Module 1

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.

Computer network/data network: A network can be defined as a group of computers and other devices connected in some way so as to be able to exchange data. A network allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes (data links). These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi. Each of the devices on the network can be thought of as a node, each node has a unique address.

Advantages of computer network:

SAC

- **It enhances communication and availability of information:** Networking, especially with full access to the web, allows ways of communication that would simply be impossible before it was developed. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world, which is a huge boon for businesses. Also, it allows access to a vast amount of useful information, including traditional reference materials and timely facts, such as news and current events.

- **It allows for more convenient resource sharing:** This benefit is very important, particularly for larger companies that really need to produce huge numbers of resources to be shared to all the people. Since the technology involves computer-based work, it is assured that the resources they wanted to get across would be completely shared by connecting to a computer network which their audience is also using.

- **It makes file sharing easier** : Computer networking allows easier accessibility for people to share their files, which greatly helps them with saving more time and effort, since they could do file sharing more accordingly and effectively.

- **It is highly flexible.** This technology is known to be very flexible, as it gives users the opportunity to explore everything about essential things, such as software without affecting their functionality. Plus, people will have the accessibility to all information they need to get and share.

- **It is an inexpensive system.** Installing networking software on your device would not cost too much, as you are assured that it lasts and can effectively share information to your peers. Also, there is no need to change the software regularly, as mostly it is not required to do so.

- **It increases cost efficiency.** With computer networking, you can use a lot of software products available on the market which can just be stored or installed in your system or server and can then be used by various workstations.

- **It boosts storage capacity.** Since you are going to share information, files and resources to other people, you have to ensure all data and content are properly stored in the system. With this networking technology, you can do all of this without any hassle, while having all the space you need for storage.

SAC

Disadvantages of computer network

- **It lacks independence.** Computer networking involves a process that is operated using computers, so people will be relying more of computer work, instead of exerting an effort for their tasks at hand. Aside from this, they will be dependent on the main file server, which means that, if it breaks down, the system would become useless, making users idle.
- **It poses security difficulties.** Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.

- **It allows for more presence of computer viruses and malware.** There would be instances that stored files are corrupt due to computer viruses. Thus, network administrators should conduct regular check-ups on the system, and the stored files at the same time.
- **Its light policing usage promotes negative acts.** It has been observed that providing users with internet connectivity has fostered undesirable behaviour among them. Considering that the web is a minefield of distractions—online games, humor sites. The huge network of machines could also encourage them to engage in illicit practices, such as instant messaging and file sharing, instead of working on work-related matters. While many organizations draw up certain policies on this, they have proven difficult to enforce and even engendered resentment from employees.
- **It requires an efficient handler.** A computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.
- **It requires an expensive set-up.** Though computer networks are said to be an inexpensive system when it is already running, its initial set up cost can still be high depending on the number of computers to be connected. Expensive devices, such as routers, switches, hubs, etc., can add up to the cost. Aside from these, it would also need network interface cards (NICs) for workstations in case they are not built in.
- **It lacks robustness.** If a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To deal with these problems, huge networks should have a powerful computer to serve as file server to make setting up and maintaining the network easier.

SAC

USES OF COMPUTER NETWORK

Business Applications: Many companies have a substantial number of computers. For example, a company may have separate computers to monitor production, keep track of inventories, and do the payroll. Initially, each of these computers may have worked in isolation from the others, but at some point, management may have decided to connect them to be able to extract and correlate information about the entire company. 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.

A computer network can provide a powerful communication medium among employees.

A third goal for increasingly many companies is doing business electronically with other companies, especially suppliers and customers.

A fourth goal that is starting to become more important is doing business with consumers over the Internet. Airlines, bookstores, and music vendors have discovered that many customers like the convenience of shopping from home.

SAC

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.

Mobile Users

Mobile computers, such as notebook computers and personal digital assistants (PDAs), are one of the fastest growing segments of the computer industry.

There are two types of transmission technology that are in widespread use. They are as follows:

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

Broadcast networks have a single communication channel that is shared by all the machines on the network.
Point-to-point networks consist of many connections between individual pairs of machines. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machines. Machine are received by all the others.

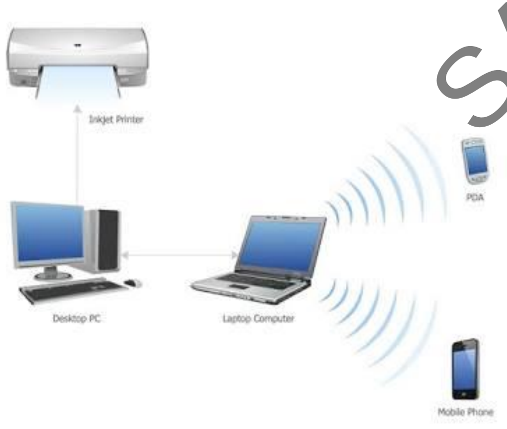
Types of computer network

1. Personal Area Network (PAN)

The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences and are managed by one person or organization from a single device.

