COMPUTER NETWORKS

Unit – I

Computer Network means the **interconnection** of a set of **autonomous computers**. The term autonomous means that the function of computers is independent of others. However, these computers can exchange information with each other through the communication channels like copper wire, fiber optics, microwaves, infrared, and communication satellites can also be used.

Components:

The five components that make up a data communication are the message, sender, receiver, medium, and protocol.

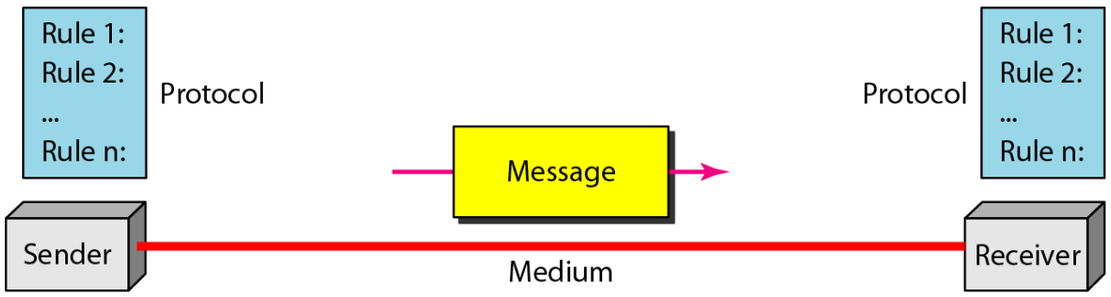
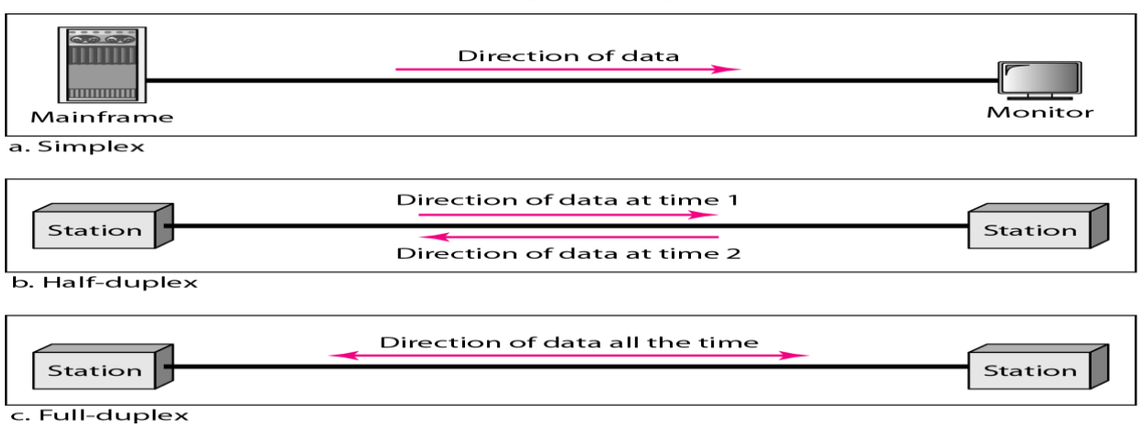


Figure 1.1 Five *components of data communication*

1. **Message:** The message is the information (data) to be communicated. The Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender**: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver:** The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium.** The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. **Protocol.** A protocol is a set of rules that maintain data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just like a person speaking French cannot be understood by a person who speaks only Japanese.

Data Flow:

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in following figure.



Simplex :

In simplex mode, the communication is unidirectional, as on a one-way road. Only one of the two devices on a link can transmit; the other can only receive (see Figure a).

Keyboards and traditional monitors are examples of simplex devices. The keyboard can only give input; the monitor can only accept output. The simplex mode can use the entire capacity of the communication channel to send data in one direction only

Half-Duplex :

In half-duplex mode, each system can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Figure b).

The half-duplex mode is like a one-lane street with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. **Walkie-talkies** are half-duplex system.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.

Full-Duplex :

In full-duplex mode (also called duplex), both systems can transmit and receive simultaneously (see Figure c).

The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is **the telephone network**. When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.

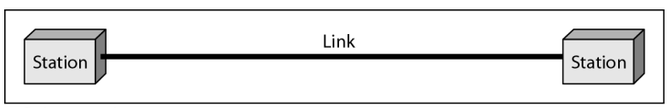
NETWORKS:

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

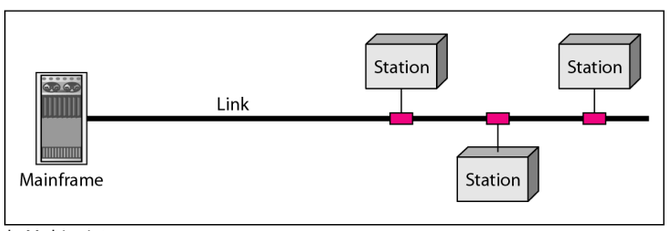
Physical Structures

Type of Connection:

There are two possible types of connections: **point-to-point and multipoint**.



a. Point-to-point



b. Multipoint

Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, (see Figure a). When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

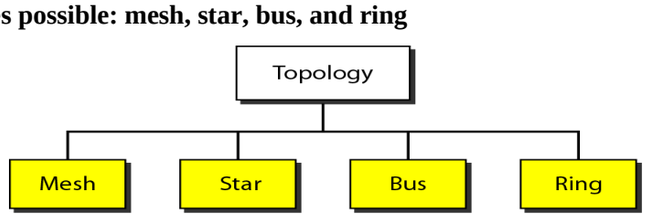
Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link (see Figure b).

In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a ***spatially*** *shared* connection. If users must take turns, it is a ***timeshared*** connection.

Topology:

The term ***topology*** refers to the way in which **a network is laid out physically: two or more devices connect to a link; two or more links form a topology**. The **topology** of a network is the **geometric representation of the relationship of all the links and linking devices** (usually called nodes) to one another.

There are **four basic topologies possible: mesh, star, bus, and ring**



Mesh topology : In a mesh topology, every device has a dedicated **point-to-point link** to every other device. The term *dedicated* means that the link carries data only between the two devices it connects.

One practical example of a mesh topology is the connection of **telephone regional offices** in which each regional office needs to be connected to every other regional office.

