CS8591 COMPUTER NETWORKS

UNIT I

INTRODUCTION AND PHYSICAL LAYER

1. INTRODUCTION

A network is a set of devices (also referred to as nodes) connected by communication links. A node can be a computer, printer or any other device capable of sending data and receiving data generated by other nodes on the network.

Data communication is the exchange of data between two devices via some form of transmission medium. The effectiveness of a data communication system depends on;

i. **Delivery**: Data must be delivered to the correct destination
ii. **Accuracy**: The system must deliver the data without any change
iii. **Timeliness**: The system must deliver the data in time.

1.1 COMPONENTS

A data communication system consists of five components. They are

i. **Message**: The message is the information or data to be communicated. Some forms of data representations are text, number, images, audio and video.
ii. **Sender**: The sender is a device that sends the message.
iii. **Receiver**: The receiver is a device that receives the message, sent by the sender.
iv. **Medium**: The medium is a physical path through which the message can be passed between the sender and the receiver.
v. **Protocol:** The protocol is a set of rules which governs the data communication. Without the protocol, two systems can be connected but not communicating. The key elements of a protocol are syntax, semantics and timing.

1.2 DIRECTION OF DATA FLOW

Line configuration refers to the attachment of communication devices to a link. There are two types of line configurations:

i. **Point-to-point:** Provides a dedicated link between two devices. The entire channel capacity is reserved for the transmission between two devices only.

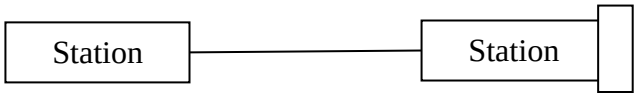


Figure 1.1 Point-to-point connection

ii. **Multipoint:** More than two specific devices share a single link. The channel capacity is shared either spatially or temporally.

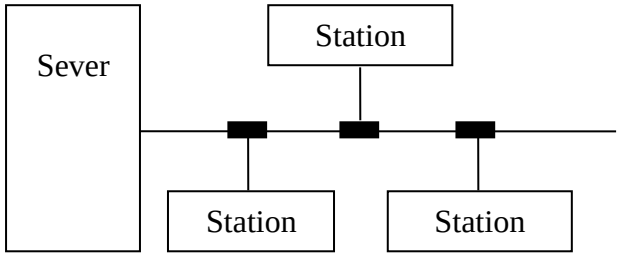


Figure 1.2 Multipoint connection

Communication between two devices can be of three types. They are;

1) **Simple:** The communication is unidirectional. Only one of the two stations on a link can transmit and other can only receive.
2) **Half-duplex**: Each station can both transmit and receive, but not at the same time. The entire capacity of the channel is taken by the station which transmits the data.
3) **Full-duplex**: Both stations can transmit and receive the data at the same time. The capacity of the channel is divided between the signals traveling in opposite directions.

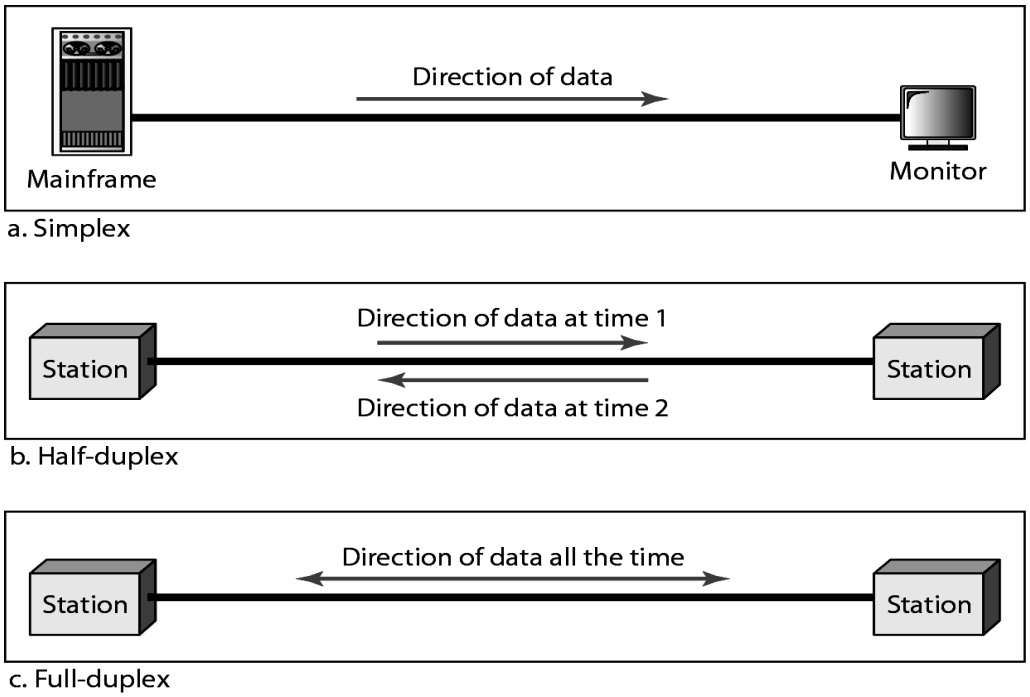


Figure 1.3 Data flow (simplex, half-duplex, and full-duplex)

1.3 CATEGORIES OF NETWORK

There are three primary categories of networks. They are,

(i) **LAN (Local Area Network)**: It is normally private and will connect the computer in a small area such as the entire computer in single company or building. The network at your business or school is an example of a LAN.

(ii) **MAN (Metropolitan Area Network)**: It is a "LAN" that has been extended so that it covers a larger area such as an entire city. Your ISP is an example of a MAN.

(iii)**WAN (Wide Area Network)**: It is a "LAN" that has been extended to cover a wider area such as multiple sites around the world, an entire country, or even the whole world. It may be private in that it connects all the sites within a single company or it may be public such as the network of computers that make up the network for running all the Google related sites around the world.

1.4 PHYSICAL TOPOLOGY

The term physical topology refers to the way in which a network is laid out physically. The topology of a network is the geometric representation of the relationship of all the links and nodes to another. There are five types of topologies. They are,

(i) Mesh topology

(ii) Star topology

(iii) Bus topology

(iv) Ring topology

(v) Hybrid topology

Mesh topology

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. A fully connected mesh network has n (n-1) physical channels to link n devices. To accommodate the links every device on the network must have (n-1) I/O ports.

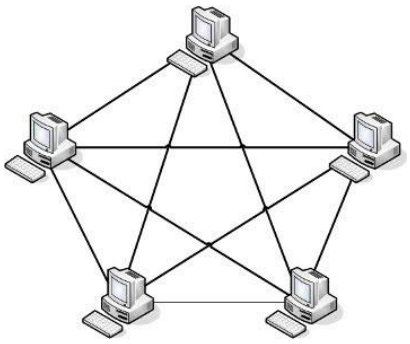


Figure 1.4 Mesh topology

Advantages:

a) Mesh topology is robust.

b) Better privacy and security.

c) Failure of one link will not disturb other links.

d) Helps the network manager to find the precise location of the fault and solution.

Disadvantages:

a) Large amount of cabling and I/O ports are required.

b) Installation and reconnection are difficult.

Star Topology

In a star topology, each device has a dedicated point-to-point link to a central controller (HUB) only. If one link fails, that link is affected. All other links remain active.

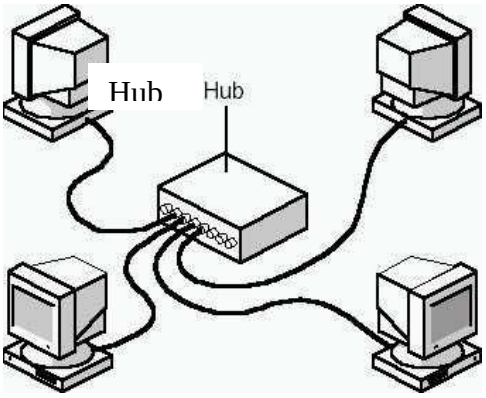


Figure 1.5 Star topology

Advantages:

a) Less expensive.
b) Star topology is robust.
c) Fault identification and fault isolation are easy.
d) Modification of star network is easy.

Disadvantages:

a) If the central hub fails, the whole network will not work.
b) Communication is possible only through the hub.

Bus topology

One long cable acts as a backbone to link all the devices in the network. Nodes are connected to the back bone by taps and drop lines. Drop line is establishing the connection between the devices and the cable. The taps are used as connectors. To keep the energy level of the signal the taps are placed in the limited distance.

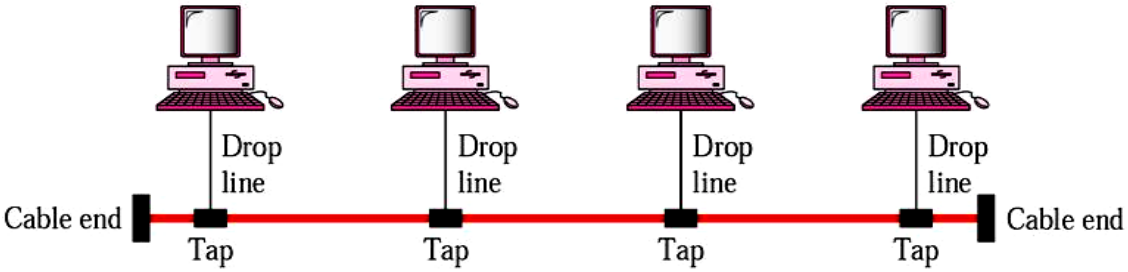


Figure 1.6 Bus topology

Advantages:

a) Easy installation.
b) Less cabling and less number of I/O port is required.
c) Less cost.

Disadvantages:

a) Network traffic is high.
b) Fault isolation and reconnection is difficult.
c) Adding new device is difficult.
d) A break in the bus cable stops all transmissions.

Ring topology

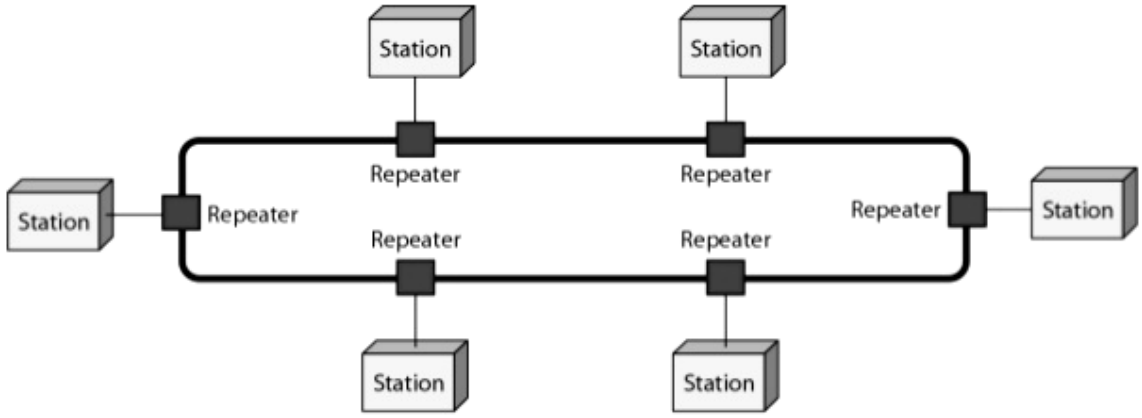


Figure 1.7 Ring topology

In a ring topology, each device has a dedicated point-to-point link with other devices. Each device is linked only to its immediate neighbors. A signal is travel along the ring in only one direction from device to device until it reaches its destination. The repeater is used to regenerate the signals during the transmission.

Advantages:

a) Easy to install and reconfigure.

b) Link failure can be easily found.

Disadvantages:

a) Maximum ring length and number of devices is limited.

b) Failure of one node on the ring affects the entire network.

c) Addition of nodes or removal of nodes disrupts the network.

d) Signal traffic is unidirectional.

`Hybrid Topology

Integration of two or more different topologies to form a resultant topology which has good points of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

For example, if there exists a ring topology in one office department while a bus topology in another department, connecting these two will result in hybrid topology. Connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star-Bus networks are most common examples of hybrid network.

