DIGITAL NOTES
ON
COMPUTER NETWORKS

B.TECH
(III YEAR – I SEM)
(2019-20)

Department of Information Technology

MALLA REDDY COLLEGE
OF ENGINEERING & TECHNOLOGY

(Autonomous Institution – UGC, Govt. of India)

Recognized under 2(f) and 12 (B) of UGC ACT 1956

Affiliated to JNTUH, Hyderabad, Approved by AICTE - Accredited by NBA & NAAC – 'A' Grade - ISO 9001:2015 Certified)

Maisammaguda, Dhulapally (Post Via. Kompally), Secunderabad – 500100, Telangana State, India

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY

III Year B.Tech IT – I Semester

L	T/P/D	C
3	-/-/-	3

(R17A0514) COMPUTER NETWORKS

Objectives:

1. To introduce the fundamental of computer networks.
2. To demonstrate the framework of TCP/IP & OSI model.
3. To know the role of various protocols in Networking.
4. To learn the detailed functioning of various network layers.

UNIT - I:

Introduction: Network, Uses of Networks, Types of Networks, Reference Models: TCP/IP Model, The OSI Model, Comparison of the OSI and TCP/IP reference model. Architecture of Internet.
Physical Layer: Guided transmission media, Wireless transmission media, Switching.

UNIT - II:

Data Link Layer - Design issues, Error Detection & Correction, Elementary Data Link Layer Protocols, Sliding window protocols
Multiple Access Protocols - ALOHA, CSMA,CSMA/CD, CSMA/CA, Collision free protocols, Ethernet- Physical Layer, Ethernet Mac Sub layer, Data link layer switching: Use of bridges, learning bridges, spanning tree bridges, repeaters, hubs, bridges, switches, routers and gateways.

UNIT - III:

Network Layer: Network Layer Design issues, store and forward packet switching connection less and connection oriented networks-routing algorithms-optimality principle, shortest path, flooding, Distance Vector Routing, Count to Infinity Problem, Link State Routing, Path Vector Routing, Hierarchical Routing; Congestion control algorithms, IP addresses, CIDR, Sub netting, Super netting, IPv4, Packet Fragmentation, IPv6 Protocol, Transition from IPv4 to IPv6, ARP, RARP.

UNIT - IV:

Transport Layer: Services provided to the upper layers elements of transport protocol- addressing connection establishment, Connection release, Error Control & Flow Control, Crash Recovery.

The Internet Transport Protocols: UDP, Introduction to TCP, The TCP Service Model, The TCP Segment Header, The Connection Establishment, The TCP Connection Release, The TCP Sliding Window, The TCP Congestion Control Algorithm

UNIT - V:

Application Layer- Introduction, providing services, Applications layer paradigms: Client server model, HTTP, E-mail, WWW, TELNET, DNS; RSA algorithm.

TEXT BOOKS:

1. Data Communications and Networking - Behrouz A. Forouzan, Fifth Edition TMH, 2013.
2. Computer Networks - Andrew S Tanenbaum, 4th Edition, Pearson Education.

REFERENCES BOOKS:

1. An Engineering Approach to Computer Networks - S. Keshav, 2nd Edition, Pearson Education.
2. Understanding communications and Networks, 3rd Edition, W. A. Shay, Cengage Learning.
3. Introduction to Computer Networks and Cyber Security, Chwan-Hwa (John) Wu, J. David Irwin, CRC Press.
4. Computer Networks, L. L. Peterson and B. S. Davie, 4th edition, ELSEVIER.
5. Computer Networking: A Top-Down Approach Featuring the Internet, James F. Kurose, K. W. Ross, 3rd Edition, Pearson Education.

Outcomes:

(1) Exploration of the various Computer Networks, Protocols and routing algorithms.

(2) Students will be in a position to understand the World Wide Web concepts and the need for network security.

(3) Ability to administrate a network and flow of information

MALLA REDDY COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

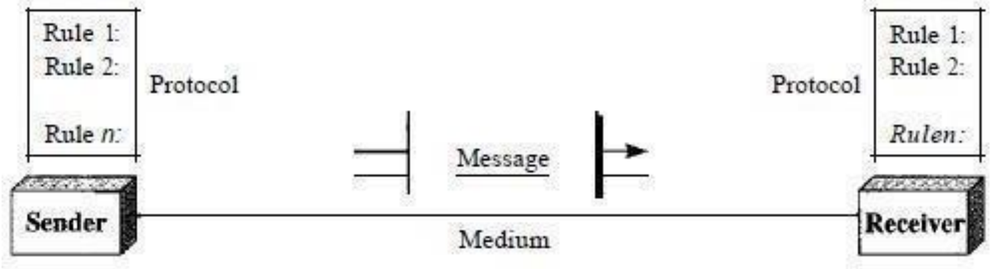
INDEX

UNIT -I
Introduction to Computer Networks

Data Communication: When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance.

Components:

A data communications system has five components.



1. Message. The message is the information (data) to be communicated. 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 govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (O or 1). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution.*

Audio:

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal. In Chapters 4 and 5, we learn how to change sound or music to a digital or an analog signal.

Video:

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal.

Data Flow

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

Simplex:

In simplex mode, the communication is unidirectional, as on a one-way street. 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 introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

Half-Duplex:

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa The half-duplex mode is like a one-lane road with traffic allowed in both directions.

When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex:

In full-duplex both stations 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. The capacity of the channel, however, must be divided between the two directions.

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.

Distributed Processing

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

Performance:

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughputs and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability:

In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security:

Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures:

Type of Connection

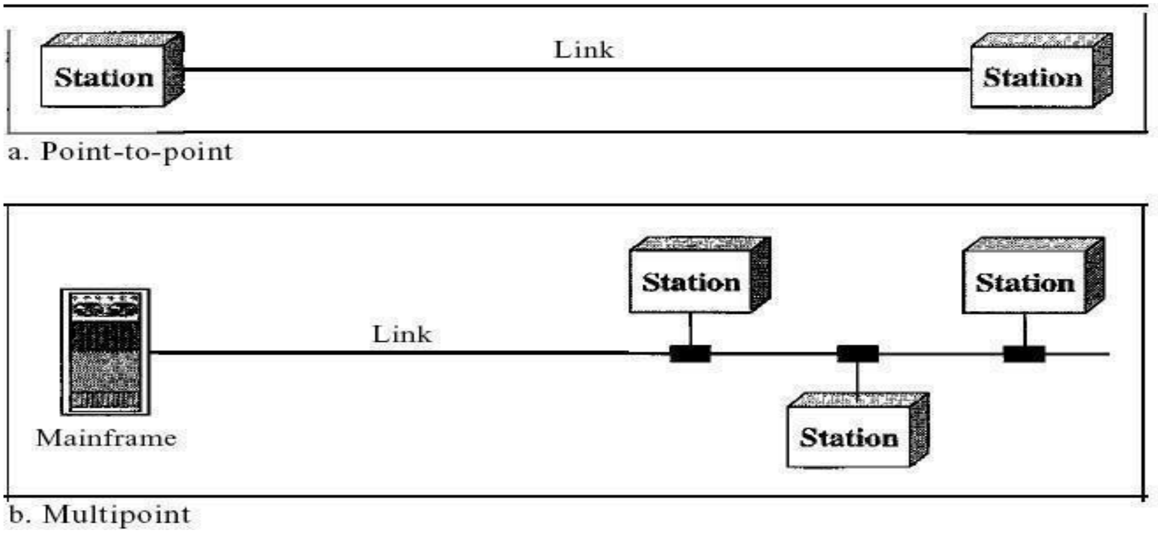
A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and 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, but other options, such as microwave or satellite links, are also possible. 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 multi drop) connection is one in which more than two specific devices share a single link. 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.

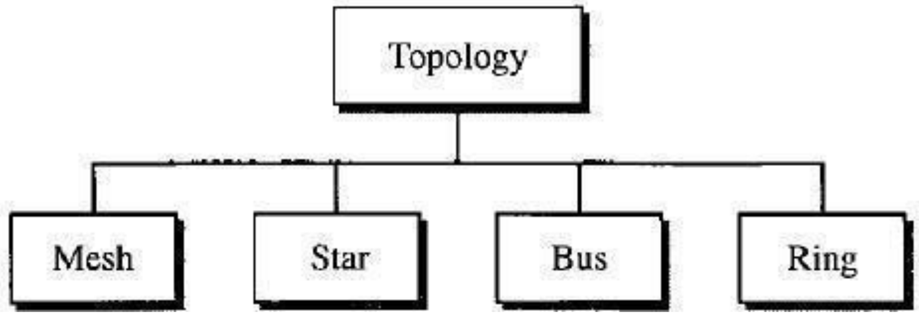


a. Point-to-point

b. Multipoint

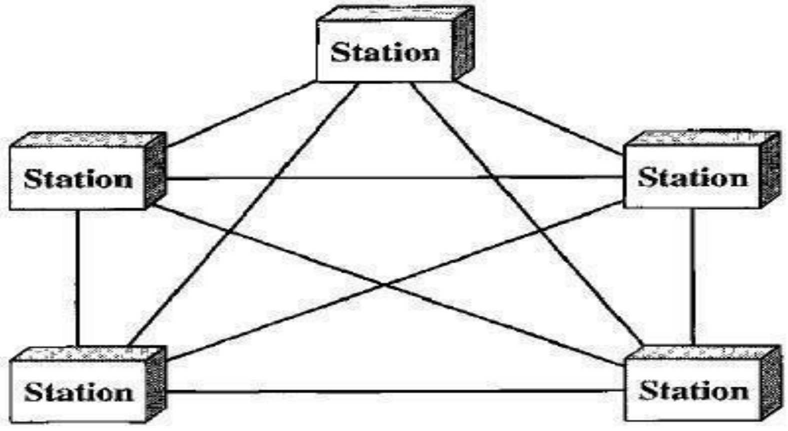
Physical Topology

The term *physical topology* refers to the way in which a network is laid out physically. One 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, andring



Mesh: 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 traffic only between the two devices it connects. 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* - I nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to *n* - 1 nodes. We need *n(n* - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need *n(n* -1) /2 duplex-mode links.

To accommodate that many links, every device on the network must have *n* – 1 input/output *(VO)* ports to be connected to the other *n* - 1 stations.



Advantages:

1. 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.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise Location of the fault and aids in finding its cause and solution.

Disadvantages:

1. Disadvantage of a mesh are related to the amount of cabling because every devicemust be connected to every other device, installation and reconnection are difficult.
2. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

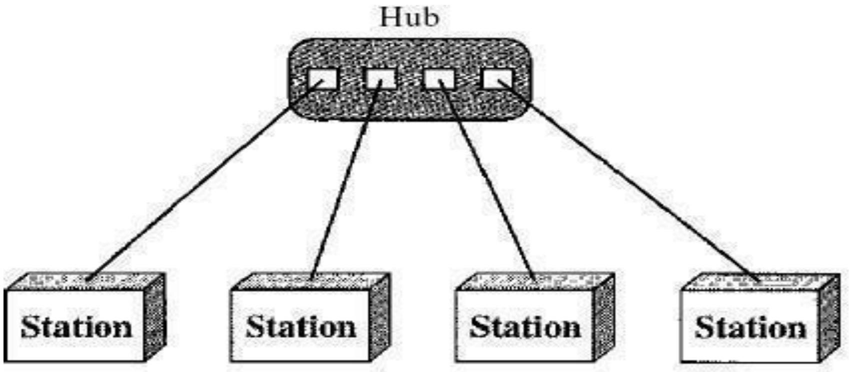
For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

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 relays the data to the other connected device.

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. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

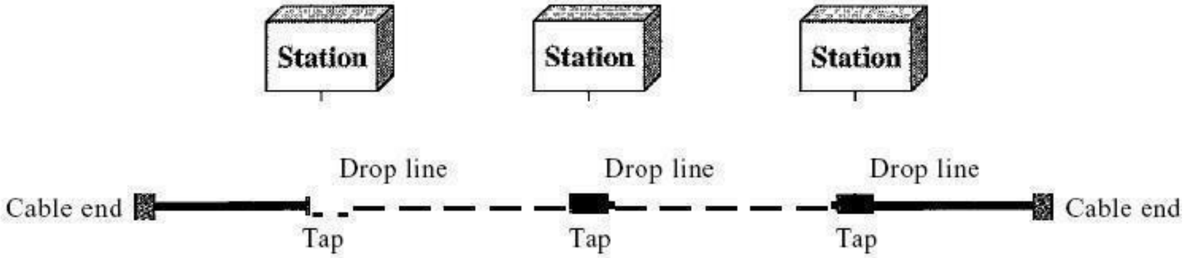
Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.



One big disadvantage of a 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:

The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network

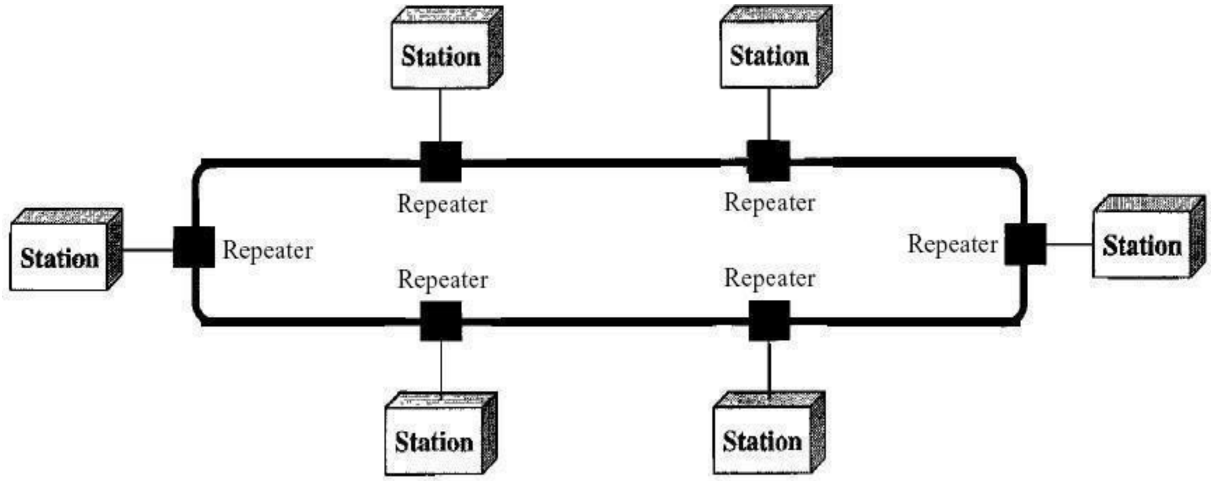


Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along 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.

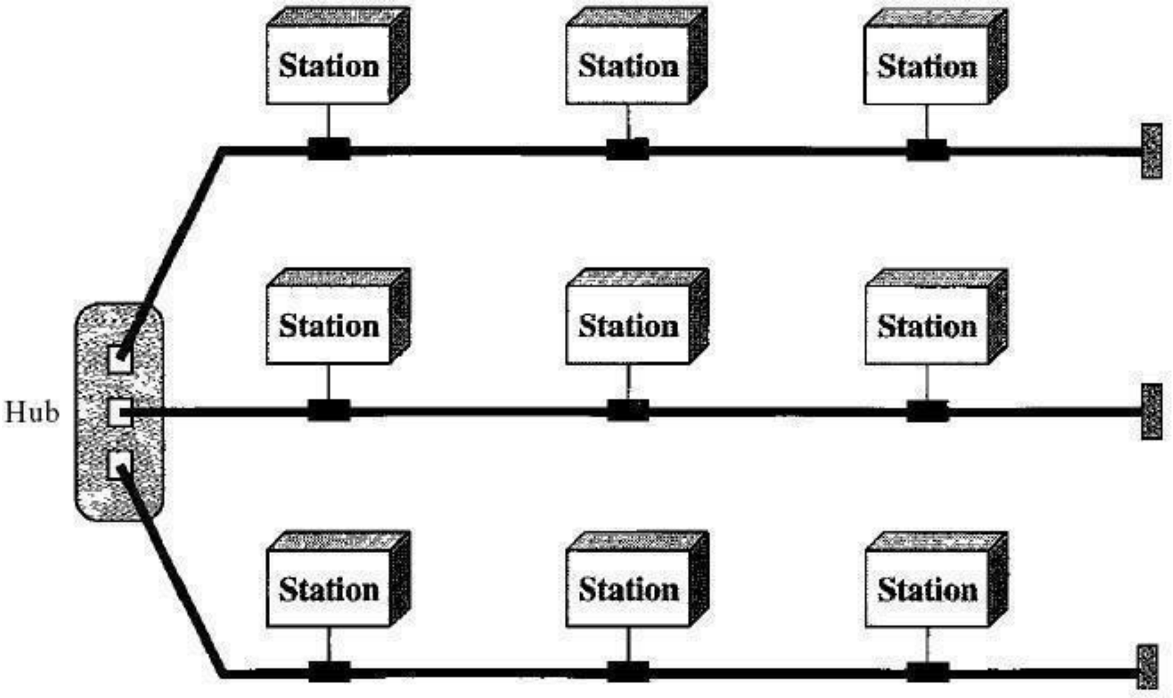
Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include 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. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

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



However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular. 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



<u>Uses of Computer Networks</u>

Had it not been of high importance, nobody would have bothered connecting computers over a network. Computer Networks with some traditional use cases at companies and for individuals and then move on to the recent developments in the area of mobile users and home networking.

1. *Business Applications*
   - i. Resource Sharing:
   - ii. Server-Client model:
   - iii. Communication Medium:
   - iv. E commerce:
2. *Home Applications*
   - i. Access to remote information
   - ii. Person-to-person communication
   - iii. Interactive entertainment
   - iv. Electronic commerce

Types or Categories of Networks

Local Area Networks:

Local area networks, generally called LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other kinds of networks by three characteristics:

(1) Their size,

(2) Their transmission technology, and

(3) Their topology.

LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management. LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors.

Newer LANs operate at up to 10 Gbps various topologies are possible for broadcast LANs. Figure1 shows two of them. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending. An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed. IEEE 802.3, popularly called Ethernet, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps. Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a Random time and tries again later.

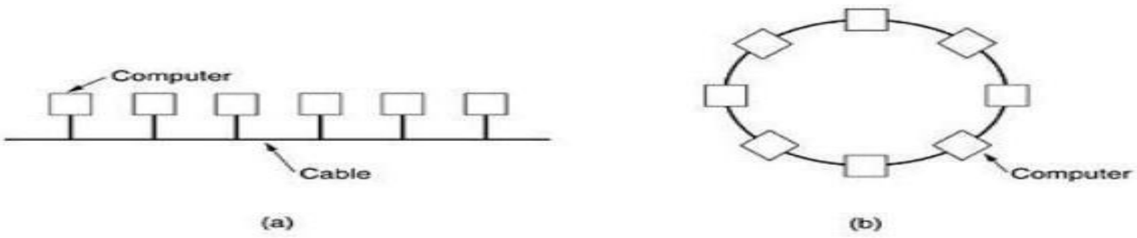


Fig.1: Two broadcast networks . (a) Bus. (b) Ring.

A second type of broadcast system is the ring. In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs. Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted. As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring. Various methods, such as having the machines take turns, are in use. IEEE 802.5 (the IBM token ring), is a ring-based LAN operating at 4 and 16 Mbps. FDDI is another example of a ring network.

Metropolitan Area Network (MAN):

A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city.

Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

Fig.2: Metropolitan area network based on cable TV.

A MAN is implemented by a standard called DQDB (Distributed Queue Dual Bus) or IEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.

Wide Area Network (WAN):

A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. Nearly all wide area networks (except those using satellites) have store-and-forward subnets. When the packets are small and all the same size, they are often called cells.

In this figure, all the packets follow the route ACE, rather than ABDE or ACDE. In some networks all packets from a given message must follow the same route; in others each packed is routed separately. Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed.

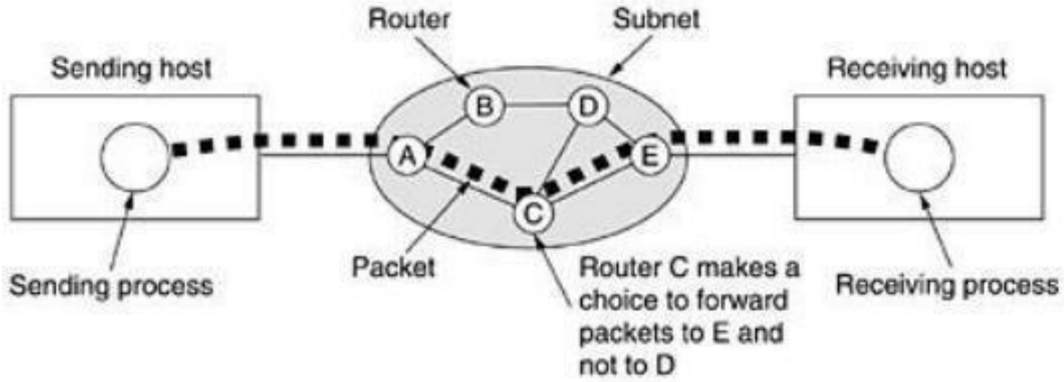


Fig.3.1: A stream of packets from sender to receiver.

Not all WANs are packet switched. A second possibility for a WAN is a satellite system. Each router has an antenna through which it can send and receive. All routers can hear the output from the satellite, and in some cases they can also hear the upward transmissions of their fellow routers to the satellite as well. Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna. Satellite networks are inherently broadcast and are most useful when the broadcast property is important.

1.3 THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks. Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication system only came into being in 1969.

In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host. By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute

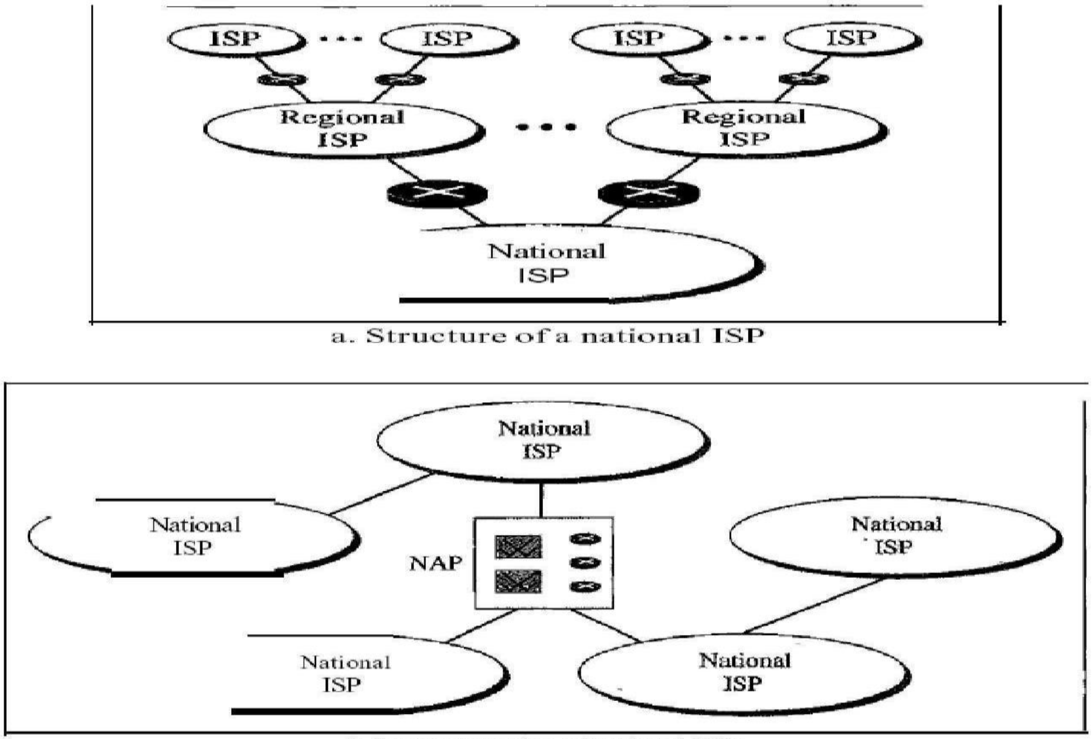
(SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol* (NCP) provided communication between the hosts.

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internet ting Projec1*. Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as

Segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet Service Providers (lSP). There are international service providers, national service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.



a. Structure of a national ISP

b. Interconnection of national ISPs

International Internet Service Providers:

At the top of the hierarchy are the international service providers that connect nations together.