To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - 1 nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to n-1 nodes. However each physical link allows communication in both directions (duplex mode).

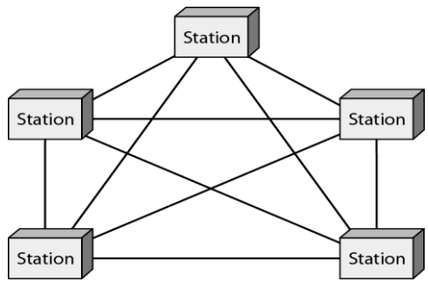


Figure: ***A fully connected mesh topology (five devices)***

Advantages of mesh topology:

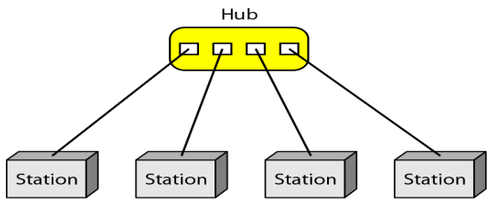
- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not fail the entire system
- There is the advantage of privacy or security. When every message travels along a dedicated line, only the specific recipient sees it. Dedicated links prevent other users from accessing the messages.
- Finally, point-to-point links make fault identification and fault correction easy.

Disadvantages of mesh topology:

- The amount of cabling and the number of I/O ports required are high.
- Every device must be connected to every other device, installation and reconnection are difficult.
- The bulk wiring can be greater than the available space (in walls, ceilings, or floors).
- The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star Topology: In a star topology, each device has a dedicated **point-to-point link** only to a central controller, usually called a **hub**. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then transfers the data to the other connected device.

The star topology is used in **local-area networks (LANs)**,



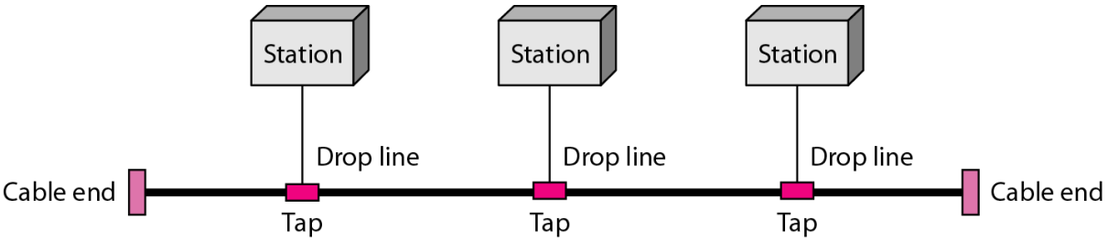
Advantages of star topology

- A star topology is less expensive than a mesh topology
- In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- less cabling needs to be housed
- Any additions, moves, and deletions involve only one connection: between that device and the hub.
- If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault correction.

Disadvantages of star topology

- Star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Bus Topology: A **bus topology** is multipoint. One long cable acts as a **backbone** to link all the devices in a network



Nodes are connected to the bus cable by **drop lines** and **taps**. A **drop line is a connection running between the device and the main cable**. A **tap** is a **connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core**. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Bus topology was the one of the first topologies used in the design of early **local area networks**. Ethernet LANs can use a bus topology, but they are less popular now

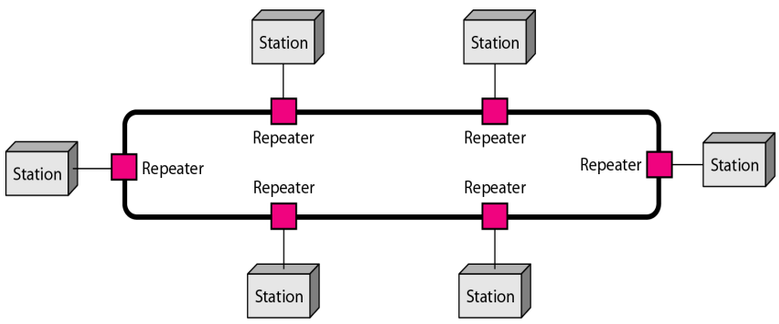
Advantages of bus topology

- ease of installation
- In a bus, this redundancy is eliminated.

Disadvantages of bus topology

- difficult reconnection and fault isolation
- A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- A fault or break in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

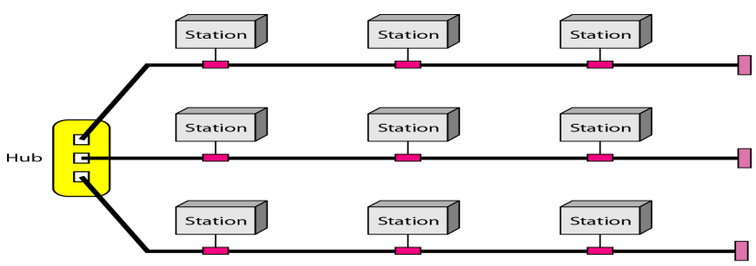
Ring Topology: In a ring topology, each device has a dedicated **point-to-point** connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. **Each device in the ring incorporates a repeater**. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages of ring topology:

- easy to install and reconfigure
- Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections

Hybrid Topology: A network can be hybrid. For example, we can have a main star topology
with each branch connecting several stations in a bus topology as shown in Figure

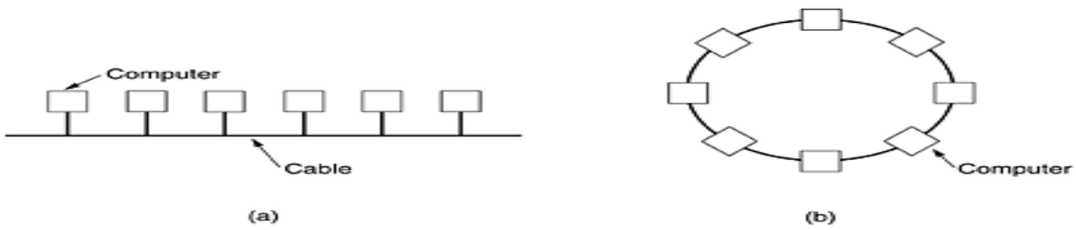


Network Models

There are 3-types of network models they are **Local-area networks**, **Metropolitan area networks** and **wide-area networks**. The type of a network is determined by its size.

