INTRODUCTION

A computer network is a set of computers connected together for the purpose of sharing resources.
Two computers are said to be interconnected if they are able to exchange information.
The most common resource shared today is connection to the internet which is a well-known example of network of networks.

Uses of computer networks:

1) Business Applications:

- Consider for example, a company may have computers for each worker, but at some point if the management decided to connect all of them. Computers to be able to distribute information throughout the company, the issue here is resource sharing.
- Here, the main goal is to make data available to anyone on the n/w without regard of the physical location of the resource or uses. The best example is common printer shared by a group of office workers.
- In smaller companies, all the computers are in a single office or in a single building. Whereas for larger companies the computers and employees may be scattered over offices at different locations.
- Here, Virtual Private Networks (VPN) is used to connect all the individual networks at different sites into one extended network.
- Company's information system consists of one or more databases and if some employees who need to access them remotely, the data are stored on powerful computers called serves which are centrally maintained by a system administrator.
- In contrast the employees have machines called clients with which they access remote data. The server and client machines are connected by a network. This network arrangement is called the client-server model.

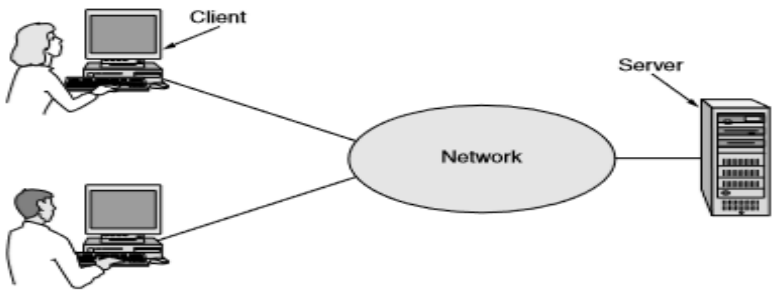


FIG. A Network with tow client and one server

- In this client-server model, two processes are involved one on client machine and one on the server machine.

- Initially communication is done by client process by sending a message over the network to server process. Now, the client waits for a reply message.
- After receiving the request the server process performs the requested work and sends the reply.

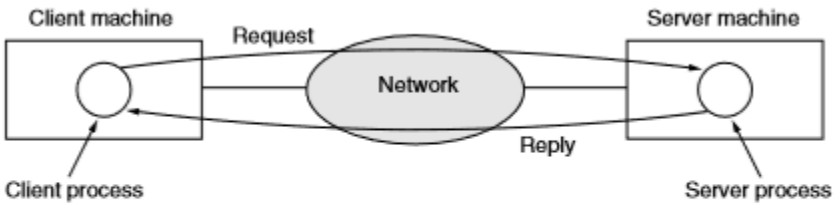


Fig. Client Server model involes requests and replies

- Another goal of computers network is that it can provide a powerful communication medium such as email (electronic mail), which employees use for a daily communication.
- Telephone calls between employees can be carried out by computer networks, this technology is called IP telephony or Voice over IP (VOIP) when internet is used.
- Desktop sharing is the technique that let the remote workers see and interact with a graphical computer screen, where when one worker makes a change to an online document the others can see the changes immediately.
- One more goal, for many companies doing business electronically with customers and suppliers where this model is called e-commerce (electronic commerce) using computer networks, manufacturers can place the orders electronically as this reduces the large inventories and enhances efficiency.

2) Home Applications:

- People earlier bought computers for word processing and games, later the reason to buy home computers was for Internet Access.
- Internet access providers' home users with connectivity to remote computers, home users can access information, communicate with otherpeople and buy products and service with e-commerce.
- Access to remote information comes in many forms, by surfing the World Wide Web for information or just for fun.
- Information includes arts, business, cooking, government, health, history, hobbies, recreation, science, sports, travel and many others.
- The step beyond newspapers along with magazines and scientific journals is provided in online digital library.
- Professional Organizations, such as ACM (www.acm.org) and the IEEE computer society (www.computer.org) have all their journals and conferences online.
- A popular model for accessing information can be done by peer-to-peer communication. Where every person can communicate with one or more other people and there is no fixed division into clients and servers.

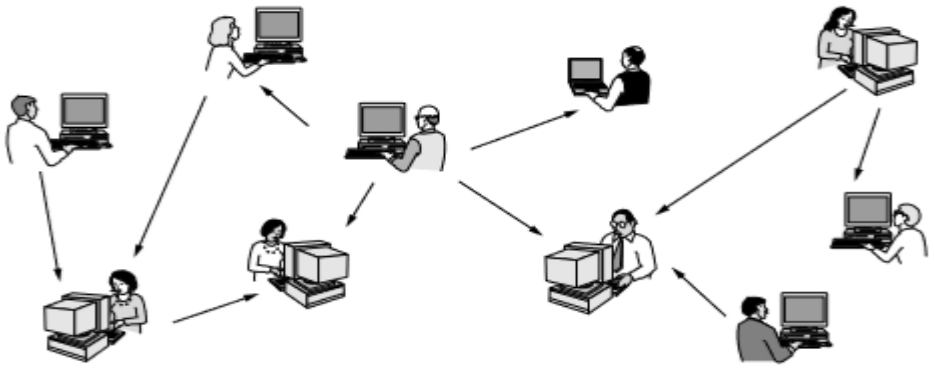


Fig. Peer to Peer System there are no fixed client & server

- In this peer-to-peer system it doesn't have any central database of content. Here each user maintains their own database locally and provides a list of other nearby people who are members of the systems.
- Peer-to-peer communication is after used to share music and videos.
- Instead of instant messaging, there is are multi-person messaging services such as twitter service that lets people send short text messages called "tweets".
- Between person-to-person communications and accessing information are social network applications. Such networking social sites are face book which lets to update personal profiles and shares the updates with others.
- Home shopping is popular and enables users to inspect the online catalogs, where some catalogs are interactive by showing products.
- Another aspect where e-commerce is widely used is access to financial institutions. People pay their bills, manage their bank accounts.
- Some forms of e-commerce have little tags based on "to" and "2" pronounced the same.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books online
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products online
P2P	Peer-to-peer	Music sharing

Figure. Some forms of e-commerce.

- Home applications have entertainment category where distribution of music, radio, television programs and movies over the Internet.
- Users can download MP3 songs, DVD-quality movies etc., Game playing is also another form of entertainment.