National Internet Service Providers:

The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).

Regional Internet Service Providers:

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

Local Internet Service Providers:

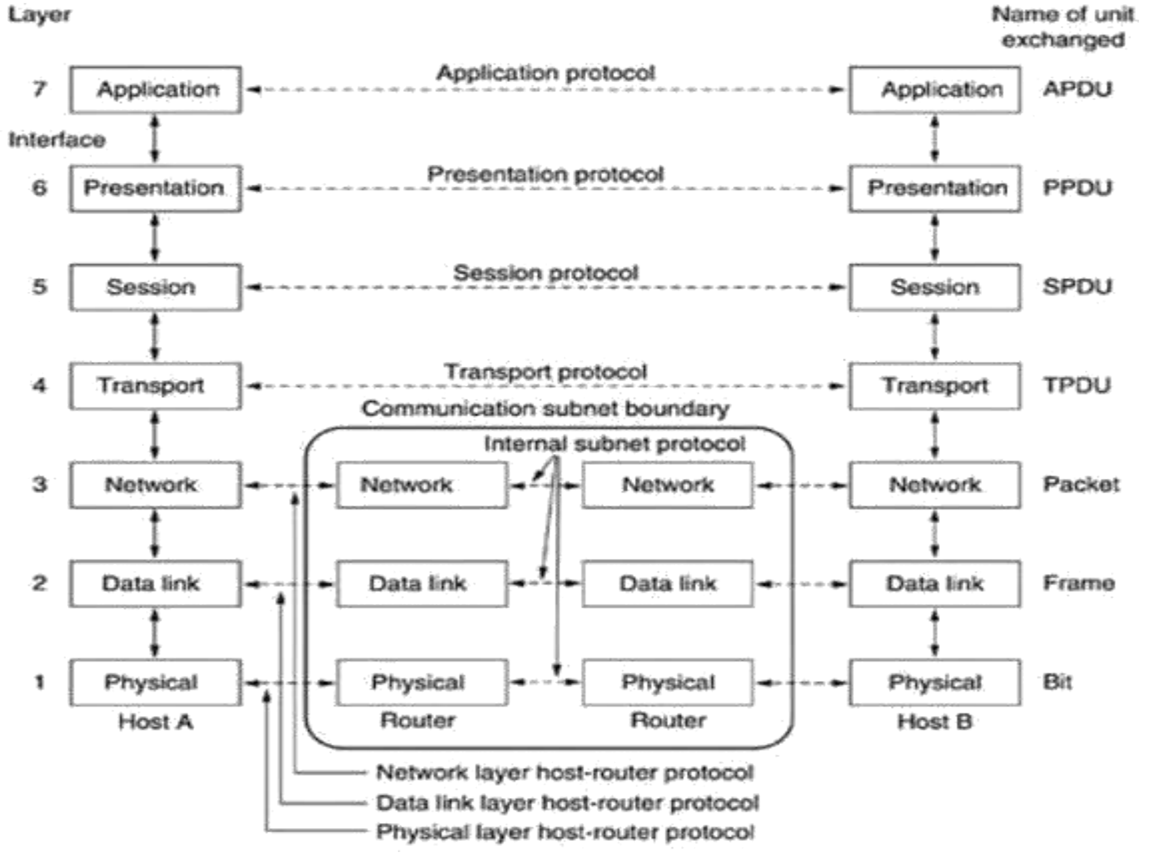
Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

1. The OSI Reference Model

The OSI model (minus the physical medium) is shown in Fig. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, 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:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. 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.



.

Fig.4: The OSI reference model

The Physical Layer:

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

The Data Link Layer:

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. 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.

Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.

The Network Layer:

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer. More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.

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 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.

The Transport Layer:

The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent. However, other possible kinds of transport service are the transporting of isolated messages, with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations. The type of service is determined when the connection is established.

The transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers,

the protocols are between each machine and its immediate neighbors, and not between the ultimate source and destination machines, which may be separated by many routers.

The Session Layer:

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

The Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

The Application Layer:

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

1.7 The TCP/IP Reference Model:

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

1. To connect multiple networks together so that they appear as a single network.
2. To survive after partial subnet hardware failures.
3. To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

1. Host-to-Network Layer
2. Internet Layer
3. Transport Layer
4. Application Layer

Host-to-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network.

Internet Layer:

This layer, called the internet layer, is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have they travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired. Note that "internet" is used here in a generic sense, even though this layer is present in the Internet.

The 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 swamp a slow receiver with more messages than it can handle.

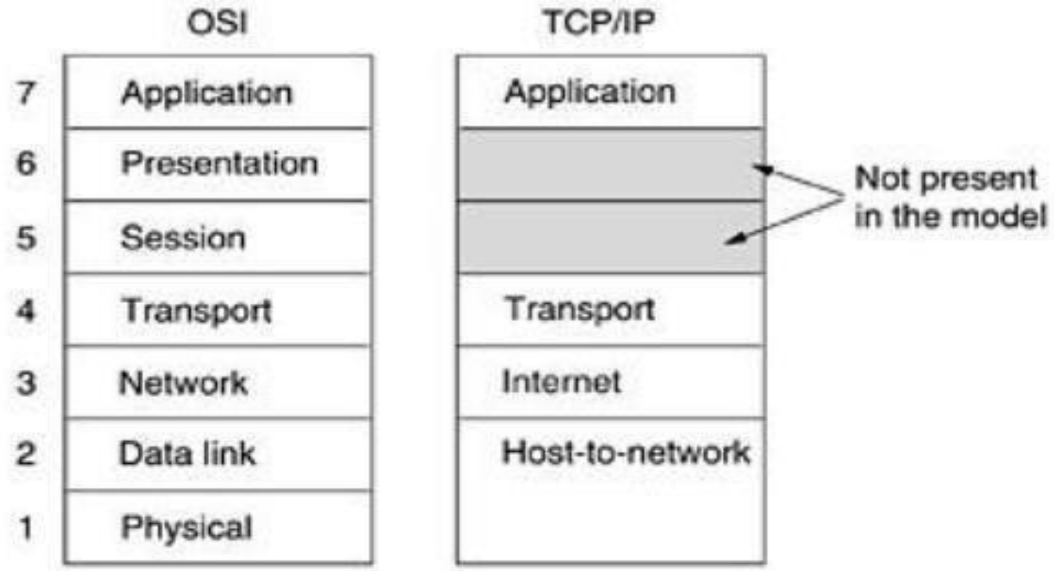


Fig.1: The TCP/IP reference model.

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 one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.2. Since the model was developed, IP has been implemented on many other networks.

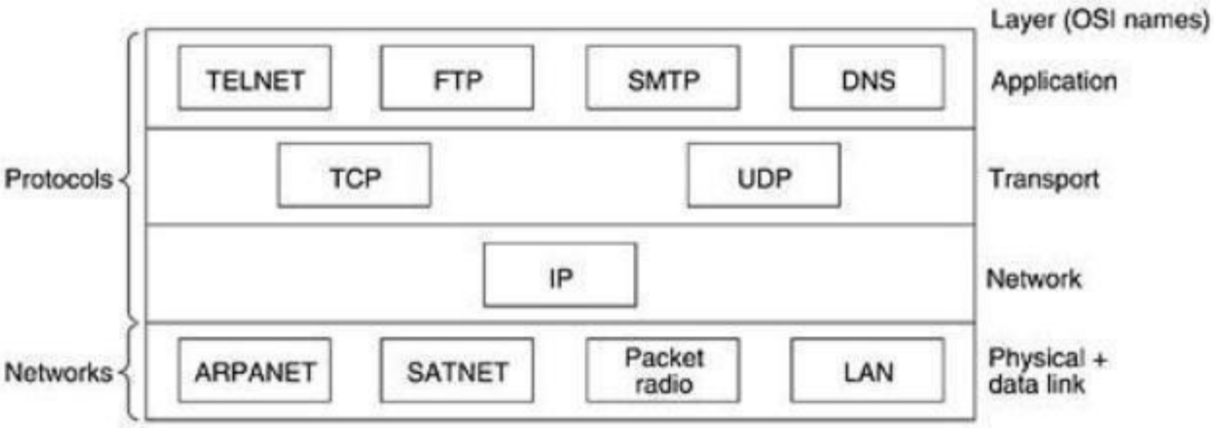


Fig.2: Protocols and networks in the TCP/IP model initially.

The Application Layer:

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

Comparison 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 users of the transport service. Despite these fundamental similarities, the two models also have many differences 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 explicit. 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.

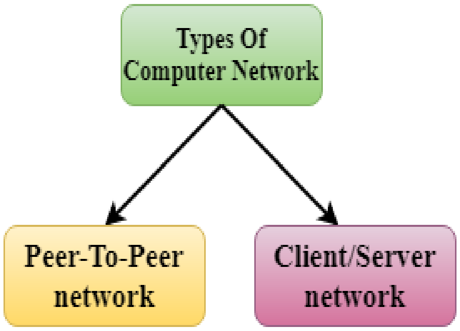
The TCP/IP model did not originally clearly distinguish between service, interface, and protocol, although people have tried to retrofit it after the fact to make it more OSI-like. For example, the only real services offered by the internet layer are SEND IP PACKET and RECEIVE IP PACKET.

Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer, where it counts (because the transport service is visible to the users). The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer

Architecture of Internet

Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

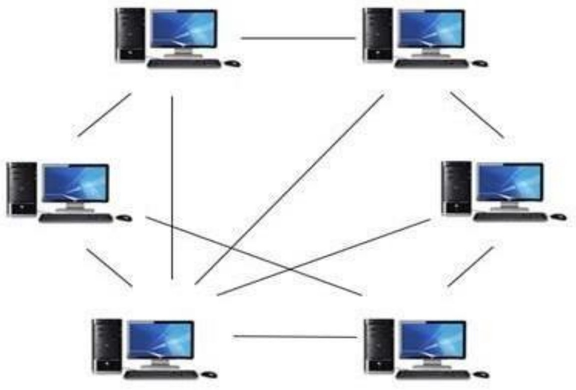
The two types of network architectures are used:



- Peer-To-Peer network
- Client/Server network

Peer-To-Peer network

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

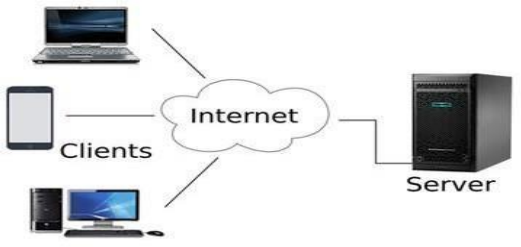
- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

Client/Server Network

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1to initiate its communication with the client 2.



Advantages Of Client/Server network:

- A Client/Server network contains the centralized system. Therefore we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client/Server network:

- Client/Server network is expensive as it requires the server with large memory.
- A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Chapter-II

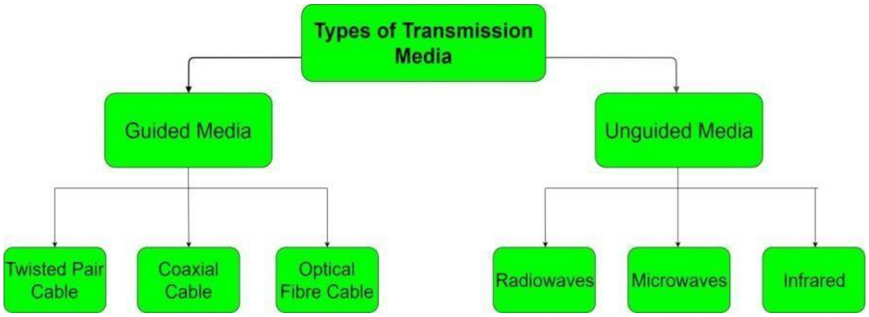
Physical Layer

I. TRANSMISSION MEDIA

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination. For example, the transmission medium for two people having a dinner conversation is the air. The air can also be used to convey the message in a smoke signal or semaphore. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

In data communications the definition of the information and the transmission medium is more specific. The transmission medium is usually free space, metallic cable or optical cable. The information is usually a signal that is the result of conversion of data from another form.

Transmission Media is broadly classified into the following types:

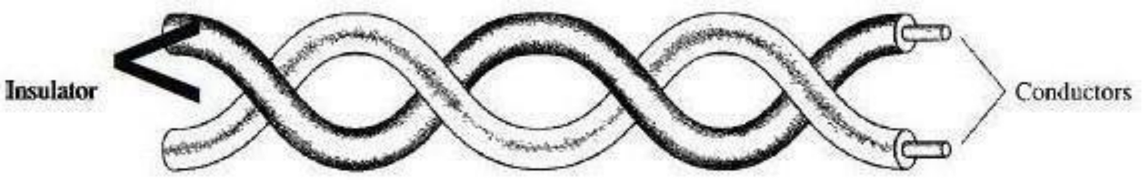


Guided Media

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

1. Twisted-Pair Cable

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



One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther). This results in a difference at the receiver. By twisting the pairs, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

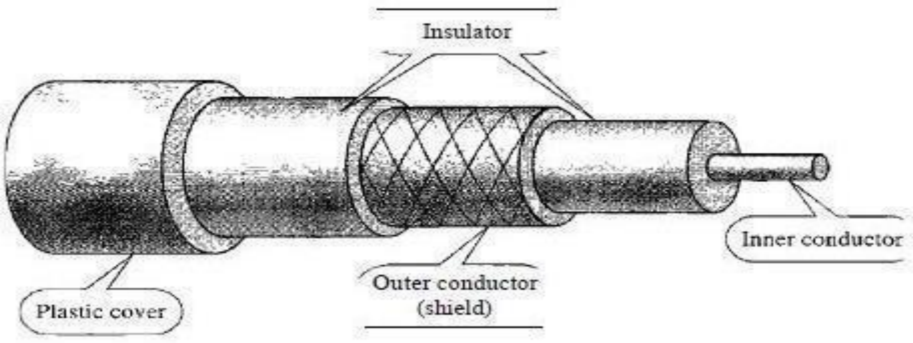
Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office-commonly consists of

Unshielded twisted pair cables. The DSL line that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables. Local-area networks, such as lOBase-T and lOOBase-T, also use twisted-pair cables.

2. Coaxial Cable

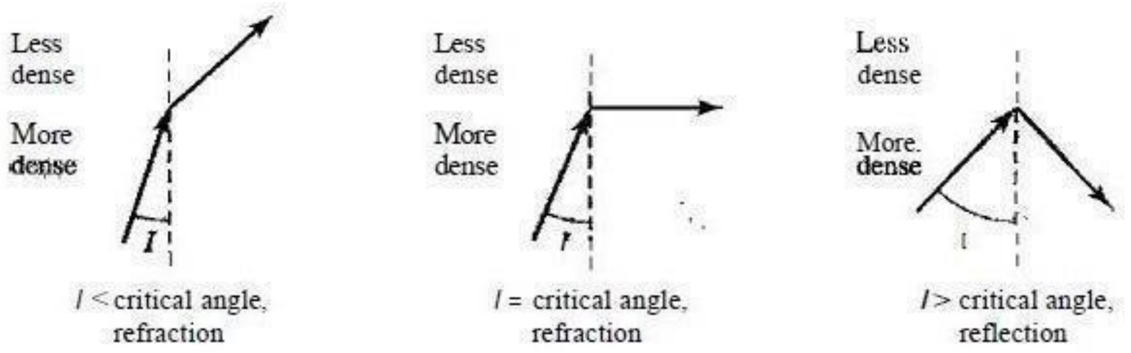
Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover (below figure).



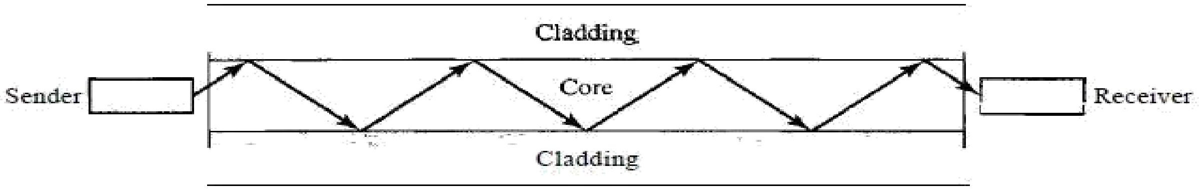
Applications

Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber-optic cable. Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Later, however, cable TV providers replaced most of the media with fiber-optic cable; hybrid networks use coaxial cable only at the network boundaries, near the consumer premises. Cable TV uses RG-59 coaxial cable. Another common application of coaxial cable is in traditional Ethernet LANs. Because of its high bandwidth, and consequently high data rate, coaxial cable was chosen for digital transmission in early Ethernet LANs.

3. <u>Fiber Optic Cable:</u> A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction. Figure 7.10 shows how a ray of light changes direction when going from a more dense to a less dense substance.

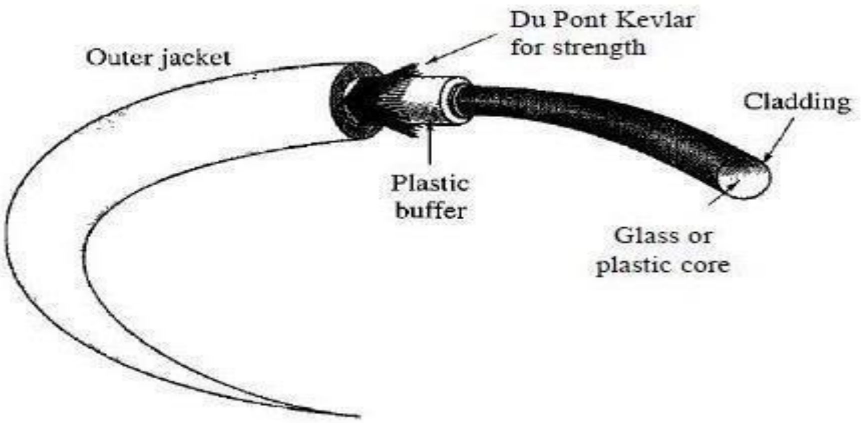

Less dense
More dense
I
I < critical angle, refraction
Less dense
More dense
I
I = critical angle, refraction
Less dense
More. dense
I
I > critical angle, reflection

As the figure shows, if the angle of incidence *I* (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. Note that the critical angle is a property of the substance, and its value differs from one substance to another.



<u>Cable Composition</u>

Figure 7.14 shows the composition of a typical fiber-optic cable. The outer jacket is made of either PVC or Teflon. Inside the jacket are Kevlar strands to strengthen the cable. Kevlar is a strong material used in the fabrication of bulletproof vests. Below the Kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.



Applications

Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer data at a rate of 1600 Gbps. The SONET network provides such a backbone. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber. Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber

Advantages

Fiber-optic cable has several advantages over metallic cable (twisted pair or coaxial).

1. **Higher bandwidth**. Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

2. **Less signal attenuation**. Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

3. **Immunity to electromagnetic interference**. Electromagnetic noise cannot affect fiber-optic cables.

4. **Resistance to corrosive materials**. Glass is more resistant to corrosive materials than copper.

Disadvantages

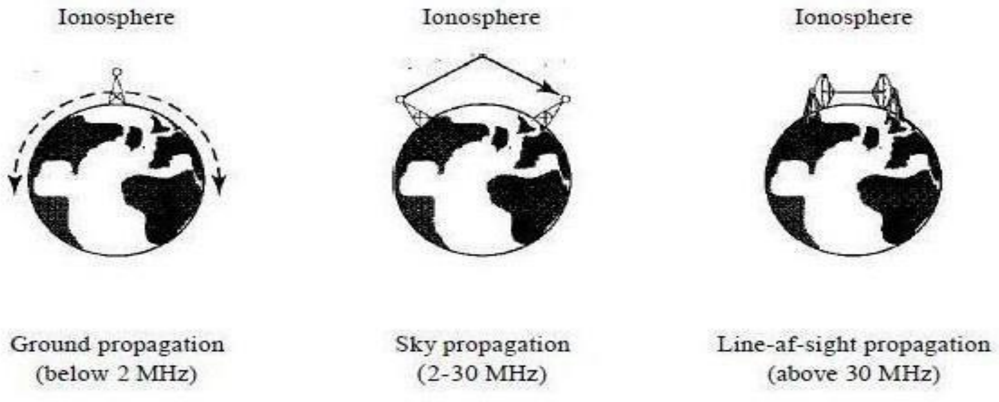
There are some disadvantages in the use of optical fiber.

1. **Installation and maintenance**. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
2. **Unidirectional light propagation**. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

3. **Cost**. The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

UNGUIDED MEDIA: WIRELESS

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.



Ground propagation (below 2 MHz)

Sky propagation (2-30 MHz)

Line-af-sight propagation (above 30 MHz)

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in Figure 7.18. In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth.

These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance. In sky propagation, higher-frequency radio waves radiate upward into the ionosphere where they are reflected back to earth.

This type of transmission allows for greater distances with lower output power. In line of sight propagation, very high frequency signals are transmitted in straight lines directly from antenna to antenna. Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

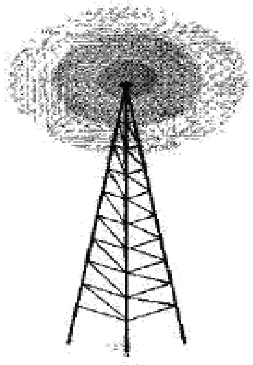
1. Radio Waves

Waves ranging in frequencies between 3 kHz and 1 GHz are called radio waves. Radio waves, for the most part, are omni directional. When an antenna transmits radio waves, they are

propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.

Omni directional Antenna

Radio waves use omni directional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas. Below figure 7.20 shows an omni directional antenna.



Applications

The omni directional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

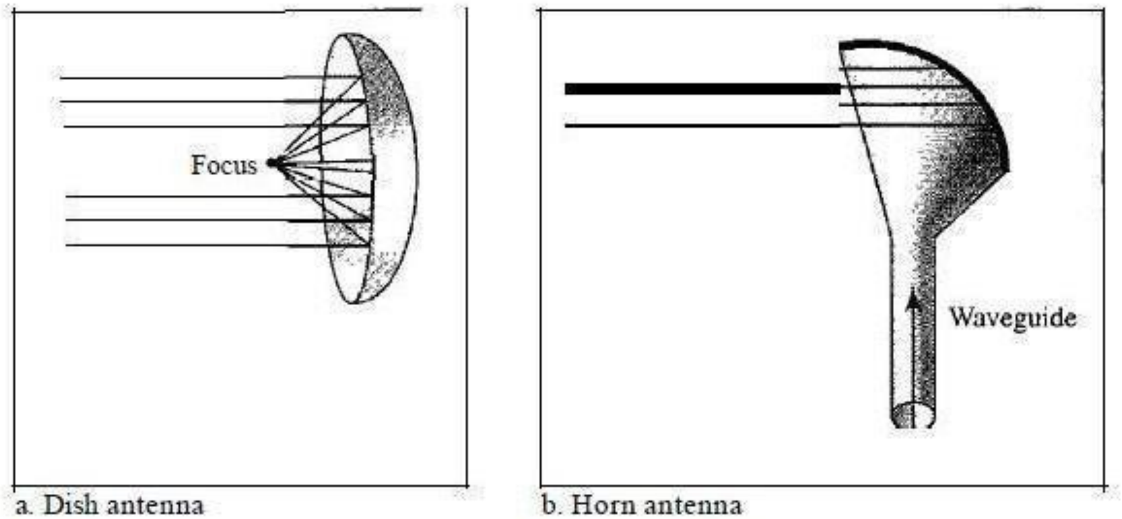
2. Microwaves

Electromagnetic waves having frequencies between I and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The following describes some characteristics of microwave propagation:

1. Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles do not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
2. Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn (see below figure). A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus.



a. Dish antenna b. Horn antenna

3. Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room. When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

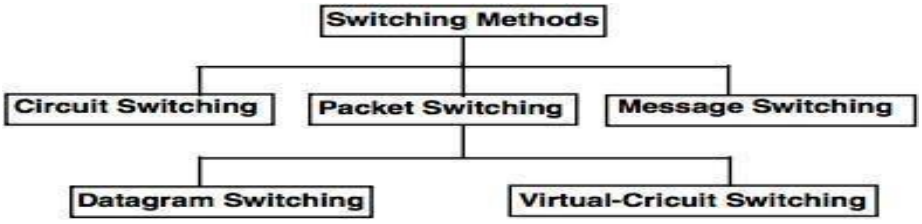
The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate. The *Infrared Data Association* (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers. For example, some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC.