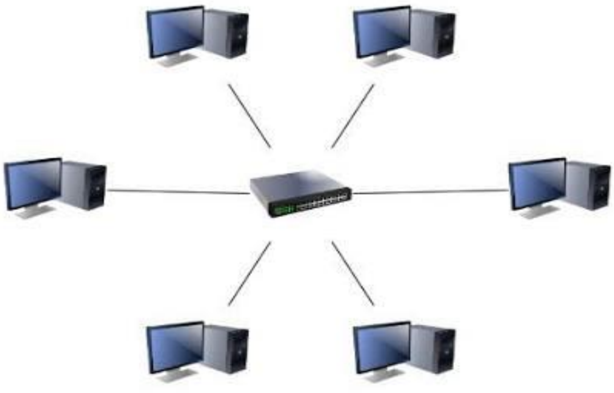
Eg : wireless computers ,keyboard &Mouse
Bluetooth embedded headphones

SAC



2. Local Area Network (LAN)

LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs



LAN (Local Area Network) links the devices in local areas such as in your campus, building etc. It provides useful way of sharing resources such as printer &scanner, sharing of file server.

3. Wireless Local Area Network (WLAN)

Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi. Typically seen in the same types of applications as LANs, these types of networks don't require that devices rely on physical cables to connect to the network.

4. Campus Area Network (CAN)

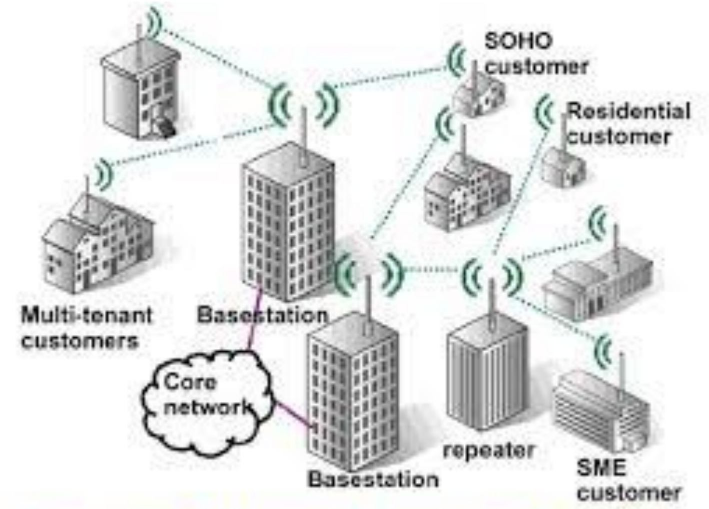
SAC

Larger than LANs, but smaller than metropolitan area networks (MANs, explained below), these types of networks are typically seen in universities, large K-12 school districts or small businesses. They can be spread across several buildings that are fairly close to each other so users can share resources.

5. Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

MAN covers a particular tower or large city. It exceeds to 32 to 40 km or 20 to 25 miles. Multiple LAN connected to form LAN. MAN provides uplink for LAN to WAN. They provide faster communication using optic cable. The backbone of MAN is high capacity &high-speed fibre optics.

