Computer Networks Notes

Contributor: Abhishek Sharma

[Founder at TutorialsDuniya.com]

Computer Science Notes

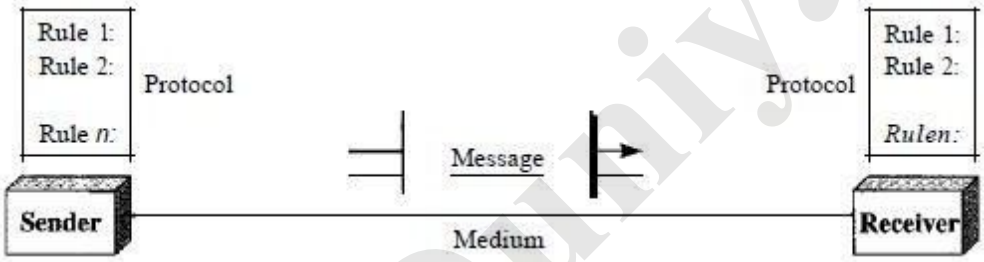
UNIT -I
Introduction to Computer Networks

1.1 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.

Computer Network: A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is connection to the Internet. Other shared resources can include a printer or a file server. The Internet itself can be considered a computer network.

1.1.1 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.

1.1.2 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 (Os or Is). 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.* For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better resolution), but more memory is needed to store the image. After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only blackand- white dots (e.g., a chessboard), a I-bit pattern is enough to represent a pixel. If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11. There are several methods to represent color images. One method is called RGB, so called because each color is made of a combination of three primary colors: *red,* green, and blue. The intensity of each color is measured, and a bit pattern is assigned to it. Another method is called YCM, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio:

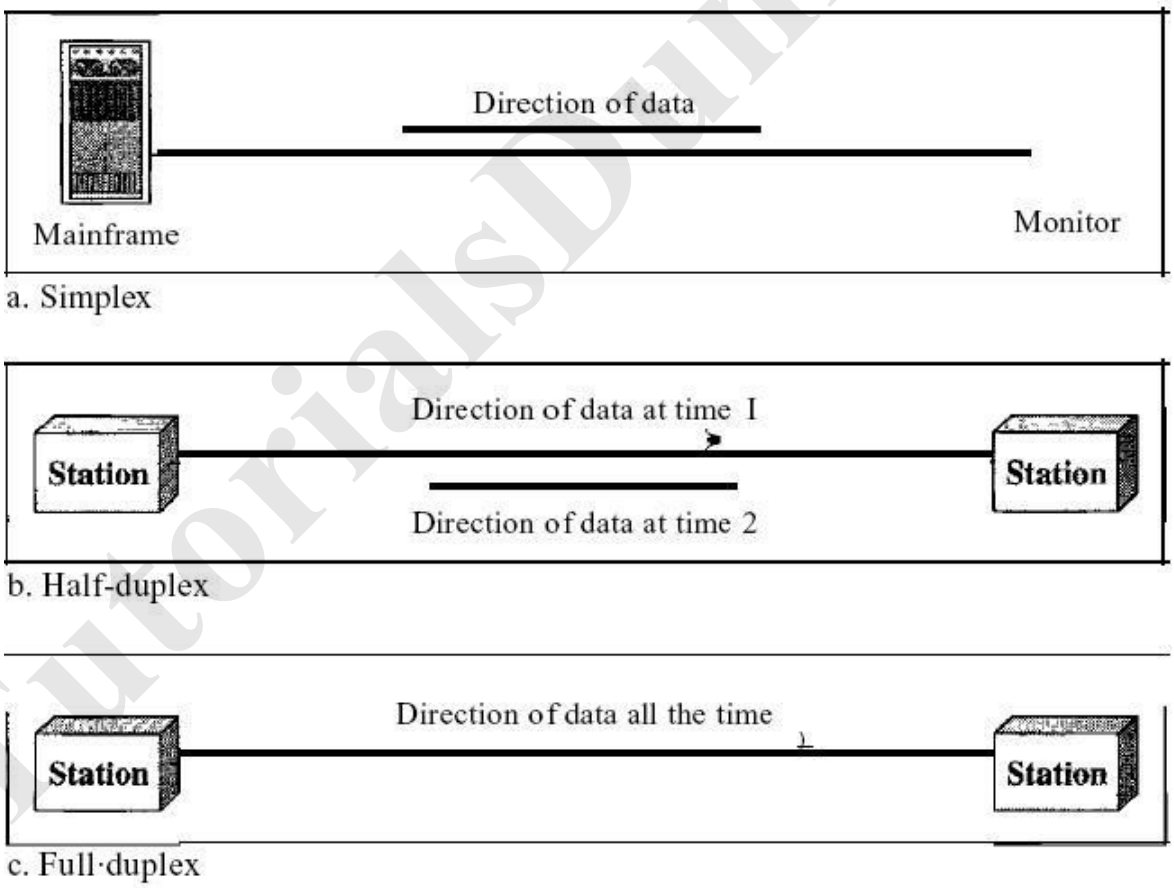
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal. In Chapters 4 and 5, we learn how to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

