Course Plan			
Module	**Contents**	**Hours**	**End Sem. Exam Marks**
I	Introduction – Uses – Network Hardware – LAN –MAN – WAN, Internetworks – Network Software – Protocol hierarchies – Design issues for the layers – Interface & Service – Service Primitives. Reference models – OSI – TCP/IP.	**07**	**15%**

INTRODUCTION

'COMPUTER NETWORK' means a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connections need not be via a copper wire; fiber optics, Microwaves, infrared, and communication satellites can also be used.

USES OF COMPUTER NETWORKS

Computer Networks can be used for

1. Business Applications
2. Home Applications
3. Mobile Users
4. Social Issues

1. Business Applications

The issue here is **resource sharing**, and the goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user. An obvious and widespread example is having a group of office workers share a common high volume networked printer which is cheaper, faster, and easier to maintain than a large collection of individual printers.

Another issue is **sharing information**. Most companies have customer records, inventories, accounts receivable, financial statements, tax information, and much more online. Company's information system consists of one or more databases and employees need to access them remotely. The employees have simpler machines called Clients and the data are stored on powerful computers called Servers. This whole arrangement is called the client-server model.

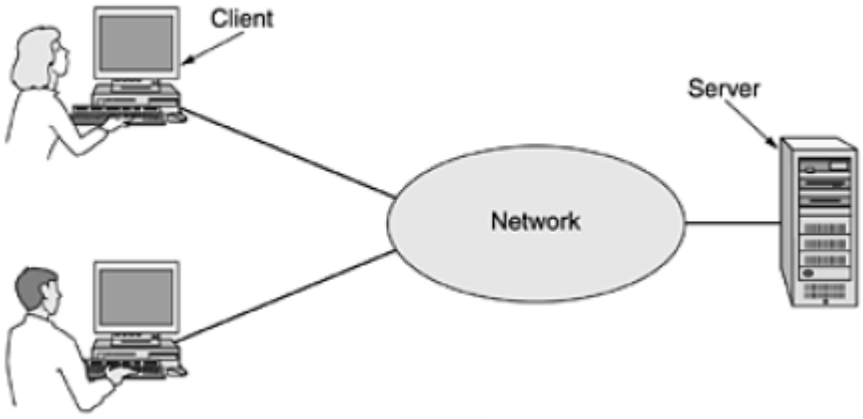

Fig: A network with two clients and one server.

A computer network can provide a powerful **communication medium** among employees where two or more people who work far apart can write a report together and also perform computer-assisted communication called videoconferencing.
A third goal is **doing business electronically with other companies**.
A fourth goal is **doing business with consumers over the Internet.**

2. Home Applications

Some of the more popular uses of the Internet for home users are as follows:
1. Access to remote information.
2. Person-to-person communication.
3. Interactive entertainment.
4. Electronic commerce.

1. Access to remote information comes in many forms. It can be surfing the World Wide Web for information or just for fun. It include online newspaper, accessing digital library
2. Person-to-person communication includes E-mail, instant messaging, discussion using worldwide newsgroups, chat rooms etc. Another type of person-to-person communication is peer-to-peer communication. Here every person can communicate with one or more other people; there is no fixed division into clients and servers.

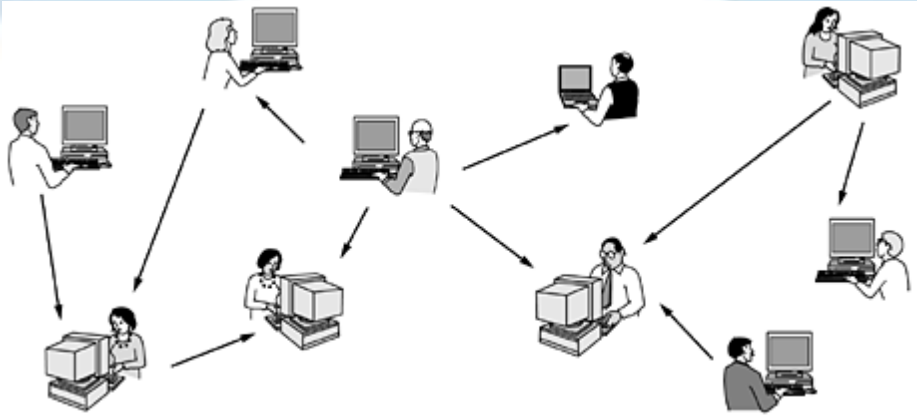

Fig: In a peer-to-peer system there are no fixed clients and servers

3. Our third category is entertainment, which is a huge and growing industry which includes video on demand, live television etc.
4. Our fourth category is electronic commerce where home shopping is already popular and enables users to inspect the on-line catalogs of thousands of companies and some of these catalogs provide the ability to get an instant video on any product by just clicking on the product's name. After the customer buys a product electronically but cannot figure out how to use it, on-line technical support may be consulted.