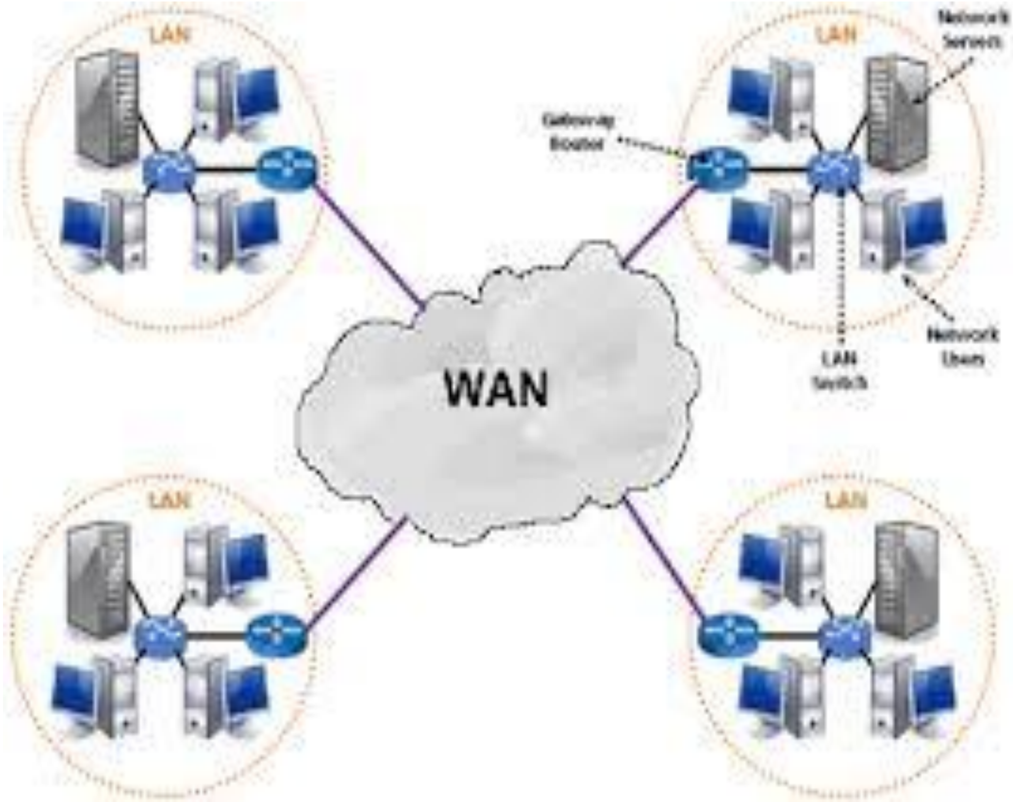


Metropolitan Area Network - www.certiology.com

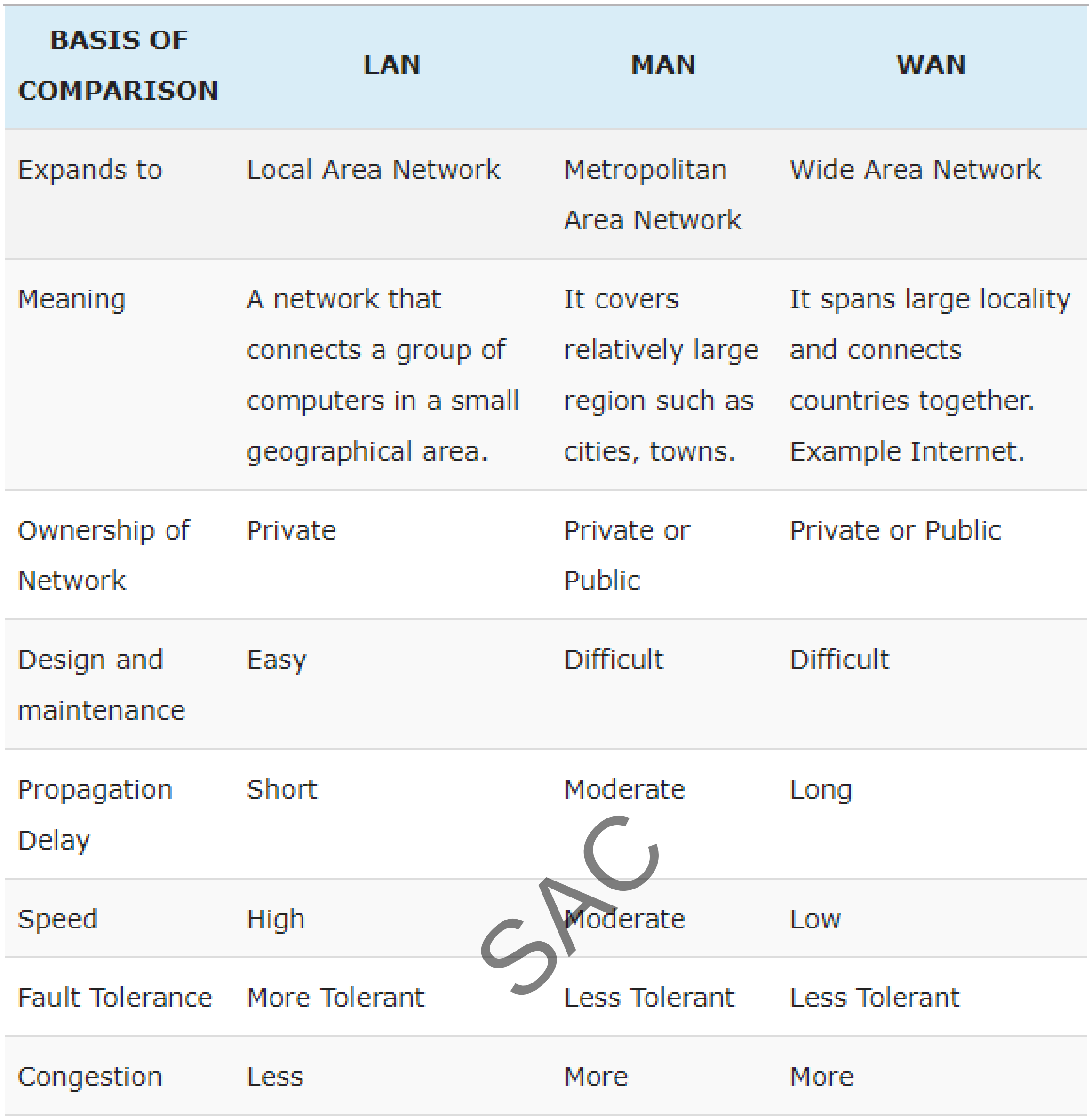
6. Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart. WAN covers a particular country. A WAN connects small network LAN & MAN.A computer user in one location can communicate with computer user in other location. It connects more than one LAN'S. It is used for large geographical area. It is active larger than 30miles.