SWITCHING

Introduction

A Network Switch is a constituent of computer network that connects two network slices and/or two network devices (switches or routers) together. Switch can be termed as a network bridge with multiple ports which helps to process and route packets at data link layer of the OSI reference model. There are some switches which have capabilities to process data at the upper layers (network layer and above). Those switches are often termed as *multilayer switches.*

For data transfer, different types of switching methods are available. They are



Types of Switching

I. Circuit Switching

- Circuit switched network consists of a set of switches connected by physical links.
- In circuit switched network, two nodes communicate with each other over a dedicated communication path.

- There is a need of pre-specified route from which data will travel and no other data is permitted.
- Before starting communication, the nodes must make a reservation for the resources to be used during the communication.
- In this type of switching, once a connection is established, a dedicated path exists between both ends until the connection is terminated.

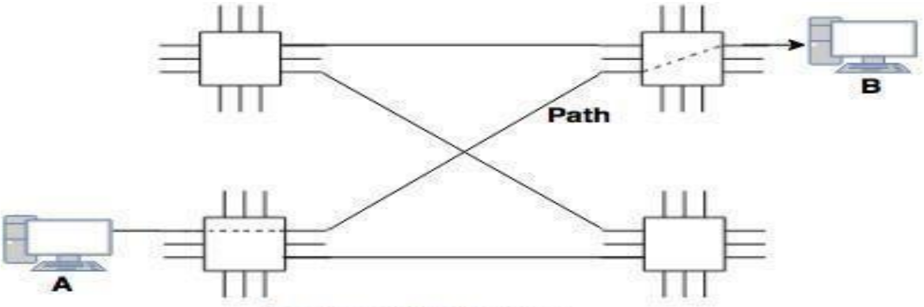


Fig: Circuit Switching

<u>Advantages of Circuit Switching:</u>

- The dedicated path/circuit established between sender and receiver provides a guaranteed data rate.
- Once the circuit is established, data is transmitted without any delay as there is no waiting time at each switch.
- Since a dedicated continuous transmission path is established, the method is suitable for long continuous transmission.

Disadvantages of Circuit Switching:

- As the connection is dedicated it cannot be used to transmit any other data even if the channel is free.
- It is inefficient in terms of utilization of system resources. As resources are allocated for the entire duration of connection, these are not available to other connections.
- Dedicated channels require more bandwidth.
- Prior to actual data transfer, the time required to establish a physical link between the two stations is too long.

II. Packet Switching

- In packet switching, messages are divided into packets of fixed or variable size.
- The size of packet is decided by the network and the governing protocol.
- Resource allocation for a packet is not done in packet switching.
- Resources are allocated on demand.
- The resource allocation is done on first-come, first-served basis.

- Each switching node has a small amount of buffer space to hold packets temporarily.
- If the outgoing line is busy, the packet stays in queue until the line becomes available.

Packet switching method uses two routing methods: 1.

Datagram Packet Switching

- Datagram packet switching is normally implemented in the network layer.
- In datagram network, each packet is routed independently through the network.
- Each packet carries a header that contains the full information about the destination.
- When the switch receives the packet, the destination address in the header of the packet is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.

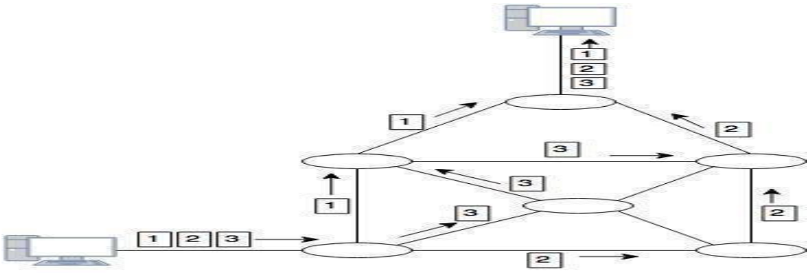


Fig: Datagram Packet Switching

2. Virtual Circuit Packet Switching

- Virtual circuit packet switching is normally done at the data link layer.
- Virtual circuit packet switching establishes a fixed path between a source and a destination to transfer the packets.
- It is also called as **connection oriented network.**

->A source and destination have to go through three phases in a virtual circuit packet switching:

I. Setup phase

ii. Data transfer phase

iii. Connection release phase

- A logical connection is established when a sender sends a setup request to the receiver and the receiver sends back an acknowledgement to the sender if the receiver agree.
- All packets belonging to the same source and destination travel the same path.
- The information is delivered to the receiver in the same order as transmitted by the sender.

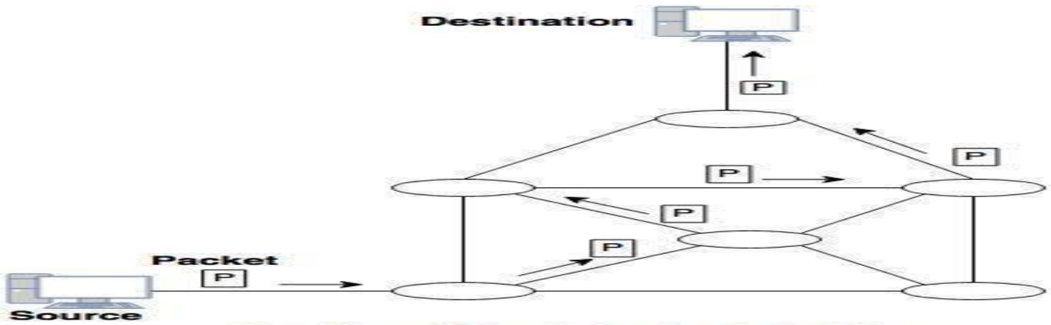


Fig: Virtual Circuit Packet Switching

Advantages of Packet Switching:

- Efficient use of Network.
- Easily get around broken bits or packets.
- Circuit Switching charges user on the distance and duration of connection but Packet Switching charges users only on the basis of duration of connectivity.

Disadvantages of Packet Switching:

- In Packet Switching Packets arriving in wrong order.
- Takes Transmission delay.

III. Message Switching

- In message switching, it is not necessary to establish a dedicated path between transmitter and receiver.
- In this, each message is routed independently through the network.
- **Store and forward –** The intermediate nodes have the responsibility of transferring the entire message to the next node. Hence, each node must have storage capacity. A message will only be delivered if the next hop and the link connecting it are both available, otherwise it'll be stored indefinitely. A store-and-forward switch forwards a message only if sufficient resources are available and the next hop is accepting data. This is called the store-and-forward property.

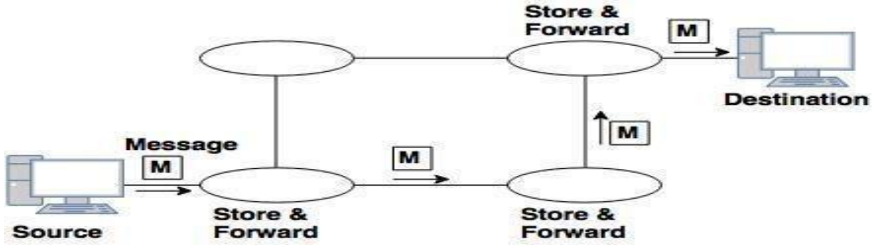


Fig: Message Switching

UNIT-II
Chapter-I
Data Link Layer

I. Introduction

The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include *framing, addressing, flow control, error control, and media access control.*

II. DATA LINK LAYER DESIGN ISSUES

The following are the data link layer design issues

1. Services Provided to the Network Layer

The network layer wants to be able to send packets to its neighbors without worrying about the details of getting it there in one piece.

2. Framing

Group the physical layer bit stream into units called frames. Frames are nothing more than "packets" or "messages". By convention, we use the term "frames" when discussing DLL.

3. Error Control

Sender checksums the frame and transmits checksum together with data. Receiver re-computes the checksum and compares it with the received value.

4. Flow Control

Prevent a fast sender from overwhelming a slower receiver.

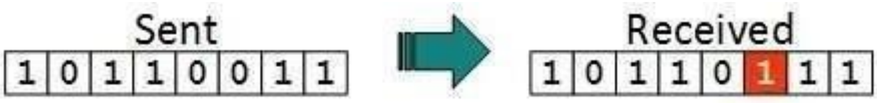
III. Error Detection & Correction

There are many reasons such as noise, cross-talk etc., which may help data to get corrupted during transmission. The upper layers work on some generalized view of network architecture and are not aware of actual hardware data processing. Hence, the upper layers expect error-free transmission between the systems. Most of the applications would not function expectedly if they receive erroneous data. Applications such as voice and video may not be that affected and with some errors they may still function well.

Types of Errors

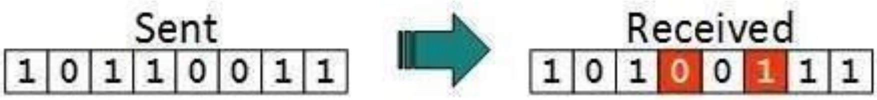
There may be three types of errors:

- **Single bit error**



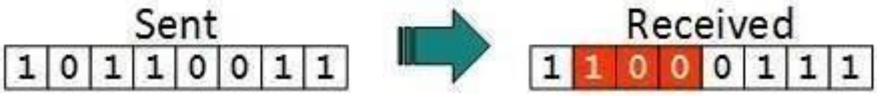
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bits in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

Errors in the received frames are detected by means of

(i)Parity Check and

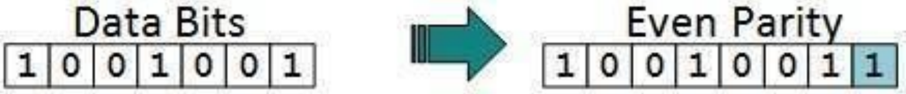
(ii)Cyclic Redundancy Check (CRC).

In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

(i) Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

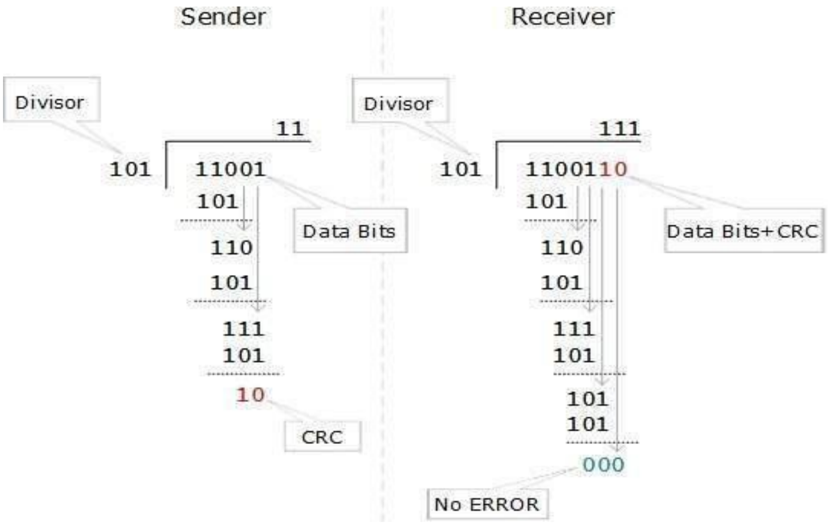


The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bits are erroneous, then it is very hard for the receiver to detect the error.

(ii) Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as code words.



At the other end, the receiver performs division operation on code words using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

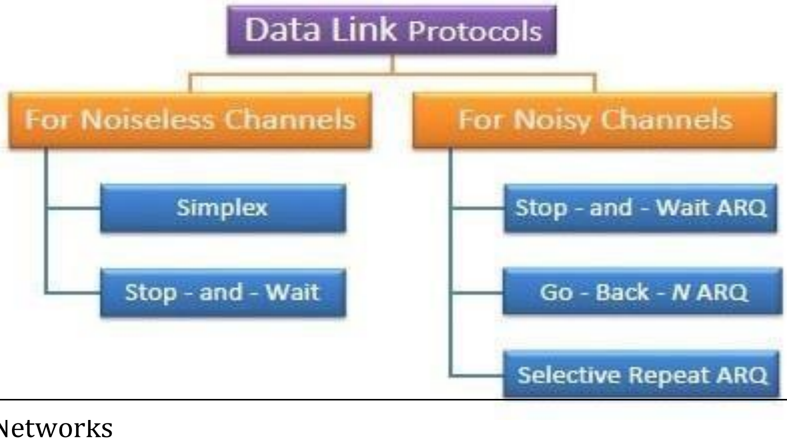
The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

IV Elementary Data Link Protocols

Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control. Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes.

Types of Data Link Layer Protocols

Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



Simplex Protocol

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong. It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channelas soon as they are available its buffer. The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.

Stop – and – Wait Protocol

Stop – and – Wait protocol is for noiseless channel too. It provides unidirectional data transmission without any error control facilities. However, it provides for flow control so that a fast sender does not drown a slow receiver. The receiver has a finite buffer size with finite processing speed. The sender can send a frame only when it has received indication from the receiver that it is available for further data processing.

Stop – and – Wait ARQ

Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ) is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.

Go – Back – N ARQ

Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Selective Repeat ARQ

This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

V. Sliding Window Protocols

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.

In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working Principle

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1. Consequently, the size of the sending window is 2^n-1. Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.

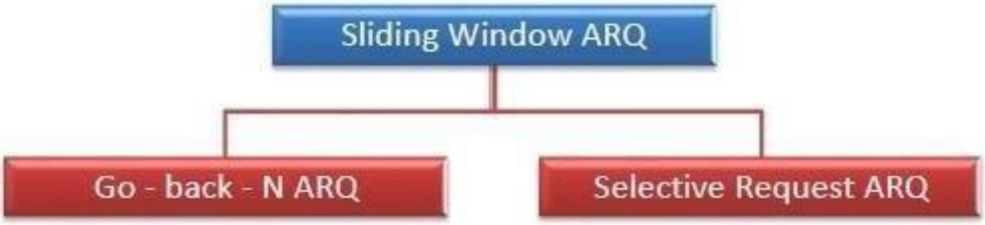
The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

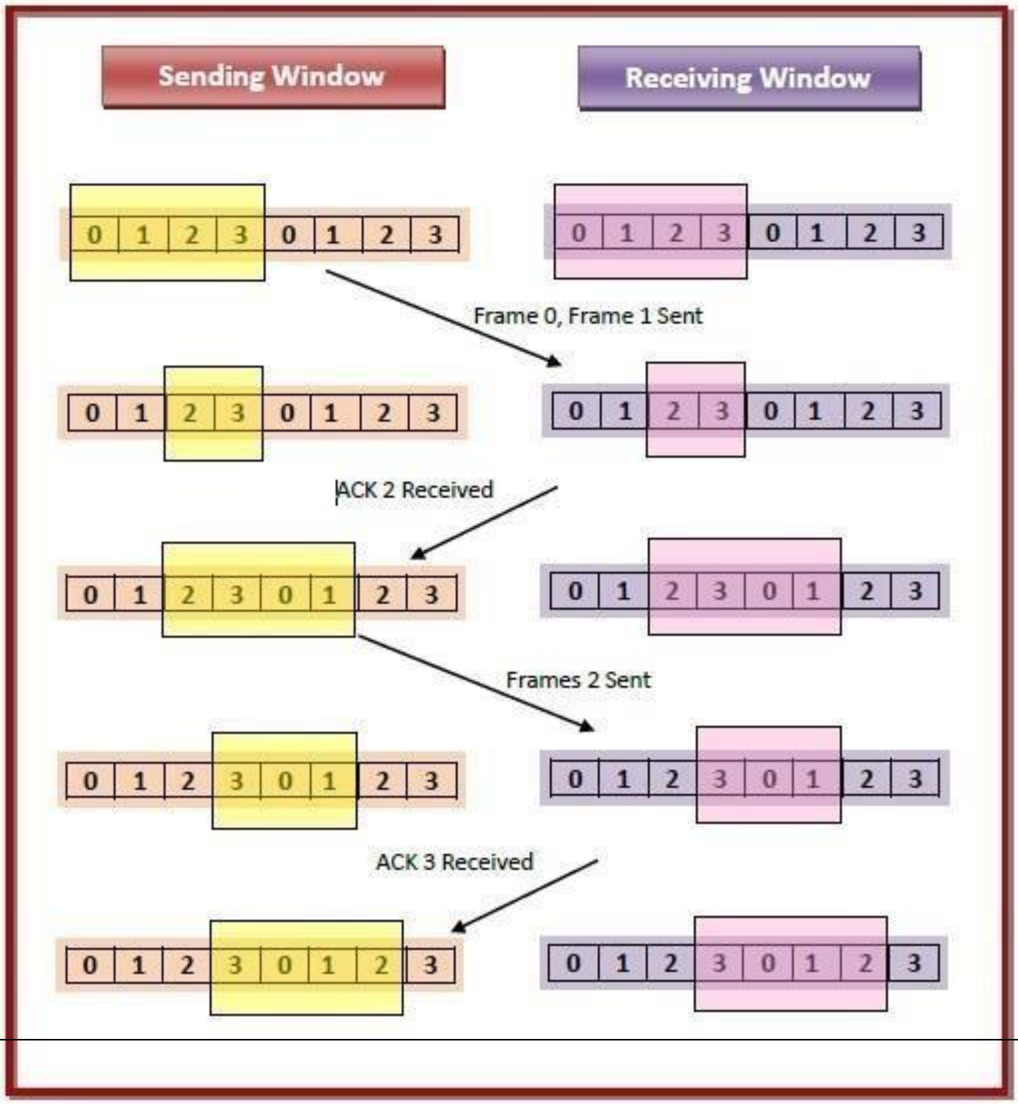
Example

Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.

Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories −





- **Go – Back – *N* ARQ**

Go – Back – *N* ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

- **Selective Repeat ARQ**

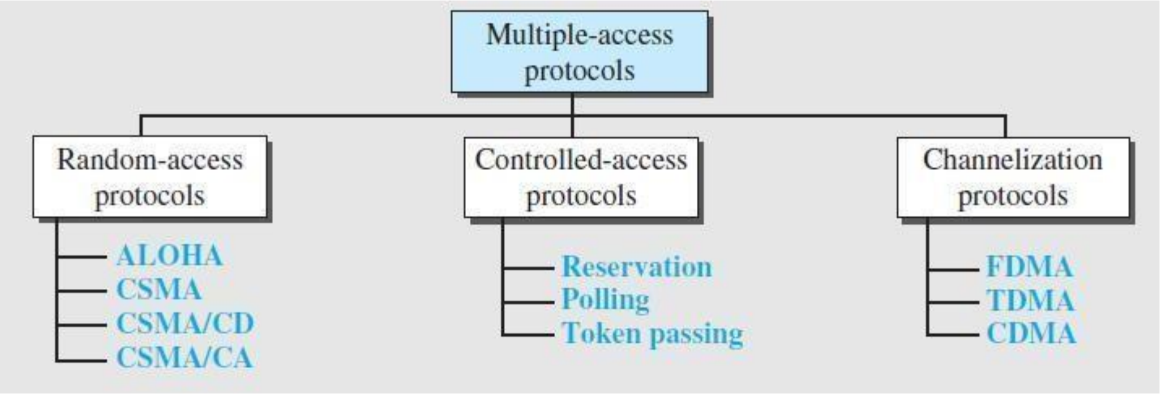
This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

Chapter-II

Multiple Access Protocols

I. MULTIPLE ACCESS PROTOCOLS

The multiple access protocols can be broadly classified into three categories namely Random access Protocols, Controlled access Protocols and Channelization Protocols (as given in below figure). Let us discuss in detail about the different protocols which are classified and as shown in below figure.



1. **Random Access Protocol:** In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium’s state(idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

(a) ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

Slotted Aloha:

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

(b) CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense The medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle.

However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data.

However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent :** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent :** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent :** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) CSMA/CD

Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.

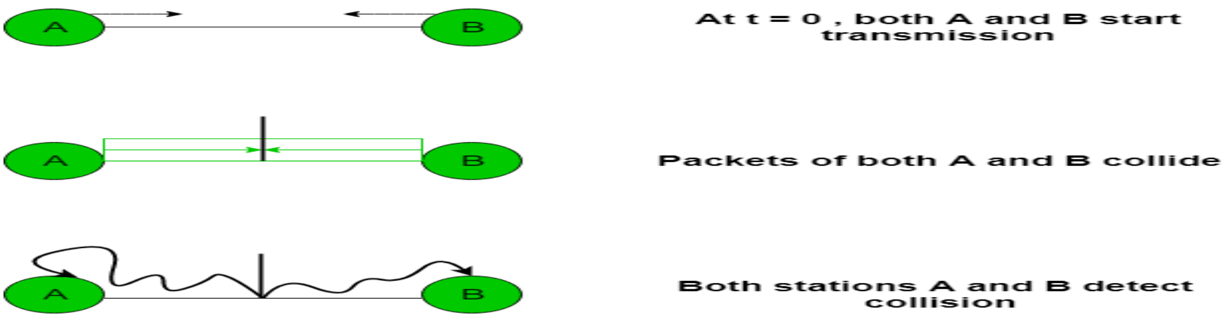
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Back-off Algorithm for CSMA/CD

Back-off algorithm is a **collision resolution** mechanism which is used in random access MAC protocols (CSMA/CD). This algorithm is generally used in Ethernet to schedule re-transmissions after collisions.

If a collision takes place between 2 stations, they may restart transmission as soon as they can after the collision. This will always lead to another collision and form an infinite loop of collisions leading to a deadlock. To prevent such scenario back-off algorithm is used.

Let us consider an scenario of 2 stations A and B transmitting some data:


A
B
At t = 0 , both A and B start transmission
A
B
Packets of both A and B collide
A
B
Both stations A and B detect collision

After a collision, time is divided into discrete slots (**T_{slot}**) whose length is equal to 2t, where t is the maximum propagation delay in the network.

The stations involved in the collision randomly pick an integer from the set K i.e {0, 1}. This set is called the contention window. If the sources collide again because they picked the same integer, the contention window size is doubled and it becomes {0, 1, 2, 3}.

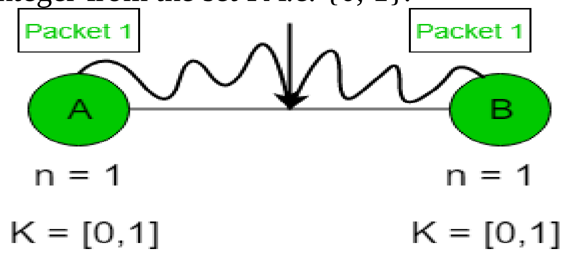
Now the sources involved in the second collision randomly pick an integer from the set {0, 1, 2, 3} and wait that number of time slots before trying again. Before they try to transmit, they listen to the channel and transmit only if the channel is idle. This causes the source which picked the smallest integer in the contention window to succeed in transmitting its frame.

So, Back-off algorithm defines a *waiting time for the stations involved in collision*, i.e. for how much time the station should wait to re-transmit.

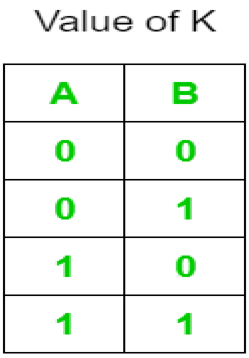
Example –

Case-1 :

Suppose 2 stations A and B start transmitting data (Packet 1) at the same time then, collision occurs. So, the collision number n for both their data (Packet 1) = 1. Now, both the station randomly pick an integer from the set K i.e. {0, 1}.



Value of K



A	B
0	0
0	1
1	0
1	1

- **When both A and B choose K = 0**
  –> Waiting time for A = 0 * T_{slot} = 0
  Waiting time for B = 0 * T_{slot} = 0

- Therefore, both stations will transmit at the same time and hence collision occurs.

Probability that A wins = 5/8

Probability that B wins = 1/8

Probability of collision = 2/8

So, probability of collision decreases as compared to Case 1.

Advantage –

- Collision probability decreases exponentially.

Disadvantages –

- **Capture effect:** Station who wins ones keeps on winning.
- Works only for 2 stations or hosts.

(d) CSMA/CA –

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred.

To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

1. **Inter frame space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called 'Inter frame space' or 'IFS'. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:

In this, the data is sent by that station which is approved by all other stations.