Another area is accessing financial institutions to pay bills, manage bank accounts, and handle investments electronically. Telelearning and Telemedicine have become important. Now there are applications like using the webcam in your refrigerator to see if you have to buy milk on the way home from work.

3. Mobile Users

- Mobile computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest growing segments of the computer industry where they use wireless networks.
- Wireless networks are of great value to fleets of trucks, taxis, delivery vehicles, and repairpersons for keeping in contact with home.
- Wireless networks are also important to the military
- Wireless networks and mobile computing are related as follows:

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

- Wireless parking meters have advantages for both users and city governments. The meters could accept credit or debit cards with instant verification over the wireless link. When a meter expires, it could check for the presence of a car (by bouncing a signal off it) and report the expiration to the police
- In Vending Machines if they issued a wireless report once a day announcing their current inventories, the truck driver would know which machines needed servicing and how much of which product to bring.
- In utility meter reading if electricity, gas, water, and other meters in people's homes were to report usage over a wireless network, there would be no need to send out meter readers. Similarly, wireless smoke detectors could call the fire department instead of making a big noise.
- Smart watches with radios, wearable computers, m-commerce etc. are some other applications.

4. Social Issues

- The widespread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks is newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise. The trouble comes when newsgroups are set up on topics that people actually care about, like politics, religion, or sex. Views posted to such groups may be deeply offensive to some people.
- People have sued network operators, claiming that they are responsible for the contents of what they carry, just as newspapers and magazines are.

- Identity theft is becoming a serious problem as thieves collect enough information about a victim to obtain get credit cards and other documents in the victim's name. Finally, being able to transmit music and video digitally has opened the door to massive copyright violations that are hard to catch and enforce.

NETWORK HARDWARE

All computer networks fit into one of the two dimensions namely

1. **Transmission Technology**, this focuses on the basic underlying physical network for e.g., whether the nodes share a communication media or each pair of node has a separate dedicated link.
2. **Scale**, which focuses on how large the network is.

Types of Transmission technology

There are two types of transmission technology

1. Broadcast links.
2. Point-to-point links

1. Broadcast links.

Broadcast have the following features:

- Use a **single communication channel** shared by all computers in the network
- **Short messages**(packets) are sent by any machine and received by all other computers on the network
- An **address** is used in the message to select the target machine.
- Some broadcast systems also support transmission to a subset of the machine called **multicasting**
- **Localized networks** use broadcasting

2. Point-to-point networks

Point-to-point networks have the following features:

- Consists of many connections between individual pairs of machines
- Message packet have to visit **one or more intermediate machines** before reaching its intended target
- **Routing algorithms** play an important role
- **Large area networks** use point to point networks

3. An alternative criterion for classifying networks is their scale. In figure we classify multiple processor systems by their physical size.

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

Fig: Classification of interconnected processors by scale (physical size)

Local Area Networks

- 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. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size, (2) their transmission technology, and (3) their topology.

- LANs are restricted in size
- LANs may use a transmission technology consisting of a cable to which all the machines are attached which runs at speeds of 10 Mbps to 100Mbps
- Various topologies are possible for broadcast LANs. Two of them are
  - Bus
  - Ring

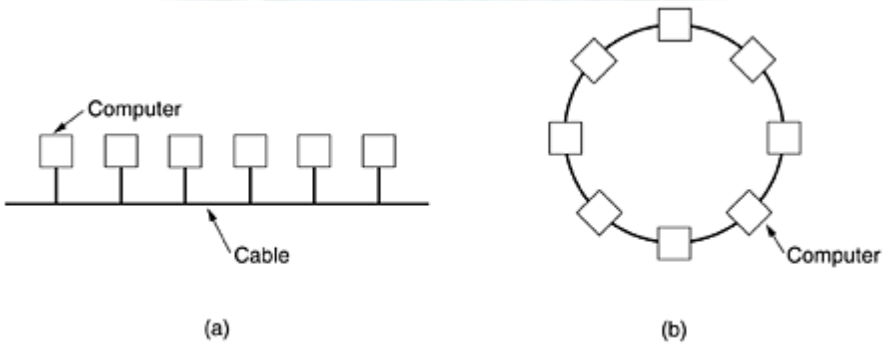

Fig: Two broadcast networks. (a) Bus. (b) Ring.