SAC


LAN
LAN
Network Servers
Gateway Router
WAN
LAN Switch
Network Users
LAN
LAN

SAC



BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More

SAC

INTERNETWORKS

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. The fulfilment of this desire requires that different, and frequently incompatible networks, be connected, sometimes by means of machines called gateways to make the connection and provide the necessary translation, both in terms of hardware and software. A collection of interconnected networks is called an internetwork or internet. An internetwork is formed when distinct networks are interconnected. Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks is called an internetwork. The most notable example of internetworking is the internet, a network of networks based on many underlying hardware technologies, but unified by an internetworking protocol standard, the internet protocol suite, often also referred to as TCP/IP.

Network Software

The first computer networks were designed with the hardware as the main concern and the software as an afterthought. This strategy no longer works. Network software is now highly structured.

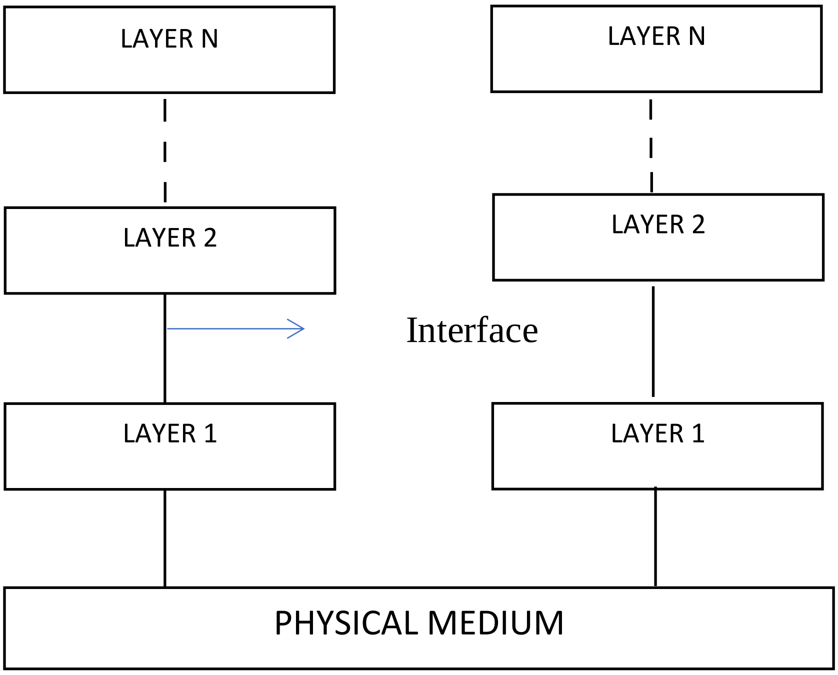
PROTOCOL

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

SAC

PROTOCOL HIERARCHIES

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. 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.



In order to understand how the actual communication is achieved between two remote hosts connected to the same network, a general network diagram is shown above divided into a series of layers. As it seen later on the on the course the actual number as well as their function of each layer differs from network to network.

SAC

Each layer passes data and control information to the layer below It. As soon as the data are collected form the next layer, some functions are performed there and the data are upgraded and passed to the next layer. This continues until the lowest layer is reached. Actual communication occurs when the information passes layer 1 and reaches the Physical medium. This is shown with the solid lines on the diagram.

Theoretically layer n on one machine maintains a conversation with the same layer in the other machine. The way this conversation is achieved is by the protocol of each layer. Protocol is collection of rules and conventions as agreement between the communication parties on how communication is to proceed. The latter is known as virtual communication and is indicated with the dotted lines on the diagram above.

Layer n of one machine carries a conversion with the layer n of another machine. The rules and conversion are collectively known as protocol. Entities comprising layers of different machine is called peer process.

The data and information is passed by each layer to the lower layer. When the lower layer is reached it is passed to the physical medium which actual communication occurs. Between the pair of adjacent layer their lies the interface. The interface defines which type of services the lower layer offers to the upper layer.

Protocols are together called ***protocol stack*** or set of protocols.

As far as the above diagram is concerned another important issue to be discussed is the interface between each layer. It defines the services and operation the lower layer offers to the one above It. When a network is built decisions are made to decide how many layers to be included and what each layer should do. So each layer performs a different function and as a result the amount of information past from layer to layer is minimized.

Design issues for a layer

- Every layer has a mechanism of connection establishment.

SAC

Since a network has many computers, some having multiple process. A machine has to specify with whom it has to establish connection. Because of having consequence of multiple destination, the addressing is needed in order to specify the specific destination.

- Another set of design decisions concerns the rules for data transfer.

In some data transfer take place in one direction and in some other it travel in both direction but not simultaneously. And there are situations were data transfer takes place simultaneously. Protocol determines how many logical channels are needed per connection.

- Error control: The physical communication circuits are not perfect. There are error detecting and error correcting codes. Both ends of the connection should agree which one is being used. The receiver must someway tell the sender which message is have been correctly received and which is not.
- Speed of sender is greater than the receiver.

There will be some kind of access from the receiver to the sender directly & indirectly about the receiver current situation.