- Another application is ubiquitous computing where homes are wired with security systems that include door and window sensors.
- A technology called RFID (Radio Frequency Identification) tags are passive chips and have no battery which are stamp sized affixed to pets, credit cards, passports, books and other items in home. RFID lets readers locate and communicate with items over a distance up to several meters.

3) Mobile Users:

- In the computer industry, mobile computers such as laptop and handheld computers are fastest growing.
- Connectivity to the Internet enables many of these mobile uses.
- Wired connection is impossible everywhere such as in cars, boats, aero planes etc., there comes on wireless networks.
- Anyone with Laptop computer and wireless modem can just be connected to internet through hotspot once their computer is on.
- Wireless networks and mobile computing are related but not identical.

Wireless	Mobile	Typical applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in unwired buildings
Yes	Yes	Store inventory with a handheld computer

Figure. Combinations of wireless networks and mobile computing.

- The main key driver of mobile, wireless applications is the mobile phone where text messaging or texting is popular.
- To accelerate the growth of mobile applications with internet facility smart phones with 3G and 4G cellular networks are used to connect to provide faster data services using Internet as well as for handling phone calls.
- To know the locations of mobile phones they are equipped with GPS (Global Positioning System) receives, where some services are intentionally location dependent.
- Another area in which mobile phones are now using is M-commerce (mobile commerce) where a short text message from mobile are used for authorized payments for movie tickets and other small items etc instead of cash and credit cards. The charge appears on mobile phone bill.
- When mobiles are equipped with NFC Technology (Near Field Communication) it acts as an RFID smartcard which interact with nearly reads for payment.
- Sensor networks are made up of nodes (such as phones or cars or other devices) that gather and wirelessly relay information they sense about the state of the physical world.

4) Social Issues:

- Network operators are responsible for the contents of what they carry. Different countries have different and conflicting laws in this area.

- Users of peer-to-peer applications had their n/w service cut off because the network operators didn't find it profitable to carry large amounts of traffic sent by those applications.
- If a big company pay well they get good service, but if small-time company uses they get poorer service as the network operators treat different companies differently.
- There is an aspect involved over content that gets pirated such as music, movies etc., in peer-to-peer networks which threatens legal actions.
- So, there is an automated system which fires off warnings to network operators and users who are suspected of infringing copyright.
- Another conflict is around the government versus citizens' rights where the goal of this system is to spy on millions of people to find the illegal activities information.
- The government doesn't have monopoly on threatening people's privacy. For example, small files called cookies that are stored on user's computers by the web browsers allows the companies to track user's activities in cyberspace.
- It may also allow the confidential information leakage over the internet such as credit card numbers, social security numbers of users etc.,
- For example, Google can read all emails and show the advertisements based on the users interests basing on the usage of its email service i.e., g-mail.
- Computer networks also provide the potential to increase privacy by sending anonymous messages.
- Internet is making possible to find information quickly but it's ill-considered, misleading or downright wrong.
- There is other information that is frequently unwanted is electronic junk mail (spam), where these spammers collect millions of e-mail addresses and send computer-generated messages to the users.
- Other contents intended for criminal behavior where web pages and email messages having some active content may contain viruses that might steal user's bank account passwords.
- Phishing messages originating from trustworthy parties try to trick users for revealing sensitive information such as credit card numbers.
- To prevent computers from impersonating people over internet these lead to the development of CAPTCHA'S.
- These CAPTCHAs asks a person to solve short recognition task for example, typing letters shown in distorted images to know that they are human but not machines.
- This process is a famous Turing test in which a person asks questions over network to judge whether the user is human or not.

Reference Models:

There are two important layered network architectures:

1. The OSI reference model and
2. The TCP/IP reference model.

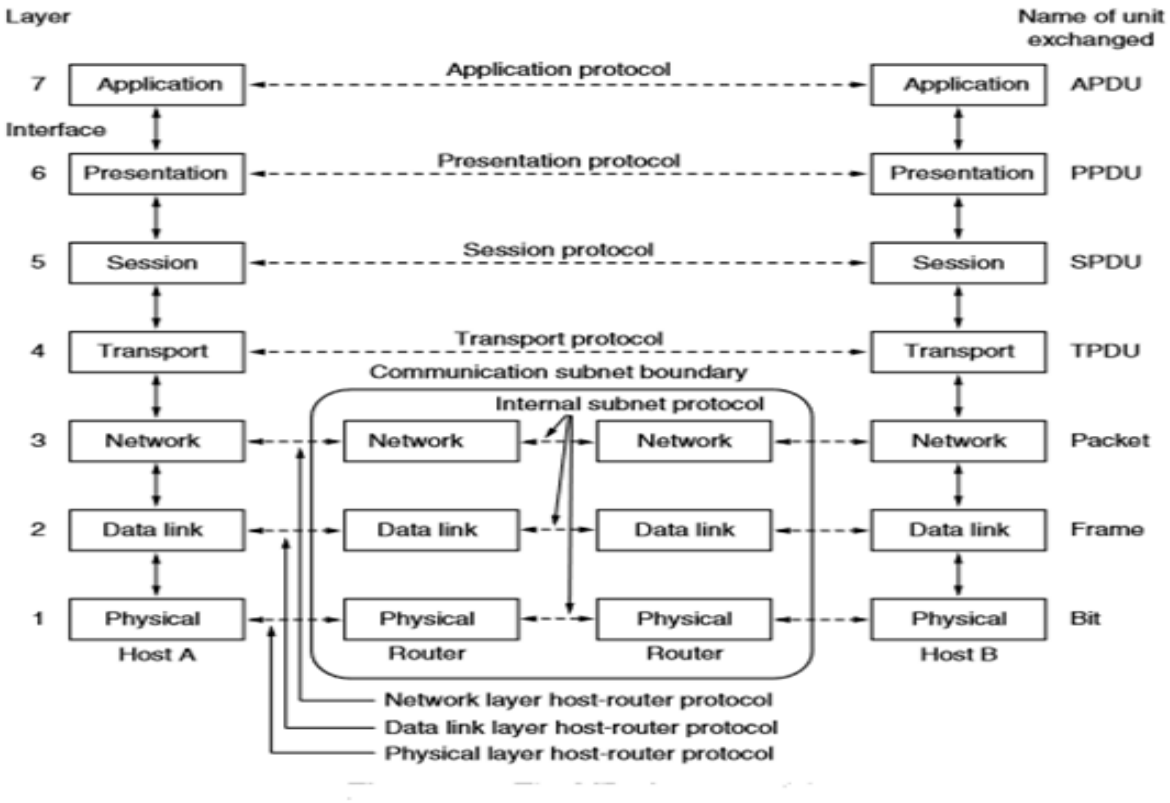
The protocols associated with the **OSI model** are not used any more, the model itself is actually quite general and still valid, and the features discussed at each layer are still very important.
The **TCP/IP model** has the opposite properties: the model itself is not of much use but the protocols are widely used.