- In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.

- In a ring, **Token** passing is the method of medium access, with only one **token** allowed to exist on the network at any one time. When a station has data to transmit, it acquires the token at the earliest opportunity, marks it as busy, and attaches the data and control information to the token to create a data frame, which is then transmitted to the next station on the ring. The frame will be relayed around the ring until it reaches the destination station, which reads the data, marks the frame as having been read, and sends it on around the ring. When the sender receives the acknowledged data frame, it generates a new token, marks it as being available for use, and sends it to the next station IEEE 802.5 (the IBM token ring), FDDI are examples of ring network.
- Advantages
  - File and program sharing
  - Sharing of expensive devices
  - Communication
  - Easy backup
  - Resource management
- Disadvantages
  - Reliability
  - Capacity
  - Power backup
  - Security
  - Limited area

Metropolitan Area Networks

- MAN is basically a bigger version of a LAN and normally uses similar technology. It is designed to extend over an entire city which covers upto 50km. A MAN may be wholly owned and operated by a private company or it may be a service provided by a public company.
- MANs are formed by connecting multiple LANs. MANs are extremely efficient and provide fast communication via high-speed carriers, such as fiber optic cables.

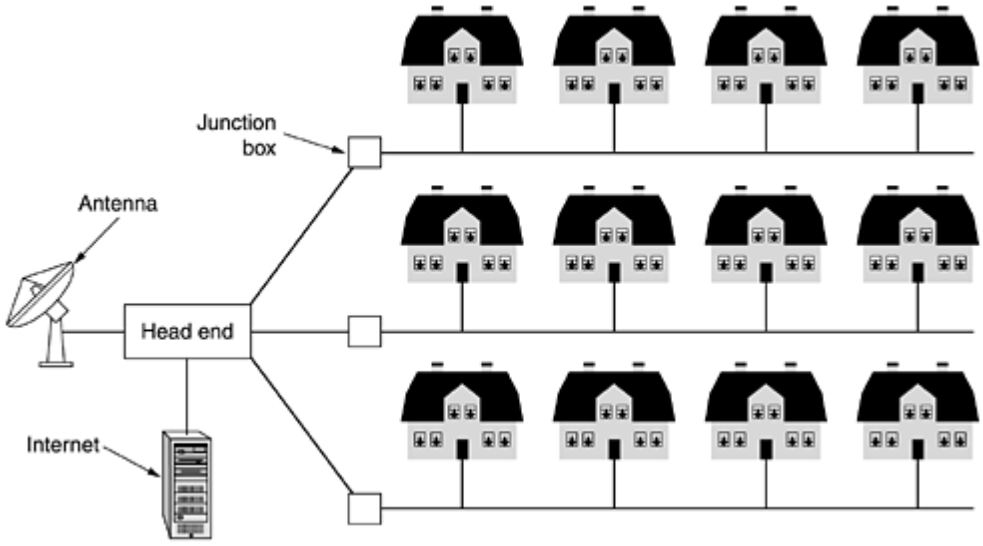

Fig: A metropolitan area network based on cable TV

- Advantages
  - Covers larger area
  - Error rates are moderate
- Disadvantages

- Needs huge space to setup
- Speed of accessing data is less
- Equipments used are expensive

Wide Area Networks

- A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines (hosts) intended for running user (i.e., application) programs.
- The hosts are connected by a communication subnet.
- The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider.
- Subnet carries messages from host to host.
- The subnet consists of two distinct components: transmission lines and switching elements. **Transmission lines** move bits between machines. They can be made of copper wire, optical fiber, or even radio links. **Switching elements** are specialized computers that connect three or more transmission lines.
- When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. These switching computers have been called by **Routers.**

