CS8591 - COMPUTER NETWORKS

UNIT I - INTRODUCTION AND PHYSICAL LAYER

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer: Performance – Transmission media – Switching – Circuit-switched Networks – Packet Switching

PART A

1. List the requirements to building a network.

- ✓ Scalable Connectivity
- ✓ Cost-Effective Resource Sharing
- ✓ Support for Common Services
- ✓ Manageability

2. Write the parameters used to measure network performance (May 2016)

- ➢ Bandwidth and Latency
- ➢ Delay×Bandwidth Product
- ➢ High-Speed Networks
- ➢ Application Performance Needs

3. What are the three criteria necessary for an effective and efficient network?

The most important criteria are

- ✓ Performance
- ✓ Reliability
- ✓ Security

Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w. *Reliability* is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. *Security* issues include protecting data from unauthorized access and viruses.

4. Group the OSI layers by function?

The seven layers of the OSI model belonging to three subgroups. Physical, data link and network layers are the *network support layers*; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the *user support layers*; they allow interoperability among unrelated software systems. The transport layer ensures *end-to-end reliable data transmission*.

5. What are the features provided by layering? (May 2013)

Two features:

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

6. Why are protocols needed?

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

7. What are the two interfaces provided by protocols?

- Service interface

- Peer interface

Service interface- defines the operations that local objects can perform on the protocol.
Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

8. Mention the different physical media?

- Twisted pair (the wire that your phone connects to)
- Coaxial cable (the wire that your TV connects to)
- Optical fiber (the medium most commonly used for high-bandwidth, long-distance links)
- Space (the stuff that radio waves, microwaves and infra red beams propagate through)

9. Explain the two types of duplex?

- *Full duplex*-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
- *Half duplex*-it supports data flowing in only one direction at a time.

10. What is spread spectrum and explain the two types of spread spectrum?

Spread spectrum is to spread the signal over a wider frequency band than normal in such a way as to minimize the impact of interference from other devices.

- Frequency Hopping
- Direct sequence

11. What are the different encoding techniques?

- NRZ
- NRZI
- Manchester
- 4B/5B

12. What are the responsibilities of data link layer?

Specific responsibilities of data link layer include the following.
a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

13. Define flow control? (NOV 2011)(May 2015) (May 2016)

Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment.

14. Mention the categories of flow control?

There are 2 methods have been developed to control flow of data across communication links.
a) Stop and wait - send one from at a time.
b) Sliding window - send several frames at a time.

15. What is a buffer?

Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.

16. What is the difference between a passive and an active hub?

An active hub contains a repeater that regenerates the received bit patterns before sending them out. A passive hub provides a simple physical connection between the attached devices.

17. For n devices in a network, what is the number of cable links required for a mesh and ring topology?

- Mesh topology – n (n-1)/2
- Ring topology – n

18. What are the two types of line configuration? (NOV 2010)

- Point-to-point & Multipoint

19. What do you meant by error control? (NOV 2010)(May 2015)

Error control is used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

20. Define Error detection (NOV 2011)

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected

Types of error:

- ✓ Single bit error
- ✓ Burst error

The three error detecting techniques are:

- Parity check
- Check sum algorithm
- Cyclic Redundancy Check

21. What is the use of Two dimensional parity in error detection? (NOV 2012)

- It is based on simple parity.
- It performs calculation for each bit position across each byte in the frame.
- This adds extra parity byte for entire frame, in addition to a parity bit for each byte.

22. What are the issues (Services) in data link layer? (NOV 2012) (May 2016) (Nov 2016)

a) Services Provided to the Network Layer
b) Framing
c) Error Control
d) Flow Control

23. Define network and computer network

A **network** is any collection of independent computers that communicate with one another over a shared network medium. A **computer network** is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

24. List the components of data communication

- ✓ Message
- ✓ Sender
- ✓ Receiver
- ✓ Medium
- ✓ Protocol

25. Define bit stuffing. Give example (MAY 2011) (May 2017)

Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

e.g, Sending side - 011111**0**10

26. What are the major duties of network layer? (MAY 2012)

- **Logical addressing** - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

27. What are the functions of application layer? (MAY 2011)

- **FTAM (file transfer, access, mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

28. Define a layer. (Nov/Dec 2013)

The OSI (Open System Interconnection) Model breaks the various aspects of a computer network into seven distinct layers. Each successive layer envelops the layer beneath it, hiding its details from the levels above.

29. What do you mean by framing? (Nov/Dec 2013) (Nov/Dec 2014)

Frames are the small data units created by data link layer and the process of creating frames by the data link layer is known as framing

30. What is protocol? What are its key elements? (NOV/DEC 2007) (May 2016)

Set of rules that govern the data communication is protocol. The key elements are

i) Syntax ii) Semantics iii) Timing

31. Define (or) mechanism of stop and wait protocol (Nov 2016)

The idea of stop-and-wait is straightforward: After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame.

32. Define sliding window algorithm

The sender can transmit several frames before needing an acknowledgement. Frames can be sent one right after another meaning that the link can carry several frames at once and its capacity can be used efficiently. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames

33. Define character stuffing

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by "escaping" the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called character stuffing.

34. List the 7 OSI layers

- Physical Layer
- Data link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

35. Define hamming distance (Nov/Dec 2014)

Hamming distance = the number of bit positions in which two code-words differ.

Eg. How to calculate ?

(Exclusive OR=XOR):

```
10001001
10110001
---------
00111000
```

=> The number of 1's give the number of different bits

36. Write down any two differences between circuit switching and packet switching (Nov/Dec 2014) (May 2017)

Circuit switching

- In circuit switching network dedicated channel has to be established before the call is made between users
- The channel is reserved between the users till the connection is active

Packet switching

- In packet switching network unlike CS network, it is not required to establish the connection initially
- The connection/channel is available to use by many users.

37. Define the terms: Bandwidth & Latency (Dec 2017)

Network performance was measured in two fundamental ways: *bandwidth* (also called *throughput*) and *latency* (also called *delay*).

- The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time
- The second performance metric, latency, corresponds to how long it takes a message to travel from one end of a network to the other.

38. Compare Byte oriented versus Bit-oriented protocol (Dec 2017)

- **Bit oriented** protocol defined as it is a communication protocol it uses individual bits for control codes that bits information should be in byte.
- **Byte oriented** protocol used for framing and communication purpose, in which bytes are used for control codes

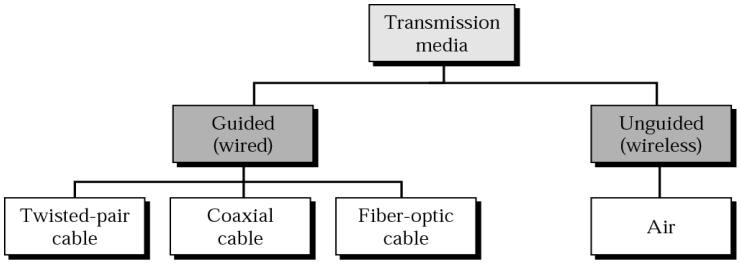
39. Define protocol layering

In data communication and networking, 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 the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering.**

40. List the types of transmission media

Communication can be made by 2 ways

1. Guided (Wired)
2. Unguided (Wireless



41. Define switching & list its types

SWITCHING

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

Type of switching

- Circuit Switching
- Packet Switching
- Message Switching

42. Define VCI

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the ***virtual-circuit identifier*** **(VCI)** or the ***label*.** A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches

43. What is the use of routing table?

The destination addresses and the corresponding forwarding output ports are recorded in the tables. The routing tables are dynamic and are updated periodically.

PART B

1. Discuss the applications, advantages and disadvantages of networks

Applications of Computer Network:-

1.Business Applications
- a.Database resource
- b.Communication Medium
- c.Electronic commerce

2.Home Applications
- a.Internet Access
- b.Personal Communication
- c.Entertainment
- d.Electronic Commerce

3.Mobile Computers
- a.Wireless networks

Advantages of Network

- **Speed**. Sharing and transferring files within Networks are very rapid. Thus saving time, while maintaining the integrity of the file.
- **Cost**. Individually licensed copies of many popular software programs can be costly. Networkable versions are available at considerable savings. Shared programs, on a network allows for easier upgrading of the program on one single file server, instead of upgrading individual workstations.
- **Security**. Sensitive files and programs on a network are passwords protected or designated as "copy inhibit," so that you do not have to worry about illegal copying of programs.
- **Centralized Software Management**. Software can be loaded on one computer (the file server) eliminating that need to spend time and energy installing updates and tracking files on independent computers throughout the building.
- **Resource Sharing**. Resources such as, printers, fax machines and modems can be shared.
- **Electronic Mail**. E-mail aids in personal and professional communication.
- **Flexible Access**. Access their files from computers throughout the firm.
- **Workgroup Computing**. Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently.