1.1.3 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 tW<D-way street with traffic flowing in both directions at the same time. In full-duplex mode, si~nals going in one direction share the capacity of the link: with signals going in the other din~c~on. This sharing can occur in two ways: Either the link must contain two physically separate t:nmsmissiIDn paths, one for sending and the other for receiving; or the capacity of the ch:arillilel 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.

1.2 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.

1.2.1 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.

1.2.2 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 throughput 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.

1.2.3 Physical Structures:

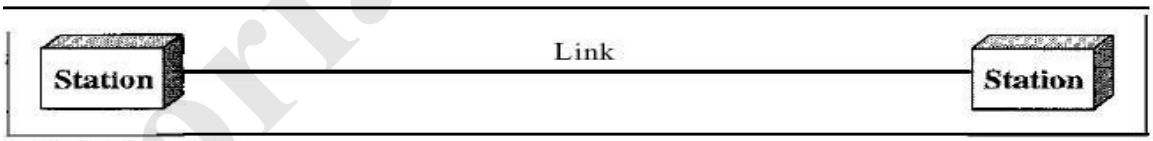
Type of Connection

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

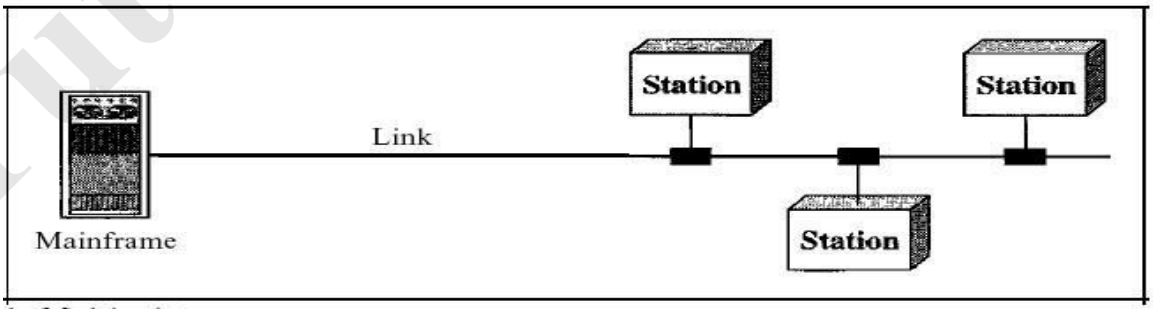
A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite 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 multidrop) 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.