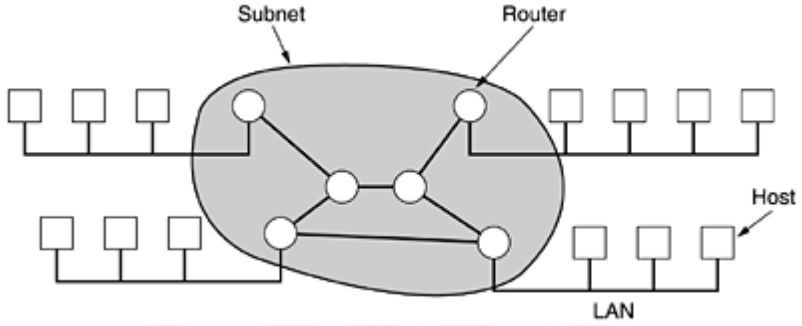

Fig: Relation between hosts on LANs and the subnet

- The principle of a packet-switched WAN (point-to-point, store and forward) is such that, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. A stream of packets resulting from some initial message is illustrated in figure.

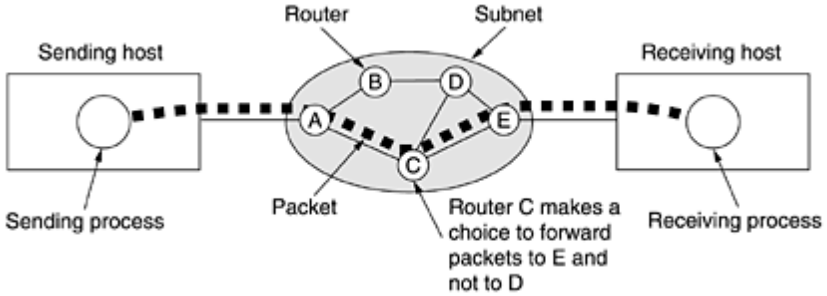

Fig: A stream of packets from sender to receiver.

- Routing decisions are made locally. When a packet arrives at router A, it is up to A to decide if this packet should be sent on the line to B or the line to C. How A makes that decision is called the routing algorithm

- Advantages
  - Can be increased without any bound
  - Share data and resources globally
- Disadvantages
  - Requires large space
  - Data access rate is less
  - Equipments to implement are expensive
  - Error rates are high

INTERNETWORKS

- A collection of interconnected networks is called an internetwork or internet
- Here different software and hardware are interconnected as one network
- Gateways are computers used to translate between the different hardware and software components of the internetwork.
- The internet is the largest example of internetworks
- A common form of internet is a collection of LANs connected by WAN.
- The Internet started in the late sixties as ARPANET, a government sponsored network between small number of universities and government centers.
- The National Science Foundation expanded ARPANET into NSFNET(Several thousand hosts in 1988)
- TCP/IP emerged as its standard network software.
- The number of hosts on the internet is more than 50 million

NETWORK SOFTWARE

Protocol Hierarchies

- A network protocol is a set of rules and standards which must be followed by network devices for proper communication among them.
- Internet protocol is most widely used
- E.g. are HTTP, TCP, UDP, FTP etc.

WHY Layers?

To reduce the design complexity of computer communications, hardware and software, the functionalities needed is organized as series of layers each built on its predecessor

- The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented
- Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer n protocol
- A five-layer network is illustrated in fig

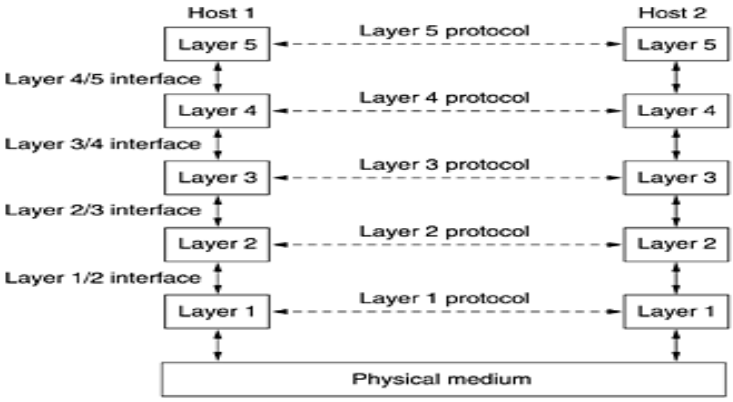

Fig: Five layer Network

- In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs. In the figure , virtual communication is shown by dotted lines and physical communication by solid lines.

Interfaces and services

- Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one.
- A set of layers and protocols is called a **network architecture**
- A list of protocols used by a certain system, one protocol per layer, is called a **protocol stack**
- A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission. Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information, such as sequence numbers, to allow layer 4 on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence.