Disadvantages of Network

- Server faults stop applications being available
- Network faults can cause loss of data.
- Network fault could lead to loss of resources
- User work dependent upon network
- Could become inefficient
- Could degrade in performance
- Resources could be located too far from users

2. Explain in detail about Networks & Discuss the types and connections of networks

Network :

A **network** is any collection of independent computers that communicate with one another over a shared network medium. A **computer network** is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

Network Criteria:

The most important criteria are
- ✓ Performance
- ✓ Reliability
- ✓ Security

Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w. ***Reliability*** is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. ***Security*** issues include protecting data from unauthorized access and viruses

TYPE OF CONNECTION:

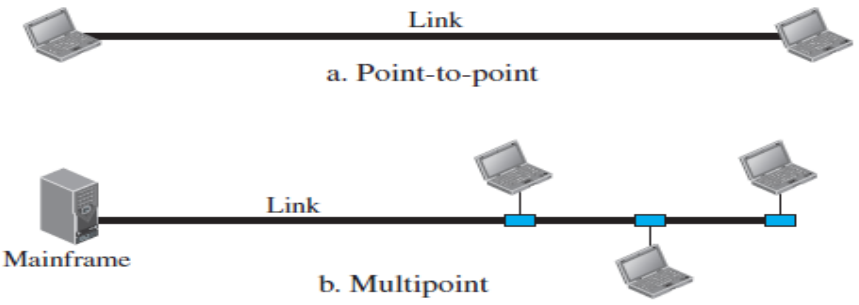
There are two types are,
1. Point to point
2. Multi point

1. Point To Point:

It provides a dedicated link between two devices of the channel. The entire capacity of the channel is reserved for transmission between those two devices.

2. Multipoint:

More than two devices can share a link by using this type of connection. It also called as multidrop. The capacity channel is shared either temporary or spatially. It simultaneously use, it is spatially shared. If it takes turns, it is time shared line configuration



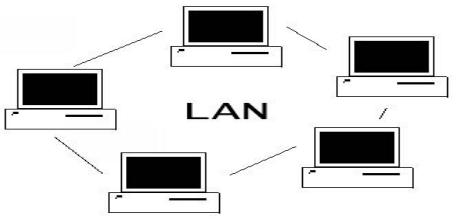
Types of Network

Computer network design is dividing into three basic types such as
- ➢ LAN (local area network),
- ➢ MAN (Metropolitan area network)

- WAN (wide area network)

LAN (Local area networks)

Generally called **LANs**, are privately-owned **networks within a single building or campus of up to a few kilometers in size.** They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.

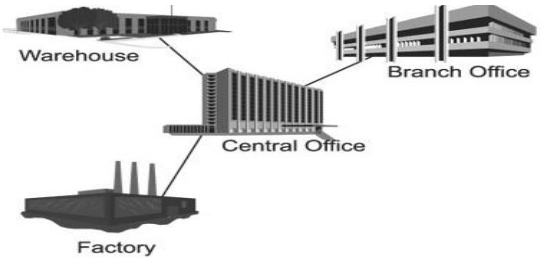


LAN configuration consists of:

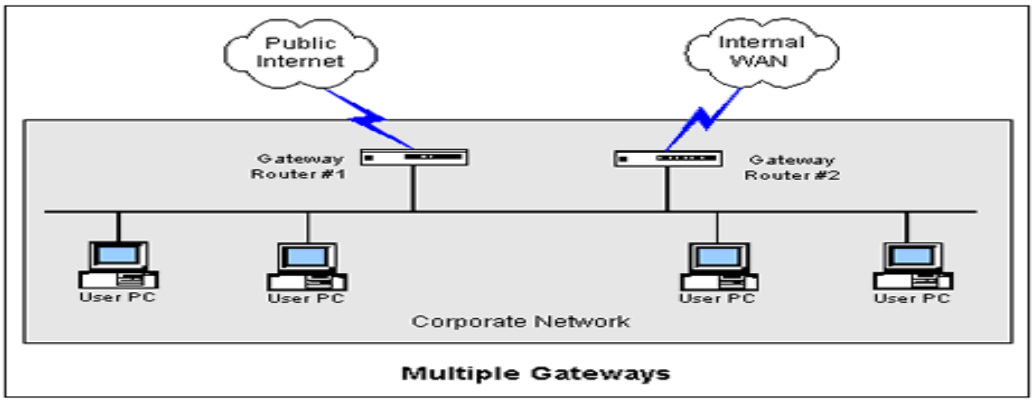
- A file server
- A workstation
- Cables

MAN (Metropolitan area network)

A metropolitan area network (MAN) is a large **computer network that usually spans a city or a large campus.** A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks and the Internet



WAN (Wide Area Network) A **WAN** spans a **large geographic area, such as a state, province or country.** WANs often connect multiple smaller networks, such as local area networks (LANs) or metro area networks (MANs). The world's most popular WAN is the Internet.



3. Discuss about topology and its types

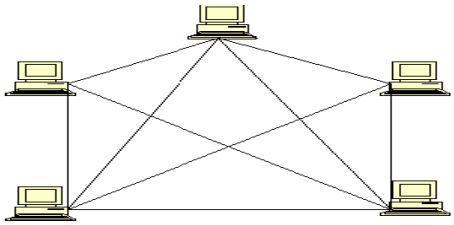
Network Topologies

Topology refers to the way a network is laid out either physically or logically. Two or more devices connect to a link; two or more links form a topology. It is the geographical representation of the relationship of all the links and linking devices to each other.

1. Mesh
2. Star
3. Tree
4. Bus
5. Ring
6. Hybrid

1. Mesh Topology:

Here every device has a dedicated point to point link to every other device. A fully connected mesh can have n(n-1)/2 physical channels to link n devices. It must have n-1 IO ports.



Advantages:

1. They use dedicated links so each link can only carry its own data load. So traffic problem can be avoided.
2. It is robust. If any one link get damaged it cannot affect others
3. It gives privacy and security
4. Fault identification and fault isolation are easy.

Disadvantages:

1. The amount of cabling and the number IO ports required are very large. Since every device is connected to each other devices through dedicated links.
2. The sheer bulk of wiring is larger then the available space
3. Hardware required to connect each device is highly expensive.

Example:

A mesh network has 8 devices. Calculate total number of cable links and IO ports needed.

Solution:

Number of devices = 8

Number of links = n (n-1)/2

= 8(8-1)/2

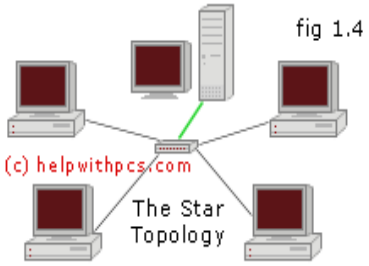
= 28

Number of port/device = n-1

= 8-1 = 7

2. STAR TOPOLOGY:

Here each device has a dedicated link to the central 'hub'. There is no direct traffic between devices. The transmission are occurred only through the central controller namely hub.



Advantages:

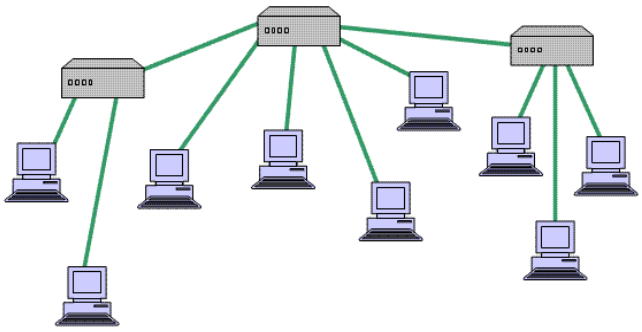
1. Less expensive then mesh since each device is connected only to the hub.
2. Installation and configuration are easy.
3. Less cabling is need then mesh.
4. Robustness.
5. Easy to fault identification & isolation.

Disadvantages:

1. Even it requires less cabling then mesh when compared with other topologies it still large.

3. TREE TOPOLOGY:

It is a variation of star. Instead of all devices connected to a central hub here most of the devices are connected to a secondary hub that in turn connected with central hub. The central hub is an active hub. An active hub contains a repeater, which regenerate the received bit pattern before sending.



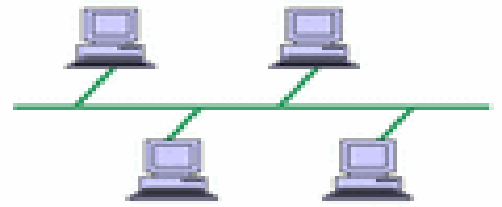
The secondary hub may be active or passive. A passive hub means it just precedes a physical connection only.

Advantages:

1. Can connect more than star.
2. The distance can be increased.
3. Can isolate and prioritize communication between different computers.

4. BUS TOPOLOGY:

A bus topology is multipoint. Here one long cable is act as a backbone to link all the devices are connected to the backbone by drop lines and taps. A drop line is the connection between the devices and the cable. A tap is the splice into the main cable or puncture the sheathing.



Advantages:

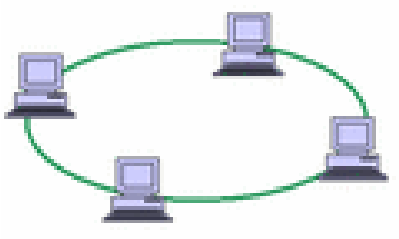
1. Ease of installation.
2. Less cabling.

Disadvantages:

1. Difficult reconfiguration and fault isolation.
2. Difficult to add new devices.
3. Signal reflection at top can degradation in quality
4. If any fault in backbone can stops all transmission

5. Ring topology

Each node is connected to exactly two other nodes, forming a ring. Can be visualized as a circular configuration. Requires at least three nodes



Advantages:

1. Easy to install.
2. Easy to reconfigure.
3. Fault identification is easy.

Disadvantages:

1. Unidirectional traffic.
2. Break in a single ring can break entire network.

6. Hybrid topology

A combination of any two or more network topologies.

4. Explain the list of requirements (challenges faced) to building a computer network (May 2017) (Nov 2017)

- ✓ Scalable Connectivity
- ✓ Cost-Effective Resource Sharing
- ✓ Support for Common Services
- ✓ Manageability

1. Scalable Connectivity

Networks (of which the Internet is the prime example) are designed to grow in a way that allows them the potential to connect all the computers in the world. A system that is designed to support growth to an arbitrarily large size is said to *scale*.