Local Area Network

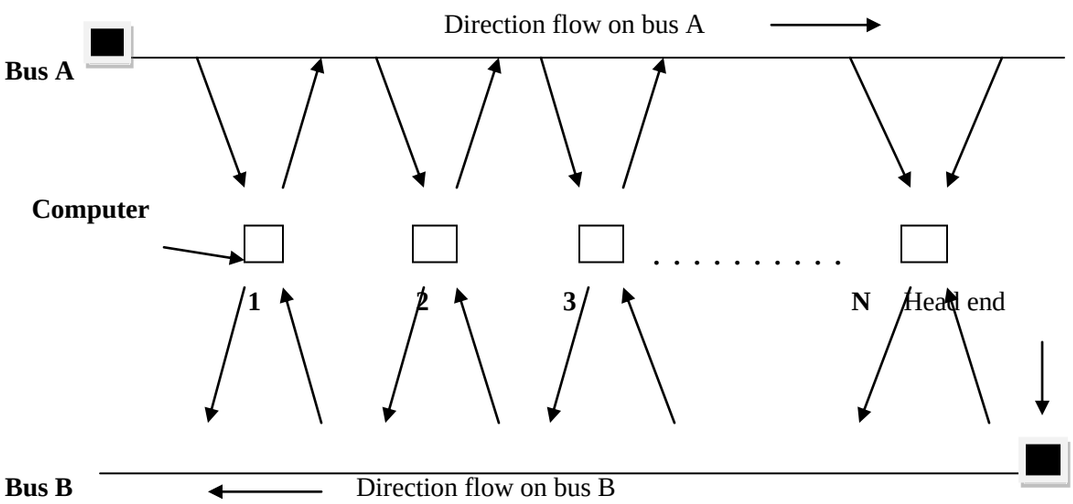
- A local area network is generally called as LANs; these are privately-owned networks with in a single building single or campus of up to a few kilometers in size.
- LANs are widely used to connect personal computers and work stations in company offices and factories to share resources like printers, and to exchange information.
- LANs are different from other networks by three characteristics (1).With their size, (2). With their transmission technology. (3).their topology.
- Currently, LAN size is limited to a few kilometers.
- LANs use a transmission Technology consisting of a single cable to which all the systems are attached, like a telephone lines.
- LANs run at a speed of 10 to 100 Mbps (mega bits/sec), having a low delay and make very few error



- Various Topologies are used for broadcasting the LANs. **The most common LAN topologies are bus, ring, and star**.
- Here it uses IEEE 802.3 popularly known as Ethernet, and IEEE 802.5 IBM Token ring

Metropolitan Area Networks

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally uses similar technology of LAN and covers the area inside a town or a city.
- Here we are using IEEE 802.6 known as DQDB(distributed queue dual bus) which contains to unidirectional buses to which all the computers are connected.
- Both the buses contain Head-End which initiates the transmission. The traffic of right side of the sender uses upper bus. And to send left side uses lower one.
- It is designed for customers who need a high-speed connectivity.

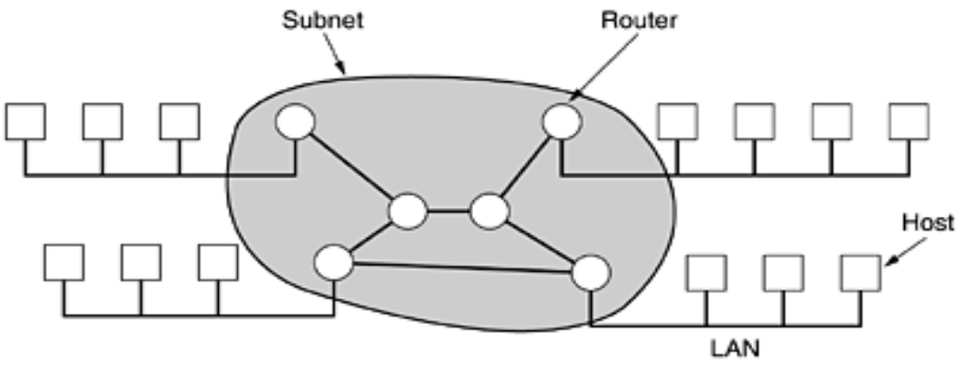


Wide Area Network

WAN provides long-distance transmission of data, voice, image and information over large geographical areas that may comprise a country, continent or even the whole world. In WANs systems are connected by a communication subnet or subnet. The job of the subnet is to carry messages from system to the system, just like a telephone which carries words from speaker to speaker

In most wide area networks the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines are also called as circuits, channels or trunks move bits between machines.

The switching elements are specialized computers used to connect two or more transmission lines connecting multiple networks known as routers.



A subnet is a point-to-point, store and forward or packet-switched subnet. Nearly all subnets are **S**tore and **F**orward subnets. Some of the possible topologies for a Point-to-Point subnets are Star, Ring, Tree, etc.

Another possibility of WAN is a satellite, where Each router has an antenna which can send and receive.

THE OSI MODEL

The OSI model is based on the proposal developed by International Standards Organization (ISO) this model is called as ISO-OSI (Open Systems Interconnection) Reference Model because it is used for connecting the open systems. That is the systems which are open for communication with other systems.

It was a first step towards the International standardization of the protocols used in various layers by Day and Zimmermann in 1983.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of **seven** separate but related layers, each of which defines a part of the process of moving information across a network.