Controlled Access Protocols

In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid collision of messages on shared medium.

The three controlled-access methods are:

1. Reservation

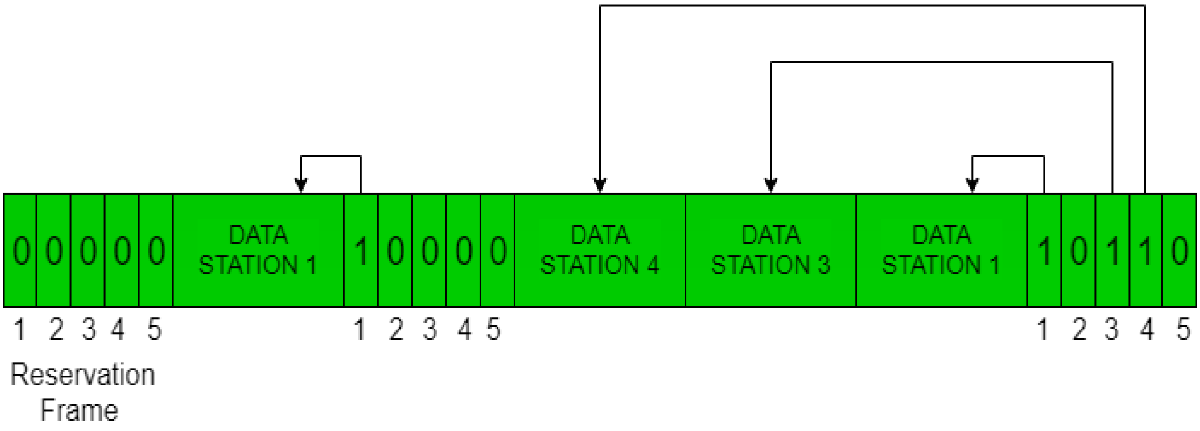
2. Polling

3. Token Passing

Reservation

- In the reservation method, a station needs to make a reservation before sending data.
- The time line has two kinds of periods:
  1. Reservation interval of fixed time length
  2. Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.
- In general, i th station may announce that it has a frame to send by inserting a 1 bit into i th slot. After all N slots have been checked, each station knows which stations wish to transmit.

The following figure shows a situation with five stations and a five slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.

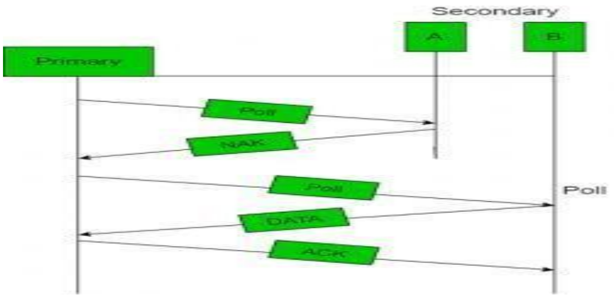


Polling

- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- Although all nodes receive the message but the addressed one responds to it and sends data,

if any. If there is no data, usually a “poll reject”(NAK) message is sent back.

- Problems include high overhead of the polling messages and high dependence on the reliability of the controller.

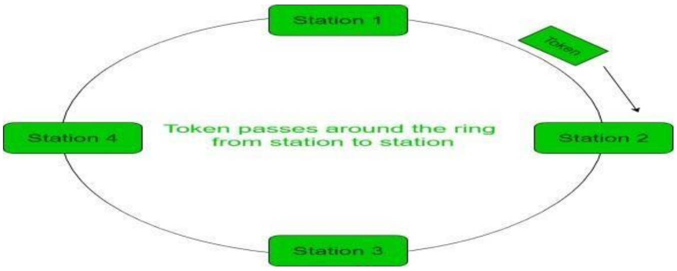


Efficiency

Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then,

Token Passing

- In token passing scheme, the stations are connected logically to each other in form ofring and access of stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in the some predefined order.
- After sending a frame, each station must wait for all N stations (including itself) to send the token to their neighbors and the other N – 1 stations to send a frame, if they have one.
- There exists problems like duplication of token or token is lost or insertion of new station, removal of a station, which need be tackled for correct and reliable operation of this scheme.



Performance

Performance of token ring can be concluded by 2 parameters:-

1. **Delay**, which is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.
2. **Throughput**, which is a measure of the successful traffic.

II. Ethernet at the Physical Layer

Ethernet is the most popular Local Area Network architecture that was jointly developed by Digital Equipment Corporation, Intel Corporation and Xerox Corporation.

It consists of certain specifications and standards as well as hardware devices and components.

Ethernet provides services corresponding to physical layer and data link layer of the OSI reference model. Each Ethernet physical layer protocol has a three part name that summarizes its characteristics. The components specified in the naming convention correspond to LAN speed, signaling method, and physical media type.

The following table summarizes the differences between the various physical-layer specifications of Ethernet:

Types of LAN Technology

Ethernet

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission.

- A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps).
- Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure.

Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet:

(i) 100 BASE-TX for use with level 5 UTP cable

(ii) 100 BASE-FX for use with fiber-optic cable

(iii) 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable.

The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Gigabit Ethernet

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as “gigabit-Ethernet-over-copper” or 1000Base-T.

Giga Ethernet is a version of Ethernet that runs at speeds **10 times faster than 100Base-T.** It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone.

Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

10 Gigabit Ethernet

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined.

III. Collision-Free Protocols

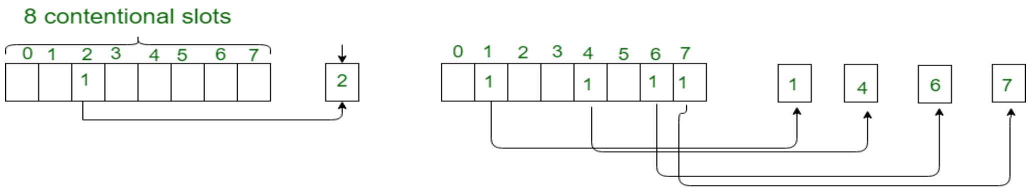
Almost collisions can be avoided in **CSMA/CD**. they can still occur during the contention period. the collision during contention period adversely affects the system performance, this happens when the cable is long and length of packet are short. This problem becomes serious as fiber optics network come into use. Here we shall discuss some protocols that resolve the collision during the contention period.

- Bit-map Protocol
- Binary Countdown
- Limited Contention Protocols
- The Adaptive Tree Walk Protocol

1. Bit-map Protocol:

Bit map protocol is collision free Protocol in In bitmap protocol method, each contention period consists of exactly N slots. if any station has to send frame, then it transmits a 1 bit in the respective slot. For example if station 2 has a frame to send, it transmits a 1 bit during the second slot.

In general Station 1 Announce the fact that it has a frame questions by inserting a 1 bit into slot 1. In this way, each station has complete knowledge of which station wishes to transmit. There will never be any collisions because everyone agrees on who goes next. Protocols like this in which the desire to transmit is broadcasting for the actual transmission are called *Reservation Protocols*.



A Bit-map Protocol.

For analyzing the performance of this protocol, We will measure time in units of the contention bits slot, with a data frame consisting of *d* time units. Under low load conditions, the bitmap will simply be repeated over and over, for lack of data frames. All the stations have something to send all the time at high load, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame.

Generally, high numbered stations have to wait for half a scan before starting to transmit low numbered stations have to wait for half a scan(N/2 bit slots) before starting to transmit, low numbered stations have to wait on an average 1.5 N slots.

2. Binary Countdown:

Binary countdown protocol is used to overcome the overhead 1 bit per binary station. In binary countdown, binary station addresses are used. A station wanting to use the channel broadcast its address as binary bit string starting with the high order bit. All addresses are assumed of the same length. Here, we will see the example to illustrate the working of the binary countdown.

In this method, different station addresses are Red together who decide the priority of transmitting. Other three stations 1001, 1100, 1011 continue. The next bit is 1 at station 1100, Swiss station 1011 and 1001 give up. Then station 110 starts transmitting a frame, after which another bidding cycle starts.

3. Limited Contention Protocols:

- Collision based protocols (pure and slotted ALOHA, CSMA/CD) are good when the network load is low.
- Collision free protocols (bitmap, binary Countdown) are good when load is high.
- How about combining their advantages

4. Adaptive Tree Walk Protocol:

- partition the group of station and limit the contention for each slot.
- Under light load, everyone can try for each slot like aloha
- Under heavy load, only a group can try for each slot
- **How do we do it:**
  1. treat every stations as the leaf of a binary tree

2. first slot (after successful transmission), all stations can try to get the slot(under the root node).

   if no conflict, fine in case of conflict, only nodes under a sub tree get to try for the next one. (depth first search)

IV. The Medium Access Sublayer (MAC)

This section deals with broadcast networks and their protocols. The basic idea behind broadcast networks is how to determine who gets to use the channel when many users want to transmit over it. The protocols used to determine who goes next on a multi access channel belong to a sub layer of the data link layer called **MAC.**

V. Data Link Layer Switching

Bridges

“A device used to connect two separate Ethernet networks into one extended Ethernet. Bridges only forward packets between networks that are destined for the other network.

Types of Bridges:

1. Transparent basic bridge
2. Source routing bridge
3. Transparent learning bridge
4. Transparent spanning bridge

Spanning tree protocol (STP)

Where two bridges are used to interconnect the same two computer network segments, spanning tree is a protocol that allows the bridges to exchange information so that only one of them will handle a given message that is being sent between two computers within the network. The spanning tree protocol prevents the condition known as a *bridge loop*.

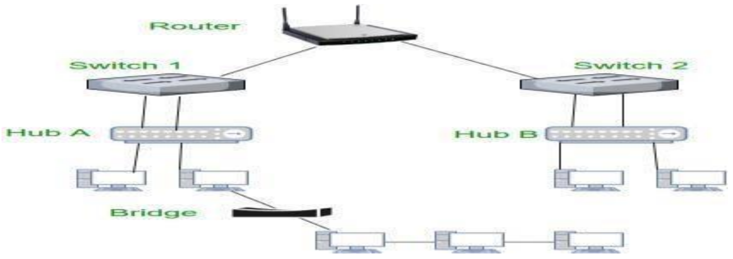
Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and B router)

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

3)Switch – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct portonly.

4. **Routers** – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch .

Unit-III

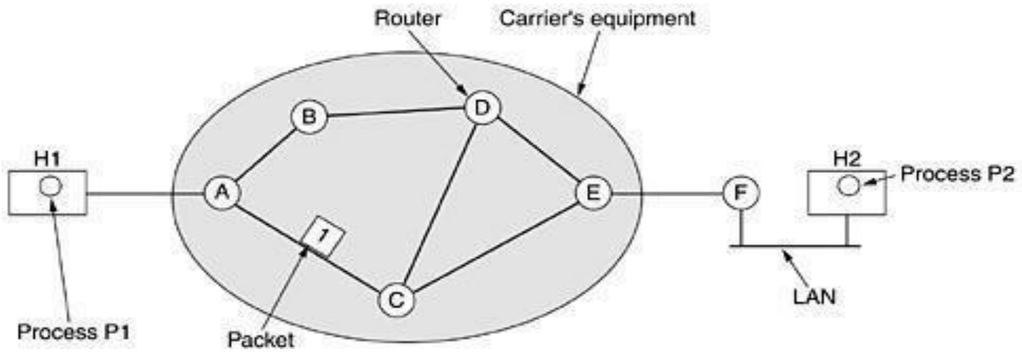
Network Layer

I. Network Layer Design Issues

1. Store-and-Forward Packet Switching

The major components of the system are the carrier's equipment (routers connected by transmission lines), shown inside the shaded oval, and the customers' equipment, shown outside the oval.
We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software, and protocols, it is probably no different from the carrier's routers.

Figure . The environment of the network layer protocols.



This equipment is used as follows. A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier. The packet is stored there until it has fully arrived so the checksum can be verified.

Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

2. Services Provided to the Transport Layer

The network layer provides services to the transport layer at the network layer/transport layer interface. An important question is what kind of services the network layer provides to the transport layer.
The network layer services have been designed with the following goals in mind.

1. The services should be independent of the router technology.

2. The transport layer should be shielded from the number, type, and topology of the routers present.

3. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

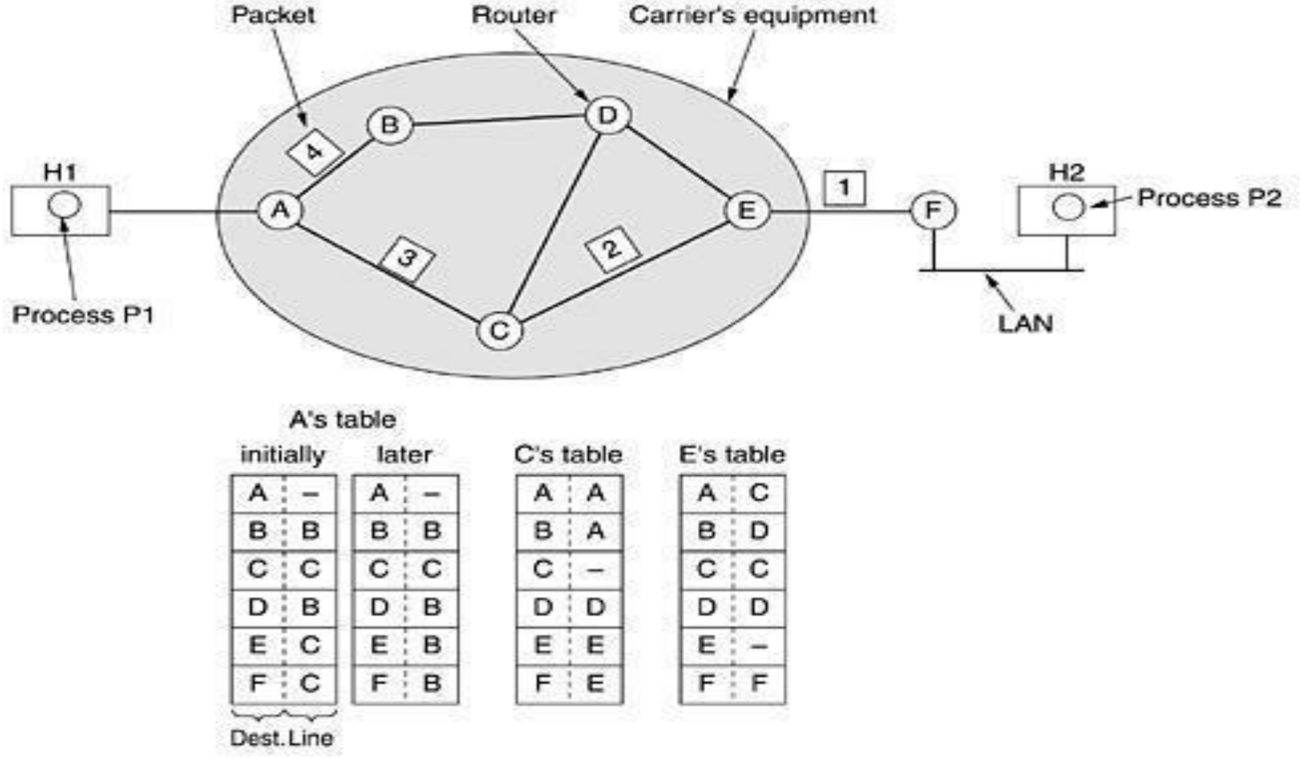
3. Implementation of Connectionless Service

Two different organizations are possible, depending on the type of service offered. If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed.

In this context, the packets are frequently called datagram's (in analogy with telegrams) and the subnet is called a datagram subnet. If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent.

The transport layer code runs on H1, typically within the operating system. It depends a transport header to the front of the message and hands the result to the network layer, probably just another procedure within the operating system.

Figure3-2 . Routing within a datagram subnet.



A's table

initially	
A	–
B	B
C	C
D	B
E	C
F	C

Dest. Line

later	
A	–
B	B
C	C
D	B
E	B
F	B

C's table	
A	A
B	A
C	–
D	D
E	E
F	E

E's table	
A	C
B	D
C	C
D	D
E	–
F	F

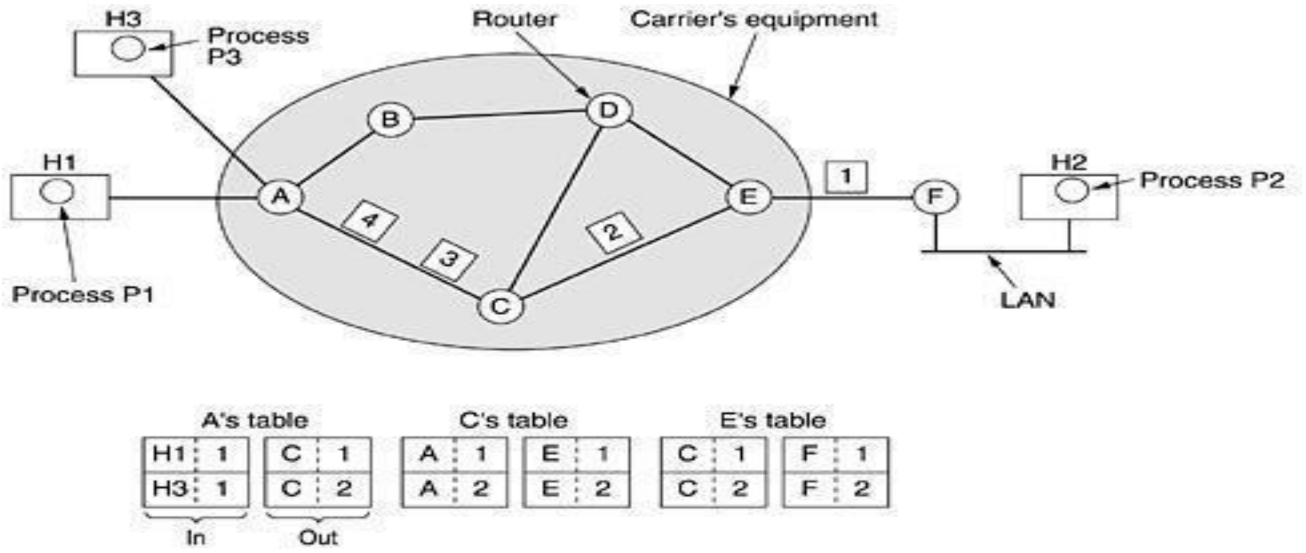
Let us assume that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets, 1, 2, 3, and 4 and sends each of them in turn to router A using some point-to-point protocol, for example, PPP.

At this point the carrier takes over. Every router has an internal table telling it where to send packets for each possible destination.

4. Implementation of Connection-Oriented Service

For connection-oriented service, we need a virtual-circuit subnet. The idea behind virtual circuits is to avoid having to choose a new route for every packet sent, as in Fig. 3-2.

Figure 3-3. Routing within a virtual-circuit subnet.

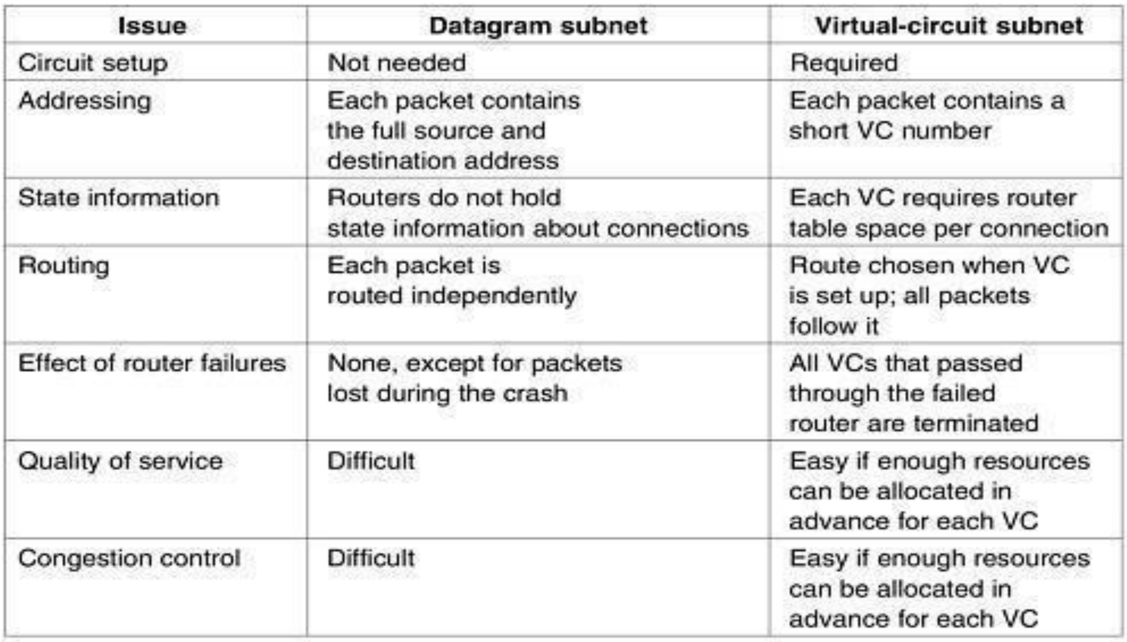


Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 and tells the subnet to establish the virtual circuit. This leads to the second row in the tables.

5. Comparison of Virtual-Circuit and Datagram Subnets

Both virtual circuits and datagram have their supporters and their detractors. We will now attempt to summarize the arguments both ways. The major issues are listed in Fig. 3-4, although purists could probably find a counterexample for everything in the figure.

Figure 3-4. Comparison of datagram and virtual-circuit subnets.



Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

<u>II. ROUTING ALGORITHMS</u>

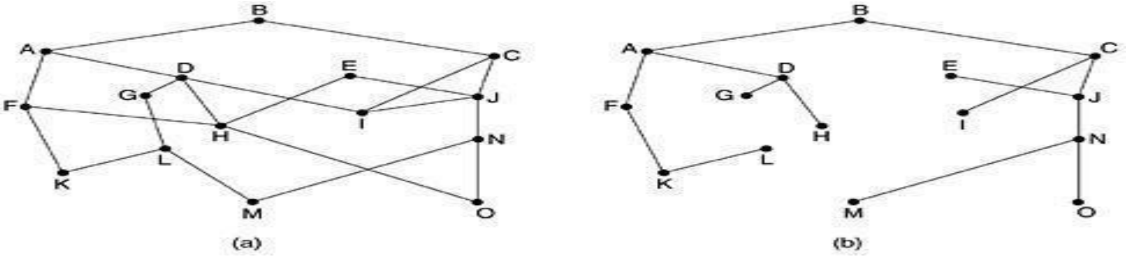
Routing algorithms can be divided into two groups:

<u>I. Non Adaptive algorithms:</u>

For this type of algorithms, the routing decision is not based on the measurement or estimations of current traffic and topology.

The Optimality Principle

- **I**f router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

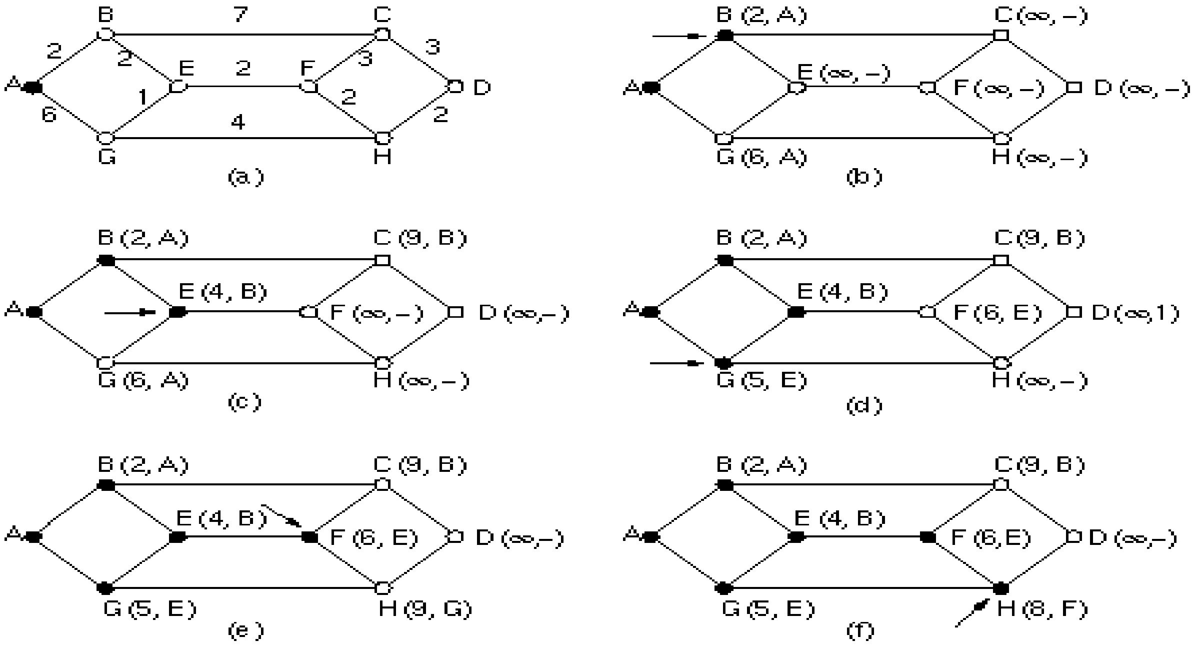


***A subnet. (b) A sink tree for router* B.**

- The set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree.
- As a direct consequence ofthe optimality principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at thedestination.
- Such a tree is called a **sink tree** where the distance metric is the number of hops. Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist.