Links, Nodes, and Clouds

A network can consist of two or more computers directly connected by some physical medium, such as a coaxial cable or an optical fiber. We call such a physical medium **a *link***, and we often refer to the computers it connects as ***nodes.***

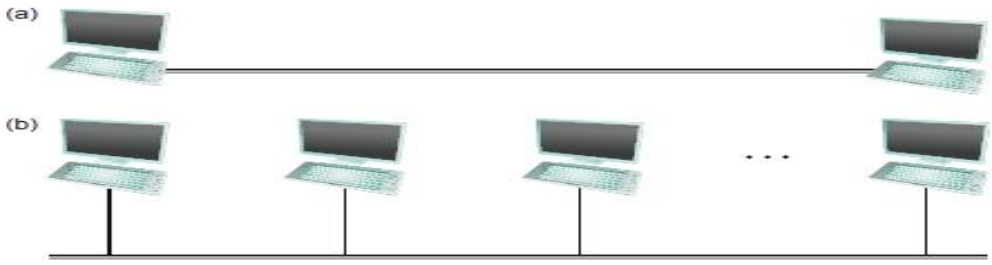


FIGURE 1.2 Direct links: (a) point-to-point; (b) multiple-access.

The cloud distinguishes between the nodes on the inside that *implement* the network (they are commonly called *switches*, and their primary function is to store and forward packets) and the nodes on the outside of the cloud that *use* the network (they are commonly called *hosts*, and they support users and run application programs).

2. Cost-Effective Resource Sharing

Given a collection of nodes indirectly connected by a nesting of networks, it is possible for any pair of hosts to send messages to each other across a sequence of links and nodes. Of course, we want to do more than support just one pair of communicating hosts—we want to provide all pairs of hosts with the ability to exchange messages.

Multiplexing can be explained by analogy to a timesharing computer system, where a single physical processor is shared (multiplexed) among multiple jobs, each of which believes it has its own private processor. Similarly, data being sent by multiple users can be multiplexed over the physical links that make up a network. There are several different methods for multiplexing multiple flows onto one physical link. One common method is *synchronous time- division multiplexing* (STDM).

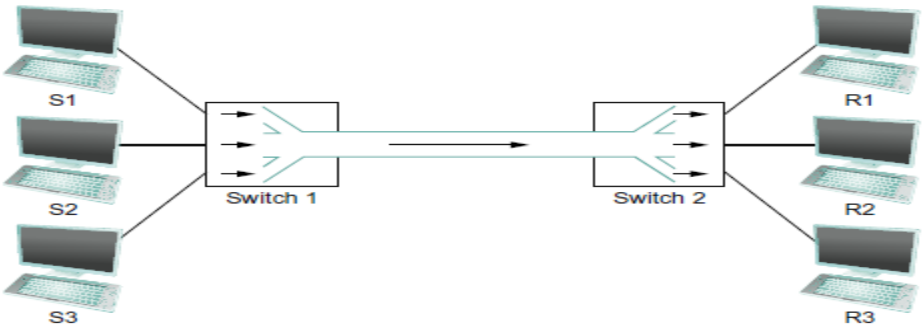


FIGURE 1.5 Multiplexing multiple logical flows over a single physical link.

3. Support for Common Services

The next requirement of a computer network is that the application programs running on the hosts connected to the network must be able to communicate in a meaningful way. From the application developer's perspective, the network needs to make his or her life easier we use a cloud to abstractly represent connectivity among a set of computers, we now think of a channel as connecting one process to another.

Diagram shows a pair of application-level processes communicating over a logical channel that is, in turn, implemented on top of a cloud that connects a set of hosts. We can think of the channel as being like a pipe connecting two applications, so that a sending application can put data in one end and expect that data to be delivered by the network to the application at the other end of the pipe

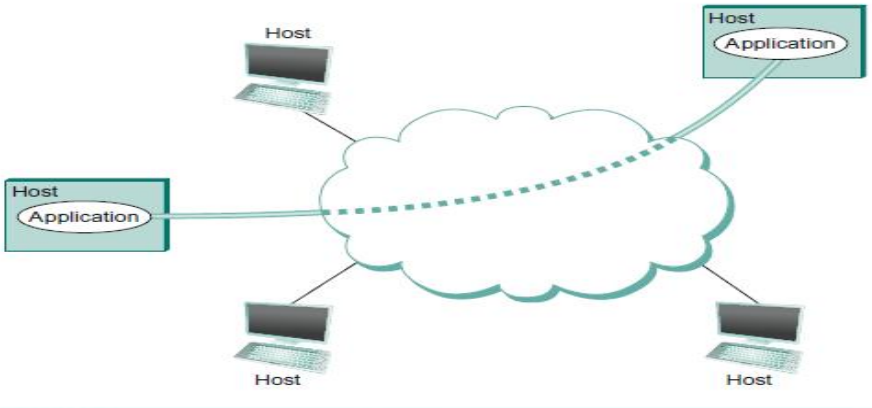


FIGURE 1.7 Processes communicating over an abstract channel.

4. Manageability

Managing a network includes making changes as the network grows to carry more traffic or reach more users, and troubleshooting the network when things go wrong or performance isn't as desired. This requirement is partly related to the issue of scalability discussed above—as the Internet has scaled up to support billions of users and at least hundreds of millions of hosts, the challenges of keeping the whole thing running correctly and correctly configuring new devices as they are added have become increasingly problematic.

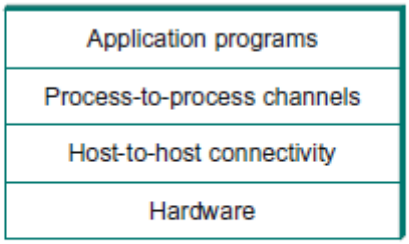
5. Discuss protocol layering in detail

Layering and Protocols

When the system gets complex, the system designer introduces another level of abstraction. It defines unifying model with important aspects of the system, encapsulated this model in interface objects and hide it from users

In network, abstraction leads to layering. Layering provides two nice features.

- It decomposes the problem of building a network into more manageable components. Rather than implementing a monolithic piece of software that does everything implement several layers, each of which solves one part of the problem.
- It provides more modular design. To add some new service, it is enough to modify the functionality at one layer, reusing the functions provided at all the other layers.



Example of a layered network system.

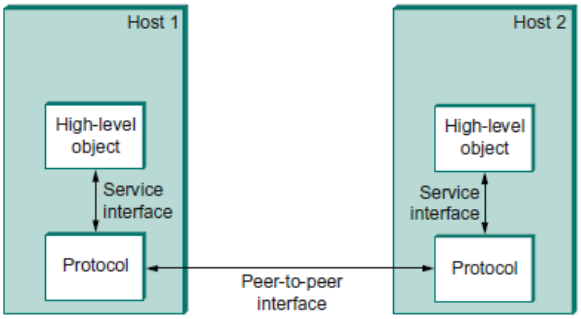
Protocols

A protocol is a set of rules that governs data communication. It defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics and timing.

Each protocol defines two different interfaces.

➢ **Service interface** - to the other objects on the same computer that want to use its communication services. This service interface defines the operations that local objects can perform on the protocol.

➢ **Peer interface** - to its counterpart (peer) on another machine. It also defines the form and meaning of messages exchanged between protocol peers to implement the communication service.



■ **FIGURE 1.10** Service interfaces and peer interfaces.

Encapsulation

Control information must be added with the data to instruct the peer how to handle with the received message. It will be added into the header or trailer.

Header - Small data structure from few bytes to few kilobytes attached to the front of message.

Trailer – Information will be added at the end of the message

Payload or message body – Data send by the program

In this case data is encapsulated with new message created by protocol at each level.

Multiplexing and De-Multiplexing

The fundamental idea of packet switching is to multiplex multiple flows of data over a single physical link. This can be achieved by adding identifier to the header message. It is known as **demultiplexing or demux key.** It gives the address to which it has to communicate.

The messages are demultiplexed at the destination side. In some cases same demux key is used on both sides and in some cases different keys are used.

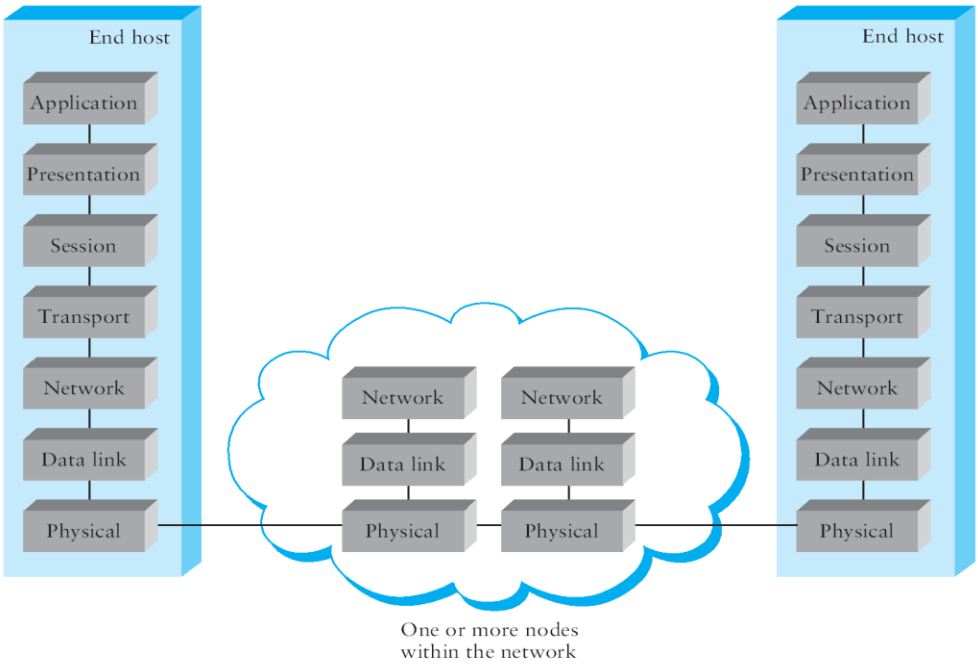
6. Explain OSI model in detail (or) Discuss ISO-OSI architecture in detail

OSI Architecture **(NOV 2012) (MAY 2012)**

ISO defines a common way to connect computer by the architecture called Open System Interconnection (OSI) architecture.