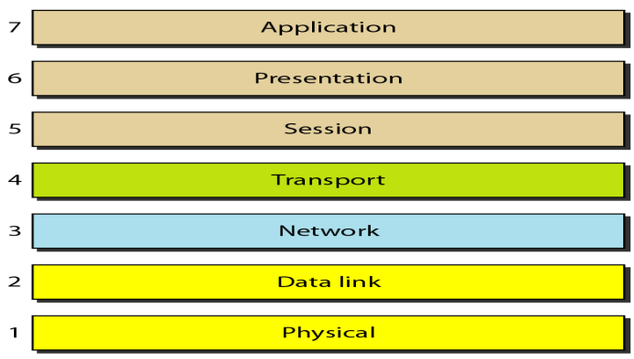


Figure: ***Seven layers of the OSI model***

The Following Figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

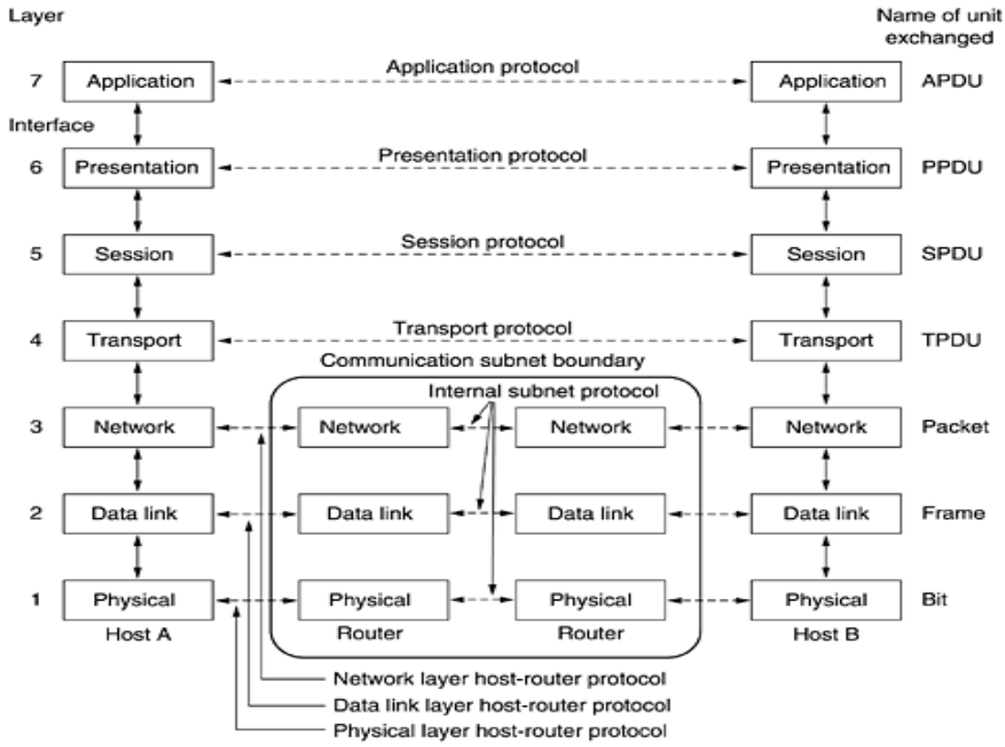


Figure: ***The OSI reference model***

The seven layers of the OSI model are divided into **three subgroups**.

Layers 1, 2, and 3-physical, data link, and network layers are known as **network support layers;** Because they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability**).**

Layers 5, 6, and 7-session, presentation, and application layers are known as **the user support layers**; they allow interoperability among unrelated software systems.

Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

LAYERS IN THE OSI MODEL : Physical Layer :

The physical layer is used for transmitting the raw bits over a communication channel. Here if the system at one side sends 1bit, it is received by the other side also as a 1bit, not as a 0 bit. The functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.

Following figure shows the position of the physical layer with respect to the transmission medium and the data link layer.

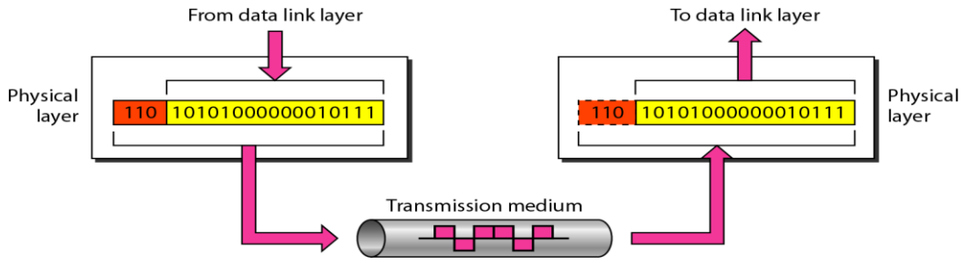


Figure: *Physical layer*

The physical layer is also concerned with the following:

- **Representation of bits:** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical.
- **Data rate:** It represents that how many number of bits can be transferred in each second is also defined by the physical layer.
- **Synchronization of bits:**The sender and receiver both must have to use the same bit rate but also must be synchronized at the bit level.

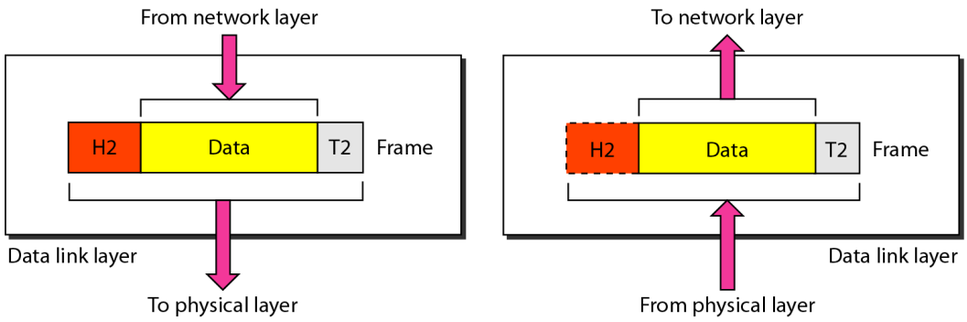
- **Line configuration:** The physical layer is concerned with the connection of devices to the media. In a **point-to-point** configuration, two devices are connected through a **dedicated link**. In a **multipoint** configuration, a link is **shared** among several devices.
- **Physical topology**: The physical topology defines how devices are connected to make a network. Ex: mesh topology, a star topology, a ring topology, a bus topology, a hybrid topology.
- **Transmission mode**: The physical layer also defines the direction of transmission

between the two devices as Simplex, Half-duplex, and Full-duplex.

Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear as an error-free to the upper layer (network layer).

Following Figure shows the relationship of the data link layer to the network and physical layers.



- **Framing:** The data link layer divides the stream of bits received from the network layer into data units called frames.
- **Physical addressing**. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control:** If the rate at which the data is absorbed by the receiver is less than the rate at which data is transferred by thesender, the data link layer uses a flow control protocols to maintain same data transfer rate between sender and the receiver
- **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and correct the damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
  - **Access control**: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has to send the data at any given time. Otherwise there is a chance of collision. For this purpose a special sub layer in the data link layer known as medium access sub layer will deal this one.