The OSI reference model:

- The OSI model was developed by the International Standards Organization (ISO) as a first step towards the international standardization of the protocols used in the various layers.
- This model is called as ISO OSI simply OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems i.e. Systems that are open for communication with other systems.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.



THE OSI REFERENCE MODEL

The Physical Layer:

- The physical layer is concerned *with transmitting raw bits over a communication channel.*
- This layer is the lowest layer in the OSI model. It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibers, copper wire or wireless etc.
- This layer decides how the bits are encoded in the medium.
- For example, on the copper wire medium, we can use different voltage levels for a certain time interval to represent '0' and '1'. We may use +5mV for 1nsec to represent '1' and -5mV for 1nsec to represent '0'. All the issues of modulation is dealt with in this layer.
- The transfer of each bit of data is the responsibility of this layer. One side sends a 1 bit it is received by the other side as a 1 bit, not as a 0 bit.
- This layer assures the transmission of each bit with a *high probability*. The transmission of the bits is not completely reliable as there is no error correction in this layer.
- There are different queries such as whether transmission may proceed simultaneously in both directions, how the initial connection is established. How it is torn down, when both sides are finished, how many pins the network connector has, and what each pin is used for are the typical questions here.

Physical layer is concerned with the following functionalities:
(Deal with the mechanical and electrical specification of the primary connections: cable, connector)

- **Physical characteristics of interfaces and medium**
- **Representation of bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding
- **Data rate :** This layer defines the rate of transmission which is the number of bits per second
- **Synchronization of bits:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
- **Line configuration:** This layer connects devices with medium: point to point configuration and Multipoint Configuration
- **Physical topology:** Devices must be connected using the topologies: Mesh, Star, Ring and Bus
- **Transmission mode:** Physical Layer definers the direction of transmission between devices: Simplex, Half Duplex, Full Duplex

The Data Link Layer*:*

- This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion.
- It does so by masking the real errors so the network layer does not see them. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially.
- If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.
- The frames may be damaged, lost or duplicated leading to errors. The error control is on **link to link** basis.
- The packet is retransmitted if the source fails to receive acknowledgment.
- Necessary for a fast transmitter to keep pace with a slow receiver.
- Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel. A special sub layer of the data link layer, the **medium access control** sub layer, deals with this problem.

Datalink layer is concerned with the following functionalities:

- **Framing:** Frames are the streams of bits received from network layer into manageable data units.
- **Physical addressing:** The data link layer adds header to the frame in order to define physical address of the sender or receiver of the frame.
- **Flow control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control

- **Error control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism.
- **Access control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.

The Network Layer:

Its basic functions are ***routing*** and ***congestion*** control.

1. Routing:

This deals with determining how packets will be routed (transferred) from source to destination. It can be of three types:

- **Static:** Routes are based on static tables that are "wired into" the network and are rarely changed.
- **Dynamic:** All packets of one application can follow different routes depending upon the topology of the network, the shortest path and the current network load.
- **Semi-Dynamic:** A route is chosen at the start of each conversation and then all the packets of the application follow the same route.

2. Congestion Control:

A router can be connected to 4-5 networks.

- If all the networks send packet at the same time with maximum rate possible then the router may not be able to handle all the packets and may drop some/all packets.
- In this context the dropping of the packets should be minimized and the source whose packet was dropped should be informed.
- The control of such congestion is also a function of the network layer. Other issues related with this layer are transmitting time, delays, jittering.
- When a packet has to travel from one network to another to get to its destination, many problems can arise.
- The addressing used by the second network may be different from that used by the first one.
- The second one may not accept the packet at all because it is too large.
- The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.
- In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

Network layer is concerned with the following functionalities:

- **Logical addressing**: It translates logical network address into physical address. Concerned with circuit, message or Packet Switching.
- **Routing:**The data is transfer in form of packets and it is responsible for handling the movement of data.

The Transport Layer:

- The transport layer will create distinct network connection for each transport connection required by the session layer.
- The data accepted by the transport layer from the session layer is split up into smaller units (fragmentation) if needed and then passed to the network layer. Correspondingly, the data provided by the network layer to the transport layer on the receiving side is re-assembled.
- The transport layer also decides the type of service that should be provided to the session layer. Transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.
- If reliable service is provided then error detection and error recovery operations are also performed. It provides error control mechanism on **end to end** basis.
- The communication is always carried out between two processes and not between two machines. This is also known as process-to-process communication.
- The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination.

Transport layer is concerned with the following functionalities:

- **Service port 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. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- **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 connectionoriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connectionoriented 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.

The Session Layer:

- It deals with the concept of **Sessions** i.e. when a user logins to a remote server he should be **authenticated** before getting access to the files and application programs
- The session layer allows users on different machines to establish and maintain sessions between them.
- During the transfer of data between two machines if the session breaks down, it is the session layer which re-establishes the connection.
- Sessions offer various services, like
- ***Dialog control*** (keeping track of whose turn it is to transmit),
- ***Token management*** (preventing two parties from attempting the same critical operation simultaneously), and ***synchronization***(check pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

Session layer is concerned with the following functionalities:

- **Manage dialog control:** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either halfduplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Token management**:management (preventing two parties from attempting the same critical operation simultaneously)
- **Synchronization:** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

The Presentation Layer:

- This layer is concerned with the syntax and semantics of the information transmitted.
- This layer ensures that the data transmitted by one gets converted in the form compatible to the machine.
- In order to make it possible for computers with different data representations to communicate data structures to be exchanged can be defined in abstract way along with standard encoding.
- The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records) to be defined and exchanged.

Presentation layer is concerned with the following functionalities:

- **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.

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

The Application Layer:

- The seventh layer contains the application protocols with which the user gains access to the network.
- The application layer contains a variety of protocols that are commonly needed by users.
- Thus the boundary between the presentation layer and the application layer represents a separation of the protocols imposed by the network designers from those being selected and implemented by the network users.

  For example commonly used protocols are HTTP (for web browsing), FTP (for file transfer) etc.

Application layer is concerned with the following functionalities:

- **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 make changes or read data), 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.