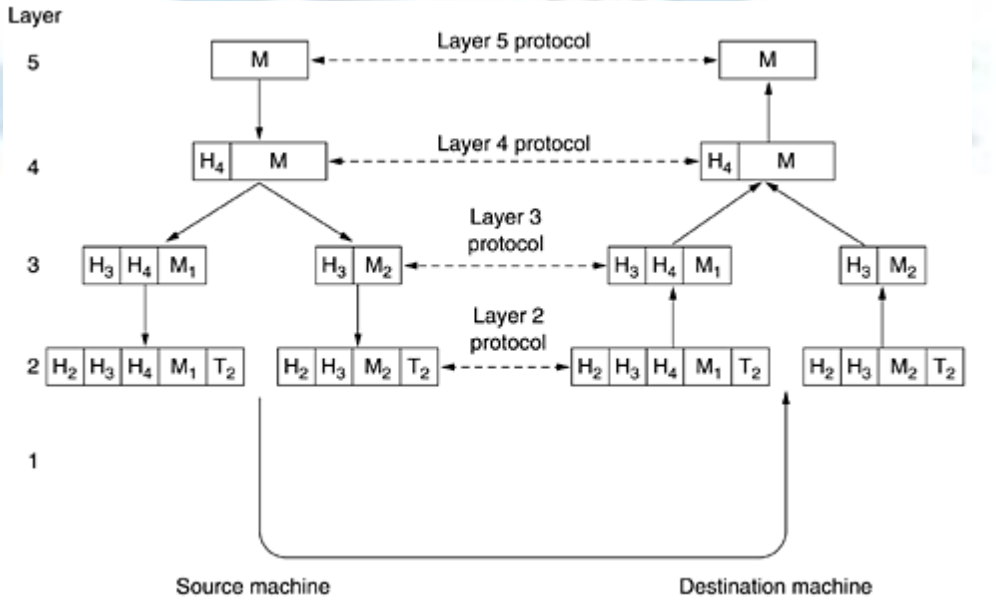

Fig: Example information flow supporting virtual communication in layer 5.

- Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 headers to each packet. In this example, M is split into two parts, M1 and M2.Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2. Layer 2 adds not only a header to each piece, but also a trailer, and gives the resulting unit to layer 1 for physical transmission. At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses.

Design Issues for the Layers

The following are the design issues

Addressing: Each layer needs an identifying mechanism for the source and the destination machine. There should be two addresses

a. Destination address
b. Source Address

Mode of Communication

The designing layer should have to keep the mode of transmission in mind. The protocol used for congestion control or media access should be considered under the mode of transmission.

Error Control: Two types of error control

a. Error detecting code
b. Error Correcting code

Sequencing

Order of the packets /Frames must be ensured by implementing sequence number in their frames. Sequence number is needed for error control and detection.

Flow Control

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

Packet size

A standard packet size is to be specified to make transmission compatible. Each strategy or modes have their own standard and this is strictly followed.

Multiplexing

Multiplexing is used in the physical layer. Multiplexing is needed when a single media or wire is used by more than one user.

Routing strategy:

a. Static Routing: In this strategy routes are predefined.
b. Dynamic Routing: In this strategy routes are chosen based on the routing algorithm.

Service Primitives

- A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity
- The primitives are normally system calls. These calls cause a trap to kernel mode, which then turns control of the machine over to the operating system to send the necessary packets.

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

- The following figure shows how the primitives are put into action and how the packets are send

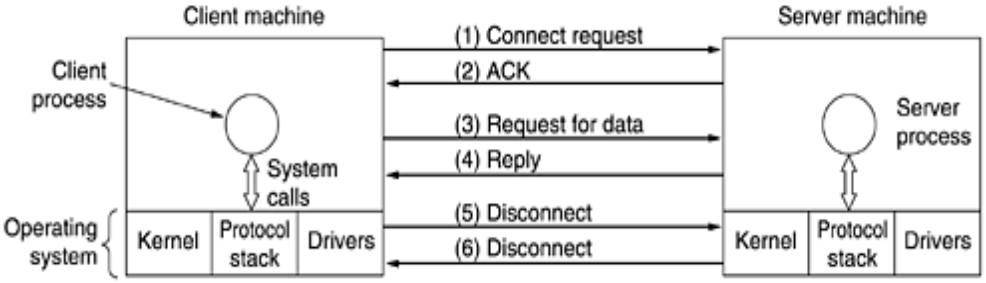

Fig: Packets sent in a simple client-server interaction on a connection-oriented network