Network Layer:

The network layer is responsible for the delivery of a packet from source to destination, possibly across multiple networks. The network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is no need for a network layer. However, if the two systems are attached to different networks with connecting devices between the networks, there is often a need for the network layer to maintain source-to-destination delivery.

Following Figure shows the relationship of the network layer to the data link and transport layers.

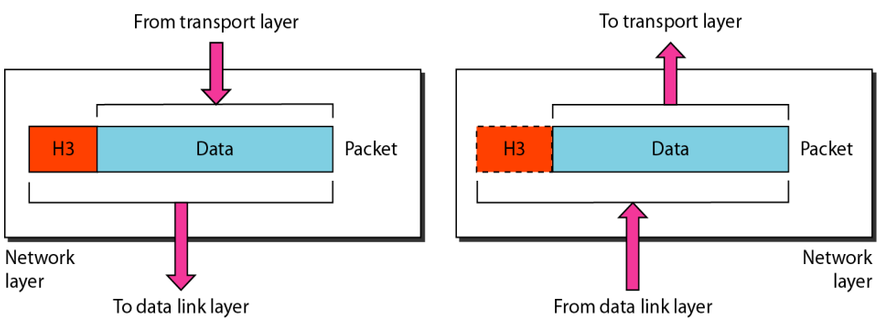


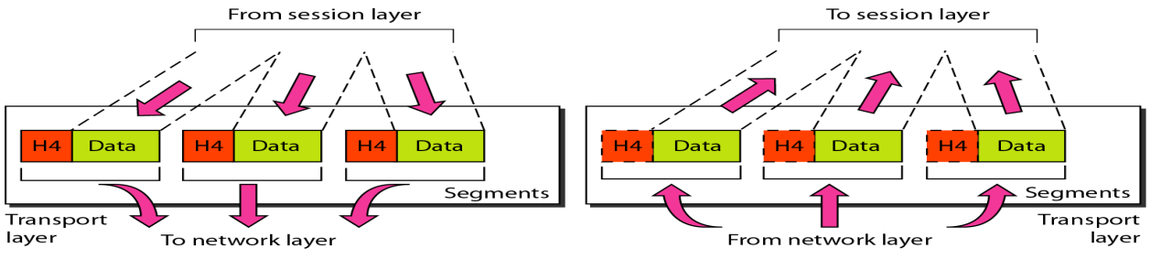
Figure: ***Network layer***

Other responsibilities of the network layer include the following:

- **Logical addressing:** The physical addressing implemented by the data link layer handles the addressing problem locally. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.
- **Routing:** When independent networks or links are connected to create internetworks(network of networks) or a large network, the connecting devices (called *routers or switches)* route or switch the packets to their final destination.
- **Congestion Control:** If there is traffic in one way of network for transferring the data. It is known as Congestion, Here we have to find another path for transferring the data by the use of congestion control protocols

Transport Layer:

- The transport layer is responsible **for process-to-process delivery of the entire message**.
- A process is an application program running on a host.
- Whereas the network layer maintainsource-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Following Figure shows the relationship of the transport layer to the network and session layers.



Transport layer

Other responsibilities of the transport layer include the following:

- **Service-point addressing:** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.
- **Segmentation and reassembly:** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- **Connection control:** The transport layer can be either connectionless or connection oriented. A **connectionless** transport layer treats **each segment as an independent packet** and delivers it to the transport layer at the destination machine. **A connection oriented** transport **layer makes a connection with the transport layer at the destination machine first before delivering the packets**. After all the data are transferred, the connection is terminated.
- **Flow control:** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- **Error control:** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

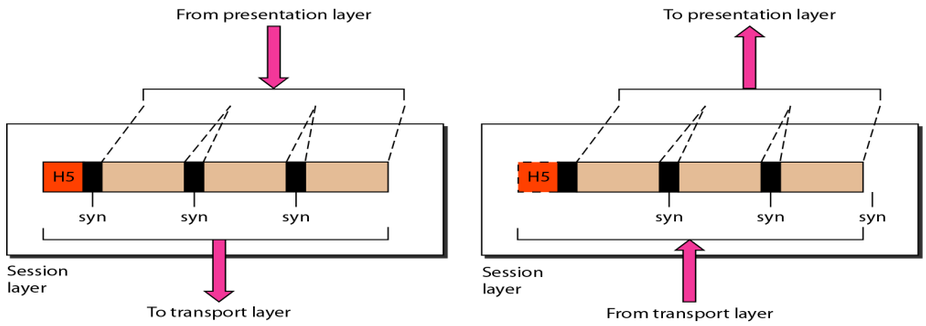
Session Layer:

Session layer allows users on different machines to establish the Sessions , maintain the sessions and synchronize the sessions.

The session layer is responsible for dialog control.

Specific responsibilities of the session layer include the following:

- **Dialog control**: one of the services of the session layer is to manage dialogue control. Sessions allow traffic in one direction or both the directions at the same time. In a network we are having many numbers of systems. If more than one system want to perform the operation, on that case which system will have the priority is the service provided by session layer, it is known as token management
- **Synchronization:** The session layer allows a concept of checkpoints, that if we are transferring a file which may take 2hours between two machines. After the completion of 1 hour if the system crashes, automatically already transferred data will be lost. For that purpose such a huge data will be divided into checkpoints.
- Following Figure illustrates the relationship of the session layer to the transport and presentation layers.



Session layer

Presentation Layer:

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- Following Figure shows the relationship between the presentation layer and the application and session layers.

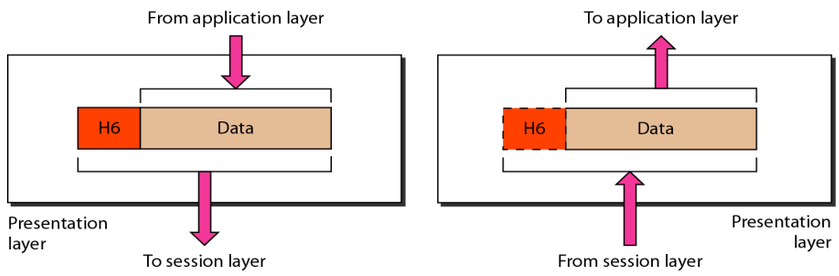


Figure: *Presentation layer*

Specific responsibilities of the presentation layer include the following:

- The presentation layer is responsible for translation, compression, and encryption.
- **Translation:** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.
- **Encryption:** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- **Compression:** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer:

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- The application layer is responsible for providing services to the user.