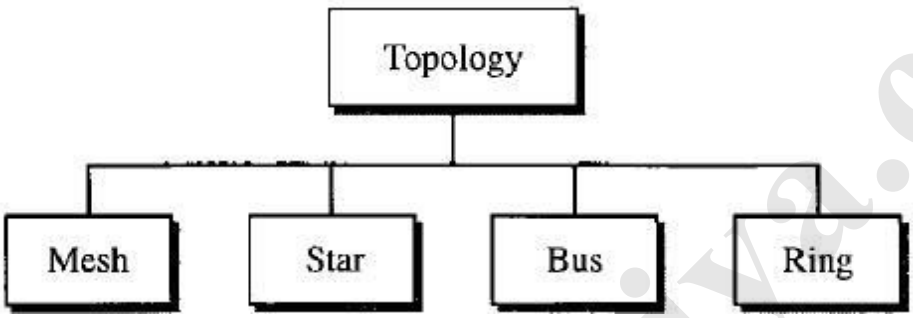
a. Point-to-point



b. Multipoint

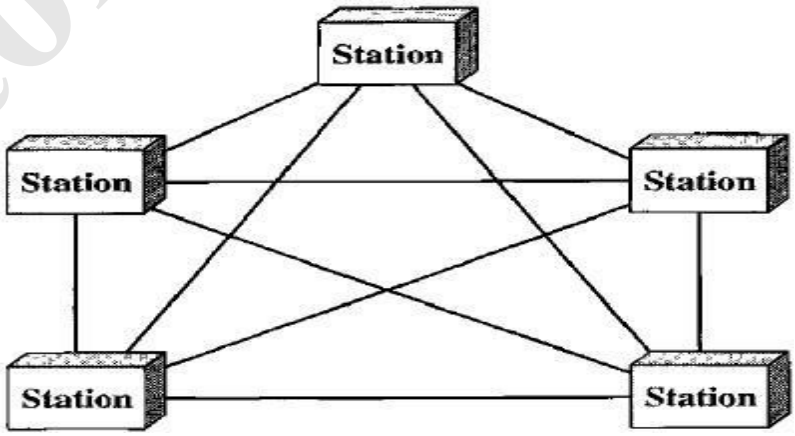
1.2.3.1 Physical Topology

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, and ring



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.

1. Disadvantage of a mesh are related to the amount of cabling because every device must 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.

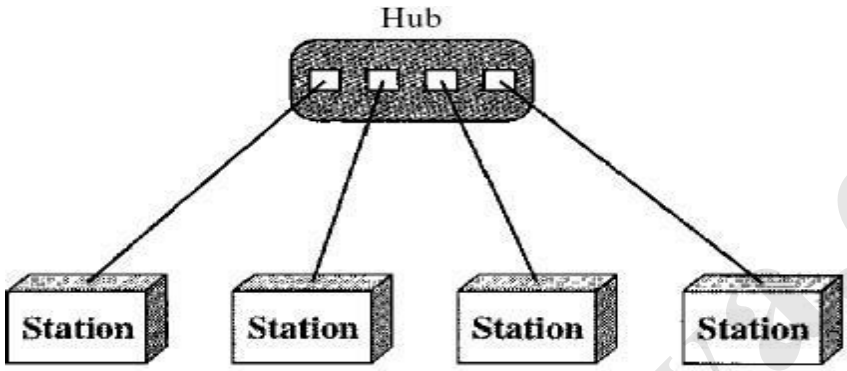
For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

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.

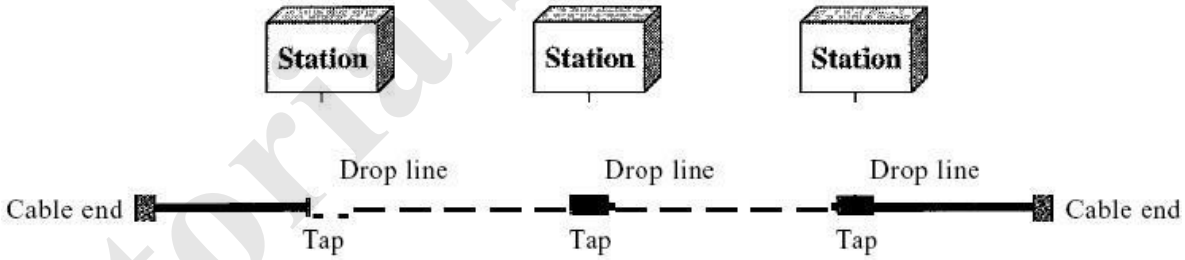
Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.



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.