The TCP/IP Reference Model:

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.

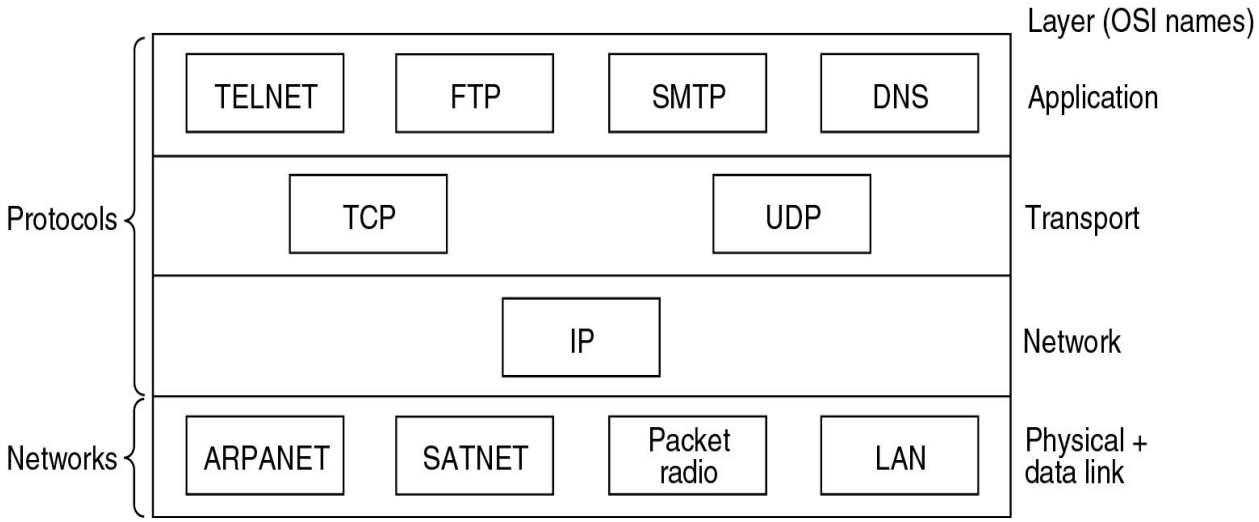


Fig: Protocols and networks in the TCP/IP model initially

Description of different TCP/IP protocols:

The Link Layer (Host-to-network Layer)

- The lowest layer in the model.
- The **link layer** describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.
- It is not really a layer, but rather an interface between hosts and transmission links.

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

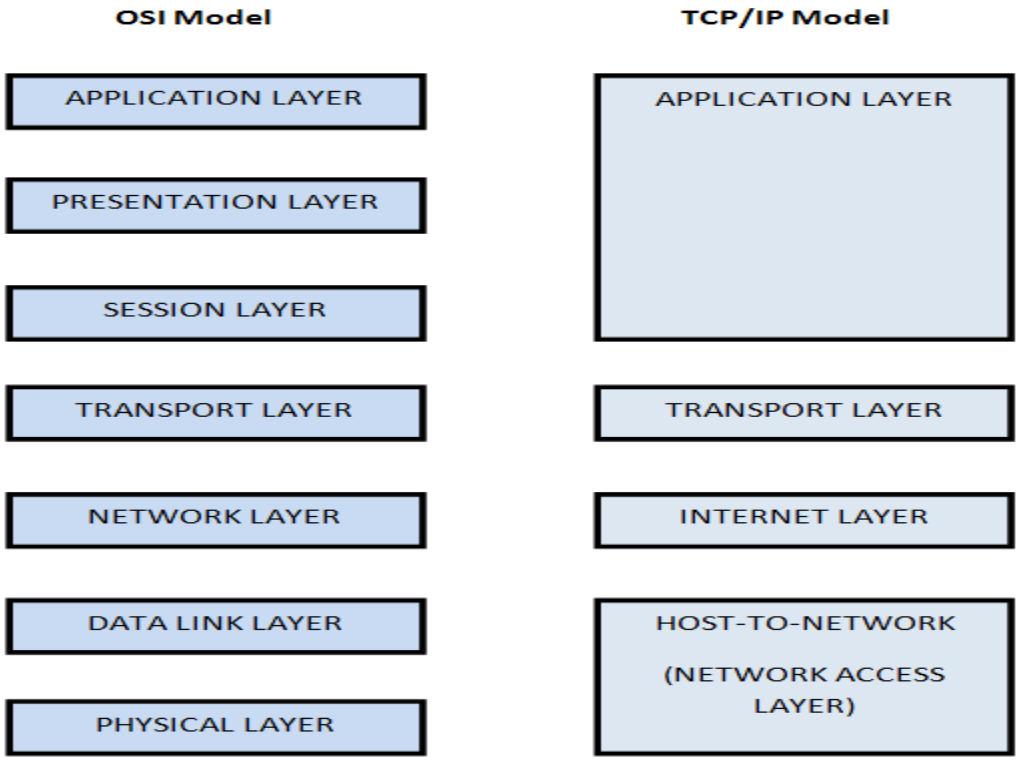
1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below

S.No	OSI Model	TCP/IP Model
1	Open System Interconnection	Transmission Control Protocol / Internet Protocol
2	OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them	In TCP/IP it is not clearly separated its services, interfaces and protocols
3	In OSI model, the protocols came after the model was described	In TCP/TP model,the protocols came first,and the model was really just a description of the existing protocols
4	The OSI model has 7 layers	The TCP/IP model has only 4 layers
5	The OSI model is a reference model	The TCP/IP model is an implementation of the OSI model
	The OSI model is layered model	The TCP/IP model is internet model
	The OSI model follows horizontal approach	The TCP/IP model follows vertical approach
6	The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection -oriented communication	The TCP/IP model supports both connectionless and connection-oriented communication in the transport layer, giving users the choice, but only

	in transport layer i.e NL – CO & CL TL - CO	connection-less communication in network layer i.e TL –CO & CL NL – CL
7	In OSI model, the protocols are better hidden.OSI is protocol independent	In TCP/IP model, the protocols are not hidden.TCP/IP is protocol dependent
8	OSI follows a horizontal approach	TCP/IP follow a vertical approach
9	Protocols are hidden in OSI model and are easily replaced as the technology changes	In TCP/IP replacing protocol is not easy



Network Standardization

The many of the network vendors and suppliers do exist with their own ideas of how things to be done. A user would get his things done by some network standards, where standards are: documented agreements containing technical specifications or other precise criteria stipulating how particular products or services should be designed or performed. Network standards define guideline that specifies the way computers access the medium to which they are attached. The well-known 802.11 standard defines communication between a wireless computer or client and an access point or between two wireless computers or clients.