  Following Figure shows the relationship of the application layer to the user and the presentation layer..

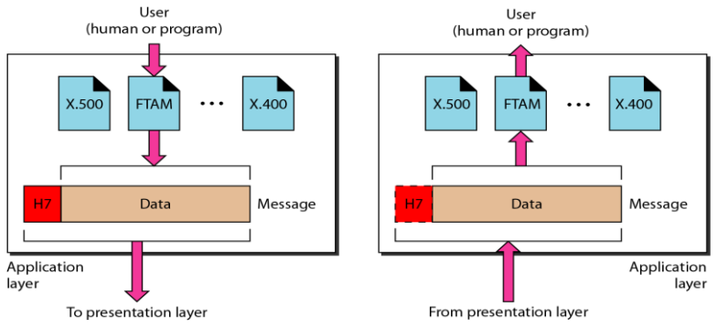
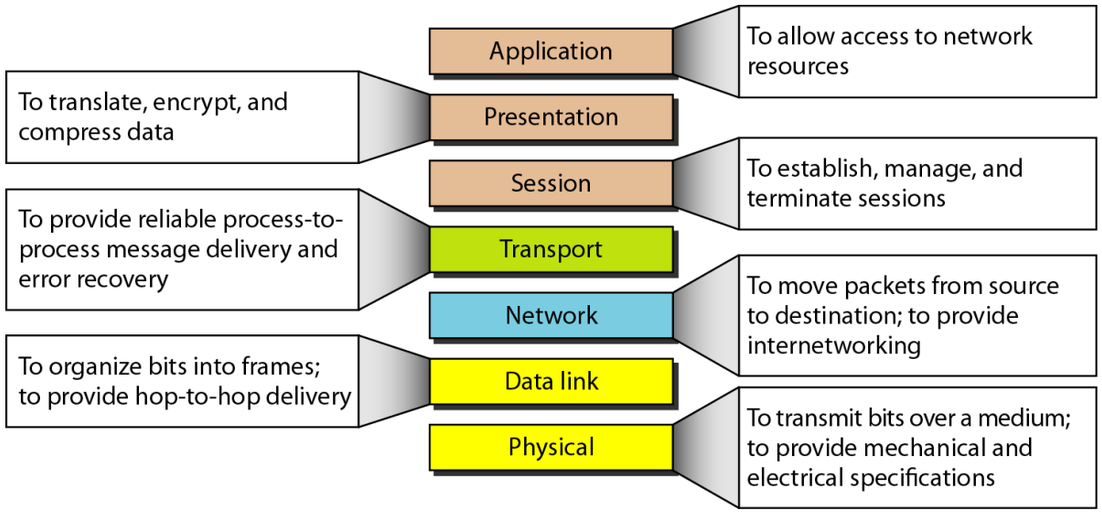


Figure: *Application layer*

Specific services provided by the application layer include the following:

- **Network virtual terminal**. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management**. This application allows a user to access files in a remote host to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services**. This application provides the basis for e-mail forwarding and storage.
- **Directory services**. This application provides distributed database sources and access for global information about various objects and services.

Summary of Layers:

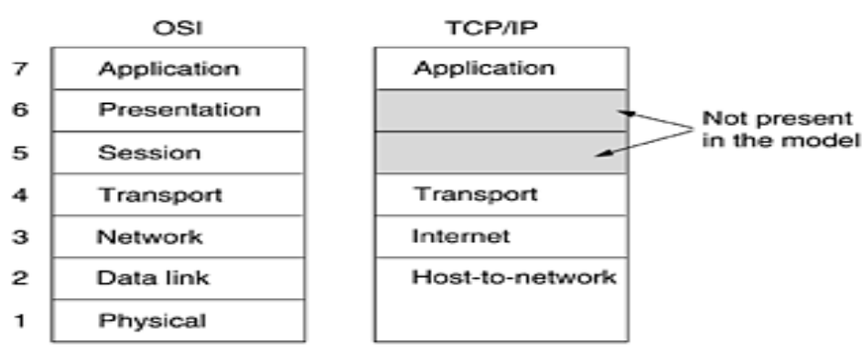


The TCP/IP Reference Model :

Let us now turn from the OSI reference model to the reference model used in the grandparent of all wide area computer networks,

The ARPANET, and its successor, the world wide Internet. It is useful to mention a few key aspects of it now. The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundreds of universities and government installations, using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so a new reference architecture was needed. This architecture later became known as the **TCP/IP Reference Model**, after its two primary protocols.

The TCP/IP reference model



The Internet Layer:

All these requirements led to the choice of a packet-switching network based on a connectionless internetwork layer. This layer, called the **internet layer**, Its job is to permit hosts to inject packets into any network and have them travel independently to the destination 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.

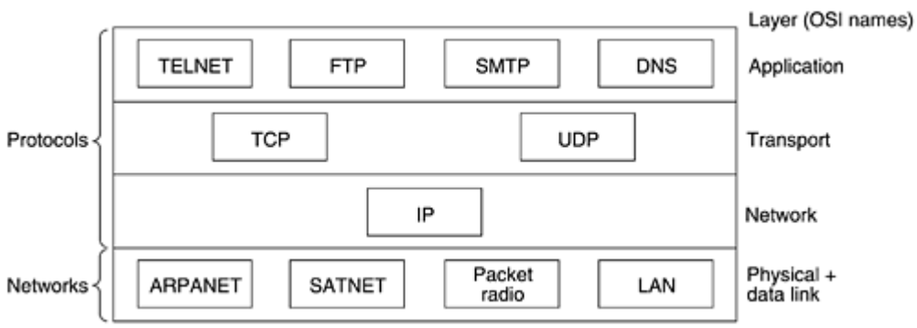
The Transport Layer:

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 to make sure a fast sender cannot transfer data accurately to a slow receiver with more messages than it can handle.