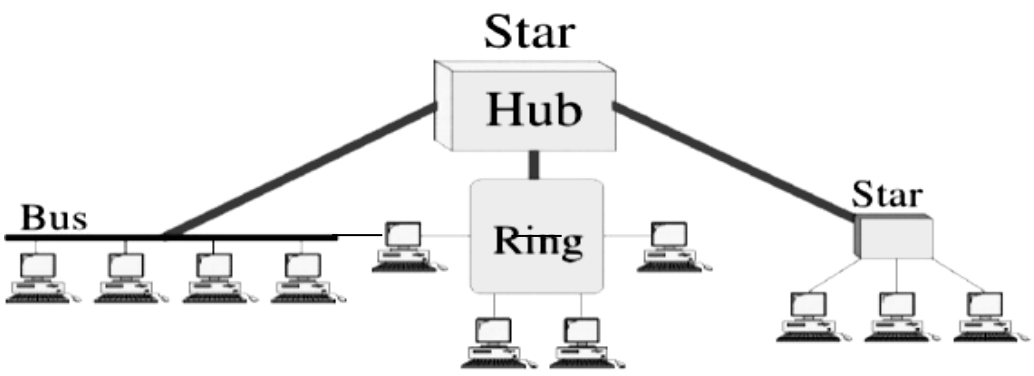


Figure 1.8 Hybrid topology

1.5 PROTOCOLS AND STANDARDS

A protocol is a set of rules that governs data communications. A protocol defines what has been communicated and when it has been communicated. The important elements of a protocol are:

a. **Syntax**: It represents the structure or format of the data.
b. **Semantics:** Gives the meaning for each section of bits, how the data is going to be interpreted and the action to be taken based on the interpretation.
c. **Timing:** It indicates when the data should be sent and how fast the data can be sent.

Protocol standards provide guidelines about the kind of interconnectivity necessary in today's market place and in international communication. Standards are of two types;

a. **Defacto**: The standard that have not been approved by an organization body but have been adopted as standards through widespread use are called Defacto standard.
b. **Dejure:** Standards that have been approved by an organized body.

2. PROTOCOL LAYERING

- A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.
- When communication is simple, we may need only one simple protocol. When communication is complex, we need to divide the task b/w different layers. We need a protocol at each layer, or protocol layering.

2.1 Scenarios

First Scenario

- In the first scenario, communication is so simple that it can occur in only one Layer (Figure 1.9).
- Assume Maria and Ann are neighbors with a lot of common ideas.
- Communication between Maria and Ann takes place in one layer, face to face, in the same language

Figure 1.9 A single - layer protocol

Second Scenario

- Maria and Ann communicate using regular mail through the post office (Figure 1.10).
- However, they do not want their ideas to be revealed by other people if the letters are intercepted.
- They agree on an encryption/decryption technique.
- The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter.

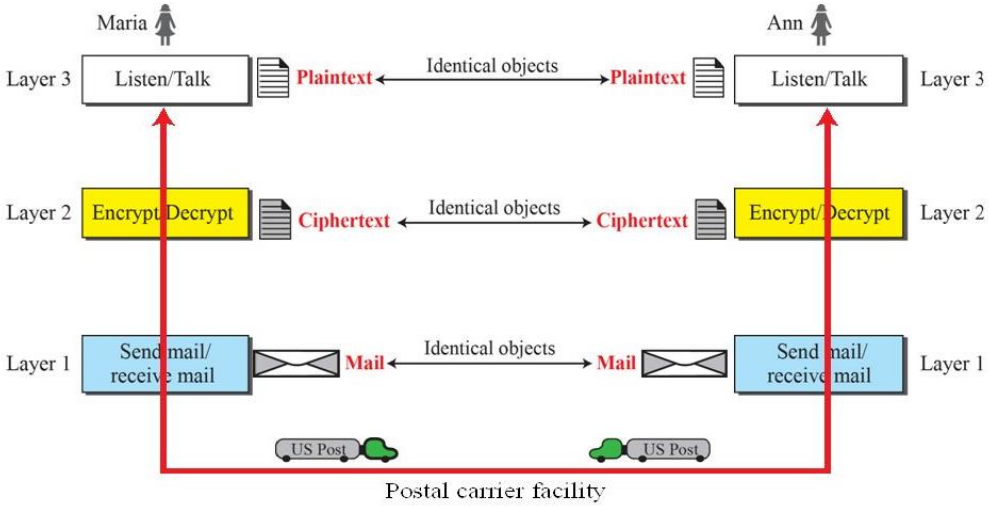


Figure 1.10 A three - layer protocol

2.1.1 Protocol Layering

- Protocol layering enables us to divide a complex task into several smaller and simpler tasks.
- Modularity means independent layers.
- A layer (module) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs.
- If two machines provide the same outputs when given the same inputs, they can replace each other.

Advantages:

1) It allows us to separate the services from the implementation.
2) There are intermediate systems that need only some layers, but not all layers.

Disadvantage:

1) Having a single layer makes the job easier. There is no need for each layer to provide a service to the upper layer and give service to the lower layer.

2.2 Principles of Protocol Layering

i) First Principle

→ If we want bidirectional communication, we need to make each layer able to perform 2 opposite tasks, one in each direction.

→ For example, the third layer task is to listen (in one direction) and talk (in the other direction).

ii) Second Principle

→ The two objects under each layer at both sites should be identical.

→ For example, the object under layer 3 at both sites should be a plaintext letter.

2.3 Logical Connections

- We have layer-to-layer communication (Figure 1.11).
- There is a logical connection at each layer through which 2 end systems can send the object created from that layer.

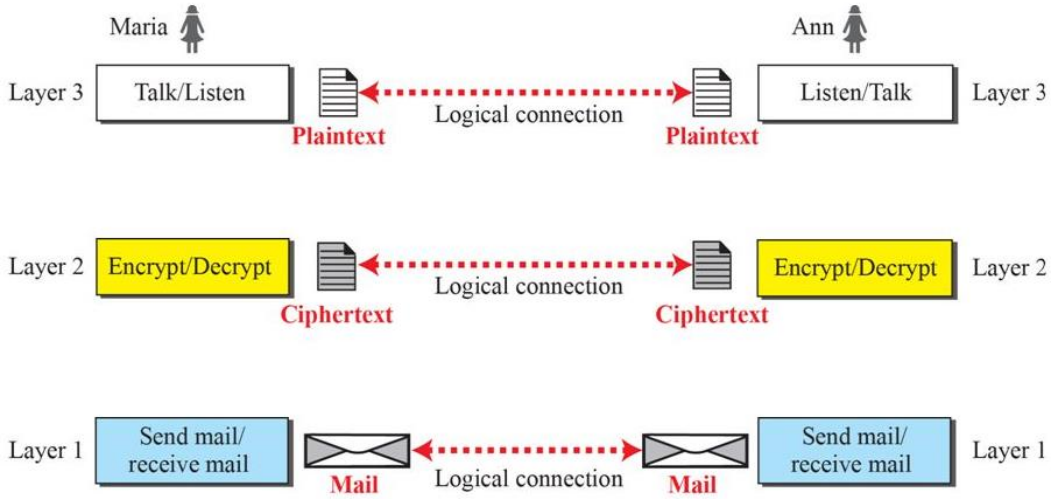


Figure 1.11 Logical connections between peer layers

3 TCP/IP PROTOCOL SUITE

TCP/IP is a protocol-suite used in the Internet today. Protocol-suite refers a set of protocols organized in different layers. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols.

Layered Architecture

Let us assume that computer A communicates with computer B as shown in Figure 1.12. As the Figure 1.13 shows, we have five communicating devices;

i. Source host(computer A)
ii. Link-layer switch in link 1
iii. Router
iv. Link-layer switch in link 2
v. Destination host (computer B)

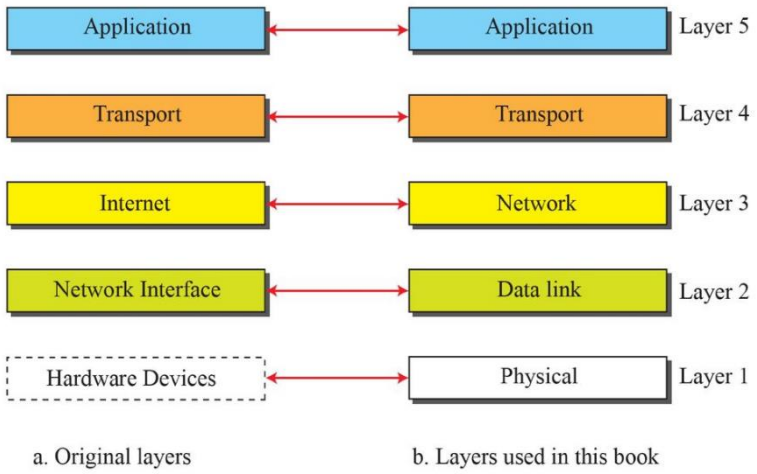


Figure 1.12 Layers in the TCP/IP protocol suite

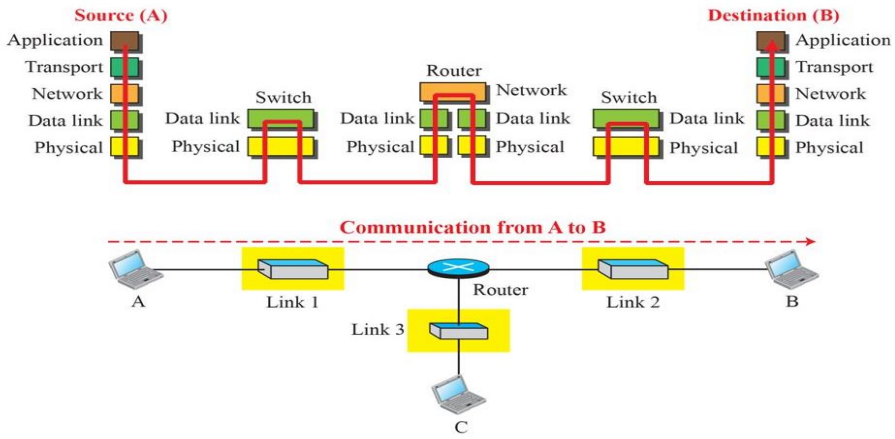


Figure 1.13 Communication through an Internet

Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts are involved in all five layers. The source host creates a message in the application layer and sends the message down the layers so that it is physically sent to the destination host.

The destination host receives the message at the physical layer and then delivers the message through the other layers to the application layer. The router is involved in only three layers; there is no transport or application layer. A router is involved in n combinations of link and physical layers, where n is the number of links the router is connected to. The reason is that each link may use its own data-link or physical protocol. A link-layer switch is involved only in two layers namely, data-link layer and physical layer.

3.2 Layers in the TCP/IP Protocol Suite

As shown in the figure1.14, the duty of the application, transport, and network layers is end-to-end. However, the duty of the data-link and physical layers is hop-to-hop. A hop is a host or router. The domain of duty of the top three layers is the internet. The domain of duty of the two lower layers is the link. In top 3 layers, the data unit should not be changed by any router or link-layer switch.

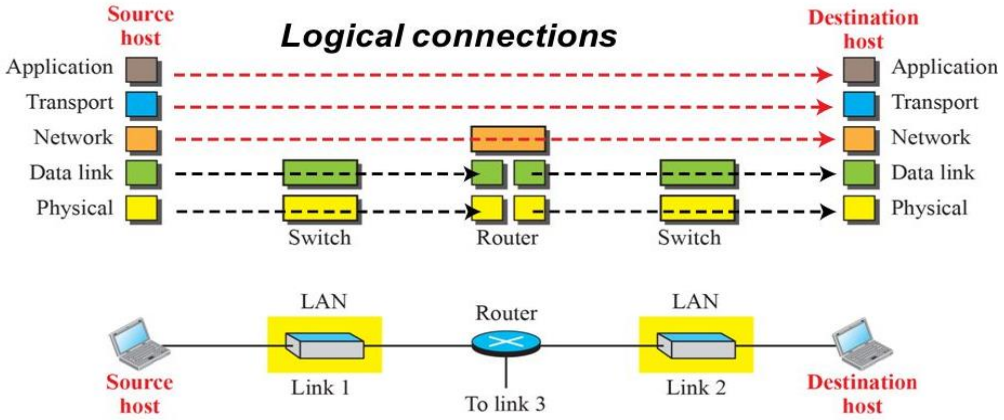


Figure 1.14 Logical connections between layers of the TCP/IP protocol suite

In bottom 2 layers, the data unit is changed only by the routers, not by the link-layer switches. Identical objects exist between two hops. Because router may fragment the packet at the network layer and send more packets than received (Figure 1.15). The link between two hops does not change the object.