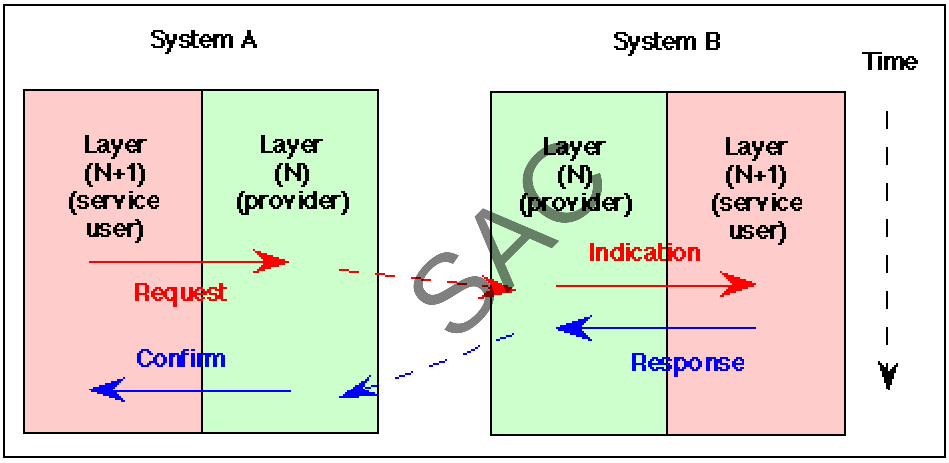
- Inability of process to accept long message.
- Very expensive to set up connection for each communication process.
- **Reliability**: It is a design issue of making a network that operates correctly even when it is made up of unreliable components.
- **Addressing:** There are multiple processes running on one machine. Every layer needs a mechanism to identify senders and receivers.
- **Error Control:** It is an important issue because physical communication circuits are not perfect. Many error detecting and error correcting codes are available. Both sending and receiving ends must agree to use any one code.
- **Flow Control** : If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers. There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on. Some process will not be in position to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting and the reassembling messages.
- **Multiplexing and De-multiplexing :** If the data has to be transmitted on transmission media separately, it is inconvenient or expensive to setup separate connection for each pair of communicating processes. So, multiplexing is needed in the physical layer at sender end and de-multiplexing is need at the receiver end.
- **Scalability :** When network gets large, new problem arises. Thus scalability is important so that network can continue to work well when it gets large.
- **Routing :** When there are multiple paths between source and destination, only one route must be chosen. This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination.
- **Confidentiality and Integrity:** Network security is the most important factor. Mechanisms that provide confidentiality defend

SAC

against threats like eavesdropping. Mechanisms for integrity prevent faulty changes to messages.

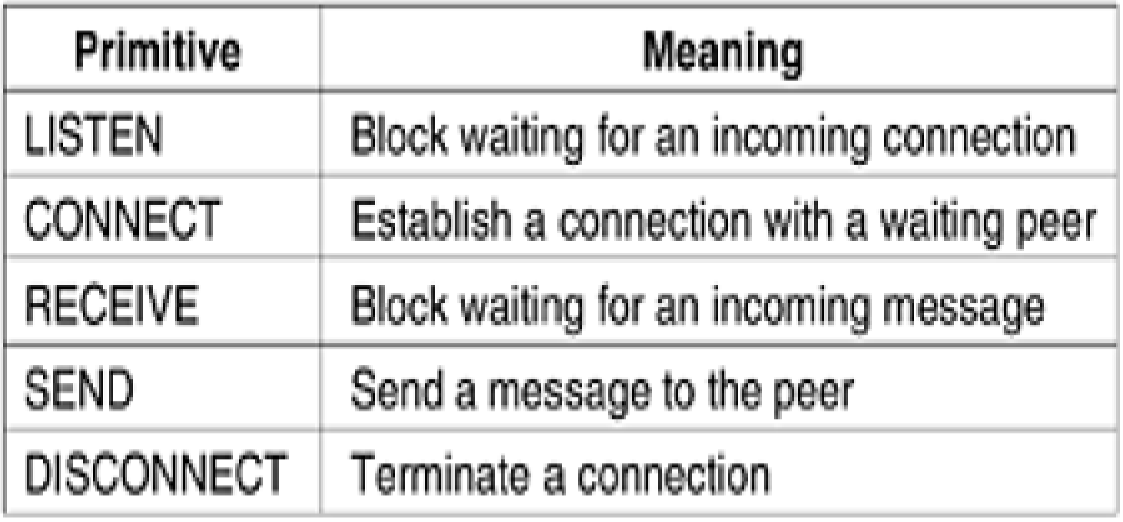
Service Primitives : Each protocol which communicates in a layered architecture communicates in a peer to peer manner with its remote protocol entity. Communication between adjacent protocol layers (i.e. within the same communications node) are managed by calling functions, called Primitives, between the layers. 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 .

- There are various types of actions that may be performed by primitives. Examples of primitives include: Connect, Data, Flow Control, and Disconnect.



SAC

Some of the services are:



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

Each primitive specifies the action to be performed or advises the result of a previously requested action. A primitive may also carry the parameters needed to perform its functions. One parameter is the packet to be sent/received to the layer above/below (or, more accurately, includes a pointer to data structures containing a packet, often called a "buffer").