Network functionality is divided into seven layers.

- **Physical Layer**
- **Data link Layer**
- **Network Layer**
- **Transport Layer**
- **Session Layer**
- **Presentation Layer**
- **Application Layer**



Organization of the layers
The 7 layers can be grouped into 3 subgroups

1. **Network Support Layers**

Layers 1,2,3 - Physical, Data link and Network are the network support layers. They deal with the physical aspects of moving data from one device to another such as electrical specifications, physical addressing, transport timing and reliability.

2. **Transport Layer**

Layer4, transport layer, ensures end-to-end reliable data transmission on a single link.

3. **User Support Layers**

Layers 5,6,7 – Session, presentation and application are the user support layers. They allow interoperability among unrelated software systems

Functions of the Layers

1. **Physical Layer**

The physical layer coordinates the functions required to transmit a bit stream over a physical medium.

The physical layer is concerned with the following:

- **Physical characteristics of interfaces and media** - The physical layer defines the characteristics of the interface between the devices and the transmission medium.
- **Representation of bits** - To transmit the stream of bits, it must be encoded to signals. The physical layer defines the type of encoding.
- **Data Rate or Transmission rate** - The number of bits sent each second – is also defined by the physical layer.
- **Synchronization of bits** - The sender and receiver must be synchronized at the bit level. Their clocks must be synchronized.
- **Line Configuration** - In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.
- **Physical Topology** - The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh, bus, star or ring topology.

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

2. Data Link Layer

It is responsible for transmitting frames from one node to next node.

The other responsibilities of this layer are

- **Framing -** Divides the stream of bits received into data units called frames.
- **Physical addressing** – If frames are to be distributed to different systems on the n/w , data link layer adds a header to the frame to define the sender and receiver.
- **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender ,the Data link layer imposes a flow ctrl mechanism.
- **Error control**- Used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.
- **Access control** -Used to determine which device has control over the link at any given time.

3. NETWORK LAYER

This layer is responsible for the delivery of packets from source to destination.

It is mainly required, when it is necessary to send information from one network to another.

The other responsibilities of this layer are

- **Logical addressing -** If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.
- **Routing** – The devices which connects various networks called routers are responsible for delivering packets to final destination.

4. TRANSPORT LAYER

- It is responsible for **Process to Process** delivery.
- It also ensures whether the message arrives in order or not.

The other responsibilities of this layer are

- **Port addressing** - The header in this must therefore include a address called port address. This layer gets the entire message to the correct process on that computer.
- **Segmentation and reassembly** - The message is divided into segments and each segment is assigned a sequence number. These numbers are arranged correctly on the arrival side by this layer.
- **Connection control** - This can either be **connectionless or connection-oriented.** The connectionless treats each segment as a individual packet and delivers to the destination. The connection-oriented makes connection on the destination side before the delivery. After the delivery the termination will be terminated.
- **Flow and error control** - Similar to data link layer, but process to process take place.

5. SESSION LAYER

This layer establishes, manages and terminates connections between applications.

The other responsibilities of this layer are

- **Dialog control** - This session allows two systems to enter into a dialog either in half duplex or full duplex.
- **Synchronization**-This allows to add checkpoints into a stream of data.

6. PRESENTATION LAYER

It is concerned with the syntax and semantics of information exchanged between two systems.

The other responsibilities of this layer are

➢ **Translation** – Different computers use different encoding system, this layer is responsible for interoperability between these different encoding methods. It will change the message into some common format.

➢ **Encryption and decryption**-It means that sender transforms the original information to another form and sends the resulting message over the n/w. and vice versa.

➢ **Compression and expansion**-Compression reduces the number of bits contained in the information particularly in text, audio and video.

7. APPLICATION LAYER

This layer enables the user to access the n/w. This allows the user to log on to remote user.

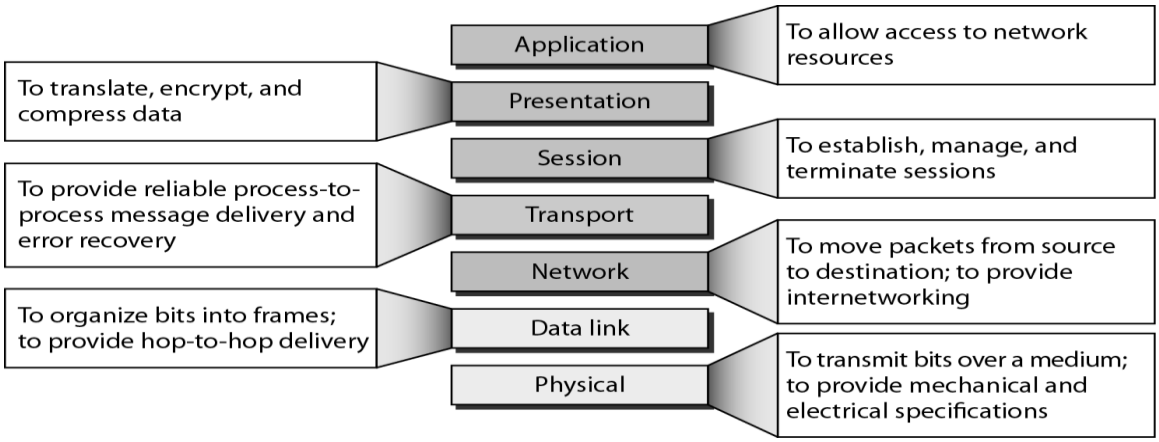
The other responsibilities of this layer are

➢ **FTAM (file transfer, access, mgmt)** - Allows user to access files in a remote host.

➢ **Mail services** - Provides email forwarding and storage.

➢ **Directory services** - Provides database sources to access information about various sources and objects.

Summary of layers

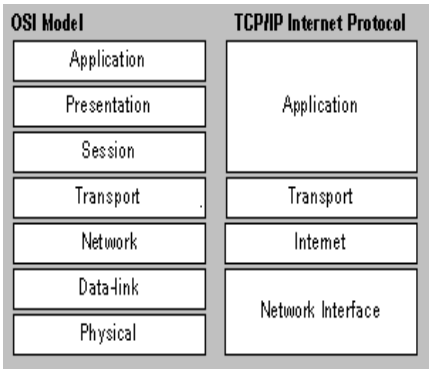


7. Explain TCP/IP protocol suite (Internet architecture) in detail (May 2015) (May 2017)

TCP/IP ARCHITECTURE

TCP/IP model is an implementation of OSI reference model. It has four layers. They are

- Network Interface Layer
- Internet Layer
- Transport (also known as Host-to-Host or Transmission) Layer
- Application Layer (known earlier as the Process Layer)