Standards fall into two categories: **de facto and de jure.**

• **De facto** (Latin for ‘‘from the fact’’) standards are those that have just happened, without any formal plan. HTTP, the protocol on which the Web runs, started life as a de facto standard. It was part of early WWW browsers developed by Tim Berners-Lee at CERN, and its use took off with the growth of the Web. Bluetooth is another ex-ample. It was originally developed by Ericsson but now everyone is using it.

• **De jure** (Latin for ‘‘by law’’) standards, in contrast, are adopted through the rules of some formal standardization body. International standardization authorities are generally divided into two classes: those established by treaty among national governments, and those comprising voluntary, non- treaty organizations. In the area of computer network standards like ISO, IEEE, ASCII.

Who’s who in the Telecommunication World?

The legal status of the world’s telephone companies varies from country to country. There are other countries in which the national government has complete monopoly on all communication, including the mail, telegraph, telephone, radio and television. In the year 1865, representatives from many companies met together to form ITU (International Telecommunication Union) where its job is to standardize international telecommunications.

ITU has three main sectors namely ITU-T, ITU-R, and ITU-D.

• ITU-T is the Telecommunication Communication Standardization Sector, which is concerned with telephone and data communication systems.

• ITU-R is the Radio communications Sector, which is concerned with coordinating the use by competing interest groups of radio frequencies worldwide.

• ITU-D is the Development Sector, which is concerned with the development of information and communication technologies in countries.

Who’s who in the International Standards World?

International standards are produced and published by ISO **(International Standards Organization)** which is founded in the year 1946. Goal is to establish international technological standards to facilitate global exchange of information and barrier-free trade. Over 17,000 standards have been issued, including the OSI standards. ISO has over 200 Technical

Committees (TCs), where TC1 deals with the nuts and bolts. JTC1 (Joint Technical Committee) deals with information technology, including networks, computers, and software.

The procedure used by ISO for adopting standards has been designed to achieve broad consensus possible. The process begins when any national standard organization needs a international standard in some area, a working group forms to come up with committee draft (CD) which is circulated to all the members of the body if its approved a revised document called Draft International Standard (DIS) is produced and circulated for comments and voting, now basing on the result final text of International Standard (IS) is prepared, approved and published.

Major Player in the standards world is **IEEE (Institute of Electrical and Electronics Engineers)**, the largest professional organization in the world.Goals are to promote development and education in electrical engineering and computer science. IEEE technical papers and standards are highly respected in the networking profession. Can purchase IEEE documents online from IEEE's Web site (www.ieee.org)

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs (WiFi)
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number; nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth, Zigbee)
802.16 *	Broadband wireless (WiMAX)
802.17	Resilient packet ring
802.18	Technical advisory group on radio regulatory issues
802.19	Technical advisory group on coexistence of all these standards
802.20	Mobile broadband wireless (similar to 802.16e)
802.21	Media independent handoff (for roaming over technologies)
802.22	Wireless regional area network

Fig: The 802 working groups. The important ones are marked with *. The ones marked with  are hibernating. The one marked with † gave up disbanded itself.

Who's who in the Internet Standards World?

The worldwide Internet has its own standardization mechanisms, very different from those of ITU-T and ISO.

ITU-T and ISO meetings are populated by corporate officials and government civil servants for whom standardization is their job. They regard standardization as a Good Thing and devote their lives to it. Internet people, on the other hand, prefer anarchy as a matter of principle. However, with hundreds of millions of people all doing their own thing, little communication can occur. Thus, standards, however regrettable, are sometimes needed.

When the ARPANET was set up, DoD created an informal committee to oversee it. In 1983, the committee was renamed the IAB (Internet Activities Board) and was given a slighter broader mission, namely, to keep the researchers involved with the ARPANET and the Internet pointed more-or-less in the same direction, an activity not unlike herding cats. The meaning of the acronym "IAB" was later changed to Internet Architecture Board.

By 1989, the Internet had grown so large that this highly informal style no longer worked. Many vendors by then offered TCP/IP products and did not want to change them just because ten researchers had thought of a better idea. In the summer of 1989, the IAB was reorganized again. The researchers were moved to the IRTF (Internet Research Task Force), which was made subsidiary to IAB, along with the IETF (Internet Engineering Task Force). The IAB was repopulated with people representing a broader range of organizations than just the research

The IAB was repopulated with people representing a broader range of organizations than just the research community. It was initially a self-perpetuating group, with members serving for a 2-year term and new members being appointed by the old ones. Later, the Internet Society was created, populated by people interested in the Internet. The Internet Society is thus in a sense comparable to ACM or IEEE. It is governed by elected trustees who appoint the IAB members.

MEDIUM ACCESS CONTROL

Data Link Layer:

This layer is the second layer of OSI System, it is a protocol layer that transfers between adjacent network nodes in a WAN (or) between nodes on the same local area network (LAN) segment.

Medium Access Control:

1) It is a sublayer of the data link layer (DLL) in the 7 layer OSI Network reference Model.

2) MAC is responsible for the transmission of data packets to and from the network interface card and to from another remotely shared channel.

3) Generally, The Network lines can be divided into two categories.

(a) Point-to-Point Connection
(b) Broadcast Channels

4) The MAC Sub layer deals with the Broadcast channel links and their protocols.

5) In Broadcast network, the main (or) key issue is how to determine who gets to use the channel, when there is competition for it.

Consider a scenario, at a meeting a people raise their hands to request permission to speak, but when only a single channel is available, it is harder to determine who should go next.

For solving the above scenario, we are having the protocols to solve it.

a) Broadcast Channels are also called as Multi-access Channels (or) Random access channels.
b) The protocols used to determine who goes next on a multi-access channel which is belong to the sublayer of the DLL i.e., called as MAC Sub layer.

Channel Allocation Problem:

1) The MAC sub layer which is useful (or) important in LAN Network.
2) We can classify the channels as Static and Dynamic

a) Static Channel:

It defines, where the number of users is stable and traffic is not bursty.

b) Dynamic Channel:

IT defines, when the number of users using the channel keeps on varying the channel is considered as a dynamic channel.