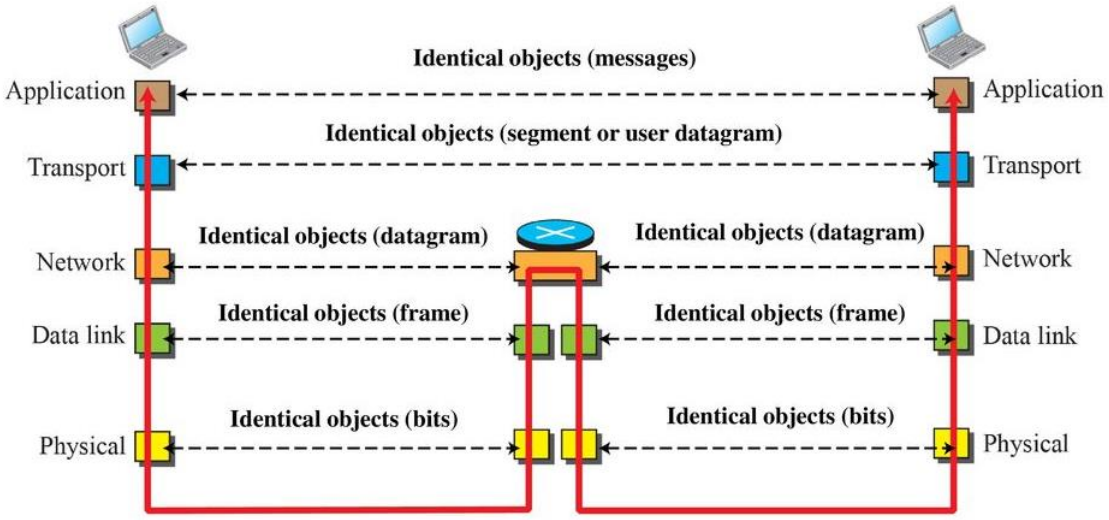


Figure 1.15 Identical objects in the TCP/IP protocol suite

3.2.1 Description of Each Layer

Physical Layer

The physical layer receives bits from the data-link layer and sends through the transmission media. The physical layer is responsible for movements of individual bits from one node to another node. Transmission media is another hidden layer under the physical layer. Two devices are connected by a transmission medium (cable or air). The transmission medium does not carry bits; it carries electrical or optical signals.

Data Link Layer

Data-link-layer (DLL) is responsible for moving frames from one node to another node over a link. The link can be wired LAN/WAN or wireless LAN/WAN. The data-link layer

- Gets the datagram from network layer

- Encapsulates the datagram in a packet called a frame.
- Sends the frame to physical layer.

TCP/IP model does not define any specific protocol. DLL supports all the standard and proprietary protocols. Each protocol may provide a different service. Some protocols provide complete error detection and correction; some protocols provide only error correction.

Network Layer

The network layer is responsible for source-to-destination transmission of data. The network layer is also responsible for routing the packet. The routers choose the best route for each packet. Why we need the separate network layer?

- The separation of different tasks between different layers
- The routers do not need the application and transport layers.
- TCP/IP model defines 4 protocols. They are;
  i. IP (Internetworking Protocol)
  ii. ARP (Address Resolution Protocol)
  iii. ICMP (Internet Control Message Protocol)
  iv. IGMP (Internet Group Message Protocol)

i) IP (Internetworking Protocol)

- IP is the main protocol of the network layer.
- IP defines the format and the structure of addresses.
- IP is also responsible for routing a packet from its source to its destination.
- It is a connection-less & unreliable protocol.
- Connection-less means there is no connection setup b/w the sender and the receiver.
- Unreliable protocol means that IP does not make any guarantee about delivery of the data and packets may get dropped during transmission.
- It provides a best-effort delivery service.
- Best effort means IP does its best to get the packet to its destination, but with no guarantees.
- IP does not provide flow control, error control and congestion control services.
- If an application requires above services, the application should rely only on the transport- layer protocol.

ii) ARP

- ARP is used to find the physical-address of the node when its Internet-address is known.
- Physical address is the 48-bit address that is imprinted on the NIC or LAN card.
- Internet address (IP address) is used to uniquely & universally identify a device in the internet.

iii) ICMP

- ICMP is used to inform the sender about datagram-problems that occur during transit.

iv) IGMP

- IGMP is used to send the same message to a group of recipients.

Transport Layer

Transport Layer protocols are responsible for delivery of a message from a process to another process. The transport layer gets the message from the application layer and encapsulates the message in a packet called a segment then sends the segment to network layer. TCP/IP model defines 3 protocols for transport layer;

i. TCP (Transmission Control Protocol)
ii. UDP (User Datagram Protocol)
iii. SCTP (Stream Control Transmission Protocol)

i) TCP

- TCP is a reliable connection-oriented protocol.
- A connection is established b/w the sender and receiver before the data can be transmitted.
- TCP provides flow control, error control and congestion control services.

ii) UDP

- UDP is the simplest of the 3 transport protocols.
- It is an unreliable, connectionless protocol.
- It does not provide flow, error, or congestion control.
- Each datagram is transported separately & independently.
- It is suitable for application program that needs to send short messages and cannot afford the retransmission.

iii) SCTP

- SCTP provides support for newer applications such as voice over the Internet.
- It combines the best features of UDP and TCP.

Application Layer

The two application layers exchange messages between each other. 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. Process-to-process communication is the duty of the application layer. TCP/IP model defines following protocols;

i. FTP (File Transfer Protocol)
ii. SMTP (Simple Mail Transfer Protocol))
iii. DNS (Domain Name System)
iv. HTTP (Hyper Text Transfer Protocol)
v. SNMP (Simple Network Management Protocol)
vi. TELNET (Terminal Network)

- SMTP is used to transport email between a source and destination.
- TELNET is used for accessing a site remotely.
- FTP is used for transferring files from one host to another.
- DNS is used to find the IP address of a computer.
- SNMP is used to manage the Internet at global and local levels.

- HTTP is used for accessing the World Wide Web (WWW).

3.3 Encapsulation and Decapsulation

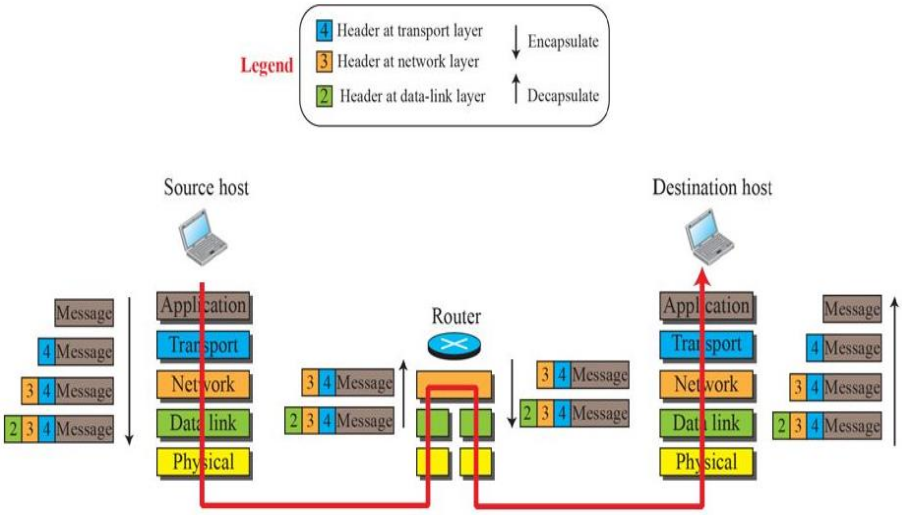


Figure 1.16 Encapsulation/ Decapsulation

Encapsulation at the Source Host (Figure 1.16)

- At the application layer, the data to be exchanged is referred to as a message.
  - ➢ A message normally does not contain any header or trailer.
  - ➢ The message is passed to the transport layer.
- The transport layer takes the message as the payload.
  - → Transport layer adds its own header to the payload.
  - → The header contains identifiers of the source and destination application programs and information needed for flow, error control, or congestion control.
  - → The transport-layer packet is called the segment (in TCP) and the user datagram (in UDP).
  - → The segment is passed to the network layer.
- The network layer takes the transport-layer packet as payload.
  - → NL adds its own header to the payload.
  - → The header contains the addresses of the source and destination hosts, some information used for error checking of the header and fragmentation information.
  - → The network-layer packet is called a datagram.
  - → The datagram is passed to the data-link layer.
- The data-link layer takes the network-layer packet as payload.
  - → DLL adds its own header to the payload.
  - → The header contains the physical addresses of the host or the next hop (the router).
  - → The link-layer packet is called a frame.
  - → The frame is passed to the physical layer for transmission

Decapsulation and Encapsulation at the Router

At the router, we have both encapsulation & encapsulation and because the router is connected to two or more links.

- Data-link layer
  - receives frame from physical layer
  - decapsulates the datagram from the frame and
  - Passes the datagram to the network layer.
- The network layer
  - Inspects the source and destination addresses in the datagram header and
  - Consults forwarding table to find next hop to which the datagram is to be delivered.
  - The datagram is then passed to the data-link layer of the next link.
- The data-link layer of the next link
  - Encapsulates the datagram in a frame and
  - Passes the frame to the physical layer for transmission.

Decapsulation at the Destination Host

At the destination host, each layer decapsulates the packet received from lower layer and removes the payload then delivers the payload to the next-higher layer

3.4 Addressing

We have logical communication between pairs of layers. Any communication that involves 2 parties needs 2 addresses: source address and destination address. We need 4 pairs of addresses as described in Figure 1.17;

i. At the application layer, we normally use names to define
- site that provides services, such as abc.com, or
- e-mail address, such abc@gmail.com

ii. **At the transport layer, addresses are called port numbers**.
- Port numbers define the application-layer programs at the source and destination.
- Port numbers are local addresses that distinguish between several programs running at the same time.

iii. At the network-layer, addresses are called IP addresses.
- IP address uniquely defines the connection of a device to the Internet.
- The IP addresses are global, with the whole Internet as the scope.

iv. At the data link-layer, addresses are called MAC addresses
- The MAC addresses defines a specific host or router in a network (LAN or WAN).
- The MAC addresses are locally defined addresses.

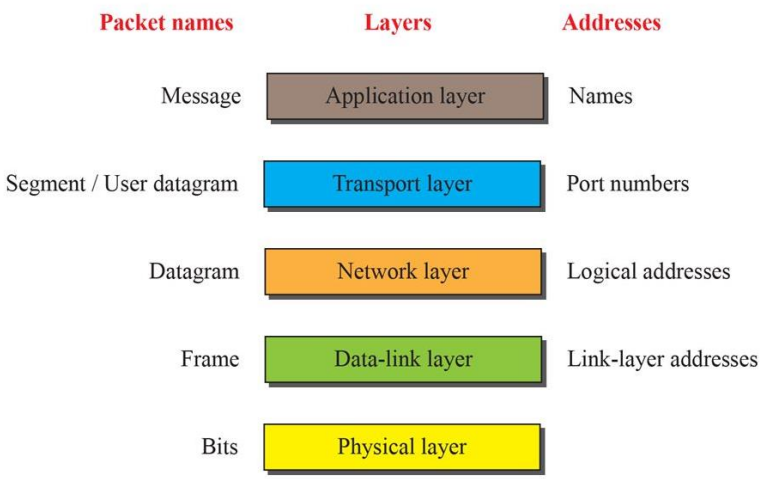


Figure 1.17 Addressing in the TCP/IP protocol suite

3.5 Multiplexing and Demultiplexing

Multiplexing means a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time) as shown in Figure 1.18. Demultiplexing means a protocol can decapsulates and deliver a packet to several next-higher layer protocols (one at a time).

i. At transport layer, either UDP or TCP can accept a message from several application-layer protocols.

ii. At network layer, IP can accept

→ a segment from TCP or a user datagram from UDP

→ a packet from ICMP or IGMP

iii. At data-link layer, a frame may carry the payload coming from IP or ARP.

