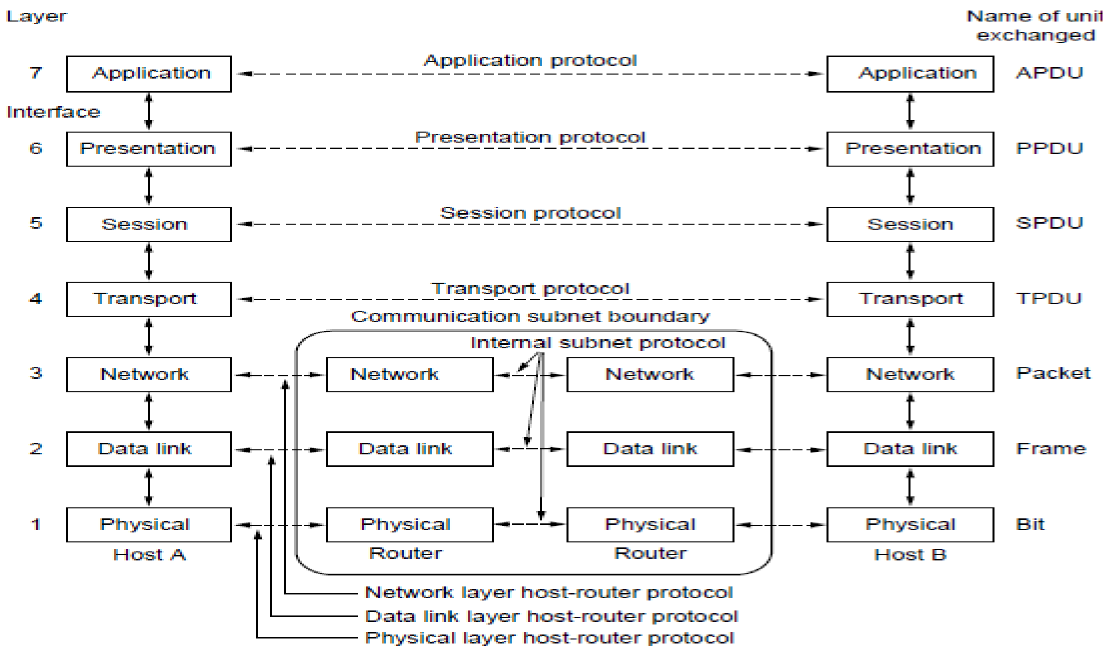
2. Each layer should perform a well-defined function.

3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be chosen to minimize the information flow across the interfaces.

5.The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy

The OSI model is not network architecture - it does not specify the exact services and protocols. It just tells what each layer should do. However, ISO has also produced standards for all the layers as a separate international standard.



The OSI reference model

1. **The Physical Layer:**The main task of the physical layer is to transmit raw bits over a communication channel.The design issue has to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit and not as a 0
   Typical questions here are:
   - how many volts should be used to represent 1 and 0,
   - how many microseconds a bit lasts,
   - whether the transmission may proceed simultaneously in both directions,
   - how the initial connection is established and how it is turn down,
   - how many pins the network connector has and what each pin is used for.

   The design issues deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer.
2. **The Data Link Layer:**The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or few thousand bytes) and transmits the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by send back an acknowledgement frame**.**
   The issues that the layer has to solve:
   - to create and to recognize frame boundaries - typically by attaching special bit patterns to the beginning and end of the frame,
   - to solve the problem caused by damaged, lost or duplicate frames (the data link layer may offer several different service classes to the network layer, each with different quality and price),
   - to keep a fast transmitter from drowning a slow receiver in data,

- if the line is bi-directional, the acknowledgment frames compete for the use of the line with data frames.

Broadcast networks have an additional issue in the data link layer: how to control access to the sharedchannel. A special sub layer of the data link layer (medium access sub layer) deals with the problem

3. **The Network Layer:**The main task of the network layer is to determine how data can be delivered from source todestination. That is, the network layer is concerned with controlling the operation of the subnet.

   The issues that the layer has to solve:

   - to implement the routing mechanism,
   - to control congestions,
   - to do accounting,
   - to allow interconnection of heterogeneous networks.

   In broadcast networks, the routing problem is simple, so the network layer is often thin or evennon-existent.

   The user of the network layer may be sure that his packet was delivered to the given destination.However, the delivery of the packets needs not to be in the order in which they were transmitted.