Static Channel Allocation:

1) The usual way of allocating a single channel such as a telephone trunk, among multiple competing users is to chop up its capacity by using one of the multiplexing schemes such as FDM.(Frequency Division Multiplexing)

2) FDM- If there are N users, the bandwidth is divided into N equal sized portions, for each user being assigned one portion, and each user has a private frequency band and there is now no interference among users.

3) Mostly, FDM Technique is suitable for when there is only a small and fixed number of users, and each of which has a heavy (buffered) load of traffic.

4) FDM Is simple and efficient technique for small and constant number of users, each of which has a steady (or) a heavy load of traffic.(eg: Carriers switching offices, FM Radio Stations)

Problems with FDM:

1) If fewer than N users are currently interested in communication, some portions of spectrum will be wasted.

2) If more than N Users want to communicate, some of them will be denied permission, if some users with allocated frequency hardly ever transmit anything.

3) Even the number of users is N and constant, when some users are in inactivity, no one use their bandwidth, so it is simple wasted.

These are the some problems it cannot be handled by FDM.

Bursty Traffic:

- The term burst transmission (or) data burst, it defines that any relatively high bandwidth transmission over a short period.
- For e.g., A download might use 2M Bits/s on avg, while having “peaks” bursting up to say 2.4M/Bits/s
- This Bursty traffic scenario, cannot handle by FDM and as well as TDM.
- Thus, none of the static channels allocation methods work well with bursty traffic.
- For bursty data traffic(peak traffic to mean traffic ratio is 1000:1)

The poor performance of static FDM can easily be seen with a simple queuing theory Calculation.

Let us find the mean Time Delay T, to send a frame onto a channel of capacity Cbps. We assume that the frames arrive randomly with an average arrival rate of lambda frames/sec, and the frames vary in length with an average length of 1/μ bits. With these parameters, the service rate of the channel is μC frames/ sec. A standard queuing theory result is

$$T = 1/\mu C - \lambda$$

Assumptions for Dynamic Channel Allocation:
There are 5 Key Assumptions: They are as Follows:

1) Independent Traffic
2) Single Channel
3) Collisions
4) Continuous (or) Slotted Time
5) Sense Assumption

- **Independent Traffic:**

  - The model consists of N independent stations (E.g. Computers, telephones), each with a program (or) user that generates frames for transmission.
  - The expected number of frames generated in an interval of length del t is , where lamda is a constant (the Arrival rate of new frames)
  - Once a frame has been generated, the station is blocked and dpoes nothing until the frame has been successfully transmitted.

- **Single Channel:**

A single channel is available for all communication. All stations can transmit on it and all can receive from it. The stations are assumed to be equally capable, though protocols may assign them different roles (e.g.: Priorities)

- **Collisions:**

If two frames are transmitted simultaneously, (or) overlap in time, a collision occurs. All stations can detect collisions. A collided frame must be retransmitted.

- **Continuous (or) slotted Time:**

  - Time may be assumed continuous, in which case frame transmission can begin at any instant.
  - In second case, the time may be slotted (or) divided into discrete intervals (called slots).
  - Frame transmissions must then begin at the start of a slot.A slot contain 0,1 (or) more frames, corresponding to an idle slot, a successful transmission (or) a collision, respectively.

- **Sense Assumption:**

  - **Carrier sense:** Stations can scene, if the channel is in use before trying to use it.
  - **No carrier sense:** Stations cannot sense the channel before trying to use it.

These are the 5 Assumptions which is helpful for analysing (or) using the multiple access methods (or) protocols.

Multiple Access Protocols:

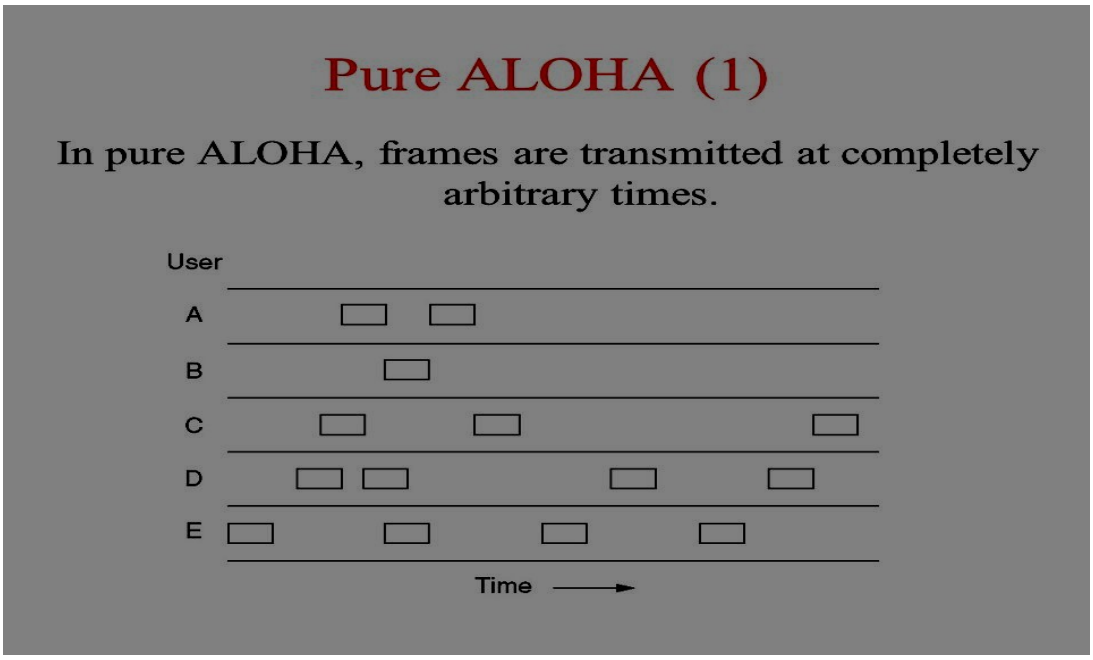
- ALOHA is a system for coordinating and arbitrating access to a shared communication network channel.
- It was developed in the 1970's by Norman Abramson at the university by Hawaii.
- This system is used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.
- Radio Broadcasting is a unidirectional wireless transmission over radio waves.
- A shared communication system like ALOHA requires a method of handling collisions that occur when two (or) more systems attempt to transmit on the channel at the same time.
- In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs and the frames that were transmitted are lost.
- ALOHA means "HELLO" ALOHA is a multiple access protocol at DLL and proposes how multiple terminals access the medium without collision.