Shortest path routing:

- Given a network topology and a set of weights describing the cost to send data across each link in the network
- Find the shortest path from a specified source to all other destinations in the network.



Note: The arrows indicate the working node

- Shortest path algorithm first developed by E. W. Dijkstra's

  a. Mark the source node as permanent.

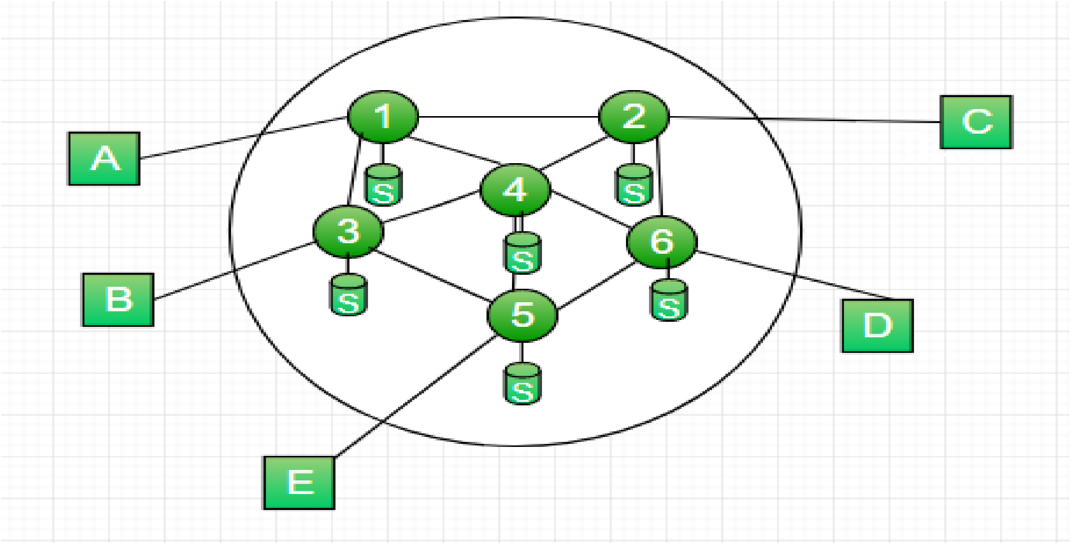
  b. Designate the source node as the working node.

  c. Set the tentative distance to all other nodes to infinity.

  d. While some nodes are not marked permanent
  Compute the tentative distance from the source to all nodes adjacent to the working node. If this is shorter than the current tentative distance replace the tentative distance of the destination and record the label of the working node there.

Flooding:

- It is a non-adaptive algorithm or static algorithm.
- When a router receives a packet, it sends a copy of the packet out on each line (except the one on which it arrived).
- To prevent form looping forever, each router decrements a hop count contained in the packet header.
- As soon as the hop count decrements to zero, the router discards the packet.



- For Example in above figure
  - A incoming packet to (1) is sent out to (2),(3)
  - from (2) is sent to (6),(4) and from (3) it is sent to (4),(5)
  - from (4) it is sent to (6),(5),(3) , from (6) it is sent to (2),(4),(5),from (5) it is sent to (4),(3)

Characteristics –

- All possible routes between Source and Destination is tried.

- All nodes directly or indirectly connected are visited

Limitations –

- Flooding generates vast number of duplicate packets
- Suitable damping mechanism must be used

II. Adaptive algorithms:

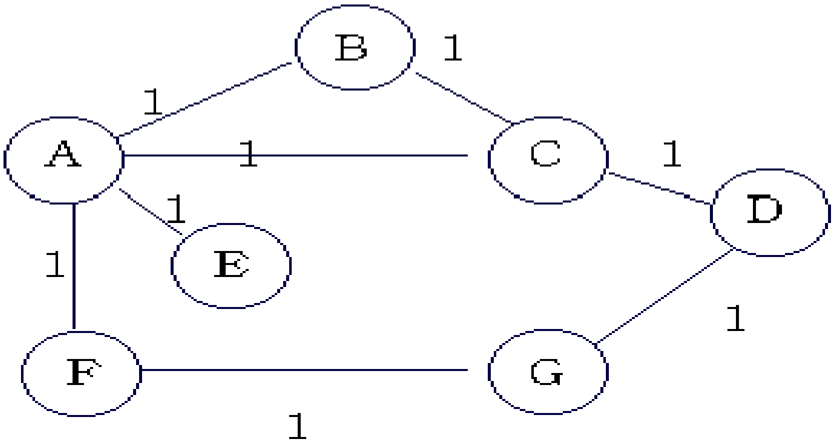
- For these algorithms the routing decision can be changed if there are any changes in topology or traffic etc.
- This is called as dynamic routing.
  The example of Dynamic Routing Algorithms are:

Distance-Vector Routing

Each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbors.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors.
2. A link that is down is assigned an infinite cost.

Example.



Information	**Distance to Reach Node**						
Stored at Node	**A**	**B**	**C**	**D**	**E**	**F**	**G**
A	0	1	1	�	1	1	�
B	1	0	1	�	�	�	�

C	1	1	0	1	�	�	�
D	�	�	1	0	�	�	1
E	1	�	�	�	0	�	�
F	1	�	�	�	�	0	1
G	�	�	�	1	�	1	0

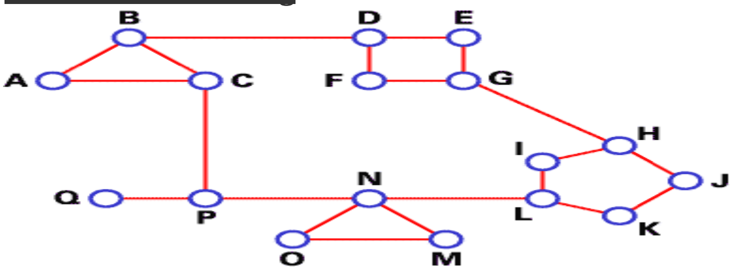
Table 1. Initial distances stored at each node(global view).

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1.

Note that each node only knows the information in one row of the table.

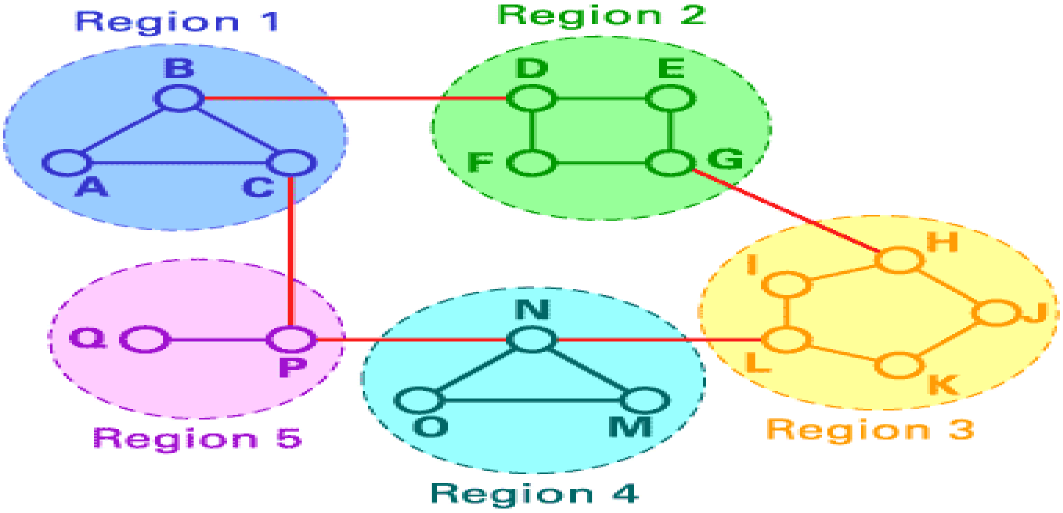
1. Every node sends a message to its directly connected neighbors containing its personal list of distance. (for example, **A** sends its information to its neighbors **B,C,E**, and **F**.)
2. If any of the recipients of the information from **A** find that **A** is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through **A**. (node **B** learns from **A** that node **E** can be reached at a cost of 1; **B** also knows it can reach **A** at a cost of 1, so it adds these to get the cost of reaching **E** by means of **A**. **B** records that it can reach **E** at a cost of 2 by going through **A**.)
3. After every node has exchanged a few updates with its directly connected neighbors, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, **B** knows that it was **A** who said " I can reach **E** in one hop" and so **B** puts an entry in its table that says " To reach **E**, use the link to **A**.)

Hierarchical Routing



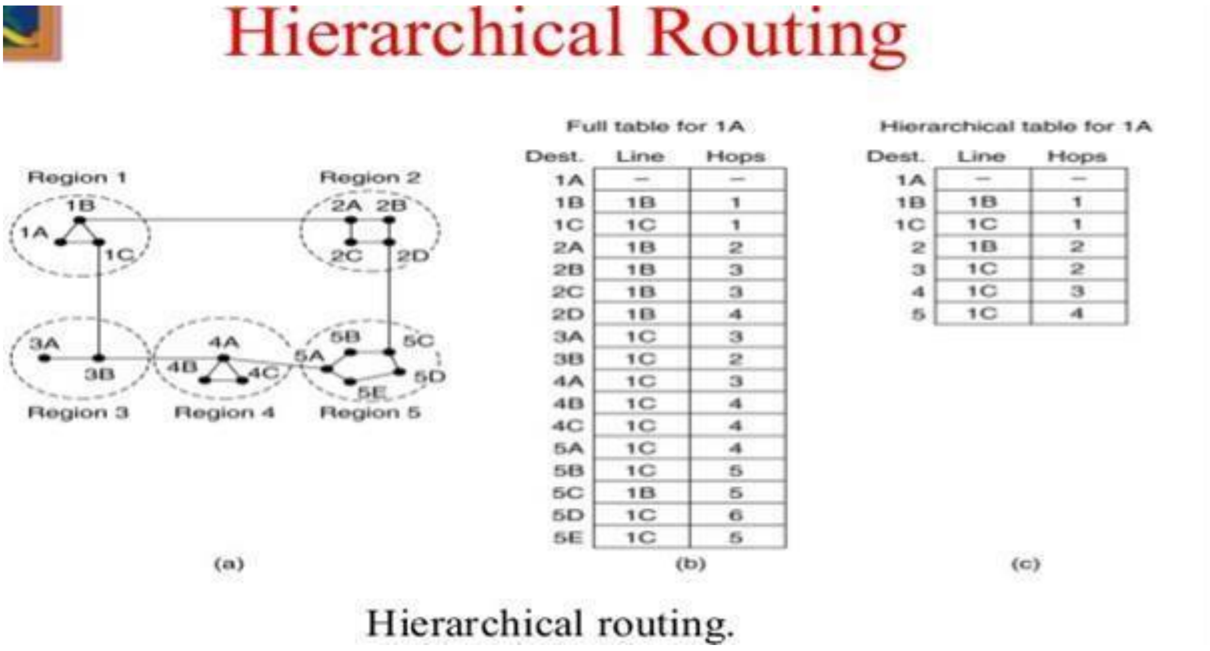
As you see, in both LS and DV algorithms, every router has to save some information about other routers. When the network size grows, the number of routers in the network increases. Consequently, the size of routing tables increases, as well, and routers can't handle network traffic as efficiently. We use **hierarchical routing** to overcome this problem. Let's examine this subject with an example:

We use DV algorithms to find best routes between nodes. In the situation depicted below, every node of the network has to save a routing table with 17 records. Here is a typical graph and routing table for A:



In hierarchical routing, routers are classified in groups known as **regions**. Each router has only the information about the routers in its own region and has no information about routers in other regions. So routers just save one record in their table for every other region. In this example, we have classified our network into five regions (see below).

If A wants to send packets to any router in region 2 (D, E, F or G), it sends them to B, and so on. As you can see, in this type of routing, the tables can be summarized, so network efficiency improves. The above example shows two-level hierarchical routing. We can also use three- or four-level hierarchical routing.



Hierarchical Routing

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

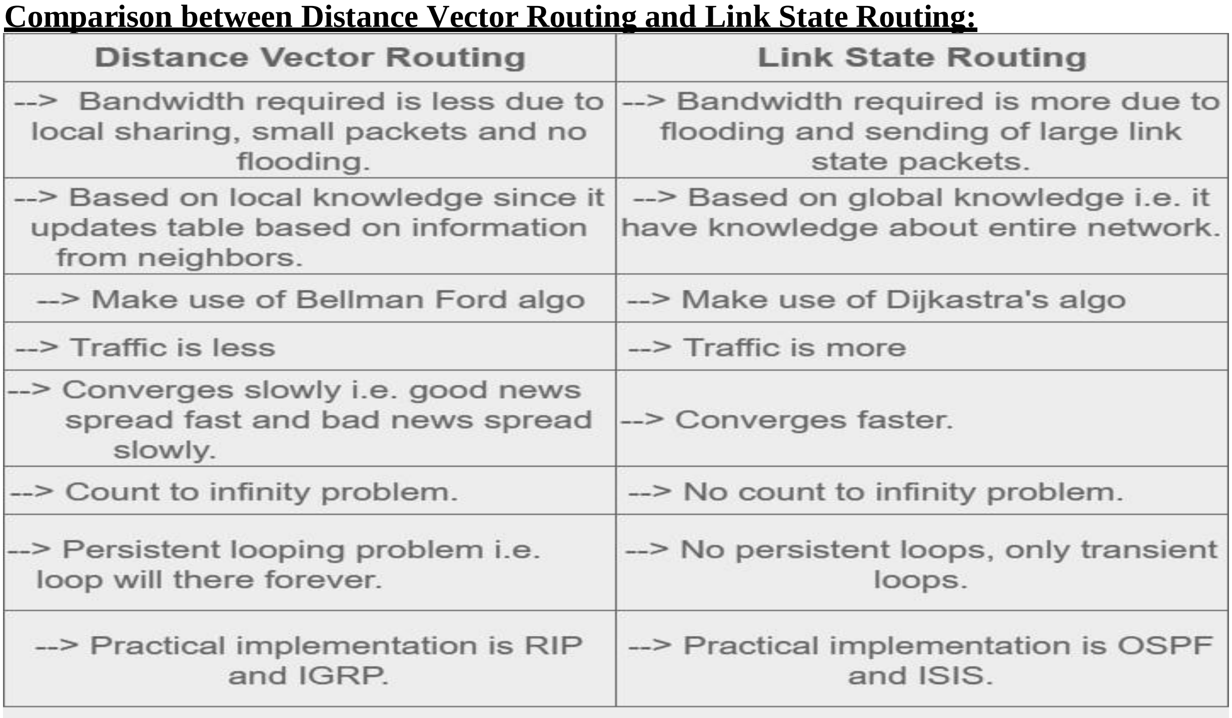
(c)

Hierarchical routing.

Link State Routing –

- It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network.
- A router sends its information about its neighbors only to all the routersthrough flooding.

Comparison between Distance Vector Routing and Link State Routing:



Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

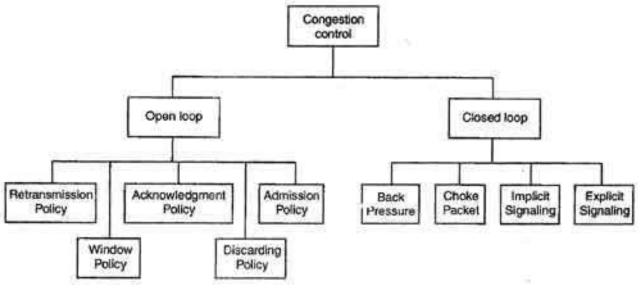
Congestion Control algorithms

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network *(i.e.* the number of packets sent to the network) is greater than the capacity of the network *(i.e.* the number of packets a network can handle.).

Network congestion occurs in case of traffic overloading.

How to correct the Congestion Problem:

Congestion Control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



Types of Congestion Control Methods

These two categories are:

1. Open loop

2. Closed loop

Open Loop Congestion Control

• In this method, policies are used to prevent the congestion before it happens.

• Congestion control is handled either by the source or by the destination.

• The various methods used for open loop congestion controlare:

Retransmission Policy

• The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.

• However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.

Window Policy

• To implement window policy, selective reject window method is used for congestion control.

Congestion control algorithms

Leaky Bucket Algorithm

• It is a traffic shaping mechanism that controls the amount and the rate of the traffic sent to the network.

• A leaky bucket algorithm shapes burst traffic into fixed rate traffic by averaging the data rate.

Token bucket Algorithm

IPv4 Sub netting

Because of the physical and architectural limitations on the size of networks, you often must break large networks into smaller sub networks. Within a network, each wire or ring requires its own network number and identifying subnet address.

Figure 1 shows two subnets in a network.

Figure 1: Subnets in a Network

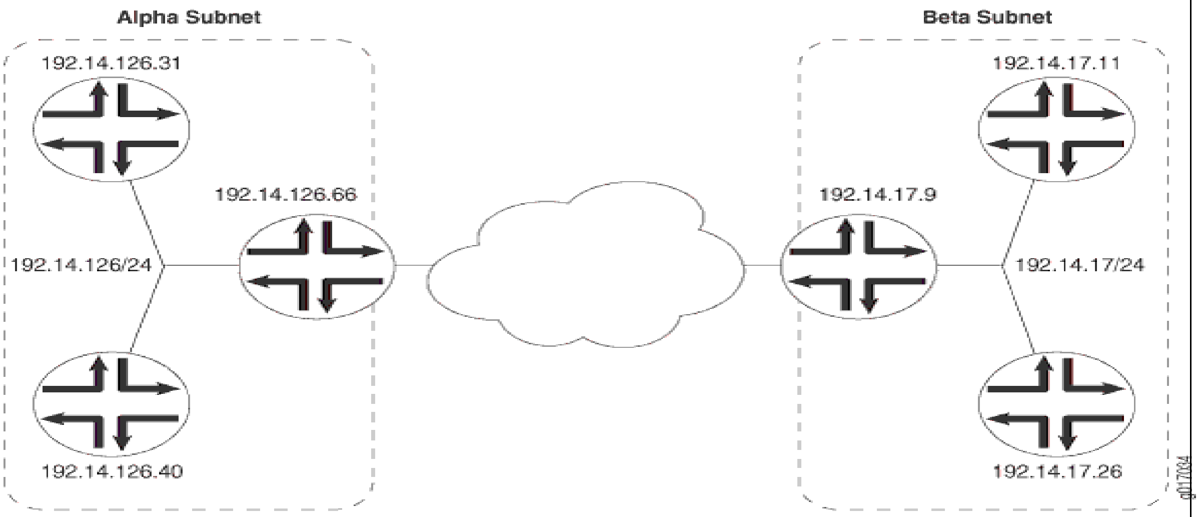


Figure 1 shows three devices connected to one subnet and three more devices connected to a second subnet. Collectively, the six devices and two subnets make up the larger network.

In this example, the network is assigned the network prefix 192.14.0.0, a class B address. Each device has an IP address that falls within this network prefix.

In addition to sharing a network prefix (the first two octets), the devices on each subnet share a third octet. The third octet identifies the subnet.

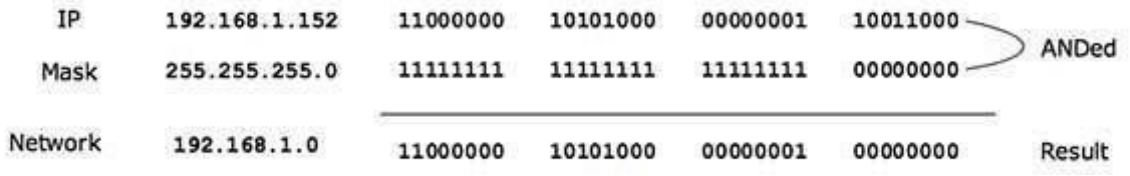
Subnet Mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both.

For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address.

Subnet Mask is also 32 bits long. If the IP address in binary is ended with its Subnet Mask, the result yields the Network address.

For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then:



IP	192.168.1.152	11000000	10101000	00000001	10011000	ANDed
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

Super netting

Super netting is the opposite of Sub netting. In sub netting, a single big network is divided into multiple smaller sub networks.

In Super netting, multiple networks are combined into a bigger network termed as a Super network or Super net.

More specifically,

(i) When multiple networks are combined to form a bigger network, it is termed as super-netting.

(ii) Super netting is used in route aggregation to reduce the size of routing tables and routing table updates.

There are some points which should be kept in mind while super netting:

(i) All the IP address should be contiguous.

(ii) Size of all the small networks should be equal and must be in form of 2^n.

(iii)First IP address should be exactly divisible by whole size of supernet.

Example – Suppose 4 small networks of class C:

200.1.0.0,
200.1.1.0,
200.1.2.0,
200.1.3.0

Build a bigger network which have a single Network Id.

Explanation – Before Super netting routing table will be look like as:

NETWORK	SUBNET	
ID	MASK	INTERFACE

200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

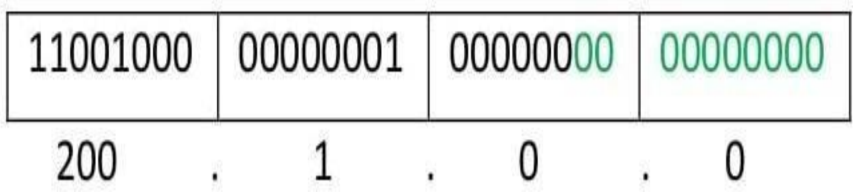
First, lets check whether three condition are satisfied or not:

Contiguous: We can easily see that all network are contiguous all having size 256 hosts. Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.

Equal size of all network:

- As all networks are of class C, so all of the have a size of 256 which in turn equalto 2^8.
- First IP address exactly divisible by total size: When a binary number is divided by 2^n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Super net Network. You can check that if last n v=bits are 0 or not.

  In given example first IP is 200.1.0.0 and whole size of super net is $4*2^8 = 2^{10}$. If last 10 bits of first IP address are zero then IP will be divisible.



11001000	00000001	00000000	00000000
200	1	0	0

Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Super net. New Super net Id will be 200.1.0.0.