There are four types of primitive used for communicating data. The four basic types of primitive are :

Request : A primitive sent by layer (N + 1) to layer N to request a service. It invokes the service and passes any required parameters.

Indication : A primitive returned to layer (N + l) from layer N to advise of activation of a requested service or of an action initiated by the layer N service.

Response : A primitive provided by layer (N + 1) in reply to an indication primitive. It may acknowledge or complete an action previously invoked by an indication primitive.

Confirm : A primitive returned to the requesting (N + l)st layer by the Nth layer to acknowledge or complete an action previously invoked by a request primitive.

To send Data, the sender invokes a Data. Request specifying the packet to be sent, and the Service Access Point (SAP) of the layer below. At the receiver, a Data. Indication primitive is passed up to the corresponding layer, presenting the received packet to the peer protocol entity.

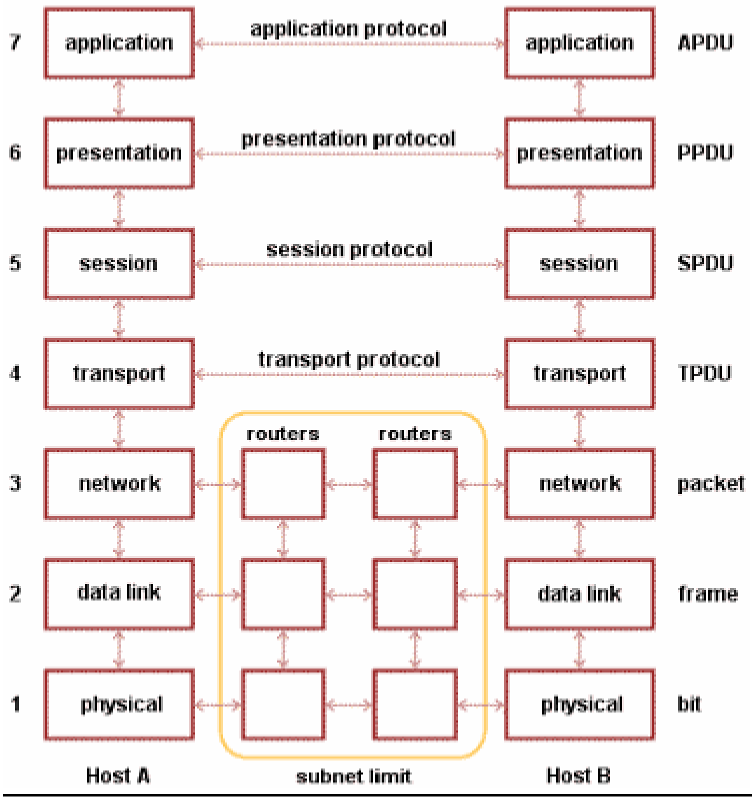
SAC

REFERENCE MODELS

1. OSI MODEL 2. TCP/IP MODEL

OSI REFERENCE MODEL

OSI stands for Open Systems Interconnection. It has 7-layers and attempts to abstract common features common to all approaches to data communications, and organize them into layers so that each layer only worries about the one above it and the one directly below it.



Although the actual data transmission is vertical, starting from the Application layer of the clients' computer all the way to the Application layer of the destination computer, each layer is programmed as though the data transmission were horizontal. This can be observed by above figure. In this figure peers are entities comprising the corresponding layers on each machine meaning that the peers that communicate using the protocol. In reality, as I stated above, no data are directly transferred from layer n on one machine to the corresponding layer on another machine.

SAC

Physical Layer

The physical layer has as a main function to transmit bits over a communication channel as well as to establish and terminate a connection to a communications medium. It is also responsible to make sure that when one side sends a '1' bit the other side will receive '1' bit and not '0' bit. The physical layer is combination of 1s and 0s.it is concerned with transmitting raw bits over a communication channel. Voltage needs for transfer.

Data Link Layer

Data link layer provides means to transfer data between network entities. At the source machine it takes the bit streams of data from the

Network Layer breaks into frames and passes them to the physical layer. At the receiving end data link layer detects and possibly corrects the errors that may occur during the transmission and passes the correct stream to the network layer. It's also concerned with flow control techniques. It controls the flow of transmission, and error detection. That is the main task of this layer is to take raw transmission facility and transform it into a line that appears free of transmission errors to the network layer. It accomplishes the task by having the sender break the input data up into data frames, transmit the data sequentially and process the acknowledgement frames sent back to the receiver. The data link layer creates and recognize the frame boundaries. This can be accomplished by attaching special bit patterns at the beginning and end of the frame.

Network Layer

This layer performs network routing, flow control and error control functions. Network routing simply means the way packets are routed from source to destination and flow control. prevents the possibility of congestion between packets which are present in the subnet simultaneously and form bottlenecks. The main task of this layer is to decide the path from multiple paths. That is the key design issue is determining how packets are routed from source to destination. They are highly dynamic.

SAC

If too many packets are present in a subnet at the same time they will get in each other’s way forming bottlenecks. The control of such congestion also belongs to this layer. When a packet has to travel from one network layer to its destination, many problems may arise. The addressing used by the second network may be different from the first one. The second packet may not accept the packet because it is too large. The protocols may differ. It is up to the network layer to overcome all these problems to allow heterogenous networks interconnected.