There are two different versions/Types of ALOHA:

1) Pure ALOHA
2) Slotted ALOHA

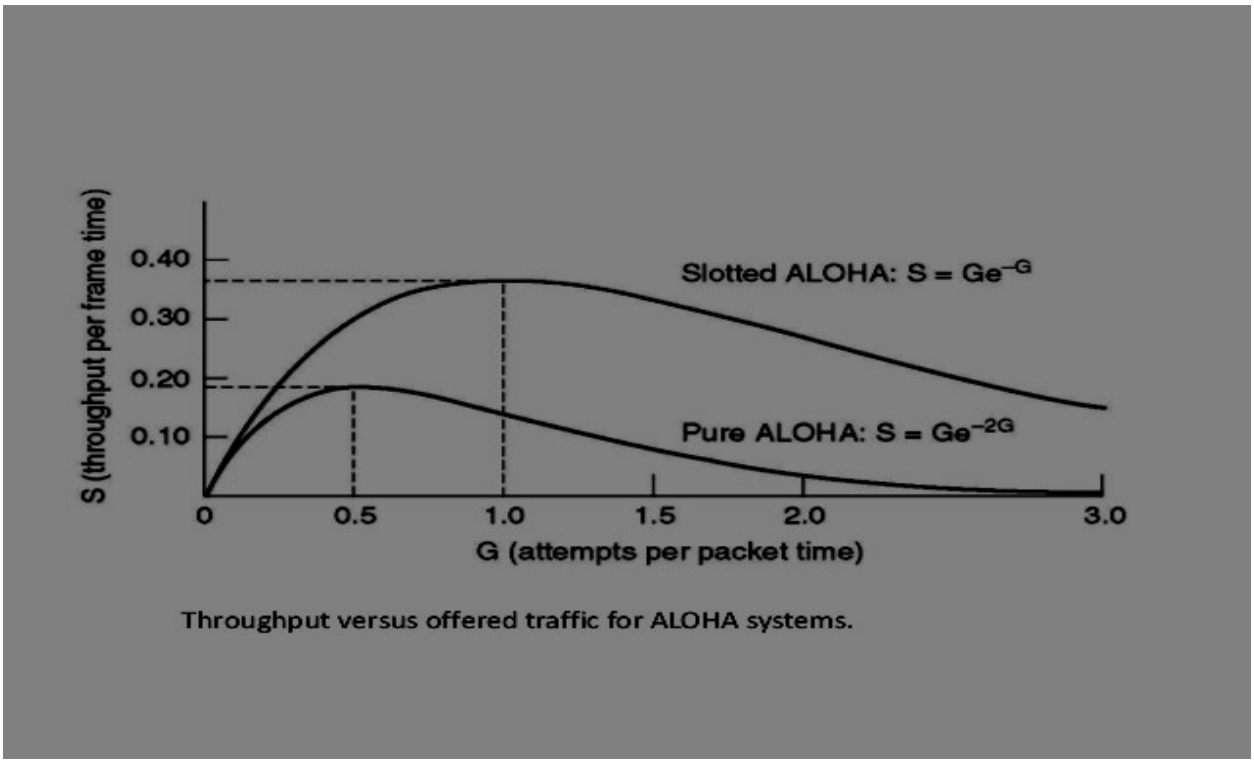
Pure ALOHA:

- In pure ALOHA, the station transmit frames whenever they have data to send.
- When two (or) more stations transmit simultaneously, there is collision and the frames are destroyed.
- In Pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within a specified time, the station assumes that the frame has been destroyed.
- If the frame is destroyed, because of collision, the station waits for a random amount of time and sends it again. This waiting time must be random, otherwise same frames will collide again and again.
- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help to avoid more collisions.
- In given fig, there are 4 stations that contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel.
- Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
- Whenever two frames try to occupy the channel at the same time, there will be collision and both will be damaged. If first bit of a new frame overlaps with just last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.



Slotted ALOHA:

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, the time of the shared channel is divided into discrete intervals called the slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.



Throughput versus offered traffic for ALOHA systems.

Carrier Sense Multiple Access Protocols:

Protocols in which stations listen for a carrier (transmission) and acts accordingly are called carrier sense protocols.

Persistent CSMA and Non Persistent CSMA:

Persistent CSMA:

- This is a simple CSMA Scheme, in which when a station has data to send, it first listens to channel to see whether anyone else transmitting at the moment, if it finds that channel is idle, the station sends the data.
- If the channel is busy, the station waits until the channel becomes idle and then transmits a frame.
- If any collisions occur at station waits a random amount of time and starts all over again.
- This protocol is named as 1-persistant because the station transmits with a probability of 1 when the channel is idle.
- If propagation delay is small, collisions happening are small. If delay is large then effect becomes more and performance gets worse.

Non-Persistent CSMA:

- In this protocol, a station senses the channel when it requires to sends frame, if no one else is sending then the station begins to send.
- If the channel is in use, the station doesn't sense the channel continuously to detect the end of previous transmission for seizing it immediately.
- Instead of it, the station waits a random period of time and then repeats the algorithm for better channel utilization, but has longer delays than 1-persistent.

P-Persistent CSMA:

- When a station becomes ready to send it senses the channel, if the channel is idle transmits with a probability P and with a probability q=1-p it defers until next slot.
- If the slot is idle, station either transmits or defers again with probabilities p and q.
- This process continues until a frame gets transmitted or till another station begins transmitting.
- If there is a collision, station waits a random amount of time and starts again.

CSMA with Collision Detection:

- The persistent and non-persistent protocols of CSMA are an improvement over ALOHA as they ensure that no station begins transmitting while the channel is busy.
- If two stations sense the channel to be idle and transmit at same time their signals collide.
- There is an improvement in these protocols that the stations can quickly detect the collision and stops transmitting immediately which same time and bandwidth.
- Here, the CSMA with collision Detection (CSMA/CD) is the basis of Ethernet LAN, where the collision detection is an analog process.
- The stations hardware listens to the channel while it is transmitting, if the signal is putting out is different from signal, it understands that collision is occurring.
- Usually the received signal must not be small compared to transmitted signal, which is difficult for wireless as signals received are 1000000 times weaker than transmitted signals.
- In the following figure of a CSMA/CD uses a conceptual Model.