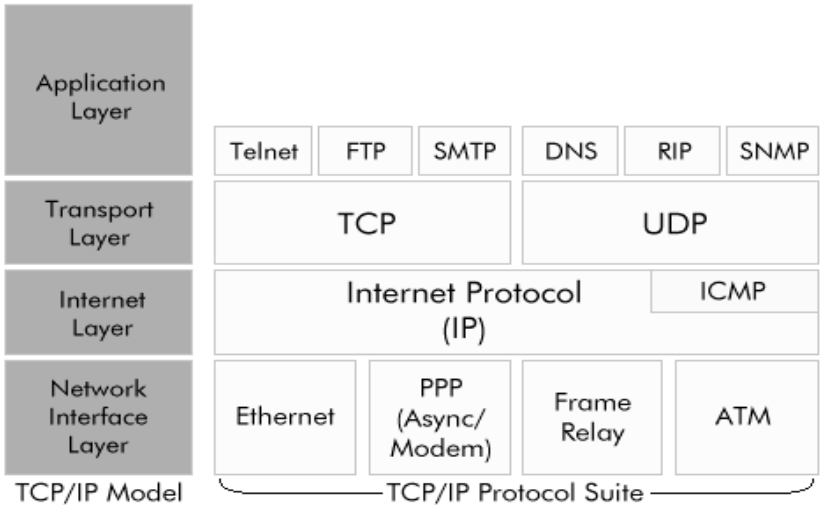


Figure 2.6 *Logical connections between layers of the TCP/IP protocol suite*

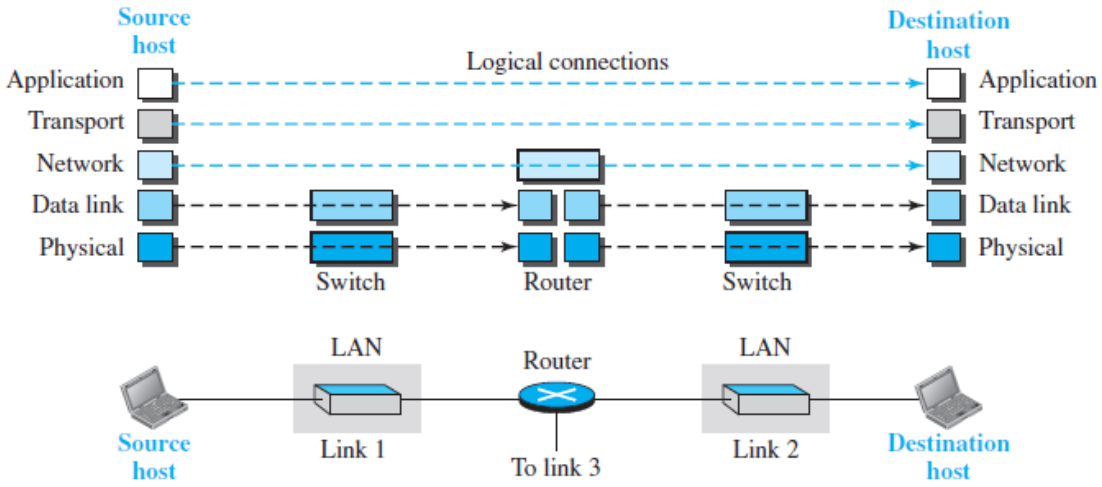
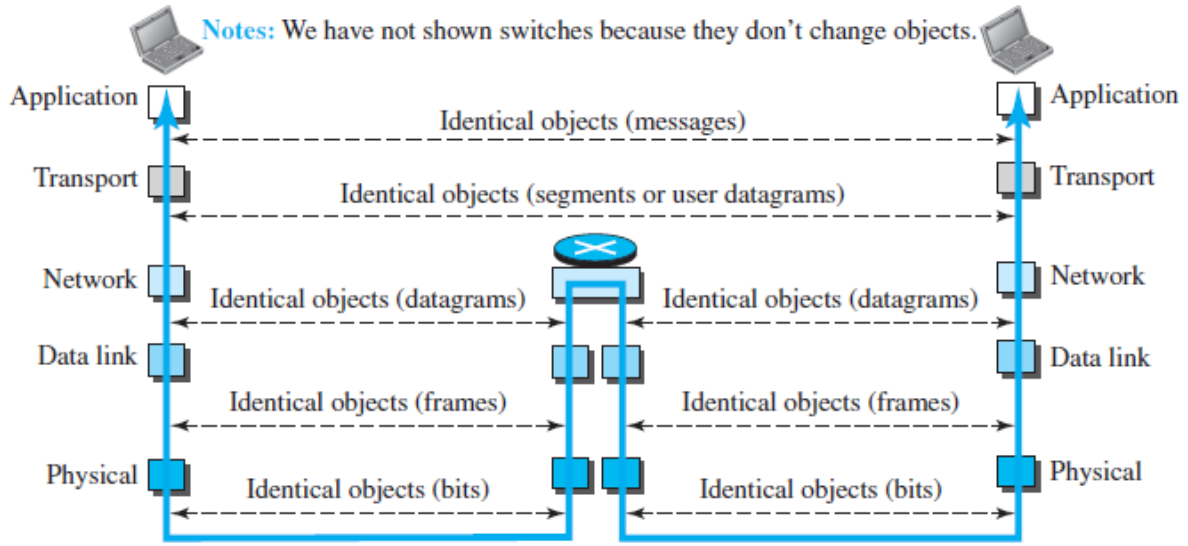


Figure 2.7 *Identical objects in the TCP/IP protocol suite*



1) Network interface layer (or) The Host to Network Layer:

Below the internet layer is great void. The TCP/IP reference model does not really say such about what happen here, except to point out that the host has connect to the network using some protocol so it can transmit IP packets over it. This protocol is not specified and varies from host to host and network to network.

2) Internet layer:

Packet switching network depends upon a connectionless internetwork layer. This layer is known as internet layer, is the linchpin that holds the whole design together. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. They may appear in a different order than they were sent in each case it is job of higher layers to rearrange them in order to deliver them to proper destination.

The internet layer specifies an official packet format and protocol known as internet protocol. The job of internet layer is to transport IP packets to appropriate destination. Packet routing is very essential task in order to avoid congestion. For these reason it is say that TCP/IP internet layer perform same function as that of OSI network layer.

3) Transport layer:

In the TCP/IP model, the layer above the internet layer is known as transport layer. It is developed to permit entities on the source and destination hosts to carry on a conversation. It specifies 2 end-to-end protocols

i) TCP (Transmission Control Protocol)
ii) UDP (User Datagram Protocol)

TCP

It is a reliable connection-oriented protocol that permits a byte stream originating on one machine to be transported without error on any machine in the internet. It divides the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination, the receiving TCP process collects the received message into the output stream. TCP deals with

flow control to make sure a fast sender cannot swamp a slow receiver with more message than it can handle.

UDP

It is an unreliable, connectionless protocol for applications that do not want TCP's sequencing on flow control and wish to offer their own. It is also used for client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

4) Application Layer:

In TCP/IP model, session or presentation layer are not present. Application layer is present on the top of the Transport layer. It includes all the higher-level protocols which are virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP).

The virtual terminal protocol permits a user on one machine to log into a distant machine and work there. The file transfer protocol offers a way to move data efficiently from one machine to another. Electronic mail was used for file transfer purpose but later a specialized protocol was developed for it.

The Application Layer defines following protocols

i) File Transfer Protocol (FTP)

It was designed to permit reliable transfer of files over different platforms. At the transport layer to ensure reliability, FTP uses TCP.

FTP offers simple commands and makes the differences in storage methods across networks transparent to the user. The FTP client is able to interact with any FTP server; therefore the FTP server must also be able to interact with any FTP client.

FTP does not offer a user interface, but it does offer an application program interface for file transfer. The client part of the protocol is called as FTP and the server part of the protocol is known as FTPd. The suffix "d" means Daemon this is a legacy from Unix computing where a daemon is a piece of software running on a server that offers a service.

ii) Hyper Text Transfer Protocol

HTTP permits applications such as browsers to upload and download web pages. It makes use of TCP at the transport layer again to check reliability.

HTTP is a connectionless protocol that sends a request, receives a response and then disconnects the connection.

HTTP delivers HTML documents plus all of the other components supported within HTML such as JavaScript, Visual script and applets.

iii) Simple Mail Transfer Protocol

By using TCP, SMTP sends email to other computers that support the TCP/IP protocol suite. SMTP provides extension to the local mail services that existed in the early years of LANs. It supervises the email sending from the local mail host to a remote mail host. It is not reliable for accepting mail from local users or distributing received mail to recipients this is the responsibility of the local mail system.

SMTP makes use of TCP to establish a connection to the remote mail host, the mail is sent, any waiting mail is requested and then the connection is disconnected. It can also return a forwarding address if the intended recipient no longer receives email at that destination. To enable mail to be delivered across differing systems, a mail gateway is used.

iv) Simple Network Management Protocol

For the transport of network management information, SNMP is used as standardized protocol. Managed network devices can be cross examined by a computer running to return details about their status and level of activity. Observing software can also trigger alarms if certain performance criteria drop below acceptable restrictions. At the transport layer SNMP protocol uses UDP.

The use of UDP results in decreasing network traffic overheads.

8. Discuss in detail about the network performance measures (Nov 2016)

Like any computer system, however, computer networks are also expected to perform well. This is because the effectiveness of computations distributed over the network often depends directly on the efficiency with which the network delivers the computation's data.

While the old programming adage "first get it right and then make it fast" is valid in many settings, in networking it is usually necessary to "design for performance." It is therefore important to understand the various factors that impact network performance.

- ✓ **Bandwidth**
- ✓ **Throughput**
- ✓ **Latency (Delay)**
- ✓ **Jitter**

Bandwidth

The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.

- ***Bandwidth in Hertz***

We have discussed this concept. Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

- ***Bandwidth in Bits per Seconds***

The term *bandwidth* can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

Throughput

The **throughput** is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bps through this link with *T* always less than *B*. In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

Latency or delay

The **latency** or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is

made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = **propagation time** + **transmission time** + **queuing time** + **processing delay**

- ***Propagation Time***

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = **Distance / (Propagation Speed)**

- ***Transmission Time***

In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later. The **transmission time** of a message depends on the size of the message and the bandwidth of the channel.

Transmission time = **(Message size) / Bandwidth**

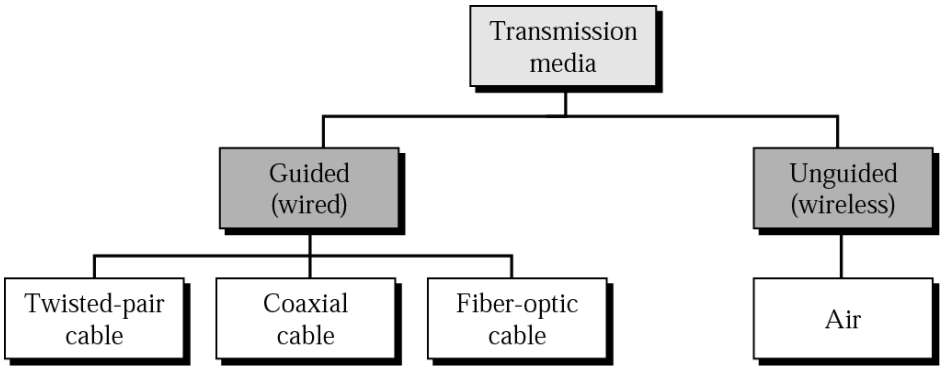
Jitter

Another performance issue that is related to delay is **jitter.** We can roughly say that jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example). If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

9. Discuss physical links (or) transmission media (or) how communication made by network?

Communication can be made by 2 ways

3. Guided (Wired)
4. Unguided (Wireless)



Guided Media

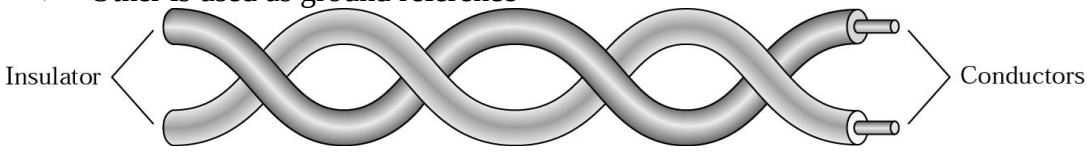
Guided media conduct signals from one device to another include Twisted-pair cable, Coaxial Cable and Fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium.