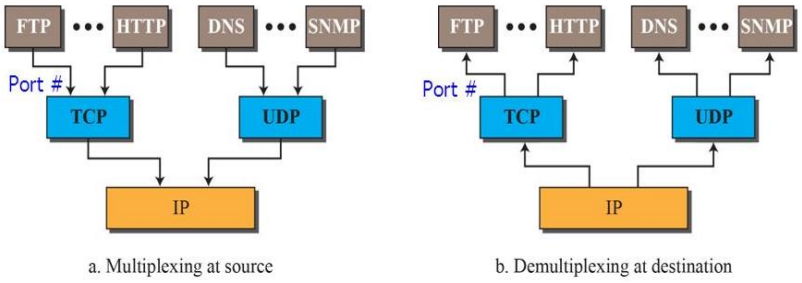


Figure 1.18 Multiplexing and Demultiplexing

4. OSI MODEL

An ISO standard that covers all the aspects of network communication is the Open System Interconnection Model. Open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. Without changing the logic of the hardware and software, two systems can communicate with the help of open system. OSI model consists of seven layers. The layers define the process of moving the information across the network. The seven layers of the OSI model are;

(1) physical layer

(2) data link layer

(3) network layer

(4) transport layer

(5) session layer

(6) presentation layer and

(7) application layer

Layered architecture

When a message travels from the sender to receiver, it may pass through many intermediate nodes. Only the first three layers of the intermediate nodes are involved in all communication. Each layer calls upon the services of the layers just below it. This is done with the help of protocols.

The processes on each machine that communicate at a given layer are called Peer-to-peer. The passing of data and network information between the layers are carried out with the help of interfaces. Interface is used to define the information and services to be provided by each layer.

4.1 OSI vs. TCP/IP

1) The four bottommost layers in the OSI model & the TCP/IP model are same (Figure 1.19). However, the Application-layer of TCP/IP model corresponds to the Session, Presentation & Application Layer of OSI model.

Two reasons for this are:

1) TCP/IP has more than one transport-layer protocol.

2) Many applications can be developed at Application layer

2) The OSI model specifies which functions belong to each of its layers. In TCP/IP model, the layers contain relatively independent protocols that can be mixed and matched depending on the needs of the system.

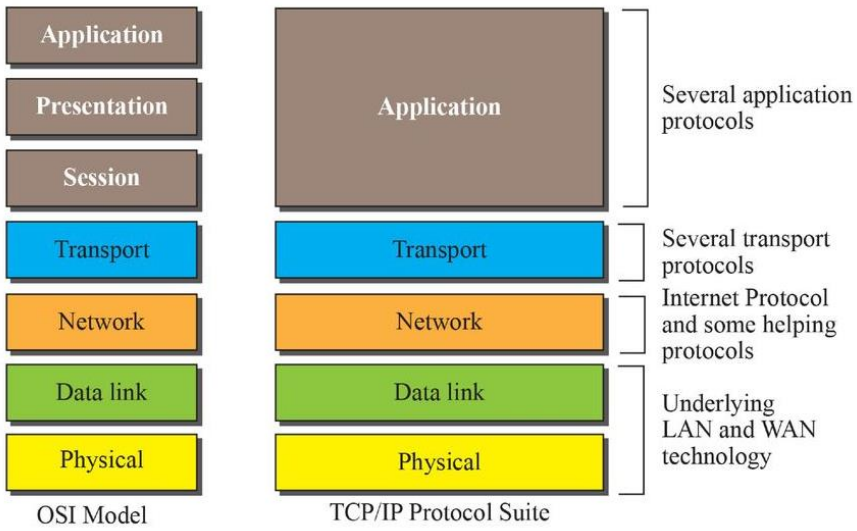


Figure 1.19 TCP/IP and OSI model

Lack of OSI Model's Success

- OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on

the suite; changing it would cost a lot.

- Some layers in the OSI model were never fully defined.
- When OSI was implemented by an organization in a different application, it did not show a high enough level of performance

4.2 Organization of the Layers

The below figure 1.20 gives an overall view of the OSI layers. The seven layers are categorized into three subgroups. Layers 1, 2, and 3-physical, data link, and network-are the network support layers. Layers 5, 6, and 7-session, presentation, and application – are the user support layers. Layer 4, the transport layer, links the two subgroups and ensures that, what the lower layers have transmitted is in a form that the upper layers can use.

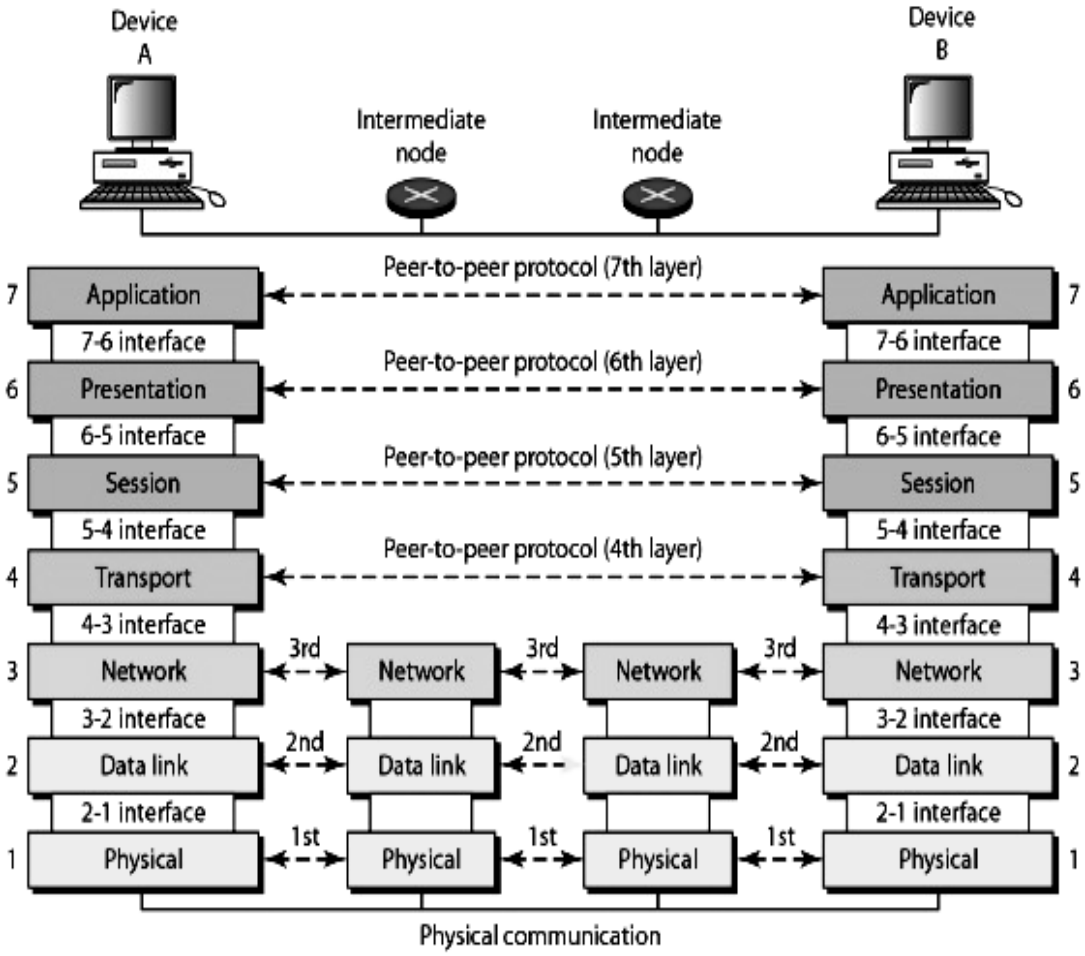


Figure 1.20 The interaction between layers in the OSI model

Network support layers deal with the physical aspects of moving data from one device to another such as electrical specifications, physical connections, physical addressing, and transport timing and reliability. User support layers allow interoperability among unrelated software systems. The upper OSI layers are always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

The process starts at the application layer then moves from layer to layer in descending, sequential order. At each layer, a **header,** or possibly a **trailer,** can be added to the data unit. The trailer is added only at layer 2. When the formatted data unit passes through the physical layer, it is changed into an electromagnetic

signal and transported along a physical link. Upon reaching its destination, the signal passes into physical layer and is transformed back into digital form. The data units are then moved back up through the OSI layers.

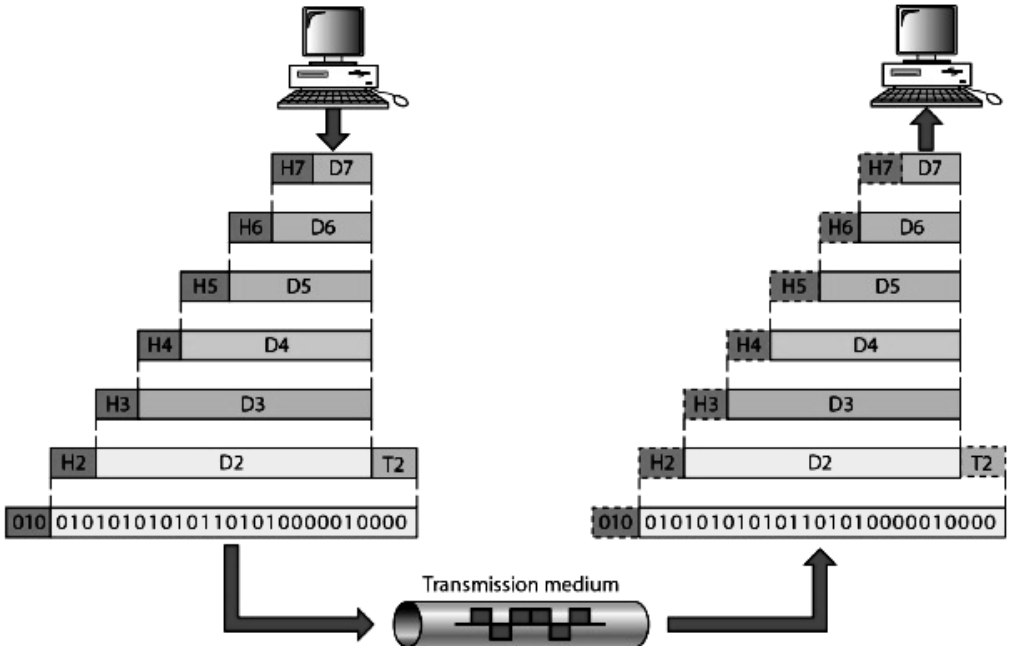


Figure 1.21 Data exchange using the OSI model

When the block of data reaches the next higher layer, the headers and trailers attached by the sending layer are removed. When the data unit reaches the application layer, the message is again in a form appropriate to the application and is made available to the recipient.

4.3 LAYERS IN THE OSI MODEL

Physical Layer

The physical layer is responsible for movements of individual bits from one hop (node) to the next. The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. Physical layer defines the procedures and functions that physical devices and interfaces have to perform for transmission of data. The physical layer is also concerned with the following:

a) **Physical characteristics of interfaces and medium:** Defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

b) **Representation of bits:** A stream of bits is encoded into signals (electrical or optical). It defines the type of encoding.

c) **Data rate:** The number of bits sent/Sec is also defined by the physical layer.

d) **Synchronization of bits:** The sender and the receiver clocks must be synchronized.

e) **Line configuration:** The connection of devices to the media (point-to-point configuration or multipoint configuration).

f) **Physical topology:** The physical topology defines how devices are connected to make a network.

g) **Transmission mode:** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data Link Layer

The data link layer is responsible for moving frames from one hop (node) to the next. Other responsibilities of the data link layer include the following:

a) **Framing:** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
b) **Physical addressing:** It adds a header to the frame to define the sender and/or receiver of the frame
c) **Flow control:** The data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
d) **Error control:** It adds reliability by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames by adding the trailer to the end of the frame.
e) **Access control:** It determine which device has control over the link at any given time, when two or more devices are connected to the same link.