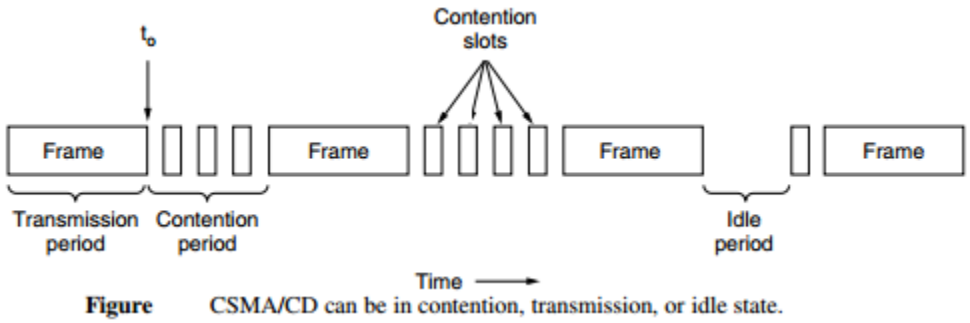


Figure CSMA/CD can be in contention, transmission, or idle state.

- At 'to' a station has finished its transmission of frame and any other station may transmit now.
- If two or more stations transmit at same time there will be collision.

- If the station detects the collision, it aborts its transmission, waits a random period of time and then tries to transmit assuming that no station has started transmitting.
- So, this model CSMA/CD consists of alternating contention and transmission periods along with idle periods when all the stations are quite.
- For suppose in the contention algorithm, two stations begins transmitting at same time to, how long it takes the stations to realize that they have collided?
- The minimum time to detect the collision is the time it takes the signal to propagate from one station to the other.
- One might assume that a station which did not detect the collision for a time equal to the full cable propagation time after starting its transmission has seized the cable.
- Seized means that all other stations knows that it is transmitting and will not interfere.

Collision free protocols:

- Some protocols that resolve the contention for the channel without any collisions at all not even during the contention period.
- In the CSMA/CD, let's suppose that there are exactly N stations each with a unique address from 0 to N-1 "wired" into it.
- It doesn't matter even though some stations are inactive and assume that propagation delay is negligible. The basic question that arises is: which station gets the channel after a successful transmission?

A Bit-Map Protocol:

- In collision free protocols the first protocol is the basic bit-map method.
- Each contention period consists of exactly N slots. If station 0 has a frame to send it transmits a 1 bit during the zeroth slot. No other station is allowed to transmit during this slot.
- In general case is a station j transmits a frame by inserting a 1 bit into slot j, after ALL N slots have passed by each station gains a knowledge of which station wants to transmit.
- At that point of they begin to transmit in a numerical order and there will be no chance of collisions.

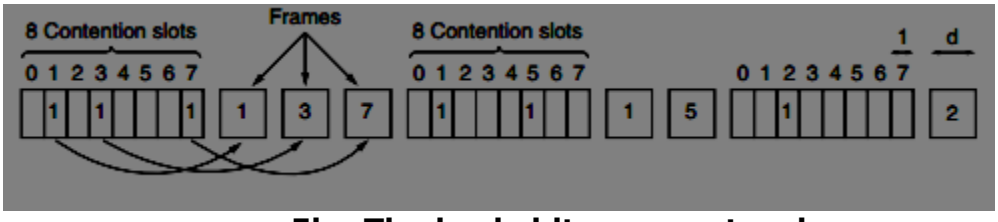


Fig: The basic bit-map protocol

- After the last ready station has transmitted its frame, all the stations can monitor as well another N bit contention period begins.

- If a station becomes ready just after its bit slot has passed by it is out of luck and must be silent until every station has had a chance and the bit map has come around again.
- Protocols like this which desire to transmit is broadcast before the actual transmission are called reservation protocols.
- The problem with this bit-map protocol is that the overhead is 1 bit per station so it doesn't scale well to networks with thousands of stations.

Token Passing:

- As the bit-map protocol lets every station to transmit a frame in an predefined order. Now, the token ring does the same things by passing a small message called token from one station to other in the same predefined order.
- Token represents a permission to send the frame.
- A station on receiving the token transmits the frame that is queued and later it passes the token to next station, if any station doesn't have frame to send it passes the token simply.
- In this token ring protocol, the topology of the network defines the order in which station sends and are connected in a single ring fashion.
- Since passing the token to next station consists of receiving the token in one direction and transmitting in other direction where the frames are transmitted in direction of token.
- This goes in a circulating fashion in the ring and reaches the destination station.
- To stop the frame circulating, stations need to remove it from the ring where only the station that has sent the frame or the station that was recipient of the frame can do so.

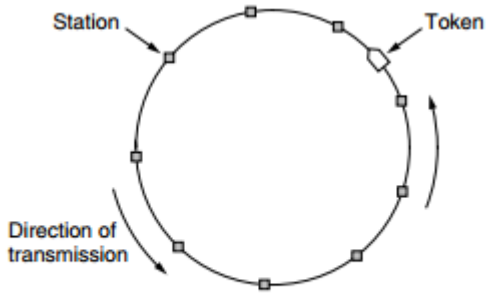


Figure Token ring.

- In the token passing there is no physical ring but channels are connected to a single long bus. Where each station uses the bus to transmit the token to next station in a predefined sequence, this protocol is called token bus.

Binary countdown:

- A station wanting to use the channel broadcasts its address as a binary bit string starting with the highest bit.

- All the addresses are assumed to be of same length and the bits in each address position from different stations are Boolean ORed together. So this protocol is a Binary countdown protocol.

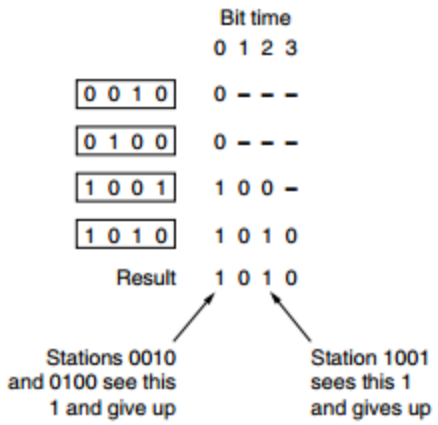


Figure The binary countdown protocol. A dash indicates silence.

- To avoid conflicts, an arbitration rule must be applied: as soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up.
- For example, if stations 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first bit time the stations transmit 0, 0, 1, and 1, respectively.
- These are ORed together to form a 1. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round.
- Stations 1001 and 1010 continue. The next bit is 0, and both stations continue. The next bit is 1, so station 1001 gives up.
- The winner is station 1010 because it has the highest address. After winning the bidding, it may now transmit a frame, after which another bidding cycle starts.