Transport Layer

The Transport Layer has as a main task to accept data from the Session layer, split them up into smaller units an passes them to the Network layer making sure that all the pieces arrive correctly to the destination. It is the first end-to-end layer all the way from source machine to destination machine unlike the first three layers which are chained having their protocols between each machine. This is shown clearly in the diagram above. This layer will ensure that the data reached to receiver without any error. And the basic function of this layer is to accept data from the session layer, split it up to smaller units if need be, pass to the network layer and ensure that all pieces arrive correctly at the other end. Also the transport layer creates a distinct network connections for each transport connection required by the session layer. If the transport connection requires high throughput the transport layer might create multiple network connections dividing the data among the network connections to improve throughput. Transport layer might multiplex several transport connections on to the same network connection in order to reduce the cost.

Session Layer

Session layer is responsible for controlling exchange information and for synchronization. This layer is for creating a session dialog control and which allows the user on different machines to establish sessions between them. session layer has the total management f synchronization .also allow a user to log into a time sharing system.one of the services of the session layer is to manage the dialogue box.

SAC

Presentation Layer

It is responsible to translate different data formats from the representation used inside the computer (ASCII) to the network standard representation and back. Computers use different codes for representing character strings so a standard encoding must be used and is handled by the presentation layer. Generally, in a few words this layer is concerned with the syntax and semantics of the information transmitted. The presentation layer performs encapsulation, description, compression and decompression. Also certain functions that are requested sufficiently often to warrant finding a general solution for them. The presentation layer is also concerned with the syntax and semantics of the information transmitted.

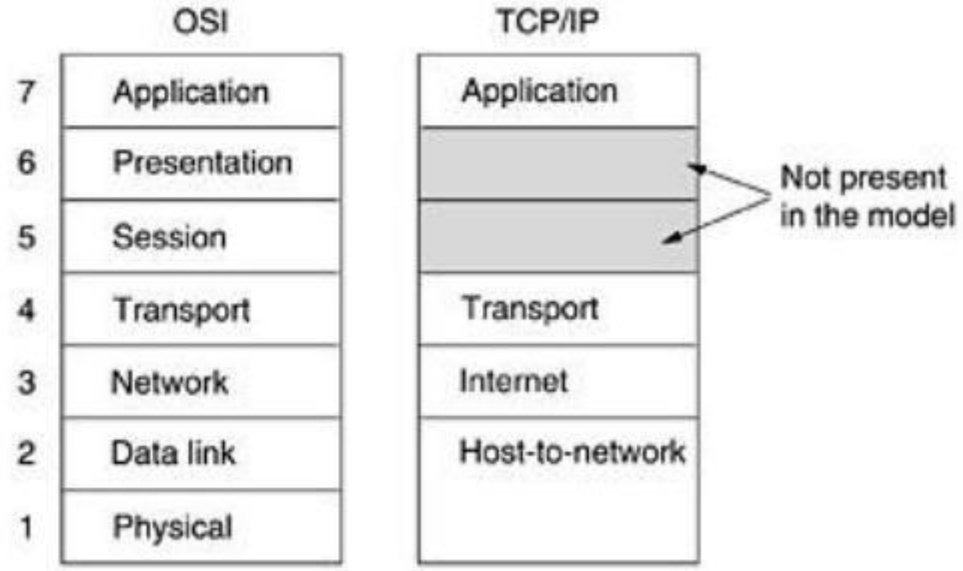
Application layer

The upper layer of this model performs common application service for the application processes meaning that software programs are written in the application layer to handle the many different terminal types that exist and map the virtual terminal software onto the real terminal. It contains a variety of protocols and is concerned with file transfer as well as electronic mail, remote job entry and various other services of general interest. This layer has a particular application. It contains a variety of protocols that are commonly needed. Another application of this layer is file transfer. Different file system has different file naming conventions, different ways of representing text lines and on.

TCP/IP REFERENCE MODEL

TCP/IP reference model was named after its two main protocols: TCP (Transmission Control Protocol) and IP (Internet Protocol). This model has the ability to connect multiple networks together in a way so that data transferred from a program in one computer are delivered safely to a similar program on another computer.

SAC



Host-to-Network Layer

It translates data and addresses information into format appropriate for an Ethernet Network or Token Ring Network. It uses a protocol (not specified due to lack of information concerned with this layer) in order for the host to connect to the network. Through this layer communication is achieved with physical links such as twisted pair or fibre optics carrying 1's and 0's. The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

Internet Layer

This layer is a connectionless internetwork layer and defines a connectionless protocol called IP. Its concerned with delivering packets from source to destination. These packets travel independently each taking a different route so may arrive in a different order than they were send. Internet layer does not care about the order the packets arrive at the destination as this job belongs to higher layers. This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer. Fig. shows this correspondence.