Network Layer

The network layer is responsible for the delivery of individual packets from the source host to the destination host. Other responsibilities of the network layer include the following;

a) **Logical addressing:** When a packet passes the network boundary, the network layer adds the logical addresses of the sender and receiver.
b) **Routing:** When independent networks or links are connected to create internetwork, the connecting devices (called routers or switches) route or switch the packets to their final destination.

Transport Layer

The transport layer is responsible for the delivery of a message from one process to another. Other responsibilities of the transport layer include the following;

a) **Service-point addressing:** The transport layer gets the entire message to the correct process on the destination system by adding a type of address called a service-point address (or port address).
b) **Segmentation and reassembly:** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers are used to reassemble the message at the destination and to identify and replace packets that were lost in transmission.
c) **Connection control:** In a connectionless service each segment is treated as independent packet and in connection oriented service each segment is treated as dependent packet. After all the data are transferred, the connection is terminated.
d) **Flow control:** Flow control is performed from end to end rather than across a single link.
e) **Error control:** At this layer the error control is performed in a process-to-process rather than across a single link.

Session Layer

The session layer is responsible for dialog control and synchronization. Specific responsibilities of the session layer include the following;

a) **Dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex or full-duplex mode.

b) **Synchronization:** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 100 pages, it is advisable to insert checkpoints after every 10 pages to ensure that each 10-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 23, the only pages that need to be resent after system recovery are pages 21 to 30.

Presentation Layer

The presentation layer is responsible for translation, compression, and encryption. Specific responsibilities of the presentation layer include the following:

a) **Translation:** The presentation layer is responsible for the interoperability between different encoding methods.

b) **Encryption:** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

c) **Compression:** Data compression reduces the number of bits contained in the information. Data compression is important in the transmission of multimedia such as text, audio, and video.

Application Layer

The application layer is responsible for providing services to the user. Specific services provided by the application layer include the following:

a) **Network virtual terminal:** A network virtual terminal is a software version of a physical terminal and it allows a user to log on to a remote host.

b) **File transfer, access, and management:** This application allows a user to access files in a remote host, to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

c) **Mail services:** This application provides the basis for e-mail forwarding and storage.

d) **Directory services:** This application provides distributed database sources and access for global information about various objects and services.

5. TRANSMISSION MEDIAS

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

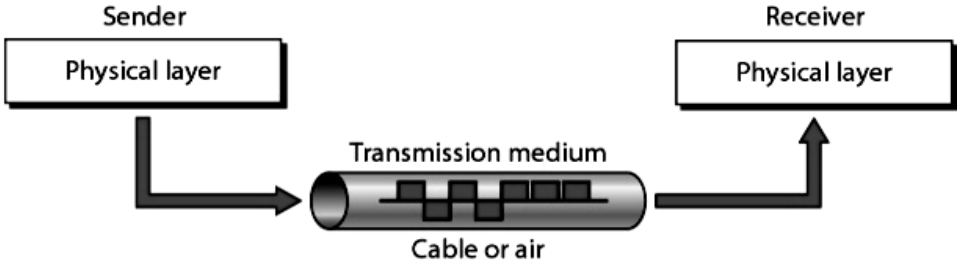
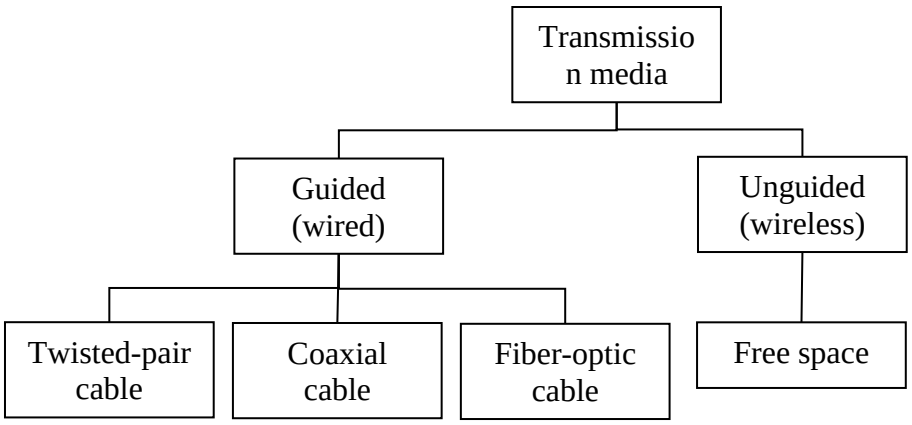


Figure 1.22 Transmission medium

Transmission media can be divided into two broad categories: Guided medium and unguided medium.



5.1 Guided Media

Guided media provide a conduit from one device to another. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

5.1.1 Twisted-Pair Cable

Twisting makes it probable that both wires are equally affected by external influences. The number of twists per unit of length has some effect on the quality of the cable.

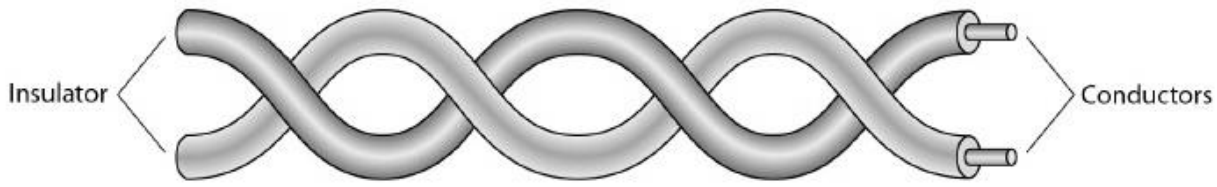


Figure 1.23 Twisted-pair cable

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk. It is bulkier and more expensive.

Connectors

The most common UTP connector is RJ45 (RJ stands for registered jack). The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

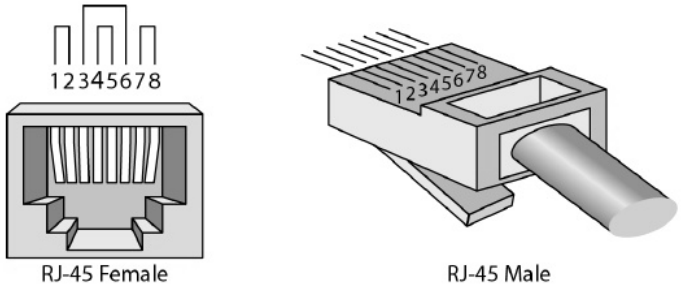


Figure 1.24 UTP connector

Categories of Unshielded Twisted-Pair Cable

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories.

Category	Specification	Data Rate (Mbps)	Use
1	Unshielded twisted-pair used in telephone	<0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT-2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Table 1.1 Categories of unshielded twisted-pair cables

Applications

a) Twisted-pair cables are used in telephone lines to provide voice and data channels.

b) Local-area networks, such as 10Base-T and 100Base-T, also use twisted-pair cables.

Performance

A twisted-pair cable can pass a wide range of frequencies. With increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz. Gauge is a measure of the thickness of the wire.

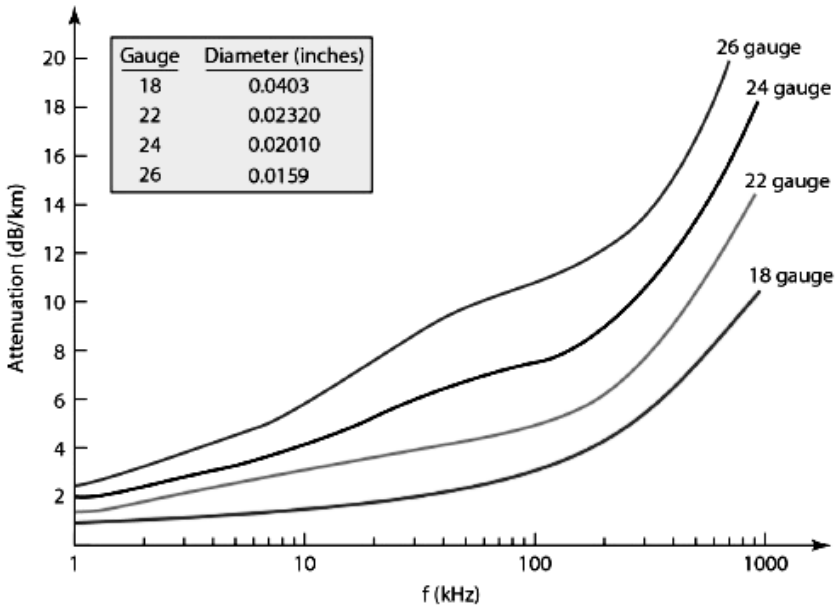


Figure 1.25 UTP Cable - Performance

5.1.2 Coaxial Cable

Coaxial cable carries signals of higher frequency ranges. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

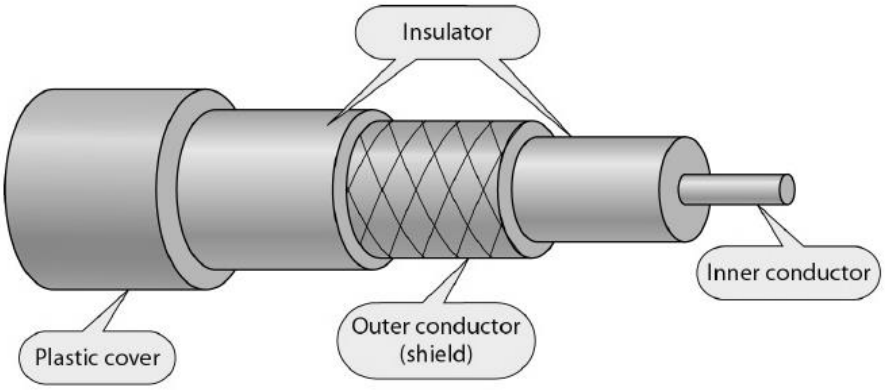


Figure 1.26 Coaxial cable

Coaxial Cable Standards

Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function.

Category	Impedance	Use

RG – 59	75Ω	Cable TV
RG – 58	50Ω	Thin Ethernet
RG – 11	50Ω	Thick Ethernet

Table 1.2 Categories of coaxial cables

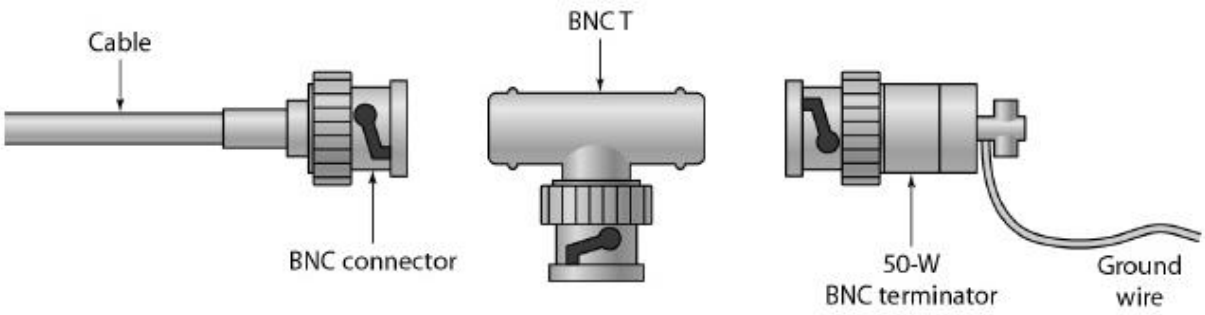
Coaxial Cable Connectors

To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNe) connector. Three popular types of connectors:

a) BNC connector - used to connect the end of the cable to a device, such as a TV set.

b) BNC T connector - The BNC T connector is used in Ethernet networks to branch out a connection to a computer or other device

c) BNC terminator - The BNC terminator is used at the end of the cable to prevent the reflection of the signal.