Reference Models

OSI Reference Model

A networking reference model defined by the ISO (International Organization for Standardization) divides computer to computer communication into seven connected layers. Such layers are known as **protocol stack** Open systems Interconnection (OSI) is a reference model that determines the way which messages should be transmitted between any two points in a network.
The different layers of OSI reference are as below

Application layer

The application layer services as window for users and application processes to access network services. It handles issues such as network transparency, resource allocation etc. This layer is not an application in itself, although some applications may perform application layer functions. This layer provides network services to the end-users. Examples of network applications are Mail, FTP, Telnet, DNS, NIS, NFS etc.
Functions of application layer

1. Authentication: authenticates the sender and receiver of the message or both.
2. File access, Transfer and Management: Allows the user at a remote site to access files on another host.
3. Directory services: Provides access to global information and database sources.

Presentation Layer

The presentation layer serves as the data translator for a network. It is usually a part of an operating system and converts incoming and outgoing data from one presentation format to another. This layer is also known as syntax layer.
Functions of presentation layer

1. Data compression: It refers to encoding the data using less number of bits.
2. Encryption: ensures security by using different algorithms for coding, passwords and log-in codes.

Session Layer

The session layer establishes a communication session between processes running on different communication entities in a network and can support a message mode data transfer. It deals with session and connection coordination.

Functions of Session Layer

1. Session Management: divides the session into subsessions by inserting check points.
2. Synchronization: Selects the order in which the dialog units must pass to the transport layer. It also gets confirmation from the receiver machine.
3. Dialog control: Controls which user will send data and at what time.
4. Closing the session: Ensures that the data transfer is completed before the session closes.

Transport Layer

The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. It ensures complete data transfer. Transport layer sub divides user-buffer into network-buffer sized datagrams and enforces desired transmission control. The transport protocols are: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

Functions of Transport layer

1. Service point addressing: Here packets are delivered to correct process.
2. End-to-end Message Delivery: ensures the entire message is delivered to the destination.
3. Segmentation and Reassembly: Divides each message into segments and assigns a sequence number tot these segments. This helps to reassemble the message if some error occurs during message transmission.
4. Connection Control: decides whether the whole packets are sent using a single path or not.

Network Layer

It determines the physical path that the data takes on the basis of network conditions, priority of service and other factors. The network layer is responsible of routing and forwarding of data packets.

Functions of network layer

1. Source to destination delivery: Transfers packets from source to destination
2. Logical addressing: adds the source and destination address in the header
3. Routing: selects the optimal path out of multiple paths so that a packet can choose so that a packet can follow.
4. Address Transformation: Interprets the logical address
5. Multiplexing: utilizes one physical line for transferring data between several devices at a time.

Data Link Layer

The data link layer is responsible for the error free transfer of data frames. This layer provides synchronization for the physical level. Data link layer defines the format of data on the network.

Data link layer sub layers:

Logical Link Control (LLC) 802.2: provides flow control

Media Access Control (MAC) 802.3: responsible for transferring packets over the network

Functions of the data link layer:

1. Framing: frames are added with a Header and a Trailer.
2. Arbitration: negotiates the access of single data channel when multiple hosts are trying to access it at the same time.
3. Physical Addresssing:primary form of physical addressing is the MAC address
4. Error Detection: detects the errors when data passed through the wire. Here a CRC(Cyclic Redundancy Check) is calculated and added to the frame trail before it is sent to the physical layer
5. Encapsulation: Some information are hidden from the higher level using encapsulation

Physical Layer

It is the cable or the physical medium itself. This layer is responsible for packaging and transmitting the data on the physical media.

Functions

1. Line configuration: defines the way in which two or more devices connected physically.
2. Data transmission
3. Topology
4. Signals