Advantages of Super netting –

- Control and reduce network traffic
- Helpful to solve the problem of lacking IP addresses
- Minimizes the routing table

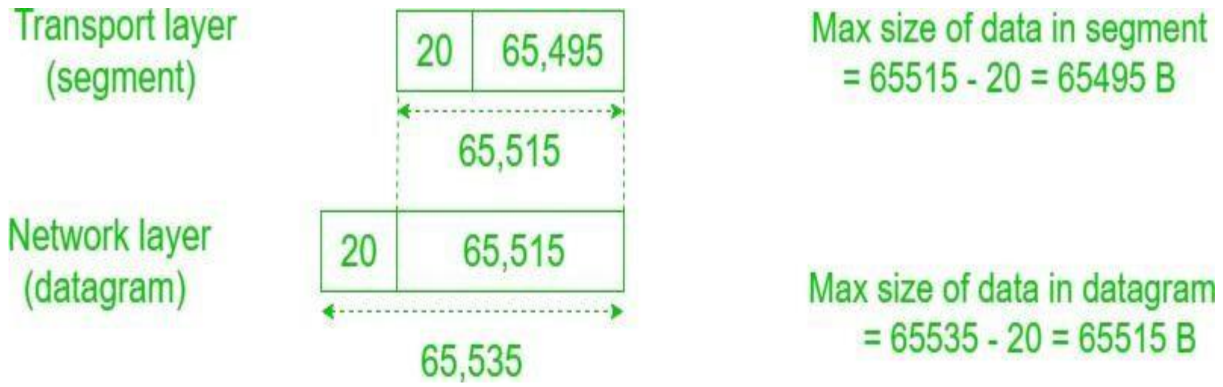
Disadvantages of Super netting –

- It cannot cover different area of network when combined
- All the networks should be in same class and all IP should be contiguous

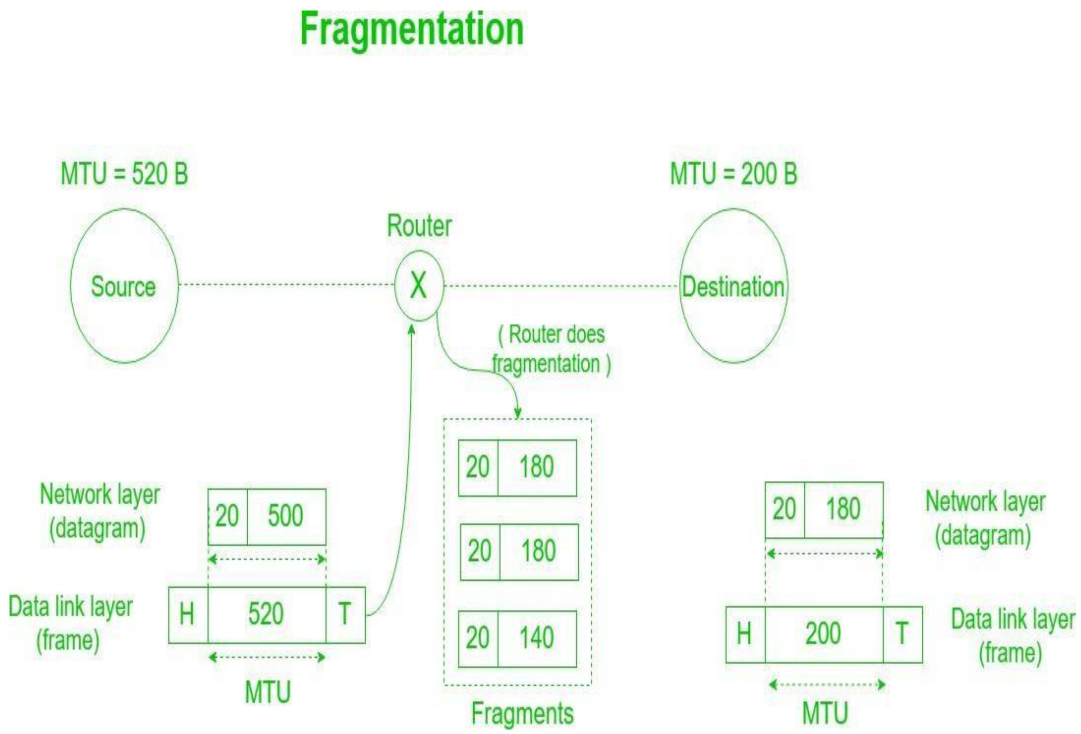
Packet Fragmentation at Network Layer

Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.

- Since there are 16 bits for total length in IP header so, maximum size of IP datagram $= 2^{16} – 1 = 65, 535$ bytes.



- It is done by network layer at the destination side and is usually done at routers.
- Source side does not require fragmentation due to wise (good) segmentation by transport layer i.e. instead of doing segmentation at transport layer and fragmentation at network layer, the transport layer looks at datagram data limit and frame data limit and does segmentation in such a way that resulting data can easily fit in a frame without the need of fragmentation.



- Receiver identifies the frame with the **identification (16 bits)** field in IP header. Each fragment of a frame has same identification number.
- Receiver identifies sequence of frames using the **fragment offset(13 bits)** field in IP header
- An overhead at network layer is present due to extra header introduced due to fragmentation.

Fields in IP header for fragmentation –

- **Identification (16 bits)** – use to identify fragments of same frame.
- **Fragment offset (13 bits)** – use to identify sequence of fragments in the frame.
- It generally indicates number of data bytes preceding or ahead of the fragment.

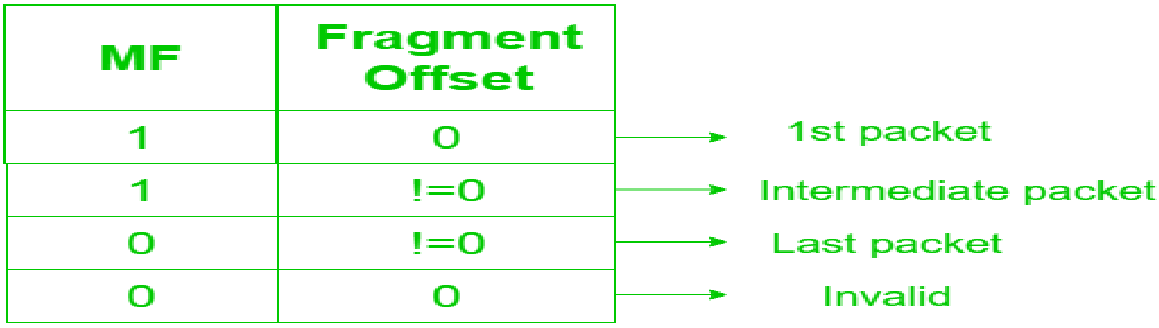
  Maximum fragment offset possible = (65535 – 20) – 1 = 65514

  {where 65535 is maximum size of datagram and 20 is minimum size of IP header}

  So, we need ceil($\log_2 65514$) = 16 bits for fragment offset but fragment offset field has only 13 bits. So, to represent efficiently we need to scale down fragment offset field by $2^{16}/2^{13} = 8$ which acts as a scaling factor. Hence, all fragments except the last fragment should have data in multiples of 8 so that fragment offset $\in$ N.
- **More fragments (MF = 1 bit)** – tells if more fragments ahead of this fragment i.e. if MF = 1, more fragments are ahead of this fragment and if MF = 0, it is the last fragment.
- **Don't fragment (DF = 1 bit)** – if we don't want the packet to be fragmented then DF is set i.e. DF = 1.

Reassembly of Fragments –

It takes place only at destination and not at routers since packets take independent path(datagram packet switching), so all may not meet at a router and hence a need of fragmentation may arise again. The fragments may arrive out of order also.



MF	Fragment Offset	
1	0	1st packet
1	!=0	Intermediate packet
0	!=0	Last packet
0	0	Invalid

Algorithm –

- Destination should identify that datagram is fragmented from MF, Fragment offset field.
- Destination should identify all fragments belonging to same datagram from Identification field.
- Identify the 1st fragment(offset = 0).
- Identify subsequent fragment using header length, fragment offset.
- Repeat until MF = 0.

Efficiency –

Efficiency (e) = useful/total = (Data without header)/(Data with header)

Throughput = e * B { where B is bottleneck bandwidth }

Example – An IP router with a Maximum Transmission Unit (MTU) of 200 bytes has received an IP packet of size 520 bytes with an IP header of length 20 bytes. The values of the relevant fields in the IP header.

Explanation – Since MTU is 200 bytes and 20 bytes is header size so, maximum length of data = 180 bytes but it can be represented in fragment offset since not divisible by 8 so, maximum length of data feasible = 176 bytes.

Number of fragments = (520/200) = 3.

Header length = 5 (since scaling factor is 4 therefore, 20/4 = 5)

Efficiency, e = (Data without header)/(Data with header) = 500/560 = 89.2 %

	20 | 176	20 | 176	20 | 148
Fragment Offset	0	22	44
MF	1	1	0
Header length	5	5	5
Total length	196	196	168

IPv6

- The IPv4 provides host to host communication systems, which are connected through the Internet.
- The **IPv6 (Internetworking Protocol, version 6)** is designed to overcome the shortfalls of the IPv4.

Advantages of IPv6

Some advantages of IPv6 over IPv4 are mentioned below:

1. Address Space : IPv6 has a 128 bit long address, which is larger than IPv4.

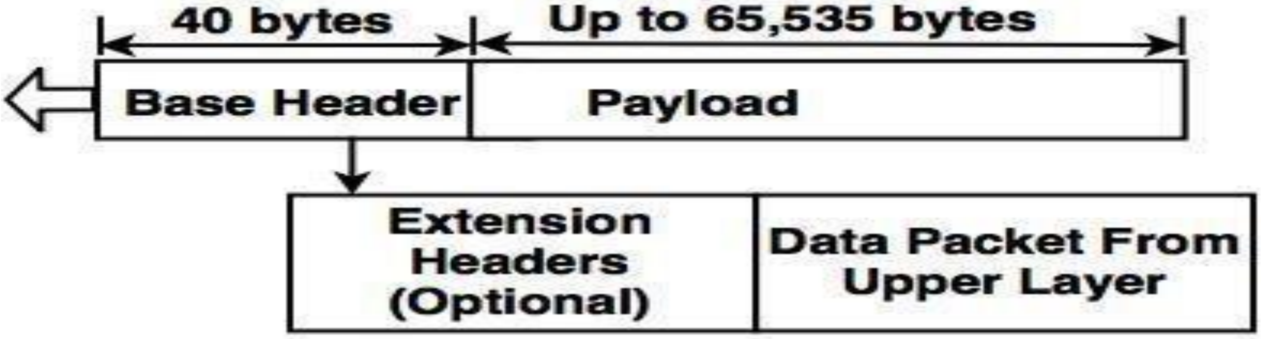
2. Header format : IPv6 has a new header format, in which options are separated from the base header and inserted between the base header and the upper layer data.

3. Extension : IPv6 is designed to allow the extension of the protocol, if required for new applications.

4. Security : Encryption and authentication mechanism provides confidentiality and integrity to the packets in IPv6.

Packet Format of IPv6

The IPv6 packet is shown in the diagram. Each packet is composed of base header and the payload. The payload consists of two fields, optional extension headers and the data from upper layer.



IPv6 Datagram Header and Payload

The Base header consists of eight fields:

1. Version : This is 4 bit field, which defines the version number of an IP and its value is 6 for IPv6.
2. Priority : This is 4 bit field, which defines the priority of the packet with respect to the traffic congestion.
3. Flow label : This is 24 bit field, which is designed to provide facility of specially handling the specific flow of the data.
4. Payload length : This is 16 bit field, which defines the length of an IP datagram excluding the base header.
5. Next header : This is 8 bit field, which defines the header that follows the base header in the datagram.
6. Hop limit : This is 8 bit field, which serves the same purpose as the TTL(Time to Live field in IPv4) field. It is a mechanism that limits the life span of the data in computer networks.
7. Source address : This is 128 bit source address field, which identifies the original source of the datagram.
8. Destination address : It is 128 bit destination address field, which identifies the original destination of the datagram.

Priority field of IPv6

Defines the priority of each packet with respect to other packets from the same source.

The IPv6 divides the traffic into two categories:

- **Congestion-Controlled Traffic :** If source can adjust itself with traffic slowdown due to congestion, the traffic is referred to as congestion controlled traffic.
- **Non Congestion-Controlled Traffic :** Non-Congestion - Controlled Traffic is a type of traffic which can accept a minimum delay.

Extension Headers

The length of the base header is 40 bytes and to provide greater functionality to the IP datagram.

It can be extended up to six extension headers.

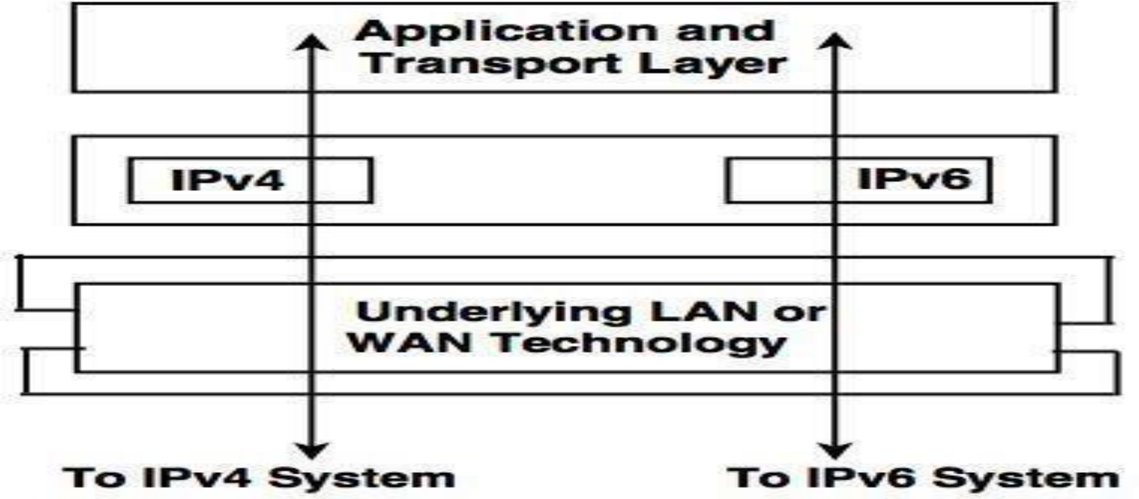
1. Hop by hop option : It is used when the source needs to pass the information to all routers visited by the datagram.
2. Source routing : It combines the concepts of the strict source route and the loose source route options of IPv4.
3. Fragmentation : The data travels through the different networks, each router first de capsulate the IPv6 datagram from the received frame, then processes it and again encapsulates in another frame.
4. Authentication : Authentication validates the message sender and ensures the integrity of the data.
5. Encrypted Security Payload (ESP) : It is an extension that provides confidentiality and protects against eavesdropping .
6. Destination option : It is used when the source needs to forward information to the destination only and not to intermediate routers.

Transition from IPv4 to IPv6

Three strategies have been invented by the IETF (Internet Engineering Task Force) to help the transition:

1. Dual stack

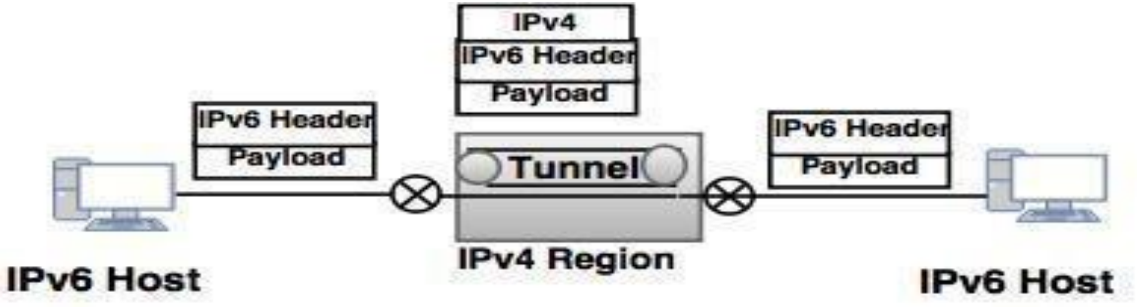
- The host should run IPv4 and IPv6 simultaneously until the entire internet uses IPv6.
- The source host queries the DNS, to determine which version can be used at thetime of sending a packet to the destination.
- If the DNS returns an IPv6 address, the source host sends an IPv6 packet.


Application and Transport Layer
IPv4
IPv6
Underlying LAN or WAN Technology
To IPv4 System
To IPv6 System

Dual Stack

2. Tunneling

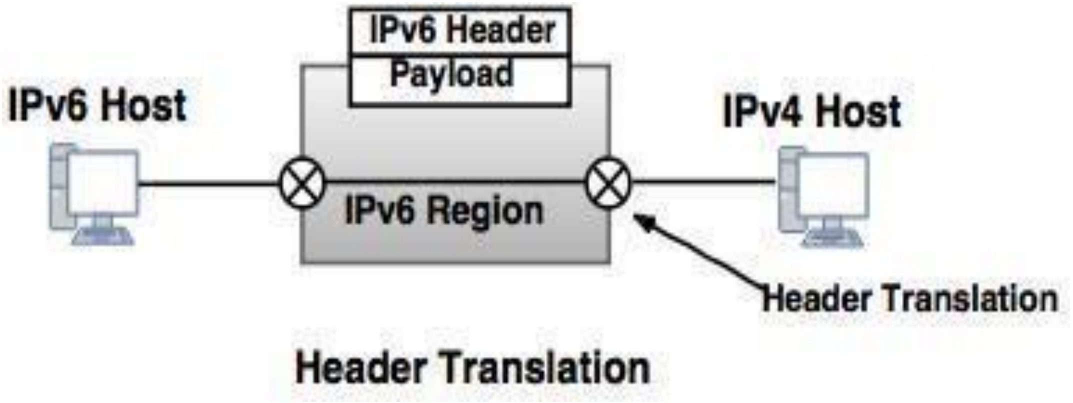
- When two computers use IPv6 and want to communicate with each other andthe packet passes through a region that uses IPv4, it is called tunneling.
- The IPv6 packet is encapsulated in an IPv4 packet, when it enters the region. It leaves the capsule when it exits the region.



Tunneling

3. Header Translation

- It is used when some of the systems use the IPv4 and the sender wants to use IPv6, but the receiver does not understand IPv6.
- The header format should be totally changed through header translation.
- The header of the IPv6 packet is converted to an IPv4 header.



Header translation procedure

1. Change the IPv6 mapped address to an IPv4 address by extracting the rightmost 32 bits.
2. Discard the value of IPv6 priority field.
3. Set the type of service field in IPv4 to be zero.
4. Calculate the checksum for IPv4 and insert in the corresponding field.
5. Ignore the Ipv6 flow label.
6. Convert the compatible extension headers to options and insert them inthe IPv4 header.

Reverse Address Resolution Protocol(RARP)

Mapping physical address to logical address

- In many situations, a host or router knows its MAC address but needs to knowits logical (IP) addresses.
- **RARP** is used to find the logical addresses for a machine that knows its physical address.
- Each host or router can be assigned with one or more logical (IP) address. These addresses are unique and independent of the physical (hardware) address of the machine.
- To create an IP datagram, a host or router is required to know its own IP address. The IP address of a machine is generally read from its configuration file stored on a disk file. A diskless machine is booted from ROM, which has a minimum booting information.

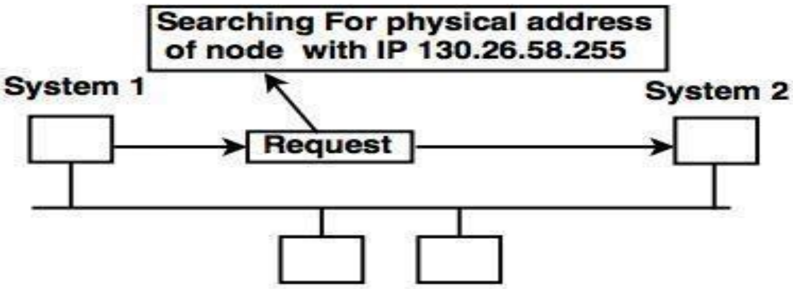
Problems with RARP

- Since it operates at low level, it requires direct address to the network, which makes it difficult for an application developer to built a server.
- It does not fully utilize the capability of a network, like Ethernet, which is enforced to send a minimum packet size, since the reply from the server contains only small piece of information i.e. 32- bit internet address.

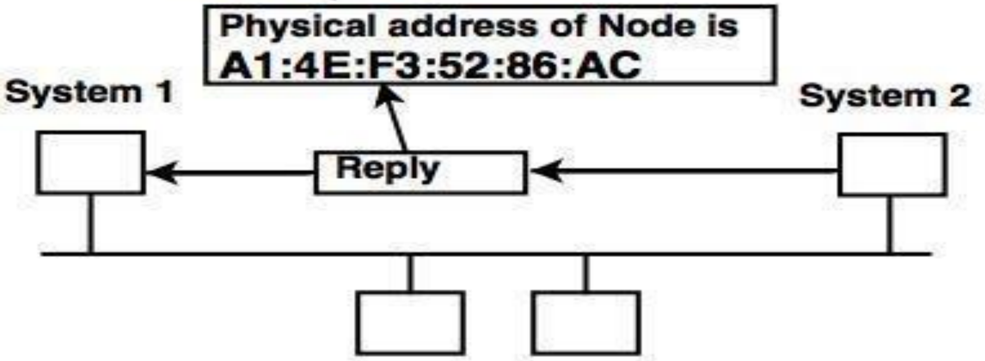
Address Resolution Protocol (ARP)

- Host or router has an IP address and needs to send another host or router (it has the logical (IP) address of the receiver).
- The logical address is obtained from the routing table, if the sender is a router.

- But, the IP datagram is encapsulated in a frame, which is able to pass through the physical network. This means that the sender needs the physical address of the receiver.

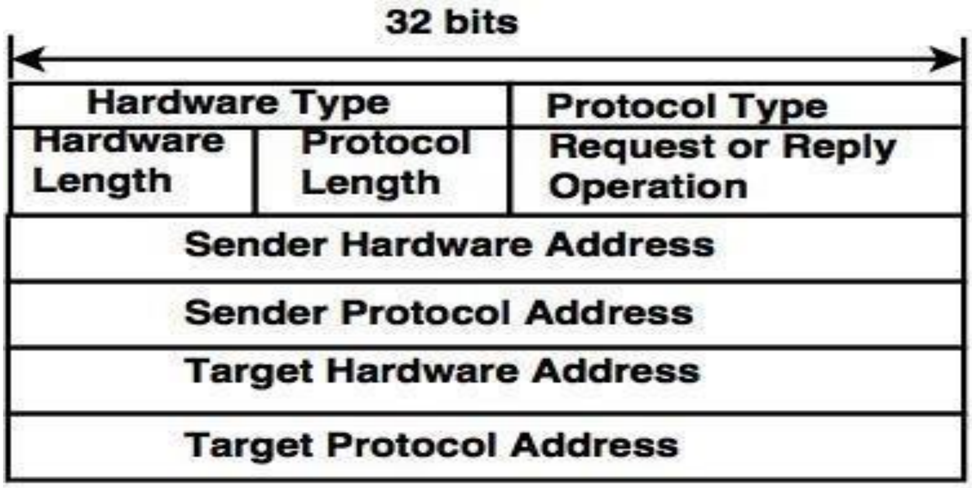

Searching For physical address of node with IP 130.26.58.255
System 1
System 2
Request

ARP Request Broadcast.



ARP Reply Unicast.

ARP Packet Format



Hardware Type		Protocol Type
Hardware Length	Protocol Length	Request or Reply Operation
Sender Hardware Address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

ARP Packet

1. Hardware type
This is 16 bit field used to define the type of the network on which ARP is running.

2. Protocol Length
This is 16 bit length used to define the protocol. For example, the value of this field in IPv4 is 0800H.

3. Hardware length
This is 8 bit field used to define the length of physical address in bytes. This value is 6 for Ethernet.

4. Protocol Length
This is 8 bit field used to define the length of logical address in bytes. This value is 4 for IPv4.

5. Operation
This is 16 bit field used to define a type of packet; ARP reply or request.

6. Sender Hardware Length
this is a variable length field used to define the physical address of the sender.

7. Sender Protocol Address
this is a variable length field used to define the logical address of the sender. This field is 4 bytes long for IP protocol.

8. Target Hardware Address
This is a variable length field used to define the physical address of the target. This field is 6 bytes long for Ethernet. For ARP request message, this field is '0' because the sender does not know the physical address of the target.

9. Target Protocol Address
This is a variable length used to define the logical address of the target. This is 4 byte long for the IPv4 protocol.

ICMPv4

- There are some occasions when IP cannot deliver the packet to the destination host. This happens if TTL(Time-to-Live) gets expired and route to the specified destination address is missing from the routing table due to insufficient buffer space of gateway for passing a specific packet.
- If router is unable to forward a packet for some reasons, the router sends an error message back to the source to report the problem.

There are two types of Messages:

1. Error- reporting messages
The error -reporting message reports a problems that a router or a host (destination) may encounter, while processing an IP packet.

2. Query messages
The query messages which occur in pairs, help a host or a network manager to get specific information from a router or another host.

For example: Nodes can discover their neighbors. Also, a host can discover and learn about routers on their network. Routers can help a node to redirect its messages.

ICMPv6

- It is an integral part of IPv6 and very useful in error reporting, diagnostic functions, neighbor discovery and a framework for extensions to implement future Internet Protocol aspects.