(a) BNC Connector (b) BNCT Connector (c) BNC Terminator

Figure 1.27 BNC connectors

Applications of the coaxial cable

a) Cable TV

b) Telecommunication

c) Traditional Ethernet LANs

Performance of the coaxial cable

The attenuation is much higher in coaxial cables than in twisted-pair cable. Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

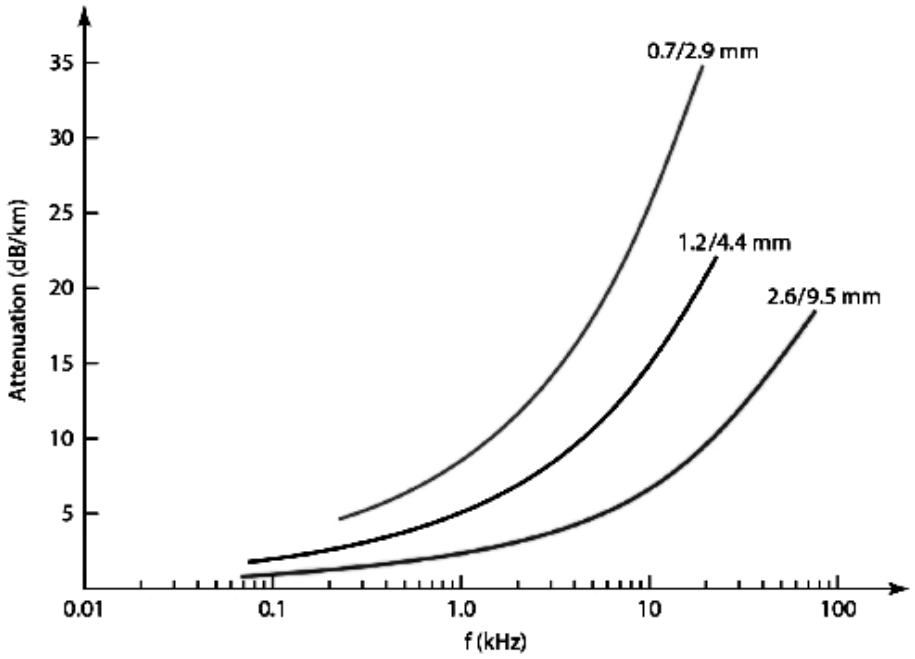
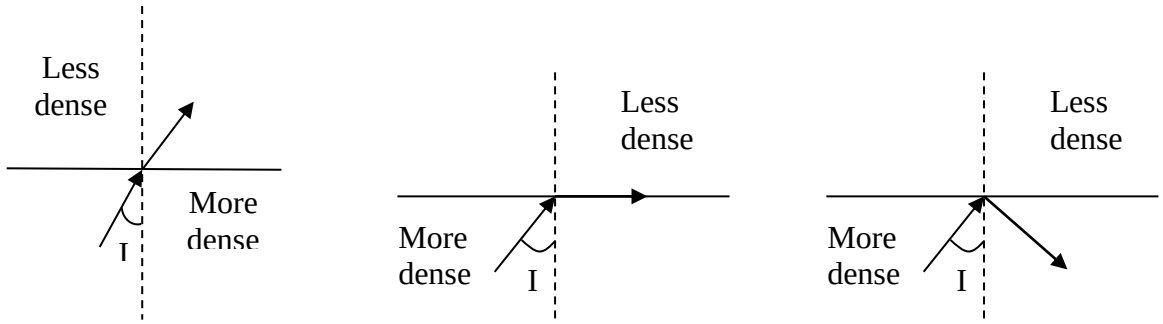


Figure 1.28 Performance of the coaxial cable

5.1.3 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 the ray changes direction.



I < Critical angle, refraction I = Critical angle, refraction I > Critical angle, refraction

Figure 1.29 Bending of light ray

Bending Of Light

a) If the angle of incidence is less than the critical angle, the ray refracts and moves closer to the surface.
b) If the angle of incidence is equal to the critical angle, the light bends along the interface.
c) If the angle of incidence is greater than the critical angle, the ray reflects and travels again in the denser substance.

The critical angle is a property of the substance, and its value differs from one substance to another. Optical fibers use reflection to guide light through a channel. Glass or plastic core is surrounded by a cladding of less dense glass or plastic. 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.

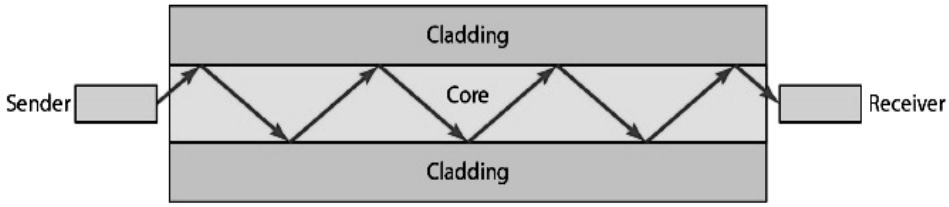
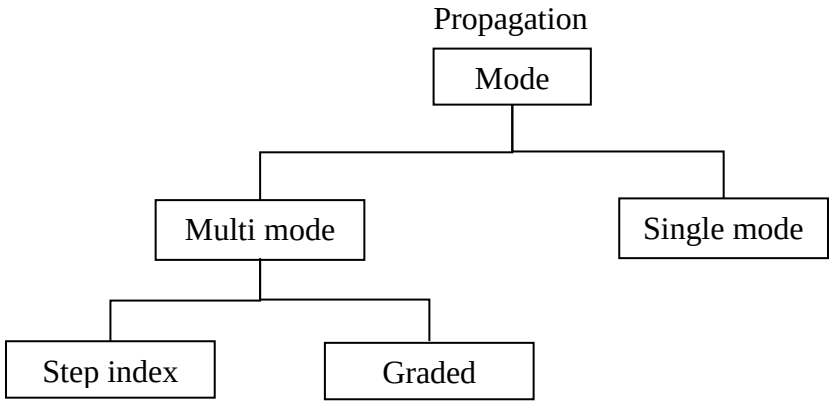


Figure 1.30 Optical fiber

Propagation modes

If the angle of incidence is less than the critical angle, the ray refracts and moves closer to the surface.



(i) **Multimode fiber:** Multiple beams from a light source move through the core in different paths. Multimode can be implemented in two forms step-index and graded-index.

(a) *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.

(b) *Multimode graded-index fiber:* The density of the core is varying. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

(ii) **Single mode:** Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber.

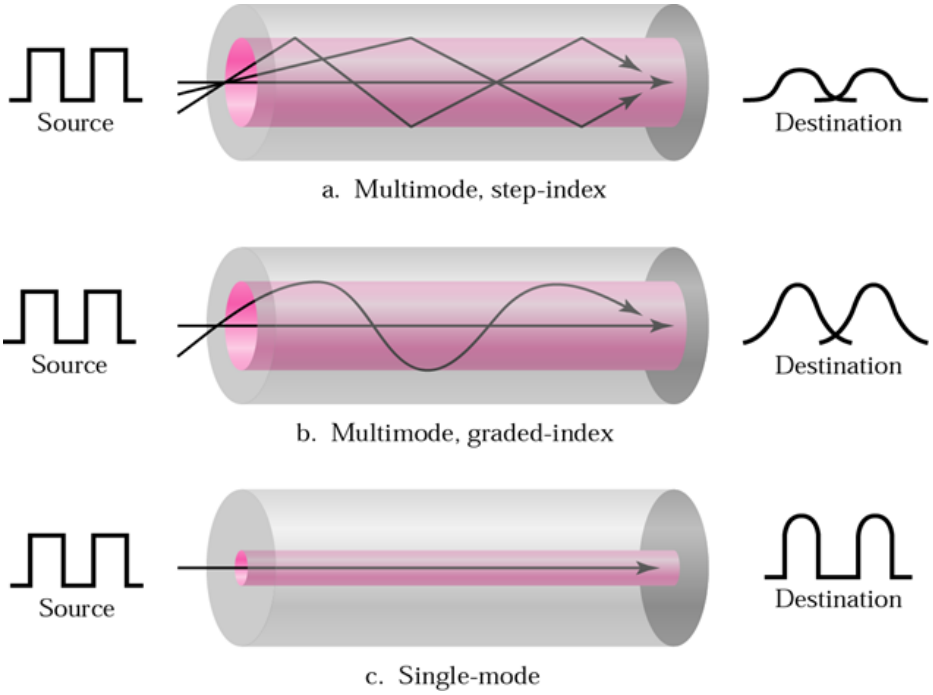


Figure 1.31 Optical fiber- Propagation modes

Fiber Sizes

Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers. The common sizes are

Type	Core (μm)	Cladding (μm)	Mode
501125	50.0	125	Multimode, graded index
62.51125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Table 1.3 Fiber types

Cable Composition

The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

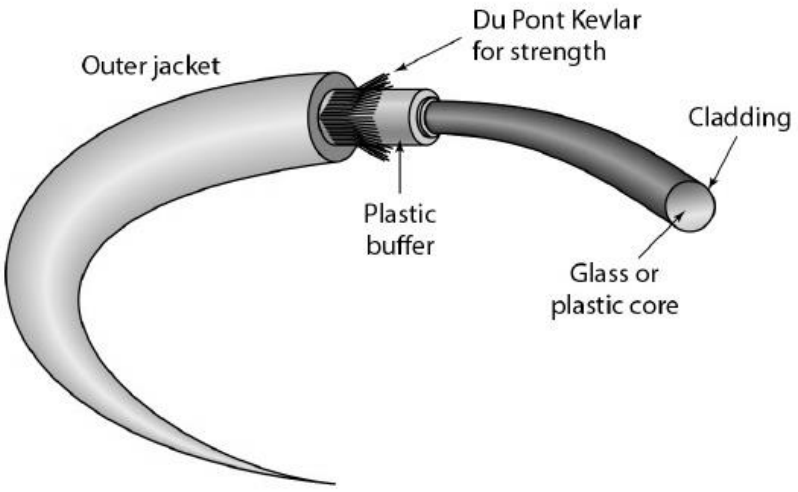


Figure 1.32 Fiber construction

Fiber-Optic Cable Connectors

a) The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system.
b) The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system. It is more reliable than SC.
c) MT-RJ is a connector that is the same size as RJ45, used in fast Ethernet

Advantages of Optical Fiber

a) Higher bandwidth
b) Less signal attenuation
c) Immunity to electromagnetic interference
d) Resistance to corrosive materials
e) Light weight
f) Greater immunity to tapping

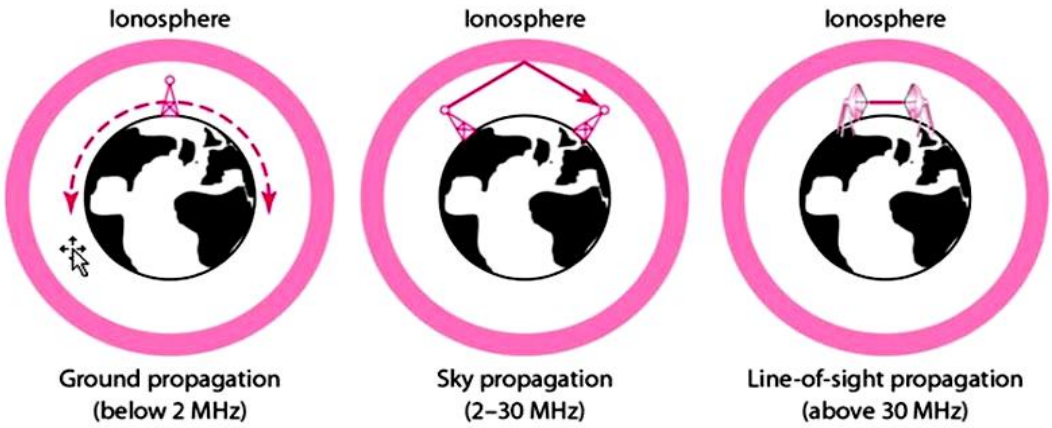
Disadvantages

a) Installation and maintenance
b) Unidirectional light propagation
c) Cost

5.2 Unguided Transmission Medias

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them. The part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, is used for wireless communication. Unguided signals can travel from the source to destination in several ways;

i) **Ground propagation:** Radio waves travel through the lowest portion of the atmosphere.
ii) S**ky propagation:** Higher frequency radio waves radiate upward into the ionosphere and they are reflected back to earth.
iii) L**ine-of-sight propagation:** Very high frequency signals are transmitted in straight lines directly from antenna to antenna



We can divide wireless transmission into 3 broad groups. They are,

i) Radio waves

ii) Microwaves

iii) Infrared waves

5.2.1 Radio waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. They are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions, means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. Radio waves with low and medium frequencies can penetrate walls. Radio waves are used for multi-communication (TV, radio, paging systems).