The second protocol in this layer, **UDP** (**User Datagram Protocol**), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely 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.

Stream Control Transmission Protocol (SCTP): The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

TCP/IP PROTOCOL SUITE:



- The TCP/IP protocol suite was developed prior to the OSI model.
- The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having **four** layers: **host-to-network, internet, transport, and application**
- However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers.
- The internet layer is equivalent to the network layer
- The application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.
- we assume that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport

functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the *application layer*

- *TCP/IP* is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

  At the transport layer, *TCP/IP* defines three protocols: **Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP)**. At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

The Application Layer:

The TCP/IP model does not have session and presentation layers. No need for them was perceived, so they were not included. Experience with the OSI model has proven that they are of little use to most applications.

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). 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. HTTP, The protocol for fetching pages on the World Wide Web.

The Host-to-Network Layer:

Below the internet layer is a great void. 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.

A Comparison of the OSI and TCP/IP Reference Models:

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar. For example, in both models the layers up through and including the transport layer are there to provide an end-to-end, network-independent transport service to processes wishing to communicate. These layers form the transport provider. Again in both models, the layers above transport are application-oriented layers, provide users a transport service.

Despite these fundamental similarities, the two models also have many differences. In this section we will focus on the key differences between the two reference models. It is important to note that we are comparing the *reference models* here, not the corresponding *protocol stacks*. Three concepts are central to the OSI model:

1. Services.
2. Interfaces.
3. Protocols.

Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicitly. Each layer performs some services for the layer above it. The *service* definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer's semantics.

A layer's *interface* tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, too, says nothing about how the layer works inside.

Finally, the peer *protocols* used in a layer are the layer's own business. It can use any protocols it wants to, as long as it gets the job done (i.e., provides the offered services). It can also change them at will without affecting software in higher layers.

These ideas fit very nicely with modern ideas about object-oriented programming.

The TCP/IP model did not originally clearly distinguish between service, interface, and protocol, although people have tried to retrofit it after the fact to make it more OSI-like. For example, the only real services offered by the internet layer are SEND IP PACKET and RECEIVE IP PACKET.

EXAMPLE NETWORKS:

NOVELL NETWARE: The most popular network system in the pc world is **Novell Netware.** It was designed when the companies are using the network of PCs than the main frame. In the network of PCs each user has a desktop PC

functioning as a client, and some other systems works as servers, providing file services, database services. Novell Netware is based on a client server model.

Novell Netware is like an OSI, but is not based on it. It looks like a TCP/IP than the OSI Reference Model.

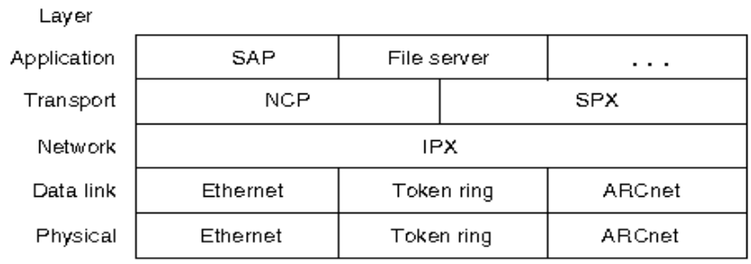


Fig 1: The Novell NetWare reference model.

The physical and data link layers can be chosen from among various industrial standards like Ethernet, IBM Token ring and ARCnet. The network layer runs an unreliable connectionless internetwork protocol known as IPX (Internet Packet Exchange). It passes packets transparently from source to destination, even if the source and destination are on different networks. IPX is functionally similar to IP, except that it uses 12-byte addresses instead of 4-byte addresses.

Above to the IPX comes a connection-oriented transport protocol called NCP (Network Core Protocol) it also provides various services like data transport. It is also known as a heart of Netware. A second protocol.SPX (sequenced Packet Exchange) is also available, it provides only transport.

The session and the presentation layers doesn't exist here, various application protocols are present in the application layer. Application layer contains a SAP (service advertising protocol). The packets are seen and collected by a special agent processes running on the router machines.

The format of an IPX packet is shown in the below fig. The *checksum* field is rarely used, since the below data link layer also provides a checksum. The packet length field tells tha actual length of the entire packet is header plus data. The transport control field counts that how many networks the packet has transferred. When this count exceeds a maximum value, then the packet is discarded. The packet type field is used to specify type of various packets.

The two addresses which contain 12 byte addresses each contain 32-bit network number, a 48-bit machine number and a 16-bit local address on that machine.

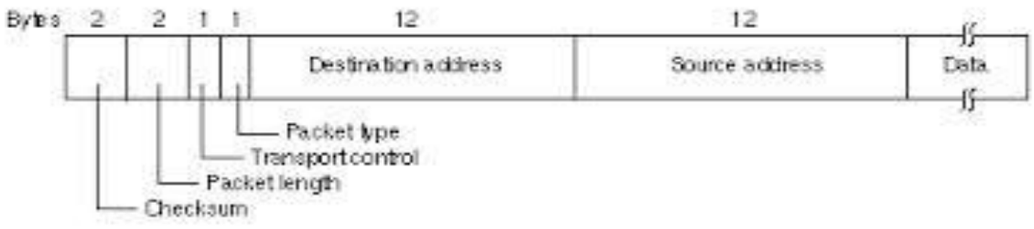


Fig. 2: A Novell NetWare IPX packet.

The ARPANET: ARPA (Advanced Research Projects Agency).ARPA was created in response to the Soviet Union's launching "Sputnik" with a mission of advanced technology. Some universities got the idea of packet switching, which was suggested by Paul Baran. After some discussions ARPA decided to build a packet switching network, consisting of a subnet and host computers

The subnet would consist of minicomputers called **IMP**s (**Interface Message Processors**) connected by 56-kbps transmission lines. For high reliability, each IMP would be connected to at least two other IMPs. The subnet was to be a datagram subnet, so if some lines and IMPs were destroyed, messages could be automatically rerouted along alternative paths.

Each node of the network consists of an IMP and a host;A host could send messages of up to 8063 bits to its IMP, then IMP break these into packets of at most 1008 bits and forward them independently toward the destination. So the subnet was the first electronic store-and-forward packet-switching network.