4. **The Transport Layer:**The basic function of the transport layer is to accept data from the session layer, split it up intosmaller units if need be, pass them to the network layer, and ensure that the pieces all arrive correctlyat the other end. All this must be done in a way that isolates the upper layers from the inevitablechanges in the hardware technology.

   The issues that the transport layer has to solve:

   - to realize a transport connection by several network connections if the session layer requires a high throughput or multiplex several transport connections onto the same network connection if network connections are expensive,
   - to provide different type of services for the session layer,
   - to implement a kind of flow control

   The transport layer is a true end-to-end layer, from source to destination. In other words, a programon the source machine carries on a conversation with a similar program on the destination machine. In lower layers, the protocols are between each machine and its immediate neighbors.

   The user of the transport layer may be sure that his message will be delivered to the destination regardless of the state of the network. He need not worry about the technical features of the network

5. **The Session Layer:**The session layer allows users on different machines to establish sessions between them. A sessionallows ordinary data transport, as does the transport layer, but it also provides enhanced servicesuseful in some applications**.**

   Some of these services are:

   - **Dialog control** - session can allow traffic to go in both directions at the same time, or in only one direction at a time. If traffic can go only in one way at a time, the session layer can help to keep track of whose turn it is.

- **Token management** - for some protocols it is essential that both sides do not attempt the same operation at the same time. The session layer provides tokens that can be exchanged. Only the side holding the token may perform the critical action.
- **Synchronization** - by inserting checkpoints into the data stream the layer eliminates problems with potential crashes at long operations. After a crash, only the data transferred after the last checkpoint have to be repeated

6. **The Presentation Layer:**The presentation layer performs certain functions that are requested sufficiently often to warrantfinding a general solution for them, rather than letting each user solve the problem. This layer is,unlike all the lower layers, concerned with the syntax and semantics of the information transmitted.

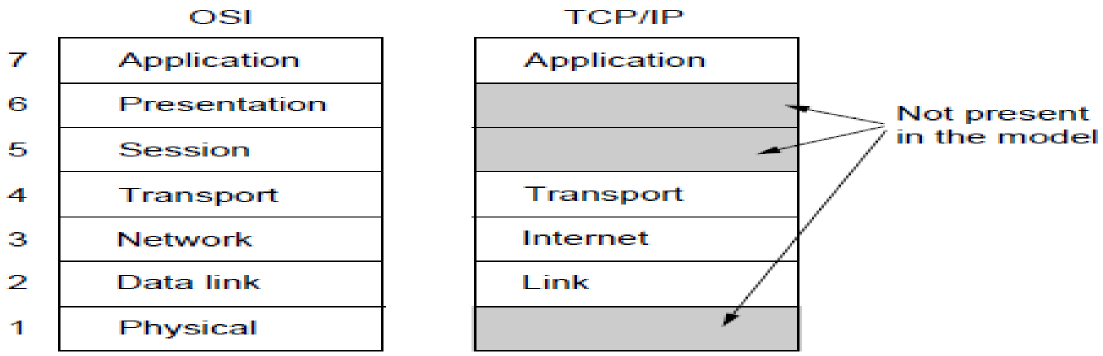
   A typical example of a presentation service is encoding data in a standard agreed upon way. Differentcomputers may use different ways of internal coding of characters or numbers. In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire". The presentation layer manages these abstract data structures and converts from the representation used inside the computer to the network standard representation and back.

7. **The Application Layer:**The application layer contains a variety of protocols that are commonlyneeded by users. One widely used application protocol is HTTP (HyperTextTransfer Protocol), which is the basis for the World Wide Web. When abrowser wants a Web page, it sends the name of the page it wants to the serverhosting the page using HTTP. The server then sends the page back. Other application

   protocols are used for file transfer, electronic mail, and network news.

<u>The TCP/ I P Reference Model:</u>TCP/ IP reference model originates from the grandparent of all computer networks, the ARPANET and now is used in its successor, the worldwide Internet**.**The TCP/IP Reference Model Layers are as follows:

- Link layer
- Internet layer
- Transport layer
- Application layer



The TCP/IP reference model

The Link Layer: The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer. It is not really a layer at all, in the normal sense of the term, but rather an interface between hosts and transmission links**.**

The Internet Layer: The internet layer is the keystone that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.