Disadvantages of Radio waves

a) Penetrate the walls

b) Omnidirectional

Figure 1.33 Omnidirectional antenna

5.2.2 Microwaves

Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional Microwave propagation is line-of-sight (antennas need to be in direct sight of each other). Very high-frequency microwaves cannot penetrate walls (a disadvantage if receivers are inside buildings). Use of certain portions of the band requires permission from authorities. Microwaves are using 2 types of antennas, they are

i) *The parabolic dish:* The parabolic dish focuses all incoming waves into a single point.

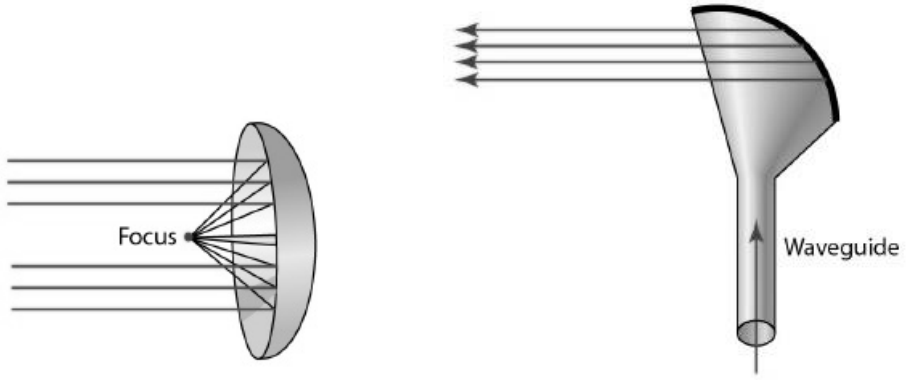
ii) *The horn:* A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head.

Applications

a) Cellular telephones

b) Satellite n/w

c) WLAN's



(a) Dish antenna (b) Horn antenna

Figure 1.34 Unidirectional antennas

5.2.3 Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz. Infrared waves having high frequencies cannot penetrate walls. Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

Differences between the guided and unguided media

Guided media	Unguided media
Signal energy propagates within the guided media	Signal energy propagates through air
Suitable for point-to-point communication	Suitable for broadcasting
Signals appears in the form of voltage	Signals appears in the form of electromagnetic waves
Ex: Twisted pair, Co-axial, Fiber optics	Ex: Radio wave, Micro wave, Infrared

6 Switching

A network is a set of connected devices. When multiple devices are connected, we must find the solution how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). In this method, the number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time.

Other topologies employing multipoint connections, such as a bus, are ruled out because the distances between devices and the total number of devices increase beyond the capacities of the media and equipment. A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.

In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

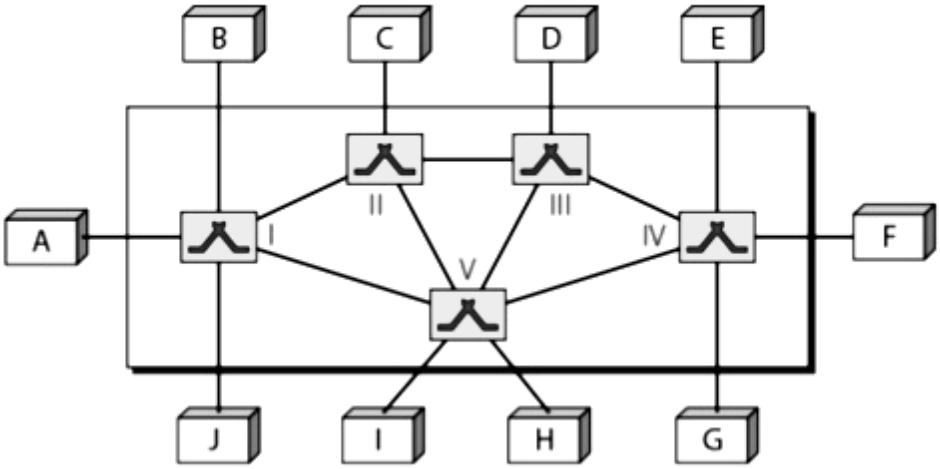


Figure 1.35 An example switched network

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links. Three methods of switching have been important;

i. Circuit switching
ii. Packet switching
iii. Message switching

We can then divide today's networks into three broad categories: circuit-switched networks, packet-switched networks, and message-switched. Packet-switched networks can further be divided into two subcategories-virtual-circuit networks and datagram networks.

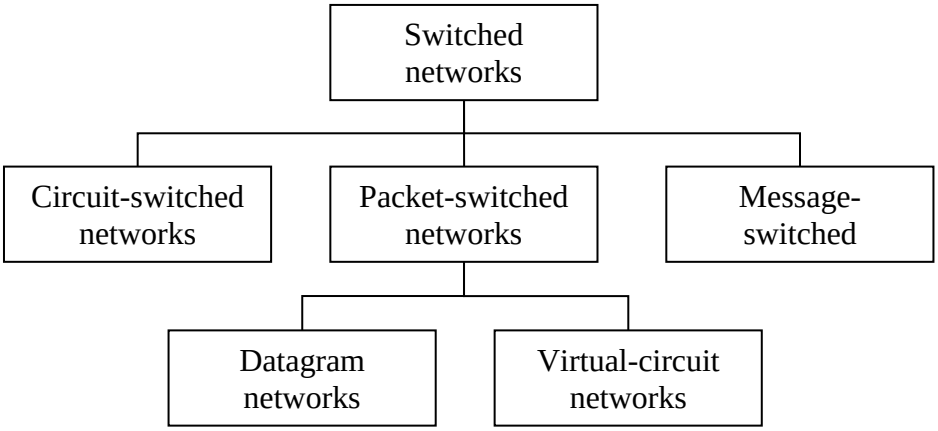


Figure 1.36 Categories of switched network

6.1 CIRCUIT SWITCHED NETWORKS

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels. A circuit-switched network with four switches and four links is shown below. Each link is divided into n (n is 3 in the figure 1.37) channels by using FDM or TDM.

When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase. A circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path.

After the dedicated path made of connected circuits (channels) is established, data transfer can take place. After all data have been transferred, the circuits are tom down. In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase. We need to emphasize several points here:

i. Circuit switching takes place at the physical layer.

ii. Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels, switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.

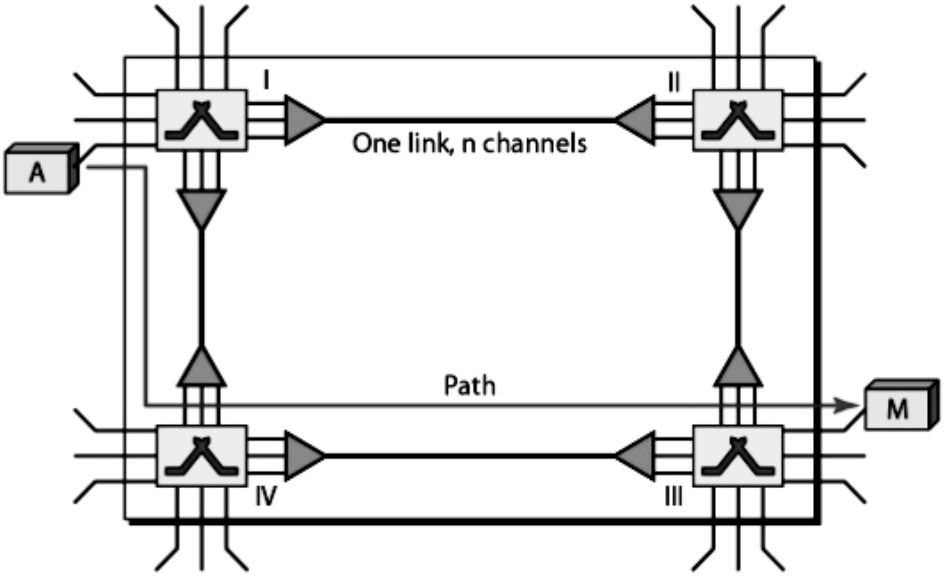


Figure 1.37 Circuit switched network

iii. Data transferred between the two stations are not packetized. There is a continuous flow of data from the source station to receiver station.

iv. There is no addressing involved during data transfer. The switches route the data based on their occupied band. End-to-end addressing is used during the setup phase.

Three phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

(i) Setup phase

- Before the communication, a dedicated circuit needs to be established.
- The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.
- In Figure1.37, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I.

- Switch I find a channel between itself and switch IV that can be dedicated for this purpose.
- Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III.
- Switch III informs system M of system A's intention at this time.
- In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A.
- Only after system A receives this acknowledgment is the connection established.
- Note that end-to-end addressing is required for creating a connection between the two end systems.

(ii) Data Transfer Phase

- After the establishment of the dedicated circuit, the two parties can transfer data.

(iii)Teardown Phase

- When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency

It can be argued that circuit-switched networks are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections. Switching at the physical layer in the traditional telephone network uses the circuit-switching approach.

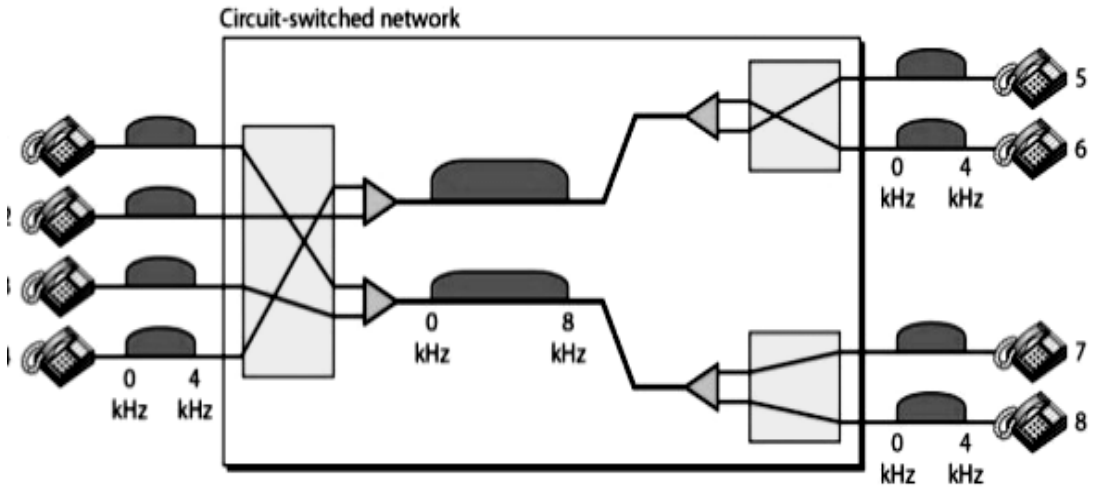


Figure 1.38 Example for circuit switched network

Disadvantages of circuit switched network

- Designed for voice communication.
- Data transmission line is often idle and its facilities wasted.
- Supports less data transmission rates only.
- Circuit switching is inflexible.
- Circuit switching sees all transmission as equal

6.2 PACKET SWITCHED NETWORK

In data communications, we need to send messages from one end system to another. The message is divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol. In packet switching, there is no resource allocation for a packet (no reserved bandwidth on the links, and no scheduled processing time for each packet). 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 is the source or destination, the packet must wait if there are other packets being processed.

6.2.1 Datagram approach

In a datagram network, each packet is treated independently of all others. Packets in this approach are referred to as datagram. Datagram switching is normally done at the network layer.

Figure 1.39 shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers.