Messages are classified in two types:

1. Error messages
2. Information messages.

- ICMPv6 messages are transported by IPv6 packets in which the IPv6 Nextheader value for ICMPv6 is set to 58.

Dynamic Host Configuration Protocol (DHCP)

DHCP definition

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters. Request for comments (RFC) 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF)- defined standard based on the BOOTP protocol.

DHCP simplifies IP address management

The primary reason DHCP is needed is to simplify the management of IP addresses on networks.

No two hosts can have the same IP address, and configuring them manually will likely lead to errors.

Components of DHCP

When working with DHCP, it’s important to understand all of the components. Below is a list of them and what they do:

- **DHCP Server:** A networked device running the DCHP service that holds IP addresses and related configuration information. This is most typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP Client:** The endpoint that receives configuration information from a DHCP server. This can be a computer, mobile device, IOT endpoint or anything else that

UNIT-IV

Transport Layer

I. Transport Layer Responsibilities

Transport Layer is the second layer of TCP/IP model. It is an **end-to-end** layer used to deliver messages to a host. It is termed as end-to-end layer because it provides a point-to-point connection **rather than** hop-to- hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in Transport Layer is a segment.

The standard protocols used by Transport Layer to enhance it's functionalities are :

(i)TCP(Transmission Control Protocol)
(ii)UDP(User Datagram Protocol)
(iii)DCCP(Datagram Congestion Control Protocol) etc.

Various responsibilities of a Transport Layer –

1. Process to process delivery –
2. End-to-end Connection between hosts –
3. Multiplexing and De multiplexing –
4. Congestion Control –
5. Data integrity and Error Correction –
6. Flow Control–

1.Process to process delivery –

Data Link Layer requires the MAC address (48 bits address contained inside the Network Interface Card of every host machine) of source- destination hosts to correctly deliver a frame and Network layer requires the IP address for appropriate routing of packets , in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host.

A **port number** is a 16 bit address used to identify any client-server program uniquely.

2.End-to-end Connection between hosts –

- Transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP.
- TCP is a secure, connection- orientated protocol which uses a handshake protocol to establish a robust connection between two end- hosts.

3. **Multiplexing and De multiplexing –**

Multiplexing allows simultaneous use of different applications over a network which are running on a host.

- Transport layer provides this mechanism which enables us to send packet streams from various applications simultaneously over a network.

4. **Congestion Control –**

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur.

- As a result retransmission of packets from the sources increase the congestion further.
- In this situation Transport layer provides Congestion Control in different ways.
- It uses **open loop** congestion control (**Retransmission Policy , Window Policy , Acknowledgment Policy etc..**) to prevent the congestion and **closed loop** congestion(**Backpressure , Choke Packet Technique etc..**) control to remove the congestion in a network once it occurred.
- TCP provides AIMD- Additive Increase Multiplicative Decrease, Leaky bucket technique for congestion control.

5. **Data integrity and Error Correction**

Transport layer checks for errors in the messages coming from application layer by using error detection codes, computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data is arrived or not and checks for the integrity of data.

6. **Flow control–**

- Transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model.
- TCP also prevents the data loss due to a fast sender and slow receiver by imposing some flow control techniques.
- It uses the method of sliding window protocol which is accomplished by receiver by sending a window back to the sender informing the size of data it can receive.

II. ELEMENTS OF TRANSPORT PROTOCOLS

The transport service is implemented by a transport protocol used between the two transport entities. The transport protocols resemble the data link protocols. Both have to deal with error control, sequencing, and flow control, among other issues. The difference transport protocol and data link protocol depends upon the environment in which they are operated.

These differences are due to major dissimilarities between the environments in which the two protocols operate, as shown in Fig.

At the data link layer, two routers communicate directly via a physical channel, whether wired or wireless, whereas at the transport layer, this physical channel is replaced by the entire network. This difference has many important implications for the protocols.

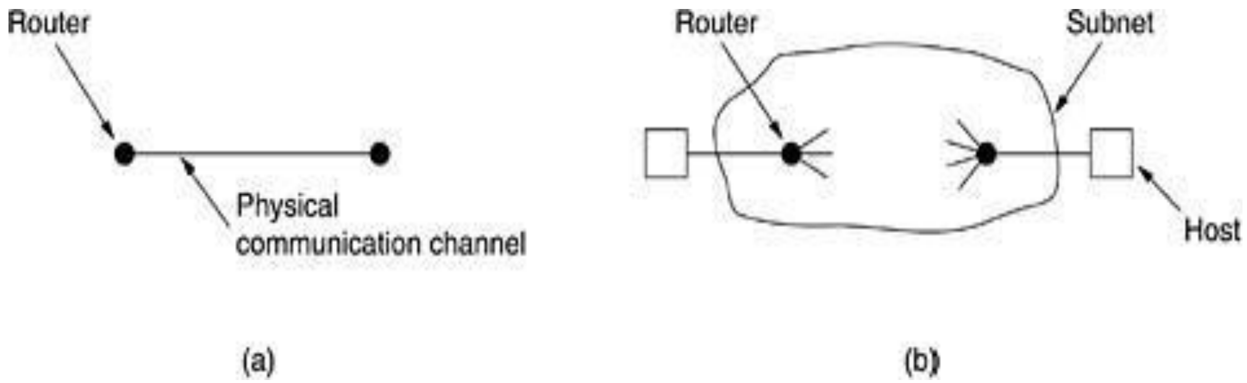


Figure (a) Environment of the data link layer. (b) Environment of the transport layer.

The transport service is implemented by a transport protocol between the 2 transport entities.

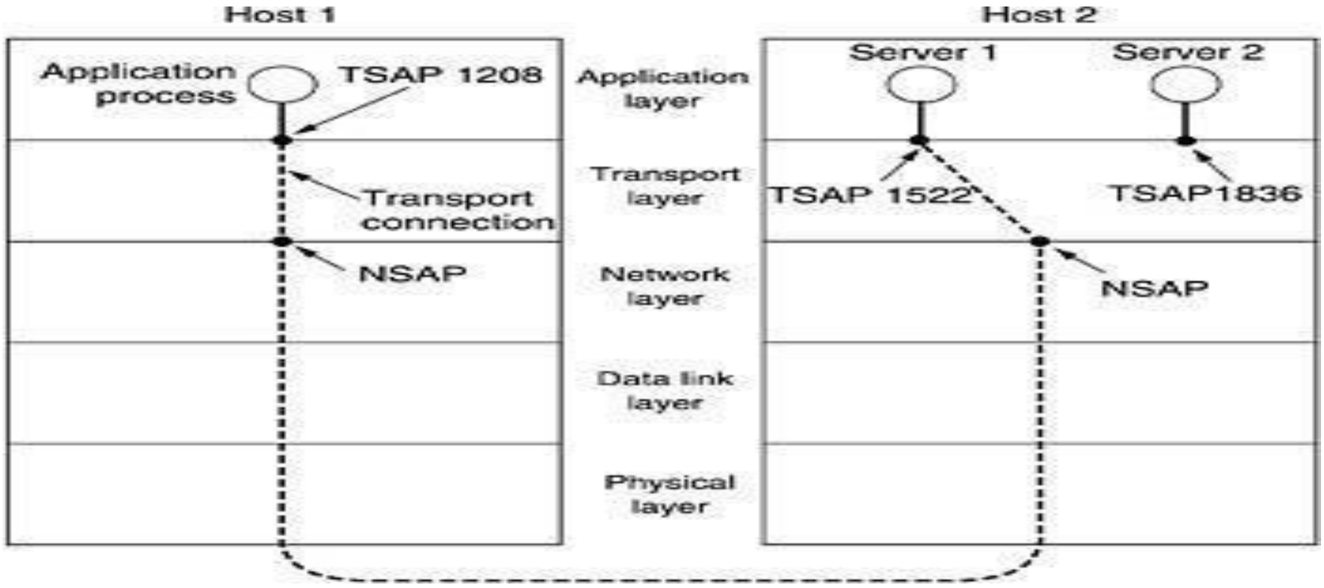


Figure 4.5 illustrates the relationship between the NSAP, TSAP and transport connection. Application processes, both clients and servers, can attach themselves to a TSAP to establish a connection to a remote TSAP.

These connections run through NSAPs on each host, as shown. The purpose of having TSAPs is that in some networks, each computer has a single NSAP, so some way is needed to distinguish multiple transport end points that share that NSAP.

The elements of transport protocols are:

1. ADDRESSING
2. Connection Establishment.
3. Connection Release.
4. Error control and flow control
5. Multiplexing.
6. Crash Recovery

1. ADDRESSING

When an application (e.g., a user) process wishes to set up a connection to a remote application process, it must specify which one to connect to. The method normally used is to define transport addresses to which processes can listen for connection requests. In the Internet, these endpoints are called **ports**.

There are two types of access points.

TSAP (Transport Service Access Point) to mean a specific endpoint in the transport layer.

The analogous endpoints in the network layer (i.e., network layer addresses) are not surprisingly called

"NSAPs (Network Service Access Points)". IP addresses are examples of NSAPs.

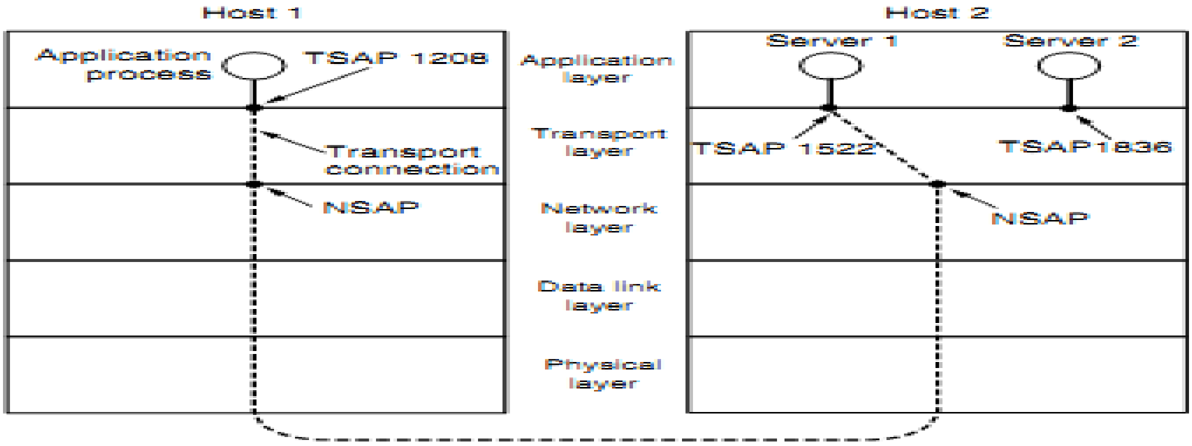


Fig 4.5: TSAP and NSAP network connections

Application processes, both clients and servers, can attach themselves to a local TSAP to establish a connection to a remote TSAP. These connections run through NSAPs on each host. The purpose of having TSAPs is that in some networks, each computer has a single NSAP, so some way is needed to distinguish multiple transport endpoints that share that NSAP.

A possible scenario for a transport connection is as follows:

1. A mail server process attaches itself to TSAP 1522 on host 2 to wait for an

incoming call. How a process attaches itself to a TSAP is outside the networking model and depends entirely on the local operating system. A call such as our LISTEN might be used, for example.

2. An application process on host 1 wants to send an email message, so it attaches itself to TSAP 1208 and issues a CONNECT request. The request specifies TSAP 1208 on host 1 as the source and TSAP 1522 on host 2 as the destination. This action ultimately results in a transport connection being established between the application process and the server.
3. The application process sends over the mail message.
4. The mail server responds to say that it will deliver the message.
5. The transport connection is released.

2. CONNECTION ESTABLISHMENT:

With packet lifetimes bounded, it is possible to devise a fool proof way to establish connections safely.

Packet lifetime can be bounded to a known maximum using one of the following techniques:

- Restricted subnet design
- Putting a hop counter in each packet
- Time stamping in each packet

Using a 3-way hand shake, a connection can be established. This establishment protocol doesn’t require both sides to begin sending with the same sequence number.

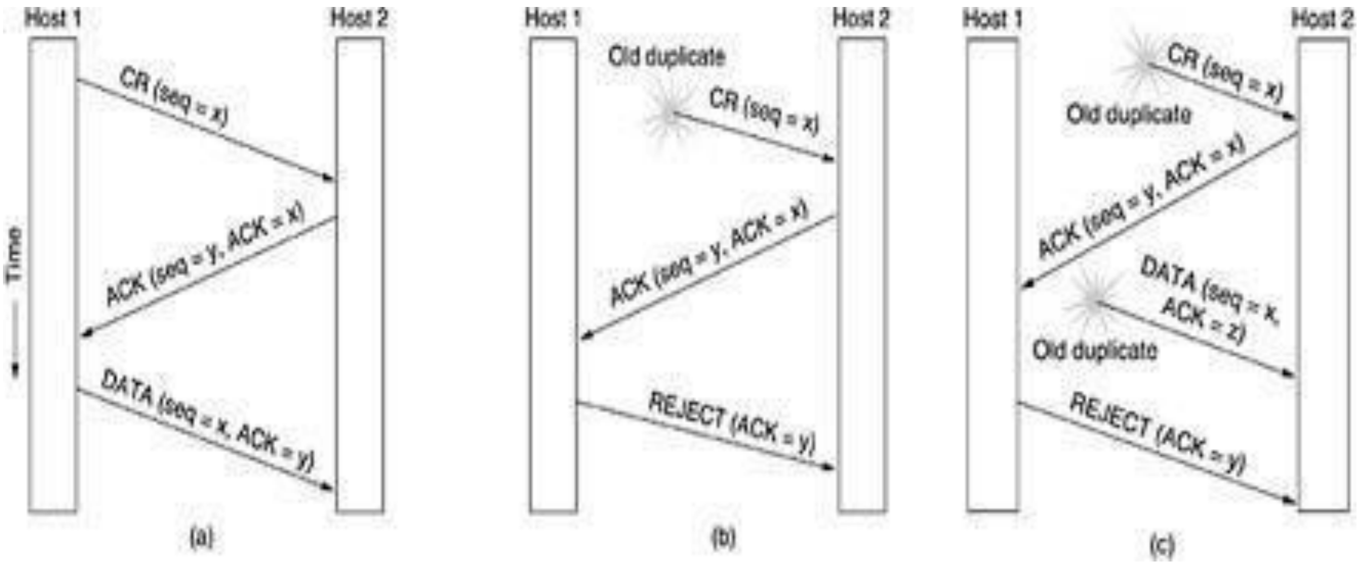


Fig 4.6: Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNEC TION REQUEST (a) Normal operation. (b) Old duplicate CONNECTION REQUEST appearing out of nowhere. (c) Duplicate

CONNECTION REQUEST and duplicate ACK .

In **fig (A)** Tomlinson (1975) introduced the **three-way handshake**.

- This establishment protocol involves one peer checking with the other that the connection request is indeed current. Host 1 chooses a sequence number, x , and sends a CONNECTION REQUEST segment containing it to host 2. Host 2 replies with an ACK segment acknowledging x and announcing its own initial sequence number, y.

- Finally, host 1 acknowledges host 2's choice of an initial sequence number in the first data segment that it sends

In **fig (B)** the first segment is a delayed duplicate CONNECTION REQUEST from an old connection.

- This segment arrives at host 2 without host 1's knowledge. Host 2 reacts to this segment by sending host1an ACK segment, in effect asking for verification that host 1 was indeed trying to set up a new connection.
- When host 1 rejects host 2's attempt to establish a connection, host 2 realizes that it was tricked by a delayed duplicate and abandons the connection. In this way, a delayed duplicate does no damage.

- The worst case is when both a delayed CONNECTION REQUEST and an ACK are floating around in the subnet.

In **fig (C)** previous example, host 2 gets a delayed CONNECTION REQUEST and replies to it.

- At this point, it is crucial to realize that host 2 has proposed using y as the initial sequence number for host 2 to host 1 traffic, knowing full well that no segments containing sequence number y or acknowledgements to y are still in existence.
- When the second delayed segment arrives at host 2, the fact that z has been acknowledged rather than y tells host 2 that this, too, is an old duplicate.
- The important thing to realize here is that there is no combination of old segments that can cause the protocol to fail and have a connection set up by accident when no one wants it.

3. CONNECTION RELEASE:

A connection is released using either asymmetric or symmetric variant. But, the improved protocol for releasing a connection is a 3-way handshake protocol.

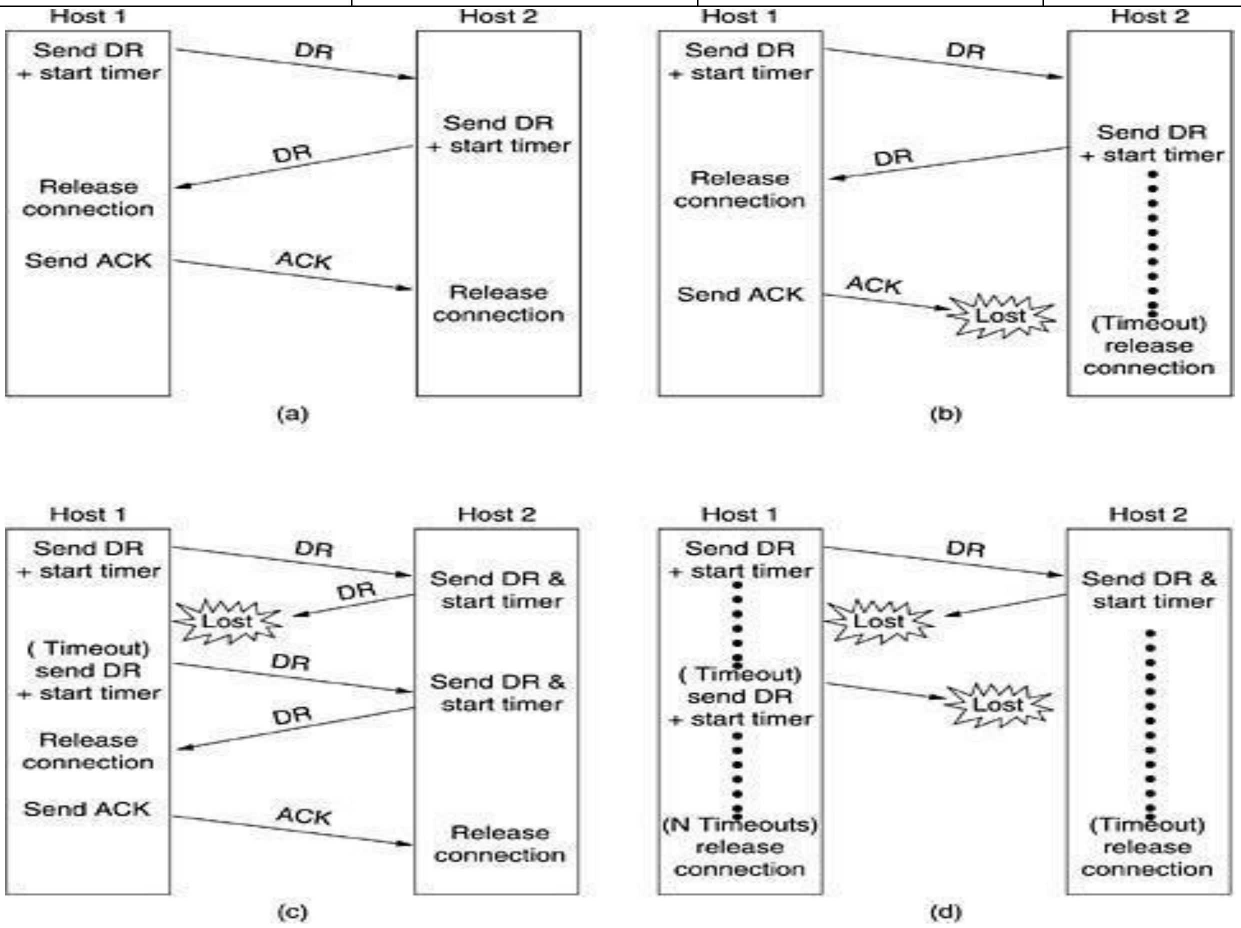
There are two styles of terminating a connection:

1) Asymmetric release and
2) Symmetric release.

Asymmetric release is the way the telephone system works: when one party hangs up, the connection is broken. **Symmetric release** treats the connection as two separate unidirectional connections and requires each one to be released separately.

TPDU- **Transaction Protocol Data Unit**.

Fig-(a)	Fig-(b)	Fig-(c)	Fig-(d)
One of the user sends a DISCONNECTION REQUEST TPDU in order to initiate connection release. When it arrives, the recipient sends back a DR-TPDU, too, and starts a timer. When this DR arrives, the original sender sends back an ACK- TPDU and releases the	Initial process is done in the same way as in fig-(a). If the final ACK-TPDU is lost, the situation is saved by the timer. When the timer is expired, the connection is released.	If the second DR is lost, the user initiating the disconnection will not receive the expected response, and will timeout and starts all over again.	Same as in fig-(c) except that all repeated attempts to retransmit the DR is assumed to be failed due to lost TPDUs. After 'N' entries, the sender just gives up and releases
connection. Finally, when the ACK-TPDU arrives, the receiver also releases the connection.			connection.



4. FLOW CONTROL AND BUFFERING:

Flow control is done by having a sliding window on each connection to keep a fast transmitter from over running a slow receiver. Buffering must be done by the sender, if the network service is unreliable. The sender buffers all the TPDUs sent to the receiver. The buffer size varies for different TPDUs.

They are:

a) Chained Fixed-size Buffers
b) Chained Variable-size Buffers
c) One large Circular Buffer per Connection

a)Chained Fixed-size Buffers:

If most TPDUs are nearly the same size, the buffers are organized as a pool of identical size buffers, with one TPDU per buffer.

b) Chained Variable-size Buffers:

This is an approach to the buffer-size problem. i.e., if there is wide variation in TPDU size, from a few characters typed at a terminal to thousands of characters from file transfers, some problems may occur:

- If the buffer size is chosen equal to the largest possible TPDU, space will be wasted whenever a short TPDU arrives.
- If the buffer size is chosen less than the maximum TPDU size, multiple buffers will be needed for long TPDUs.

To overcome these problems, we employ variable-size buffers.

c) One large Circular Buffer per Connection:

A single large circular buffer per connection is dedicated when all connections are heavily loaded.

1. Source Buffering is used for low band width bursty traffic
2. Destination Buffering is used for high band width smooth traffic.
3. Dynamic Buffering is used if the traffic pattern changes randomly.

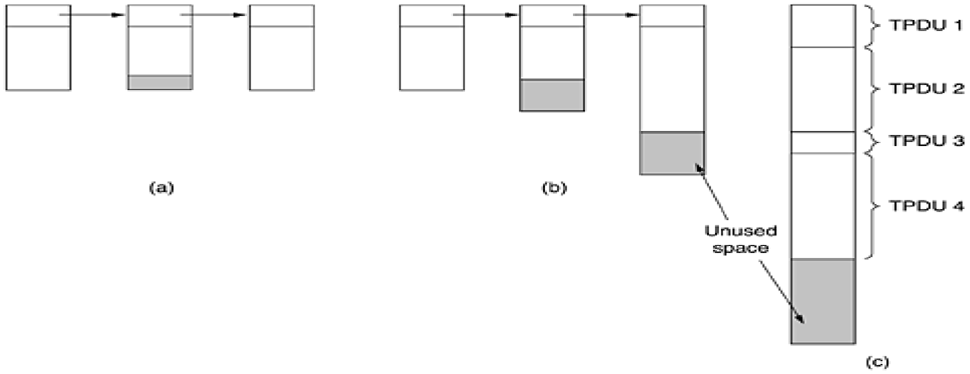


Figure 4.7. (a) Chained fixed-size buffers. (b) Chained variable-sized buffers. (c) One large circular buffer per connection.