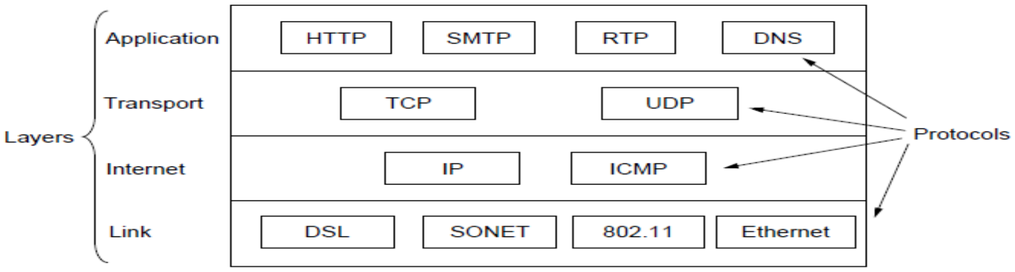
The internet layer defines an official packet format and protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol) that helps it function. The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly a major issue here, as is congestion.

The Transport Layer: The layer above the internet layer in the TCP/ IP model is now usually called transport layer. It isdesigned to allow peer entities on the source and destination hosts to carry on a conversation, the same as in the OSI transport layer. Two end-to-end protocols have been defined here:

- **TCP (Transmission Control Protocol**) is a reliable connection-oriented protocol that allows abyte stream originating on one machine to be delivered without error on any other machine inthe internet. It fragments the incoming byte stream into discrete messages and passes eachone onto the internet layer. At the destination, the receiving TCP process reassembles thereceived messages into the output stream. TCP also handles flow control.
- **UDP (User Datagram Protocol**) is unreliable, connectionless protocols for applications thatdo not want TCP's sequencing or flow control and wish to provide their own. It is also widelyused for one/shot, client/server type request/ reply queries and applications in which promptdelivery is more important than accurate delivery.

The Application Layer: The application layer is on the top of the transport layer. I t contains all the higher level protocols. Some of them are:

- Virtual terminal (TELNET) - allows a user on one machine to log into a distant machine and work there.
- File transfer protocol (FTP) - provides a way to move data efficiently from one machine toanother.
- Electronic mail (SMTP) - specialized protocol for electronic mail.
- Domain name service (DNS) - for mapping host names onto their network addresses.



The TCP/IP reference model with some protocols

A Comparison of the OSI and TCP Reference Models: The OSI and the TCP/ IP reference models have much in common:

- they are based on the concept of a stack of independent protocols,
- they have roughly similar functionality of layers,
- the layers up and including transport layer provide an end-to-end network-independent transport service to processes wishing to communicate.

The two models also have many differences (in addition to different protocols):Probably the biggest contribution of the OSI model is that it makes the clear distinction between its three central concepts that are

- services
- interfaces
- protocols

- ♦ Each layer performs some services for the layer above it. The service definition tells what the layer does, not how entities above it access it or how the layer works.
- A layer’s interface tells the processes above it how to access it including the specification of the parameters and the expected results. But it, too, says nothing about how the layer works inside.
- The peer protocols used in a layer are its own business. It can use any protocol as long as it provides the offered services.
- The TCP/ IP model did not originally clearly distinguish between service, interface, and protocol. As a consequence, the protocol in the OSI model are better hidden than in the TCP/ IP model and can be replaced relatively easily as the technology changes.
- The OSI reference model was devised before the protocols were invented. The positive aspect of this was that the model was made quite general, not biased toward one particular set of protocols. The negative aspect was that the designers did not have much experience with the subject and did not have a good idea of which functionality to put into which layer (e.g. some new sub layers had to be hacked into the model).
- With the TCP/ IP the reverse was true: the protocols came first, and the model was just a description of the existing protocols. As a consequence, the model was not useful for describing other non-TCP/ IP networks.
- An obvious difference between the two models is the number of layers.
- Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both types of communication in the network layer, but only connection-oriented communication in the transport layer. The TCP/ IP model has only connectionless mode in the network layer but supports both modes in the transport layer. The connectionless choice is especially important for simple request-response protocols.

The Network Core: There are two fundamental approaches to moving data through a network of linksand switches: circuit switching and packet switching**.**

1.3.1 Packet Switching: In packet-switched networks, these resources needed along the path are not reserved; a session’s messages use the resources on demand, and as a consequence, may have to wait (that is, queue) for access to a communication link. To send a message from a source end system to a destination end system,the source breaks long messages into smaller chunks of data known as packets. Between source and destination, each packet travels through communication linksand packet switches. Packets are transmitted over each communication link at a rateequal to the full transmission rate of the link. So, if a source end system or a packetswitch is sending a packet of L bits over a link with transmission rate R bits/sec, thenthe time to transmit the packet is L/R seconds.