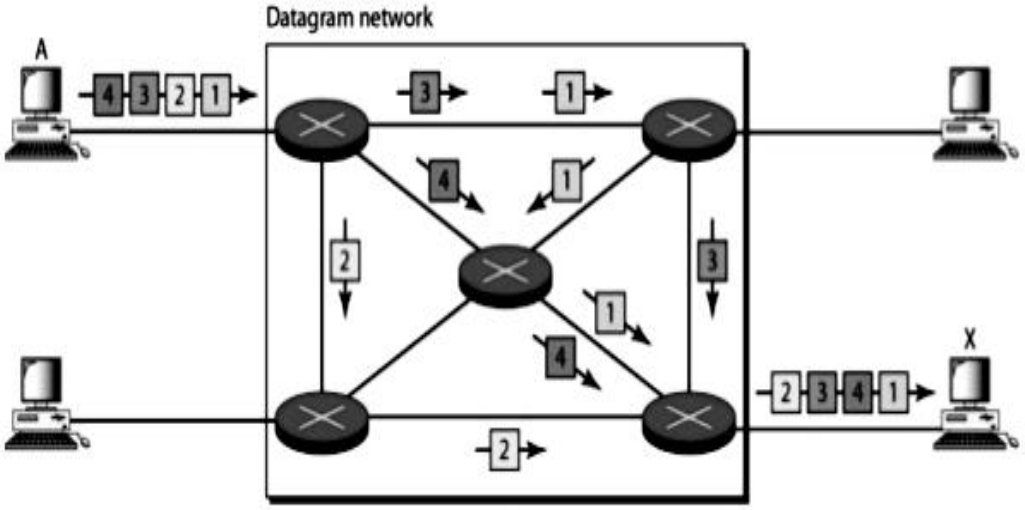


Figure 1.39 A datagram network with five switches (routers)

- All four packets (or datagram) belong to the same message but may travel different paths to reach their destination.
- This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X.
- Due to this the datagram of a transmission to arrive at their destination out of order with different delays between the packets.
- Packets may also be lost or dropped because of a lack of resources.
- It is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.
- The datagram networks are sometimes referred to as connectionless networks.
- There are no setup or teardown phases.

Routing table

If there are no setup or teardown phases, how the packets are routed to their destinations. In a datagram network each switch has a routing table which is based on the destination address, and the corresponding

forwarding output ports are recorded in the tables. The routing tables are dynamic and are updated periodically. This is different from the table of a circuit switched network in which each entry is created when the setup phase is completed and deleted when the teardown phase is over.

Destination address	Output port
1232	1
4150	2
.	.
9130	3

Table 3.2 Sample routing table

Destination Address

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded. This address remains the same during the entire journey of the packet.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network, because resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent.

Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Not all packets in a message necessarily travel through the same switches, so the delay is not uniform for the packets of a message.

Applications

- The Internet has chosen the datagram approach to switching at the network layer.
- It uses the universal addresses defined in the network layer to route packets from the source to the destination.

6.2.2 Virtual circuit networks

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both. They are,

(i) As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.

(ii) Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

(iii) As in a datagram network, data are packetized and each packet carries an address in the header (it defines what should be the next switch and the channel on which the packet is being carried), not end-to-end jurisdiction.

(iv) As in a circuit-switched network, all packets follow the same path established during the connection.

(v) A virtual-circuit network is implemented in the DLL; a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

Classification

Virtual Circuit Networks are again classified into two types. They are,

(i) Switched VC – Different VC is provided between two users

(ii) Permanent VC – The same VC is provided between two users on a continuous basis

Addressing

Two types of addressing are involved in virtual circuit networks.

(i) Global – used to create a virtual-circuit identifier (VCI)

(ii) Local – Data transfer

Virtual-Circuit Identifier

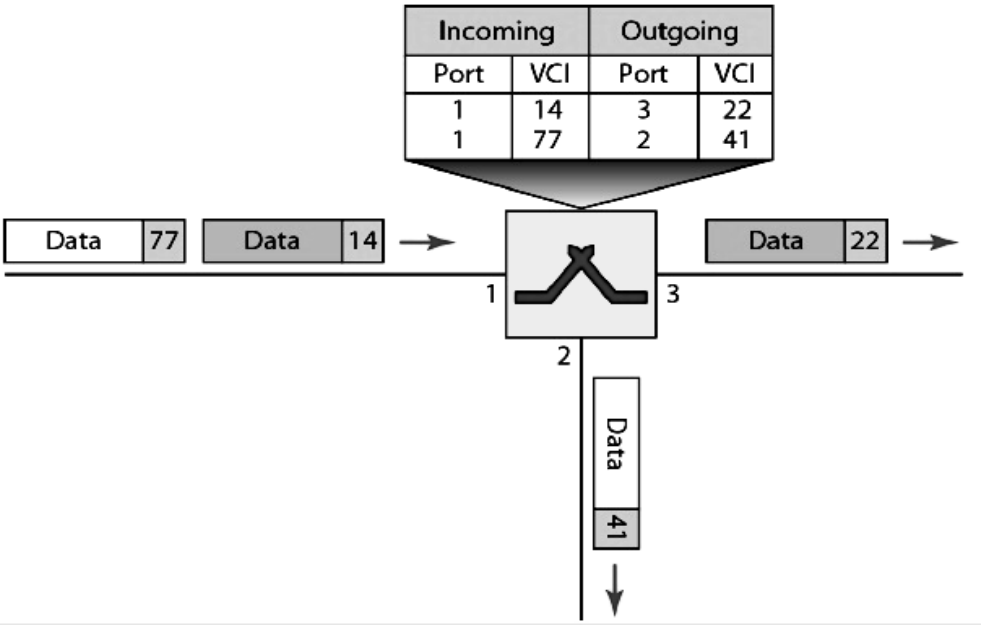


Figure 1.40 Switch and tables in a virtual-circuit network

- The identifier is a small number used by a frame between two switches.
- When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCI.

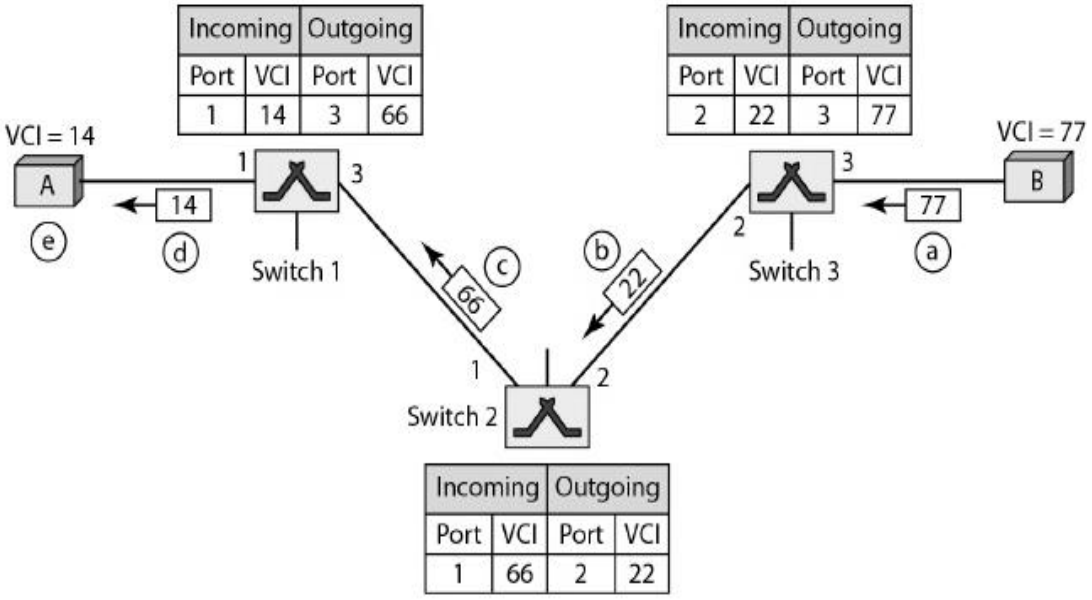


Figure 1.41 Source-to-destination data transfer in a virtual-circuit network

Three Phases

Virtual circuit networks consists of the following three phases.

(i) Setup phase: The source and destination use their global addresses to help switches make table entries for the connection.

(ii) Data transfer phase: Data transfer occurs between these two phases.

(iii) Teardown phase: The source and destination inform the switches to delete the corresponding entry.

Efficiency

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.

6.3 STRUCTURE OF A SWITCH

Crossbar Switch

A crossbar switch connects *n* inputs to *m* outputs in a grid, using electronic micro switches (transistors) at each cross point. The major limitation of this design is the number of cross points required. To connect *n* inputs to *m* outputs using a crossbar switch requires *n* x *m* cross points.

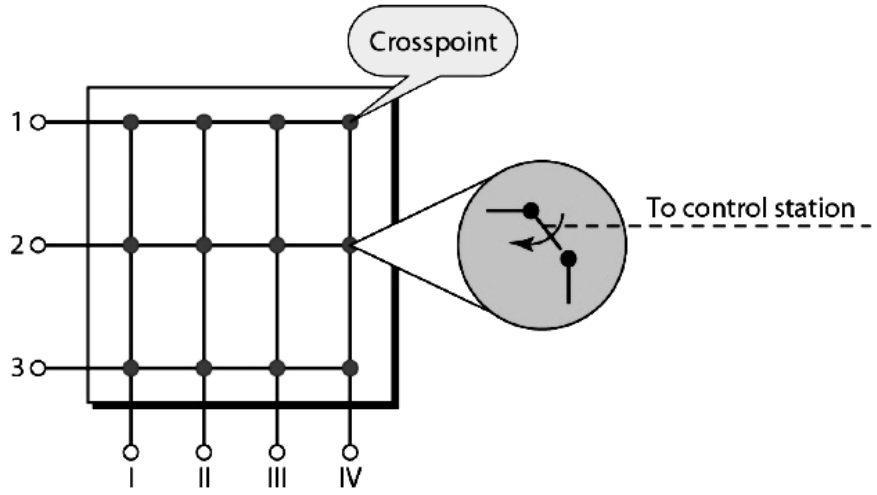


Figure 1.42 Crossbar switch with three inputs and four outputs

Time-Division Switch

Time-division switching uses time-division multiplexing (TDM) inside a switch. The most popular technology is called the time-slot interchange (TSI).

Figure 1.43 combines a TDM multiplexer, a TDM demultiplexer, and a TSI consisting of random access memory (RAM) with several memory locations. The size of each location is the same as the size of a single time slot. The number of locations is the same as the number of inputs. The RAM fills up with incoming data from time slots in the order received. Slots are then sent out in an order based on the decisions of a control unit.

Imagine that each input line wants to send data to an output line according to the following pattern:

1→ 3 2 →4 3→1 4→2

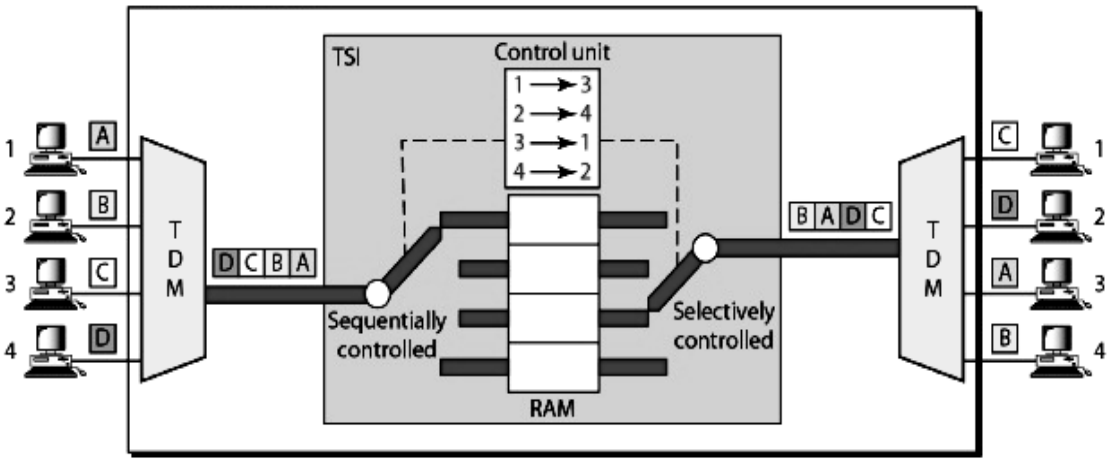


Figure 1.43 Time-division switch

Time-space-time Switch

The advantage of space-division switching is that it is instantaneous. Its disadvantage is the number of cross points required to make space-division switching. The advantage of time-division switching is that it needs no cross points. Its disadvantage is the TSI (Processing each delay at each connection). To overcome these problems, we combine space-division and time-division technologies to take advantage of the best of both.

6.4 MESSAGE SWITCHING

- Store and forward technology.
- When a node receives a message stores it until the appropriate route is free. If the node finds that the route is free, then it sends the message.
- No direct link between the source and the destination, Routing technology is used here.