5. MULTIPLEXING:

In networks that use virtual circuits within the subnet, each open connection consumes some table space in the routers for the entire duration of the connection. If buffers are dedicated to the virtual circuit in each router as well, a user who left a terminal logged into a remote machine, there is need for multiplexing. There are 2 kinds of multiplexing:

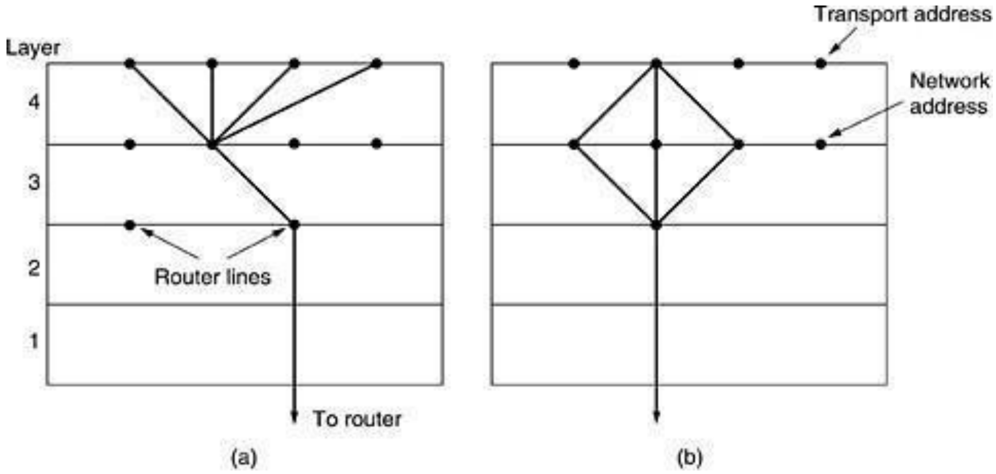


Figure 4.8. (a) Upward multiplexing. (b) Downward multiplexing

(a). UP-WARD MULTIPLEXING:

In the above figure, all the 4 distinct transport connections use the same network connection to the remote host. When connect time forms the major component of the carrier's bill, it is up to the transport layer to group port connections according to their destination and map each group onto the minimum number of port connections.

(b). DOWN-WARD MULTIPLEXING:

- If too many transport connections are mapped onto the one network connection, the performance will be poor.
- If too few transport connections are mapped onto one network connection, the service will be expensive.

6. Crash Recovery

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

Chapter-2
The Internet Transport Protocols

I. UserDatagram Protocol(UDP)

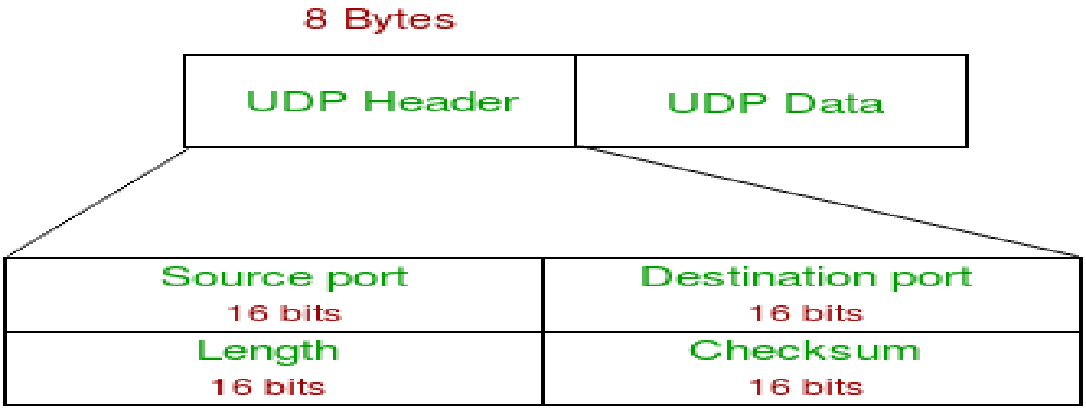
Like IP, UDP is connectionless and unreliable protocol. It doesn't require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.

UDP transmits the data in form of a datagram.

UDP Header

UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary header information and remaining part consist of data.

UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.



1. **Source Port :** Source Port is 2 Bytes long field used to identify port number of source.
2. **Destination Port :** It is 2 Bytes long field, used to identify the port of destined packet.
3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

II. Introduction to TCP (TRANSMISSION CONTROL PROTOCOL)

It was specifically designed to provide a reliable end-to end byte stream over an unreliable network. It was designed to adapt dynamically to properties of the inter network and to be robust in the face of many kinds of failures.

The different issues to be considered are:

i. The TCP Service Model
ii. The TCP Protocol
iii. The TCP Segment Header
iv. The Connection Management
v. TCP Transmission Policy
vi. TCP Congestion Control

III. The TCP Service Model

- TCP service is obtained by having both the sender and receiver create end points called **SOCKETS.**
- Each socket has a socket number(address)consisting of the IP address of the

host, called a **“PORT”** (= TSAP –Transport Services Access Point)

- To obtain TCP service a connection must be explicitly established between a socket on the sending machine and a socket on the receiving machine.
- All TCP connections are full duplex and point to point i.e., multicasting or broadcasting is not supported.
- A TCP connection is a byte stream, not a message stream i.e., the data is delivered as chunks.

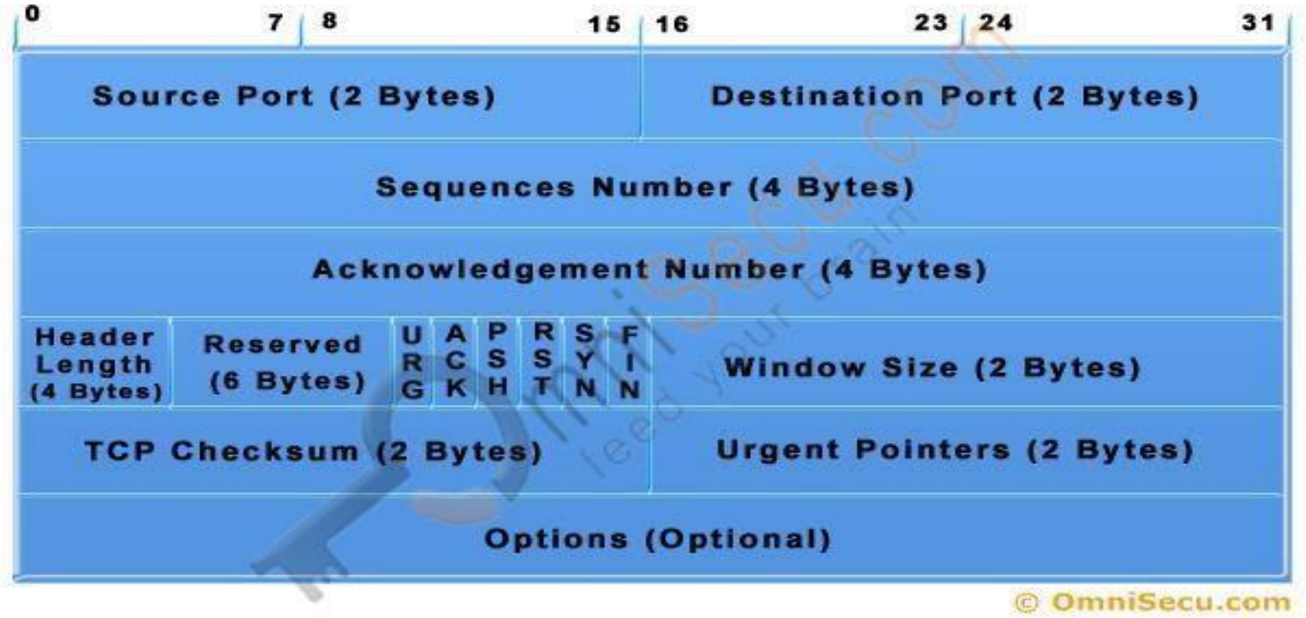
Sockets:

A socket may be used for multiple connections at the same time. In other words, 2 or more connections may terminate at same socket. Connections are identified by socket identifiers at same socket. Connections are identified by socket identifiers at both ends. Some of the sockets are listed below:

Ports: Port numbers below 256 are called Well- known ports and are reserved for standard services.

IV. TCP Segment Header

Transmission Control Protocol (TCP) Segment Header consists the following fields.



Transmission Control Protocol (TCP) Segment Header.

Source port: 16 Bit number which identifies the Source Port number (Sending Computer's TCP Port).

Destination port: 16 Bit number which identifies the Destination Port number (Receiving Port).

Sequence number: 32 Bit number used for byte level numbering of TCP segments. If you are using TCP, each byte of data is assigned a sequence number.

If SYN flag is set (during the initial three way handshake connection initiation), then this is the initial sequence number. The sequence number of the actual first data byte will then be this sequence number plus 1. For example, let the first byte of data by a device in a particular TCP header will have its sequence number in this field 50000. If this packet has 500 bytes of data in it, then the next packet sent by this device will have the sequence number of 50000 + 500 + 1 = 50501.

Acknowledgment Number: 32 Bit number field which indicates the next sequence number that the sending device is expecting from the other device.

Header Length: 4 Bit field which shows the number of 32 Bit words in the header. Also known as the Data Offset field. The minimum size header is 5 words (binary pattern is 0101).

Reserved: Always set to 0 (Size 6 bits).

Control Bit Flags: We have seen before that TCP is a Connection Oriented Protocol. The meaning of Connection Oriented Protocol is that, before any data can be transmitted, a reliable connection must be obtained and acknowledged.

Control Bits govern the entire process of connection establishment, data transmissions and connection termination. The control bits are listed as follows: They are:

URG: Urgent Pointer.

ACK: Acknowledgement.

PSH: This flag means Push function. Using this flag, TCP allows a sending application to specify that the data must be pushed immediately. When an application requests the TCP to push data, the TCP should send the data that has accumulated without waiting to fill the segment.

RST: Reset the connection. The RST bit is used to RESET the TCP connection due to unrecoverable errors. When an RST is received in a TCP segment, the receiver must respond by immediately terminating the connection. A RESET causes both sides immediately to release the connection and all its resources. As a result, transfer of data ceases in both directions, which can result in loss of data that is in transit. A TCP RST indicates an abnormal termination of the connection.

SYN: This flag means synchronize sequence numbers. Source is beginning a new counting sequence. In other words, the TCP segment contains the sequence number of the first sent byte (ISN).

FIN: No more data from the sender. Receiving a TCP segment with the FIN flag does not mean that transferring data in the opposite direction is not possible. Because TCP is a fully duplex connection, the FIN flag will cause the closing of connection only in one direction. To close a TCP connection gracefully, applications use the FIN flag.

Window: indicates the size of the receive window, which specifies the number of bytes beyond the sequence number in the acknowledgment field that the receiver is currently willing to receive.

Checksum: The 16-bit checksum field is used for error-checking of the header and data.

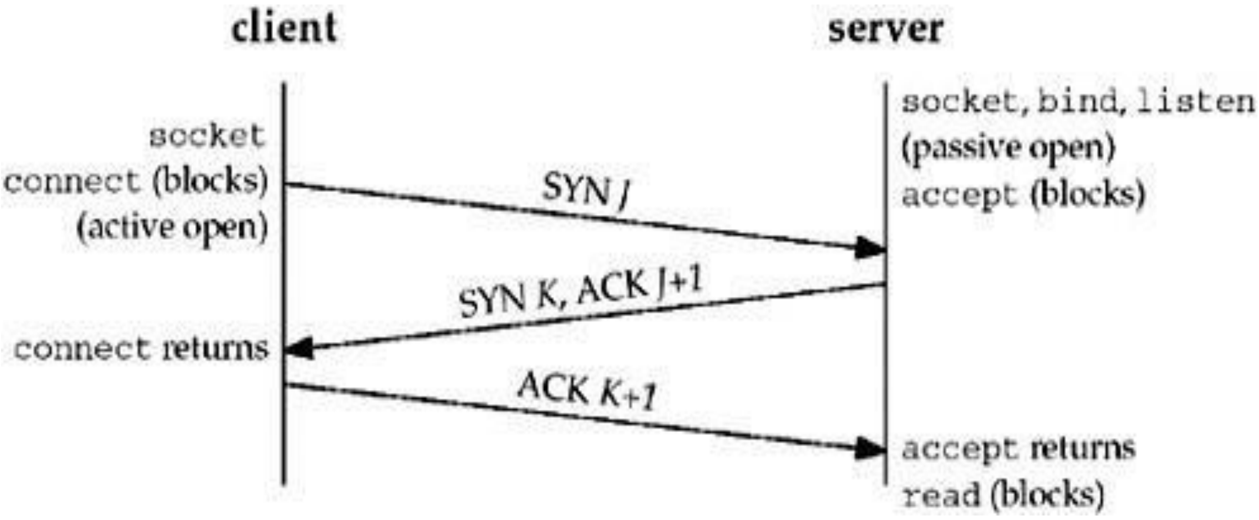
Urgent Pointer: Shows the end of the urgent data so that interrupted data streams can continue. When the URG bit is set, the data is given priority over other data streams (Size 16 bits).

V. TCP Connection Establishment

To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

1. SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment’s sequence number to a random value A.
2. SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number (A + 1), and the sequence number that the server chooses for the packet is another random number, B.
3. ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A + 1, and the acknowledgement number is set to one more than the received sequence number i.e. B + 1.

At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.



VI. TCP Connection Termination

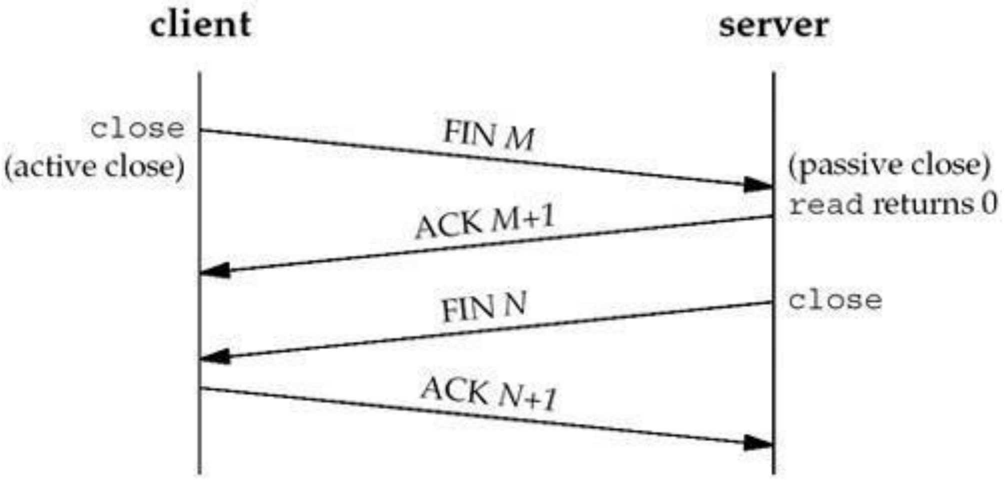
While it takes three segments to establish a connection, it takes four to terminate a connection.

1. **One application calls close first, and we say that this end performs the *active close*. This end's TCP sends a FIN segment, which means it is finished sending data.**

2. The other end that receives the FIN performs the *passive close*. The received FIN is acknowledged by TCP. The receipt of the FIN is also passed to the application as an end-of-file (after any data that may have already been queued for the application to receive), since the receipt of the FIN means the application will not receive any additional data on the connection.
3. Sometime later, the application that received the end-of-file will close its socket. This causes its TCP to send a FIN.
4. The TCP on the system that receives this final FIN (the end that did the active close) acknowledges the FIN.

Since a FIN and an ACK are required in each direction, four segments are normally required. We use the qualifier "normally" because in some scenarios, the FIN in Step 1 is sent with data. Also, the segments in Steps 2 and 3 are both from the end performing the passive close and could be combined into one segment. We show these packets in Figure 2.3.

Figure 2.3. Packets exchanged when a TCP connection is closed.



VII. TCP Sliding Window

The working of the TCP sliding window mechanism can be explained as below.

The sending device can send all packets within the TCP window size (as specified in the TCP header) without receiving an ACK, and should start a timeout timer for each of them.

The receiving device should acknowledge each packet it received, indicating the sequence number of the last well-received packet. After receiving the ACK from the receiving device, the sending device slides the window to right side.

VIII. TCP Congestion Control

Congestion in Network-

- Congestion leads to the loss of packets in transit.
- So, it is necessary to control the congestion in network.
- It is not possible to completely avoid the congestion.

Congestion Control-

Congestion control refers to techniques and mechanisms that can-

- Either prevent congestion before it happens
- Or remove congestion after it has happened

TCP Congestion Control-

TCP reacts to congestion by reducing the sender window size.

The size of the sender window is determined by the following two factors-

1. Receiver window size
2. Congestion window size

Receiver Window Size-

Receiver window size is an advertisement of-

"How much data (in bytes) the receiver can receive without acknowledgement?"

- Sender should not send data greater than receiver window size.
- Otherwise, it leads to dropping the TCP segments which causes **TCP Retransmission**.
- So, sender should always send data less than or equal to receiver window size.
- Receiver dictates its window size to the sender through TCP Header.

2. Congestion Window-

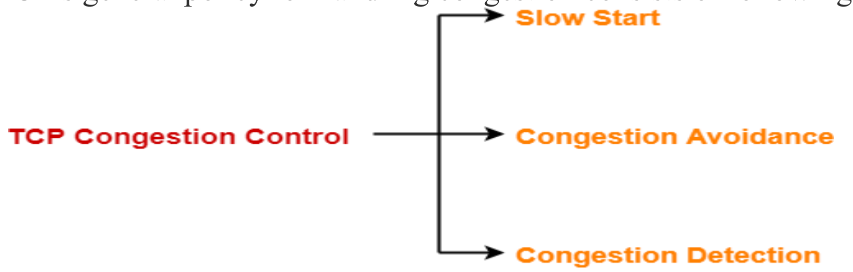
- Sender should not send data greater than congestion window size.
- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.
- So, sender should always send data less than or equal to congestion window size.
- Different variants of TCP use different approaches to calculate the size of congestion window.
- Congestion window is known only to the sender and is not sent over the links.

So, always-

Sender window size = Minimum (Receiver window size, Congestion window size)

TCP Congestion Policy-

TCP's general policy for handling congestion consists of following three phases-



1. Slow Start Phase-

- Initially, sender sets congestion window size = Maximum Segment Size (1 MSS).
- After receiving each acknowledgment, sender increases the congestion window size by 1 MSS.
- In this phase, the size of congestion window increases exponentially.

Congestion window size = Congestion window size + Maximum segment size

2. Congestion Avoidance Phase-

After reaching the threshold,

- Sender increases the congestion window size linearly to avoid the congestion.
- □ On receiving each acknowledgement, sender increments the congestion window size by 1.

Congestion window size = Congestion window size + 1

3. Congestion Detection Phase-

When sender detects the loss of segments, it reacts in different ways depending on how the loss is detected-

Case-01: Detection On Time Out-

- Time Out Timer expires before receiving the acknowledgement for a segment.
- This case suggests the stronger possibility of congestion in the network.
- There are chances that a segment has been dropped in the network.

UNIT-V
Application Layer

Introduction

The **Application layer** provides services that directly support user applications, such as database access, e-mail, and file transfers.

It also allows applications to communicate with applications on other computers as though they were on the same computer.

When an application program uses network services, this is the layer it will access. For example, a web browser uses the Application layer to make requests for files and web pages; the Application layer then passes those requests down the stack, with each succeeding layer carrying out its specified task.

I. Application Layer Services

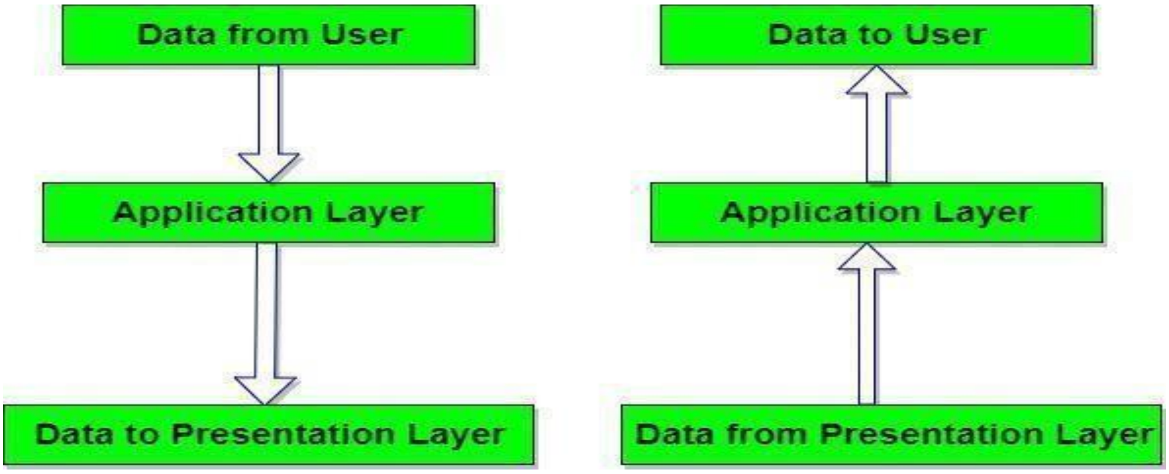
a. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.

b. **Network Virtual Terminal:** It allows a user to log on to a remote host.

c. **Directory Services:** This layer provides access for local

information about various services.

d. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.



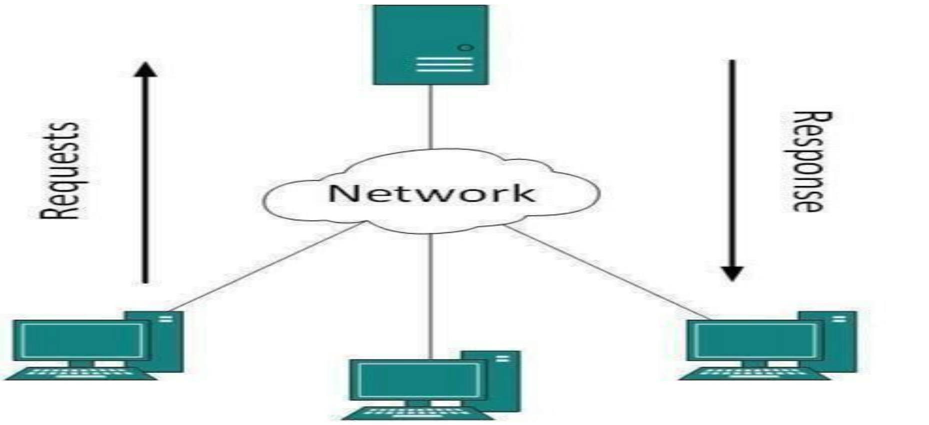
II. Application Layer Paradigms

Client-Server Model

Two remote application processes can communicate mainly in two different fashions:

- **Peer-to-peer:** Both remote processes are executing at same level and they exchange data using some shared resource.
- **Client-Server:** One remote process acts as a Client and requests some resource from another application process acting as Server.

  In client-server model, any process can act as Server or Client. It is not the type of machine, size of the machine, or its computing power which makes it server; it is the ability of serving request that makes a machine a server.



A system can act as Server and Client simultaneously. That is, one process is acting as Server and another is acting as a client. This may also happen that both client and server processes reside on the same machine.

Hyper Text Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

Domain Name System(DNS)

The Domain Name System (DNS) works on Client Server model. It uses UDP protocol for transport layer communication. DNS uses hierarchical domain based naming scheme.

The DNS server is configured with Fully Qualified Domain Names (FQDN) and email addresses mapped with their respective Internet Protocol addresses.

A DNS server is requested with FQDN and it responds back with the IP address mapped with it. DNS uses UDP port 53.

Simple Mail Transfer Protocol(SMTP)

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available.
When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.

TELNET:

Telnet stands for the **Tel**ecommunications **Net**work. It helps in terminal emulation. It allows Telnet client to access the resources of the Telnet server. It is used for managing the files on the internet. It is used for initial set up of devices like switches. The telnet command is a command that uses the Telnet protocol to communicate with a remote device or system. Port number of telnet is 23.

Command

```
telnet [\\RemoteServer]
\\RemoteServer : Specifies the name of the server to which you want to connect
```

World Wide Web

- The World Wide Web (WWW) is a collection of documents and other web resources which are identified by URLs, interlinked by hypertext links, and can be accessed and searched by browsers via the Internet.
- World Wide Web is also called the Web and it was invented by Tim Berners-Lee in 1989.
- Website is a collection of web pages belonging to a particular organization.
- The pages can be retrieved and viewed by using browser.

Let us go through the scenario shown in above fig.

- The client wants to see some information that belongs to site 1.
- It sends a request through its browser to the server at site 2.
- The server at site 1 finds the document and sends it to the client.

RSA Algorithm

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys.
This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the integers are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.