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a glass cable that accepts and transports signals in the form of light.

Twisted Pair Cable

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

- One of the wires is used to carry signals to the receiver
- Other is used as ground reference



Interference and cross talk may affect both the wires and create unwanted signals, if the two wires are parallel.

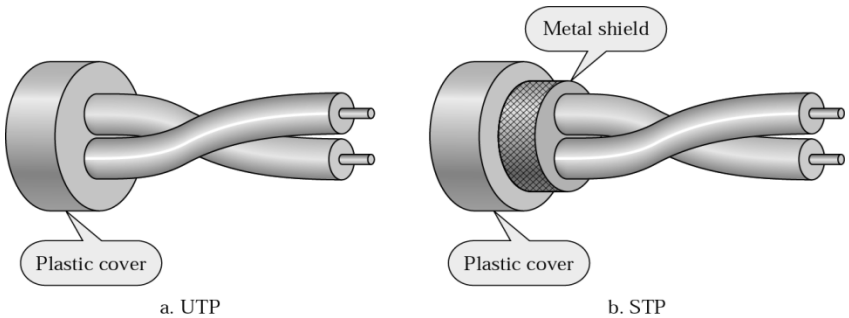
By twisting the pair, a balance is maintained. Suppose in one twist one wire is closer to noise and the other is farther in the next twist the reverse is true. Twisting makes it probable that both wires are equally affected by external influences.

Twisted Pair Cable comes into two forms:

- **Unshielded**
- **Shielded**

Unshielded versus shielded Twisted-Pair Cable

- Shielded Twisted-Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors.
- Metal casing improves that quality of cable by preventing the penetration of noise or cross talk.
- It is more expensive. The following figure shows the difference between UTP and STP



Applications

- Twisted Pair cables are used in telephone lines to provide voice and data channels.
- Local area networks also use twisted pair cables.

Connectors

The most common UTP connector is RJ45.

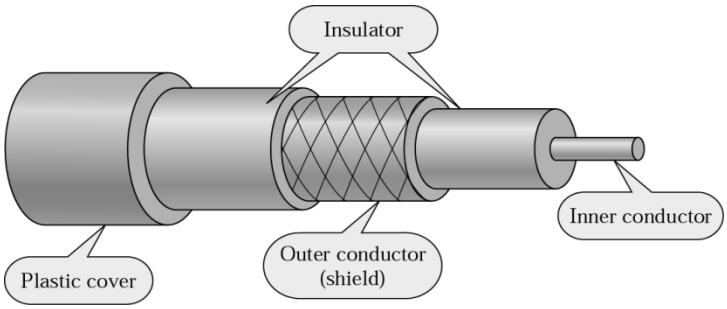
Coaxial Cable

Coaxial cable (coax) carries signals of higher frequency ranges than twisted pair cable.

Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, and with outer conductor of metal foil.

The outer metallic wrapping serves both as a shield against noise and as the second conductor and the whole cable is protected by a plastic cover.

]



Categories of coaxial cables

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

Applications

- It is used in analog and digital telephone networks
- It is also used in Cable TV networks
- It is used in Ethernet LAN

Connectors

- BNC connector – to connect the end of the cable to a device
- BNC T - to branch out network connection to computer
- BNC terminator - at the end of the cable to prevent the reflection of the signal.

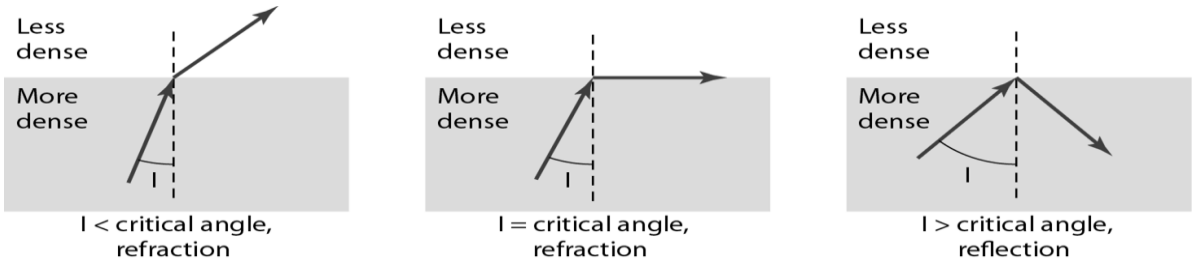
Fiber Optic Cable

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.

Properties of light

- Light travels in a straight line as long as it moves through a single uniform substance. If traveling through one substance suddenly enters another, ray changes its direction.

Bending of light ray

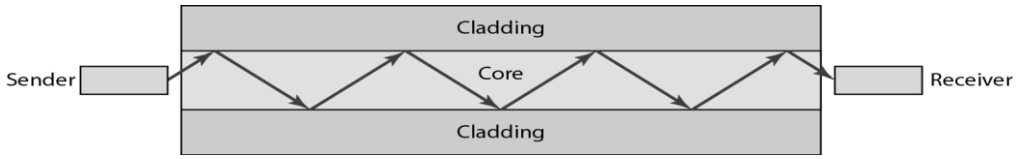


If the angle of incidence(the angle the ray makes with the line perpendicular to the interface between the two medium) is less than the critical angle the ray refracts and move closer to the surface.

If the angle of incidence is equal to the critical angle, the light bends along the interface.

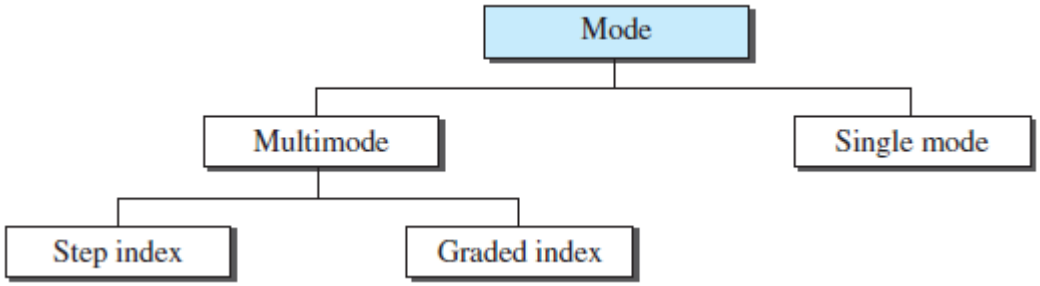
If the angle of incidence is greater than the critical angle, the ray reflects and travels again in the denser substance. Critical angle differs from one medium to another medium.

Optical fiber use reflection to guide light through a channel.



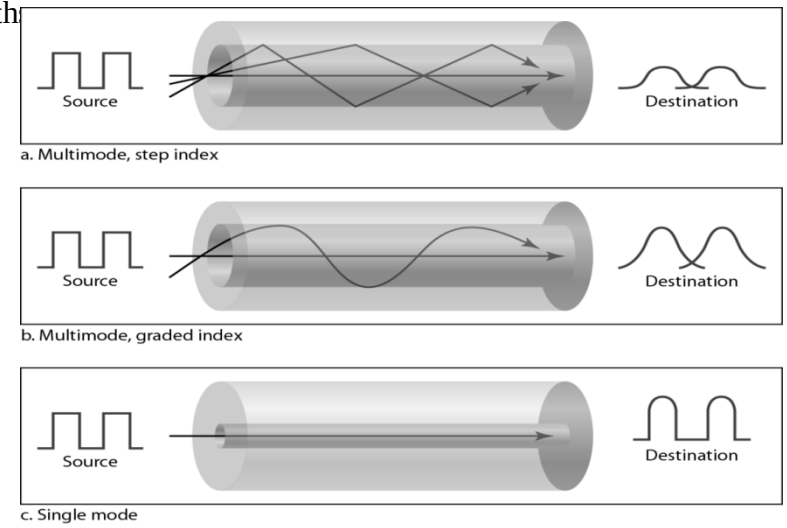
A Glass or plastic core is surrounded by a cladding of less dense glass or plastic.

Propagation Modes



Multimode

In the multiple mode, multiple light beams from a source move through the core in different path



- **Multimode-Step-Index fiber:** The density of core remains constant from the centre to the edge.

  A ray of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface there is an abrupt change to a lower density that changes the angle of the beam's motion.
- **Multimode- Graded -Index fiber:** The density is varying. Density is highest at the centre of the core and decreases gradually to its lowest at the edge.

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 multimedia fiber.

Connectors

- **Subscriber channel** (SC) **connector** is used for cable TV.
- **Straight-tip** (ST) **connector** is used for connecting cable to networking devices.