Store-and-Forward Transmission: Most packet switches use store-and-forward transmission at the inputs to thelinks. Store-and-forward transmission means that the packet switch must receivethe entire packet before it can begin to transmit the first bit of the packet onto theoutbound link.

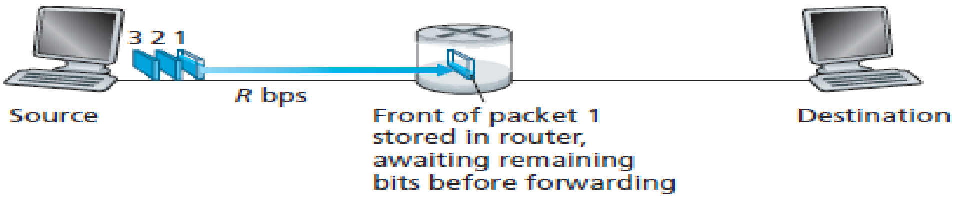


Figure 1.11 ◆ Store-and-forward packet switching

The general case of sending one packet from source to destinationover a path consisting of N links each of rate R theend-to-end delay is:

$$d_{\text{end-to-end}} = N\frac{L}{R}$$

Queuing Delays and Packet Loss: Each packet switch has multiple links attached to it. For each attached link, the packet switch has an output buffer (also called an output queue), which storespackets that the router is about to send into that link. If an arriving packet needs to be transmitted onto a link butfinds the link busy with the transmission of another packet, the arriving packet mustwait in the output buffer. Thus, in addition to the store-and-forward delays, packetssuffer output buffer queuing delays. These delays are variable and depend on thelevel of congestion in the network. Since the amount of buffer space is finite, anarriving packet may find that the buffer is completely full with other packets waitingfor transmission. In this case, packet loss will occur—either the arriving packetor one of the already-queued packets will be dropped.

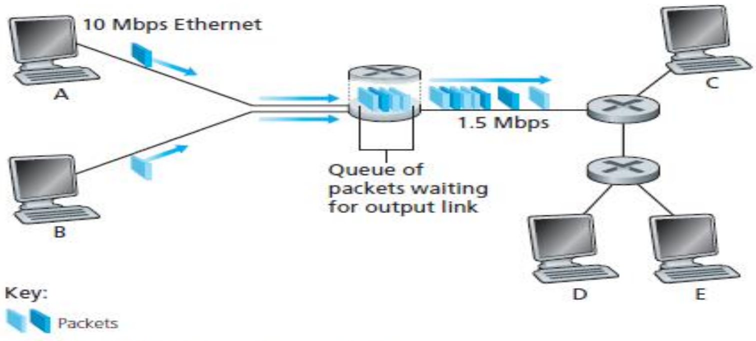


Figure 1.12 ◆ Packet switching

Forwarding Tables and Routing Protocols: In the Internet, every end system has an address called an IP address. When asource end system wants to send a packet to a destination end system, the sourceincludes the destination’s IP address in the packet’s header. As with postal addresses,this address has a hierarchical structure. When a packet arrives at a router in thenetwork, the router examines a portion of the packet’s destination address and forwardsthe packet to an adjacent router. More specifically, each router has aforwarding table that maps destination addresses (or portions of the destinationaddresses) to that router’s outbound links. When a packet arrives at a router, therouter examines the address and searches its forwarding table, using this destinationaddress, to find the appropriate outbound link. The router then directs the packet tothis outbound link.

1.3.2 Circuit Switching: In circuit-switched networks, the resources needed along a path (buffers, link transmission rate) to provide for communication between the end systems are reserved for the duration of the communication session between the end systems. Traditional telephone networks are examples of circuit-switched networks. Before the sender can send the information,the network must establish a connection between the sender and the receiver. Inthe jargon of telephony, this connection is called a circuit. Figure 1.13 illustrates a circuit-switched network. In this network, the four circuitswitches are interconnected by four links. Each of these links has four circuits,so that each link can support four simultaneous connections. Thus, in order for Host A to communicate withHost B, the network must first reserve one circuit on each of two links. In this example,the dedicated end-to-end connection uses the second circuit in the first link andthe fourth circuit in the second link. Because each link has four circuits, for eachlink used by the end-to-end connection, the connection gets one fourth of the link’stotal transmission capacity for the duration of the connection. Thus, for example, ifeach link between adjacent switches has a transmission rate of 1 Mbps, then eachend-to-end circuit-switch connection gets 250 kbps of dedicated transmission rate.