SAC

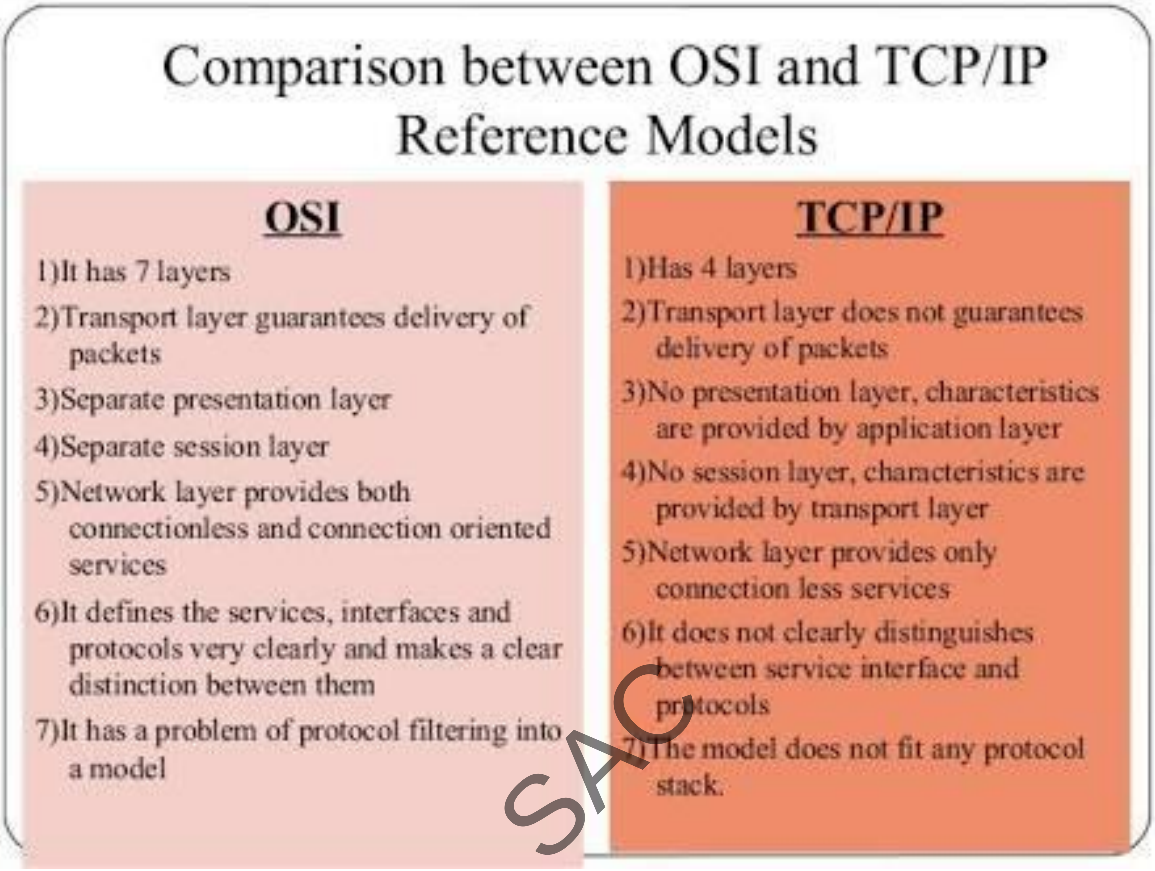
Transport Layer

It contains two end-to-end protocols. TCP is a connection-oriented protocol and is responsible for keeping track of the order in which packets are sent and reassemble arriving packets in the correct order. It also ensures that a byte stream originating on one machine to be delivered without error on any other machine on the internet. The incoming byte stream is fragmented into discrete messages and is passed to the internet layer. With an inverse process, at the destination, an output stream is produced by reassembling the received massage. UDP is the second protocol in this layer and it stands for User Datagram Protocol. In contrast to TCP, UDP is a connectionless protocol used for applications operating on its own flow control independently from TCP. It is also an unreliable protocol and is widely used for applications where prompt delivery is more important than accurate delivery. such as transmitting speech or video. The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It fragments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control 26 to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

SAC

Application Layer

It is the upper layer of the model and contains different kinds of protocols used for many applications It includes virtual terminal TELNET for remote accessing on a distance machine, File Transfer Protocol FTP and e-mail (SMTP). It also contains protocols like HTTP for fetching pages on the www and others. The TCP/IP model does not have session or presentation layers. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig.6.2. The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.



Comparison between OSI and TCP/IP Reference Models

OSI	TCP/IP
1)It has 7 layers	1)Has 4 layers
2)Transport layer guarantees delivery of packets	2)Transport layer does not guarantees delivery of packets
3)Separate presentation layer	3)No presentation layer, characteristics are provided by application layer
4)Separate session layer	4)No session layer, characteristics are provided by transport layer
5)Network layer provides both connectionless and connection oriented services	5)Network layer provides only connection less services
6)It defines the services, interfaces and protocols very clearly and makes a clear distinction between them	6)It does not clearly distinguishes between service interface and protocols
7)It has a problem of protocol filtering into a model	7)The model does not fit any protocol stack.

SAC