Advantages of Optical Fiber

- Noise resistance

- Less signal attenuation
- Light weight

Disadvantages

- Cost
- Installation and maintenance
- Unidirectional
- Fragility (easily broken)

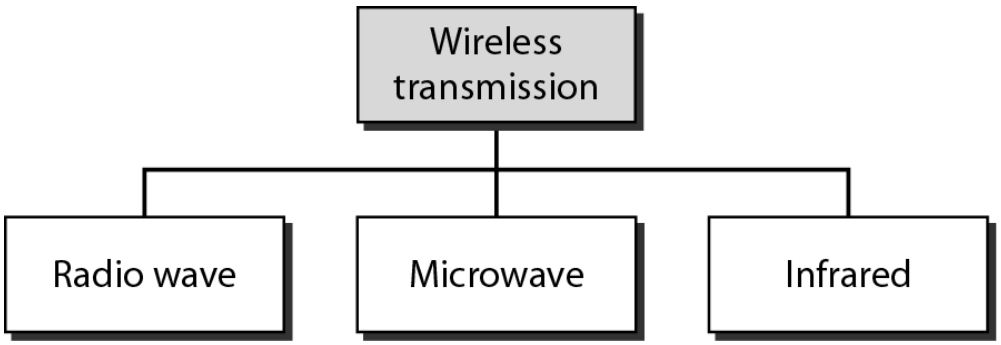
Unguided media

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 air and thus available to anyone who has device capable of receiving them.

Unguided signals can travel from the source to destination in several ways:

- **Ground propagation** – waves travel through lowest portion on atmosphere.
- **Sky propagation** – High frequency waves radiate upward into ionosphere and reflected back to earth.
- **Line-of-sight propagation** – Very high frequency signals travel in a straight line



Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.

Properties

- Radio waves are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- Radio waves, particularly those of low and medium frequencies, can penetrate walls.

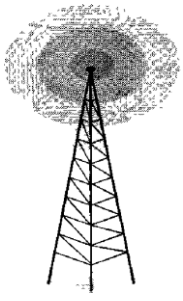


Fig:Omnidirectional antenna

Disadvantages

- The omnidirectional property has a disadvantage, that the radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

- As Radio waves can penetrate through walls, we cannot isolate a communication to just inside or outside a building.

Applications

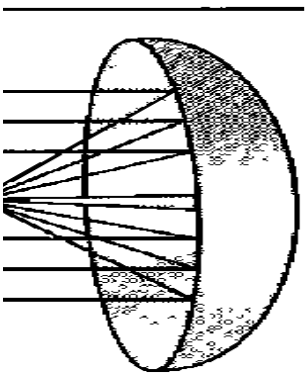
Radio waves are used for multicast communications, such as radio and television, and paging systems.

Microwaves

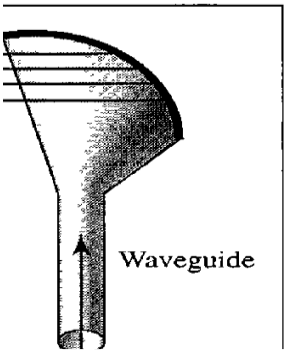
Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.

Properties

- Microwaves are unidirectional.
- Sending and receiving antennas need to be aligned
- Microwave propagation is line-of-sight
- Very high-frequency microwaves cannot penetrate walls



a) ParabolicDish antenna



b)Horn antenna

- Parabolic Dish antenna focus all incoming waves into single point
- Outgoing transmissions are broadcast through a horn aimed at the dish.

Disadvantage

- If receivers are inside buildings, they cannot receive these waves

Applications

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

Infrared

- Electromagnetic waves with frequencies from 300 GHz to 400 THz are called infrared rays
- Infrared waves, having high frequencies, cannot penetrate walls.

Applications

- Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

10. Discuss in detail the concepts of Packet Switched Networks (Packet Switching)

Introduction

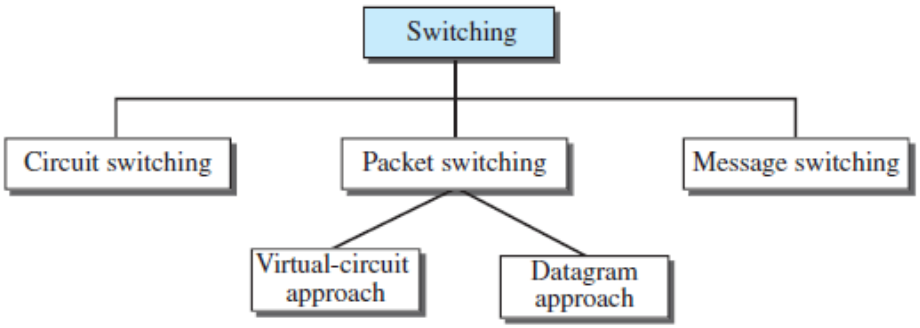
SWITCHING

- To make communication among multiple devices efficiently, a process used is called switching.
- A switched network consists of a series of interlinked nodes called switches.

Type of switching

- Circuit Switching
- Packet Switching
- Message Switching

Figure 8.2 *Taxonomy of switched networks*



Advantages of packet switching over circuit switching are as follows:

- Circuit switching is suitable for **voice communication**. When circuit switched links are used for data transmission, the link is often idle and its facilities wasted.
- The **data rate** of circuit switched connections for data transmission is very slow.
- Circuit switching is **inflexible**. Once a circuit has been established, that the path taken by all parts of the transmission whether or not it remains the most efficient.
- Circuit switching treats all transmission as equal. That means, there is no priority among the transmission of data.

The mostly widely used switching technique for data transmission *is packet switching.*
In this, the data are transmitted in the form of *packets*.
If the length of the packet is too long then it is broken-up into multiple packets.
Each packet contains data and also a header with control information.

PACKET SWITCHING:

There are two popular approaches to packet switching:

- Datagram approach and
- Virtual circuit approach

Datagram Approach:

- In the datagram approach, each packet is treated independently from all others.

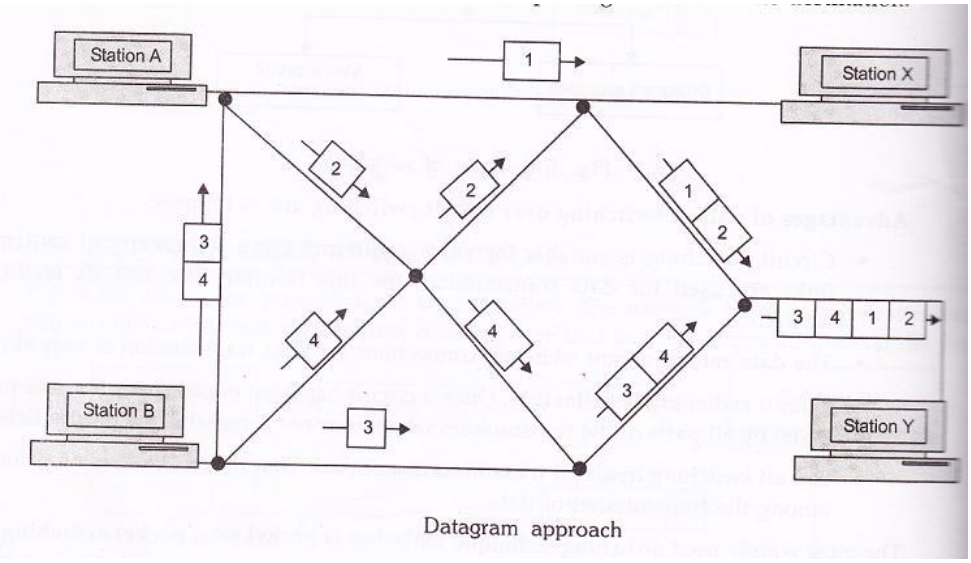
- A datagram is a multipacket of the same message and it works on the principle of 'send' and 'forget'.

The features of datagram are as follows:

- Circuit setup is not needed.
- Each packet contains both source and destination address.
- Each packet routed independently.
- Few packets are lost during crash.
- No effect or router failure.

Example

- The below figure shows how the datagram approach can be used to deliver four packets from station A to station Y.
- In this example, all four packets belong to the same message but may go by different paths to reach their destination.
- This approach can cause the datagrams of a transmission to arrive at their destination out of order.
- In most protocols, it is the responsibility of transport layer to reorder the datagrams before passing them on to the destination.

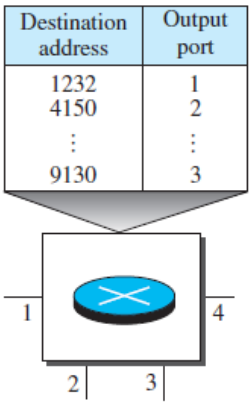


Datagram approach

Routing Table

In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. This is different from the table of a circuit switched network (discussed later) in which each entry is created when the setup phase is completed and deleted when the teardown phase is over

Figure 8.8 *Routing table in a datagram network*



A switch in a datagram network uses a routing table that is based on the destination address.

Virtual Circuit Approach:

- In the virtual circuit approach, the relationship between all packets belonging to a message or session is preserved.
- A single route is chosen between sender and receiver at the beginning of the session.
- When the data are sent, all packets of the transmission travel one after another along that route.

Virtual circuit transmission is implemented in two formats:

- Switched Virtual Circuit (SVC)
- Permanent Virtual Circuit (PVC)

Switched Virtual Circuit (SVC)

- In the **switched virtual circuit (SVC)** method, a virtual circuit is created whenever it is needed exits only for the duration of the specific exchange.
- If the station A wants to send four packets to station X, first it requests the establishment of a connection to station X.
- Once the connection is established, the packets are sent one after another and in sequential order. When the last packet has been received, the connection is released and that virtual circuit ceases to exist.
- Only one single route exists for the duration of transmission. Each time that station A wants to communicate with station X, a new route is established.