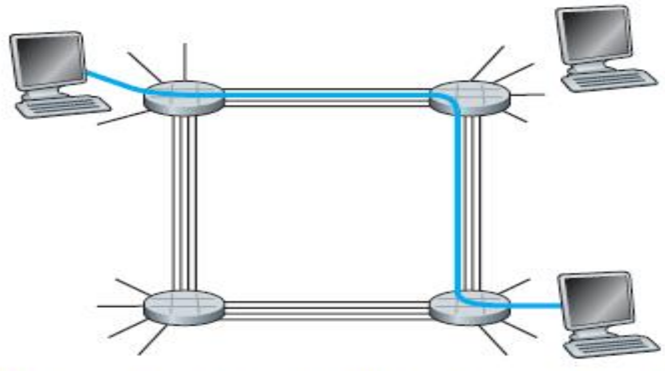


Figure 1.13 ♦ A simple circuit-switched network consisting of four switches and four links

Multiplexing in Circuit-Switched Networks: A circuit in a link is implemented with either frequency-division multiplexing(FDM) or time-division multiplexing (TDM). With FDM, the frequency spectrumof a link is divided up among the connections established across the link. Specifically, the link dedicates a frequency band to each connection for theduration of the connection.For a TDM link, time is divided into frames of fixed duration, and each frame is divided into a fixed number of time slots. When the network establishes a connectionacross a link, the network dedicates one time slot in every frame to this connection.These slots are dedicated for the sole use of that connection, with one time slotavailable for use (in every frame) to transmit the connection’s data.

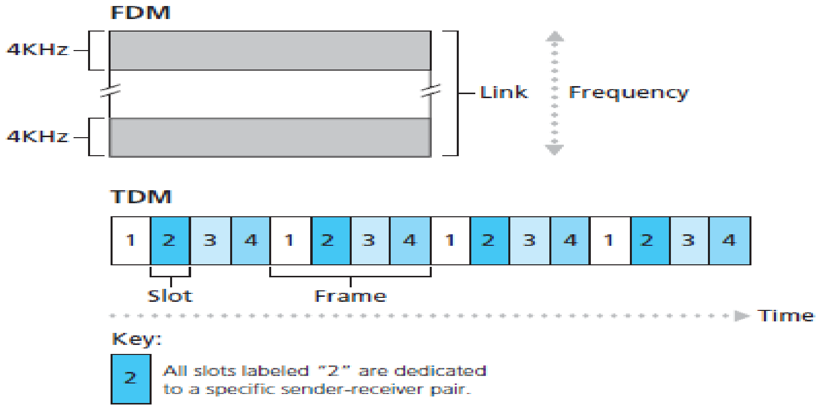
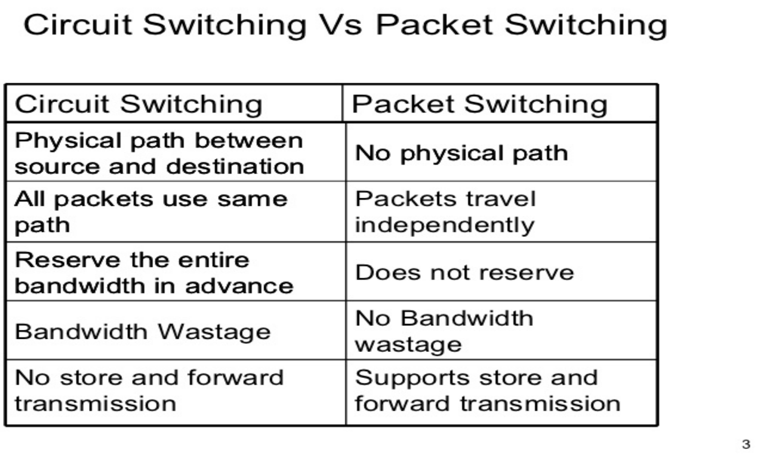


Figure 1.14 ♦ With FDM, each circuit continuously gets a fraction of the bandwidth. With TDM, each circuit gets all of the bandwidth periodically during brief intervals of time (that is, during slots)

Differences between Packet switching and Circuit Switching:



Circuit Switching Vs Packet Switching

Circuit Switching	Packet Switching
Physical path between source and destination	**No physical path**
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

3