ARPA then put out a tender for building the subnet. Twelve companies bid for it. After evaluating all the proposals, ARPA selected BBN, and awarded it a contract to build the subnet and write the subnet software. BBN chose to use specially modified Honeywell DDP-316 minicomputers with 12K 16-bit words of core memory as the IMPs. The IMPs did not have disks, The IMPs were interconnected by 56-kbps lines leased from telephone companies.

The software was split into two parts: subnet and host. The subnet software consisted of the IMP end to the host-IMP connection, the IMP-IMP protocol, and a source IMP to destination IMP protocol designed to improve reliability. The original ARPANET design is shown in below figure.

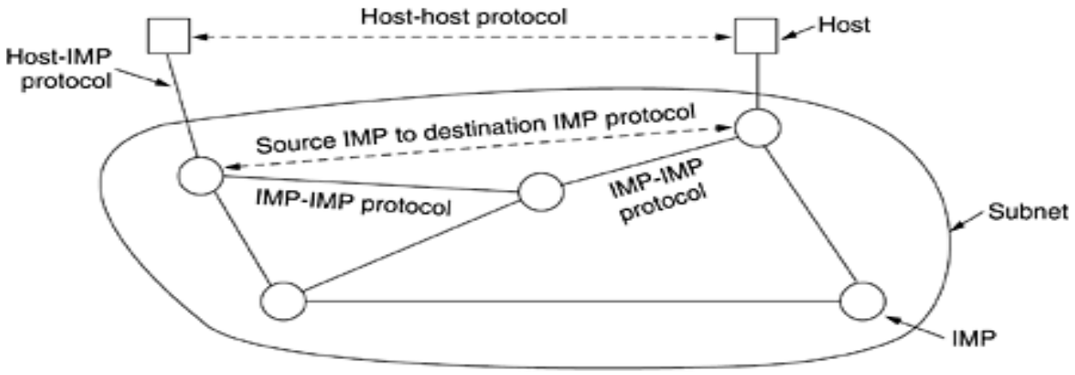


Fig 3: The original ARPANET design

NSFNET: NSF (the U.S. National Science Foundation) saw the enormous impact that the ARPANET was having on university research, allowing scientists across the country to share data and collaborate on research projects. This lack of universal access prompted NSF to set up a virtual network,

CSNET, Centered around a single machine at BBN that supported dial-up lines and had connections to the ARPANET and other networks. NSF decided to build a backbone network to connect its six supercomputer centers,

Each supercomputer was given a little brother, consisting of an LSI-11 microcomputer called a **fuzzball**. The fuzzballs were connected with 56-kbps leased lines and formed the subnet, the same hardware technology as the ARPANET used. The software technology was different however: the fuzzballs spoke TCP/IP right from the start, making it as a first TCP/IP WAN.

NSF also funded some 20 regional networks that connected to the backbone to allow users at thousands of universities, research labs, libraries, and museums to access any of the supercomputers and to communicate with one another. The complete network, including the backbone and the regional networks, was called **NSFNET**. It connected to the ARPANET through a link between an IMP and a fuzzball.

Consequently, NSF encouraged MERIT, MCI, and IBM to form a nonprofit corporation, **ANS** (**Advanced Networks and Services**). In 1990, ANS took over NSFNET and upgraded the 1.5-Mbps links to 45 Mbps to form **ANSNET**.

During the 1990s, many other countries and regions also built national research networks, often patterned on the ARPANET and NSFNET. These included EuropaNET and EBONE in Europe, which started out with 2-Mbps lines and then upgraded to 34-Mbps lines.

INTERNET: The number of networks, machines, and users connected to the ARPANET grew rapidly after TCP/IP became the only official protocol on January 1, 1983. When NSFNET and the ARPANET were interconnected, the growth became exponential.

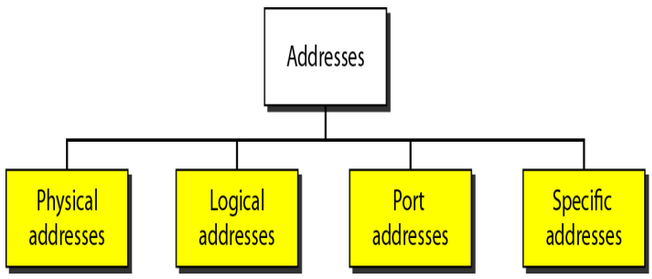
Traditionally the Internet and its predecessors had four main applications:

1. **E-mail.** The ability to compose, send, and receive electronic mail has been around since the early days of the ARPANET and is enormously popular. Many people get dozens of messages a day and consider it their primary way of interacting with the outside world, far outdistancing the telephone and snail mail. E-mail programs are available on virtually every kind of computer these days.
2. **News.** Newsgroups are specialized forums in which users with a common interest can exchange messages. Thousands of newsgroups exist, devoted to technical and nontechnical topics, including computers, science, recreation, and politics. Each newsgroup has its own etiquette, style, and customs, and woe betide anyone violating them.

3. **Remote login.** Using the telnet, rlogin, users anywhere on the Internet can log on to any other machine on which they have an account.
4. **File transfer.** Using the FTP program, users can copy files from one machine on the Internet to another. Vast numbers of articles, databases, and other information are available this way.

ADDRESSING

Four levels of addresses are used in an internet employing the *TCP/IP* protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses



Physical Addresses

- The physical address, also known as the **link address**, is the address of a node as defined by its LAN or WAN.
- It is included in the frame used by the data link layer.
- It is the lowest-level address.
- The physical addresses have authority over the network (LAN or WAN).
- The size and format of these addresses vary depending on the network.

Logical Addresses

- Logical addresses are necessary for universal communications that are independent of underlying physical networks.
- Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
- A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.
- No two publicly addressed and visible hosts on the Internet can have the same IP address.

Port Addresses

- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host.
- However, arrival at the destination host is not the final objective of data communications on the Internet.
- The end objective of Internet communication is a process communicating with another process.
- For example, computer A can communicate with computer C by using TELNET.
- At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a **port address**. A port address in TCP/IP is 16 bits in length.

Specific Addresses

Some applications have user-friendly addresses that are designed for that specific address. Examples include the e-mail address (for example, sacet@ac.in) and the Universal Resource Locator (URL) (for example, www.sacet.ac.in).