Permanent Virtual Circuit (PVC)

- In the **permanent Virtual Circuit (PVC)** method, the same virtual circuit is provided between two users on a continuous basis.

- This circuit is dedicated to the specific users. No one else can use it, because it is always in place.
- It can be used without connection establishment and connection termination.

Two SVC users may get a different route every time they request a connection whereas two PVC users always get the same route.

Comparison between Virtual circuit and Datagram

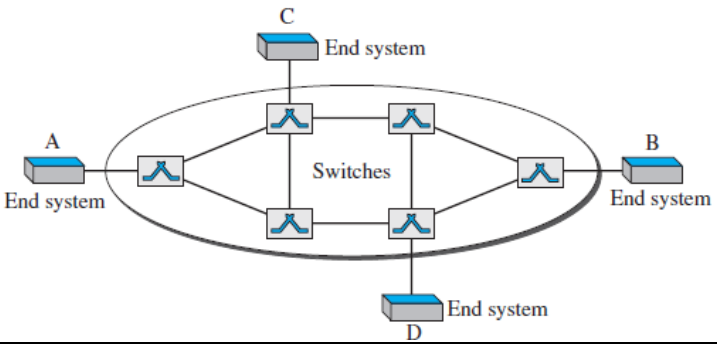
Datagram approach	Virtual circuit approach
In datagram approach, each packet is treated independently, thus they can follow different routes.	In virtual circuit approach, all packets follow the same route.
Packets can arrive at the destination in different order.	Packets should reach the destination in the same order.
Connection establishment is not required before transmission	Connection establishment is required.

Virtual-Circuit Networks – characteristics

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

1. As in a circuit-switched network, there are **setup and teardown phases** in addition to the data **transfer phase**.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what the next switch should be and the channel on which the packet is being carried), not end-to-end jurisdiction. The reader may ask how the intermediate switches know where to send the packet if there is no final destination address carried by a packet. The answer will be clear when we discuss virtual-circuit identifiers in the next section.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data-link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.

Figure 8.10 *Virtual-circuit network*



Addressing

In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier).

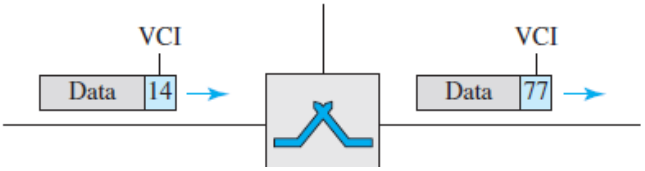
Global Addressing

A source or a destination needs to have a global address—an address that can be unique in the scope of the network or internationally if the network is part of an international network. However, we will see that a global address in virtual-circuit networks is used only to create a virtual-circuit identifier, as discussed next.

Virtual-Circuit Identifier

The identifier that is actually used for data transfer is called the ***virtual-circuit identifier*** **(VCI)** or the ***label.*** A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches.

Figure 8.11 *Virtual-circuit identifier*



Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: **setup, data transfer, and teardown**.

- In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.
- In the teardown phase, the source and destination inform the switches to delete the corresponding entry.
- Data transfer occurs between these two phases.

11. Compare circuit switching with packet switching Nov/Dec 2011

Circuit Switching Vs Packet Switching

Introduction

- In circuit switching dedicated communication path is available between two stations.
- It is easier to double the capacity of a packet switched network than a circuit network.
- A circuit network is heavily dependent on the number of channel available.
- It is easier to expand a packet Switching System.
- Circuit switched technologies takes double the cost for more boxes.
- Example: Internet Traffic of the telephone network

Circuit Switching:

Advantages

- Circuit is dedicated to the call-no interference, no sharing
- Guaranteed the full bandwidth for the duration of the call

- Guaranteed quality of service

Disadvantages

- Inefficient-the equipment may be unused for a lot of the call, if no data is being sent, the dedicated still remains open
- Takes a relatively long time to set up the circuit
- During a crisis or disaster, the network may become unstable or unavailable.
- It was primarily developed for voice traffic rather than data traffic.

Packet Switching:

Advantages

- More security
- Bandwidth used to full potential
- Devices of different speeds can communicate
- Not affected by line failure(redirects signal)
- Availability-do not have to wait for a direct connection to become available
- During a crisis or disaster, when the public telephone network might stop working, e-mails and texts can still be sent via packet switching

Disadvantages

- Under heavy use there can be a delay
- Data packets can get lost or become corrupted.
- Protocols are needed for a reliable transfer
- Not so good for some types data streams.

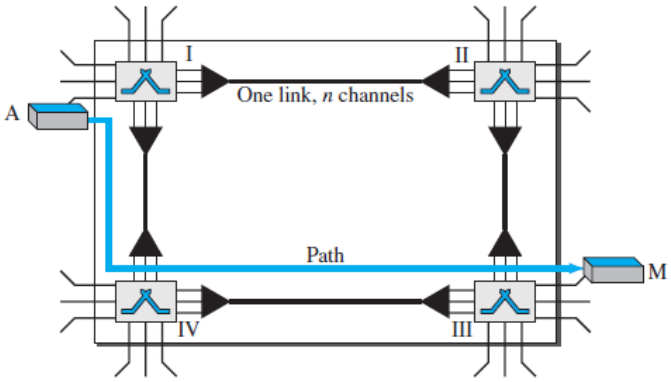
  Example: Real-Time Video streams can lose frames due to the way packets arrive out of sequence.

12. Explain in detail about circuit switched networks

A **circuit-switched network** consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link.

Figure 8.3 shows a trivial circuit-switched network with four switches and four links. Each link is divided into *n* (*n* is 3 in the figure) channels by using FDM or TDM

Figure 8.3 *A trivial circuit-switched network*



We have explicitly shown the multiplexing symbols to emphasize the division of the link into channels even though multiplexing can be implicitly included in the switch fabric.

The end systems, such as computers or telephones, are directly connected to a switch. We have shown only two end systems for simplicity. 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, the **data-transfer phase** can take place. After all data have been transferred, the circuits are torn down.

We need to emphasize several points here:

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels (bandwidth in FDM and time slots in TDM), switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the **teardown phase.**
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to end addressing 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.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) 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. For example, in Figure 8.3, 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 finds 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.

Data-Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

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

OLD REGULATION - UNIVERSITY QUESTIONS

B.E/B.TECH NOVEMBER/DECEMBER 2014 (2008 regulation)

2 MARKS

1. What is meant by framing (Q.NO 44)
2. Define hamming distance (Q.NO 50)

16 MARKS

1. Discuss the issues in the data link layer (16) (Q.NO 9)
2. Explain in detail the error detecting codes (16) (Q.NO 10)

B.E/B.Tech April May 2015

2 MARKS

1. What do you mean by error control?(Q.NO 34)
2. Define flow control (Q.NO 27)

16 MARKS

1. Discuss in detail about Internet Architecture (16) (Q.NO 6)
2. What is the need for error detection? Explain with typical examples. Explain methods used for error detection and error correction (16) (Q.NO 10 & 13)

B.E/B.Tech Nov-Dec 2015

2 MARKS

1. State the issues of data link layer (Q.NO 37)
2. Define the term protocol (Q.NO 45)

16 MARKS

1. Draw the OSI network architecture and explain the functionalities of every layer in detail (16) (Q.NO 5)
2. Explain the various flow control mechanisms (16) (Q.NO 11)

B.E/B.Tech April-May 2016

2 MARKS

1. Define flow control. (Q.NO 27)
2. Write the parameters used to measure network performance (Q.NO 3)

16 MARKS

1. Explain any two error detection mechanism in detail (16) (Q.NO 10)
2. Explain in detail about HDLC & PPP (8+8) (Q.NO 9)

B.E/B.Tech Nov-Dec 2016

2 MARKS

1. List the services provided by data link layer (Q.NO 37)
2. Write the mechanism of stop and wait flow control (Q.NO 46)

16 MARKS

1. Draw the OSI network architecture and explain the functionalities of every layer in detail (16) (Q.NO 5)
2. a)Discuss in detail about the network performance measures (8) (Q.NO 8)
   b) Explain selective-repeat ARQ flow control method.(8) (Q.NO 11)

B.E/B.Tech April-May 2017

PART A

1. Distinguish between packet switched & circuit switched networks. (Q.NO 51)
2. What is meant by bit stuffing? Give example (Q.NO 40)

PART B

1. i) Explain the challenges faced in building a network (10) (Q.NO 4)
   ii) Obtain the 4-bit CRC code for the data bit sequence 10011011100 using the polynomial x^4+x^2+1 (3) (Q.NO 14)

2.i) With a protocol graph explain the architecture of internet (7) (Q.NO 6)
ii) Consider a bus LAN with a number of equally spaced stations with a data rate of 9 Mbps and a bus length of 1 km. What is the mean time to send a frame of 500 bits to another station, measured from the beginning of transmission to the end of reception? Assume a propagation speed of 150 m/s. If two stations begin to monitor and transmit the same time, how long does it need to wait before interference is noticed? (6) (Q.NO 15)

B.E/B.Tech Nov-Dec 2017

PART A

1. Define the terms: Bandwidth & Latency (Q.NO 52)
2. Compare Byte oriented versus Bit-oriented protocol (Q.NO 53)

PART B

1. With a neat sketch, explain the architecture of an OSI seven layer model (13) (Q.NO 5)
2. Discuss the approaches used for error detection in networking (13) (Q.NO 10)

PART C

1. Outline the steps involved in building a computer network. Give the detailed description for each step (15) (Q.NO 4)