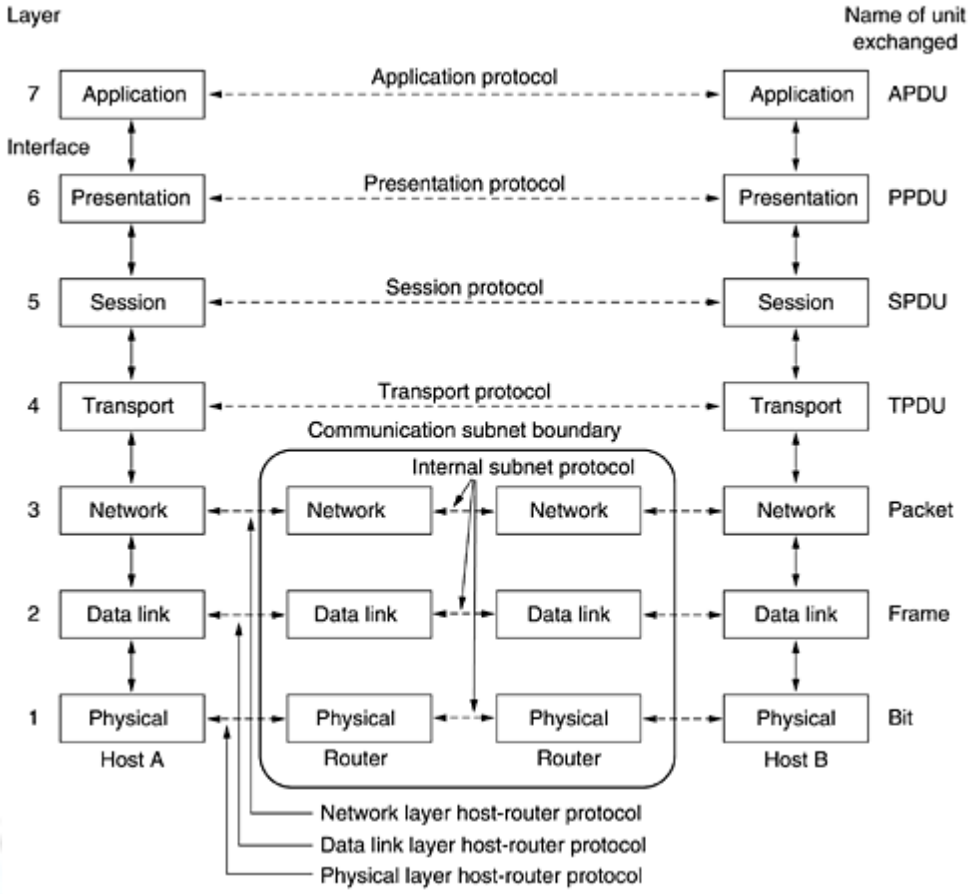

Fig: Layers of ISO/OSI Model

TCP/IP Reference Model

Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide. Its simplicity and power has led to its becoming the single network protocol of choice in the world today. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.

This model was initially developed & used by ARPANET (Advanced Research Project Agency Network). ARPANET was a **community of researchers** sponsored by the U.S. department of defense. It connects many universities and government installations using leased telephone lines .Certainly the **ARPAnet is the best- known TCP/IP network.**

The most accurate name for the set of protocols is the "**Internet protocol suite**". **TCP and IP are two of the protocols in this suite**. The Internet is a collection of networks. Term "Internet" applies to this entire set of networks. Like most networking software, **TCP/IP is modelled in layers**. This layered representation

leads to the term **protocol stack**, which refers to the stack of layers in the protocol suite. It can be used for positioning the TCP/IP protocol suite against other network software like Open System Interconnection (OSI) model.

By dividing the communication software into layers, the protocol stack allows for division of labor, ease of implementation and code testing, and the ability to develop alternative layer implementations. Layers communicate with those above and below via concise interfaces. In this regard, a layer provides a service for the layer directly above it and makes use of services provided by the layer directly below it. For example, the IP layer provides the ability to transfer data from one host to another without any guarantee to reliable delivery or duplicate suppression.

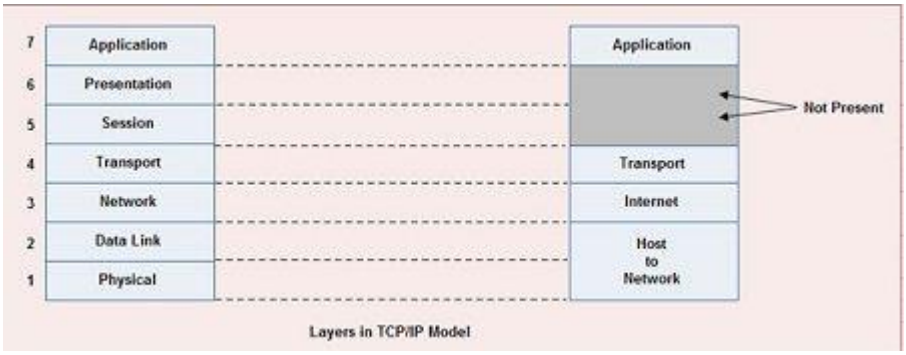

Fig: Comparison between Layers of ISO-OSI Model and Layers of TCP/IP Model

TCP/IP is a family of protocols. A few provide "low- level" functions needed for many applications. These include IP, TCP, and UDP. Others are protocols for doing specific tasks, e.g. transferring files between computers, sending mail, or finding out who is logged in on another computer**. Initially TCP/IP was used mostly between minicomputers or mainframes.** These machines had their own disks, and generally were self contained.

Application Layer

The application layer is provided by the program that uses **TCP/IP for communication**. An application is a user process cooperating with another process usually on a different host (there is also a benefit to application communication within a single host**). Examples of applications include Telnet and the File Transfer Protocol (FTP).**

Transport Layer

The transport layer provides the **end-to-end data transfer by delivering data from an application to its remote peer**. Multiple applications can be supported simultaneously. The most-used transport layer protocol is the **Transmission Control Protocol (TCP),** which provides **connection-oriented reliable data delivery**, **duplicate data suppression, congestion control, and flow control**.

Another transport layer protocol is the **User Datagram Protocol.** It provides **connectionless, unreliable, best-effort service**. As a result, applications using UDP as the transport protocol have to provide their own **end-to-end integrity, flow control, and congestion control,** if desired. Usually, UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

Internetwork Layer

The **internetwork layer**, also called the **internet layer or the network layer**, provides the "**virtual network**" image of an internet this layer shields the higher levels from the physical network architecture below it**. Internet Protocol (IP) is the most important protocol in this layer**. It is a connectionless protocol

that does not assume reliability from lower layers. **IP does not provide reliability, flow control, or error recovery.**

These functions must be provided at a higher level. IP provides a routing function that attempts to deliver transmitted messages to their destination. A **message unit** in an IP network is called an **IP datagram**.

This is the basic unit of information transmitted across TCP/IP networks. Other internetwork-layer protocols **are IP, ICMP, IGMP, ARP, and RARP**.

Network Interface Layer

The network interface layer, also called **the link layer or the data-link layer or Host to Network Layer**, is the interface to the actual network hardware. **This interface may or may not provide reliable delivery**, and may be packet or stream oriented.

In fact, **TCP/IP does not specify any protocol here**, but can use almost any network interface available, which illustrates the flexibility of the IP layer. Examples are **IEEE 802.2, X.25, ATM, FDDI, and even SNA.TCP/I** specifications do not describe or standardize any network-layer protocols; they only standardize ways of accessing those protocols from the internet work layer.

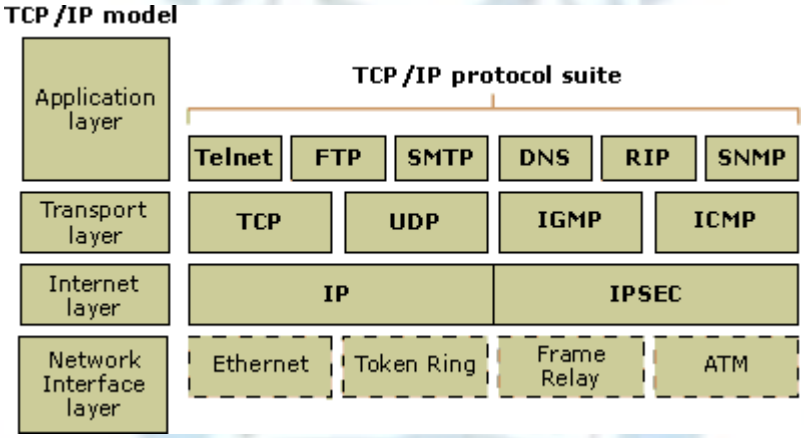

Fig: TCP/IP Model

University questions April 2018

3marks

1. **How are computer networks classified on the basis of physical size?**
2. **What are the reasons for using Layered Architecture in Computer Networks?**
3. **Define the terms protocols and interface.**

9marks

1. **a) What are the OSI service primitives for connection oriented service(5)**
   b) List out the key design issues that occur in Computer Networks (4)
2. **a) Describe the ISO/OSI layered architecture with the help of neat diagram(5)**
   b) Write notes on IEEE 802.5 standard.(4)