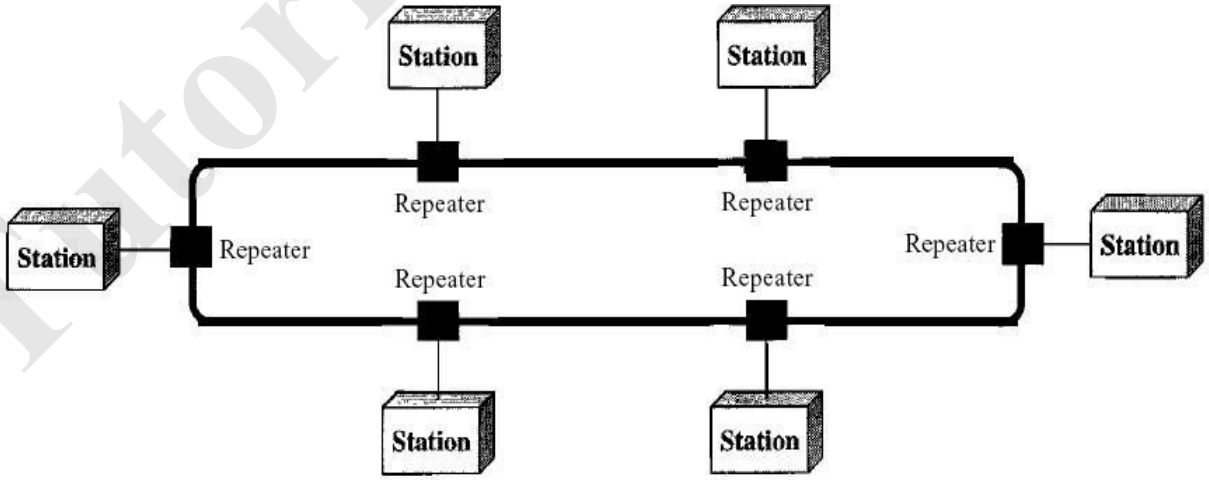
Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same 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.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

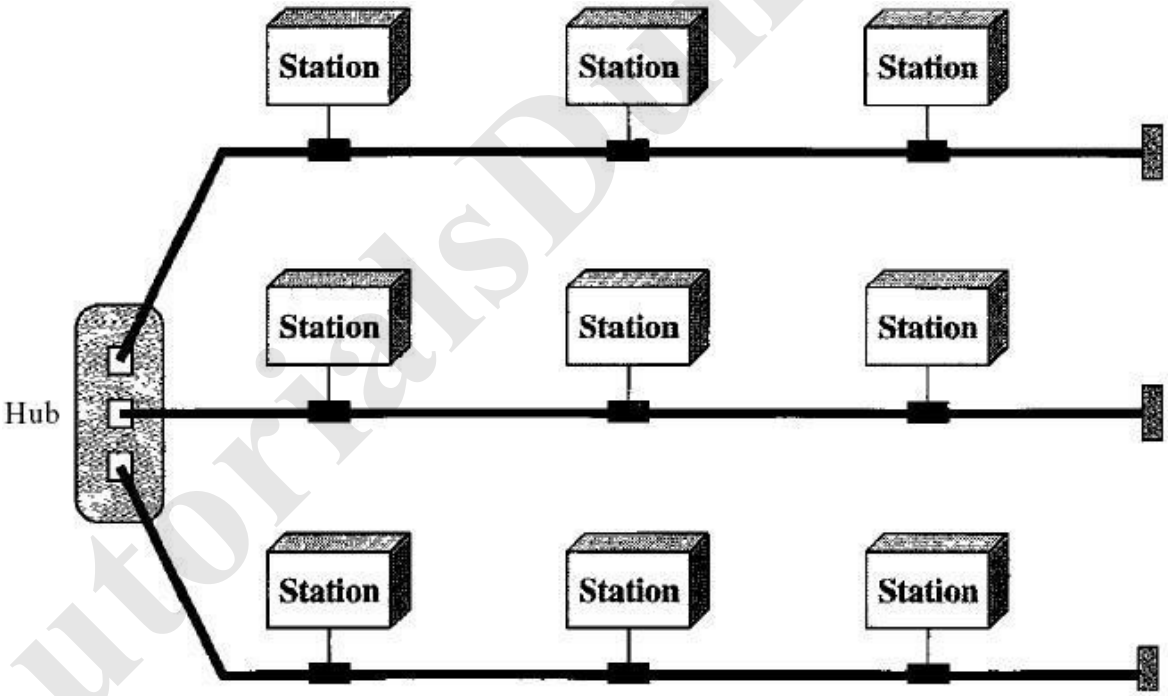
Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular.

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



A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

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



1.2.4 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 kilometres 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.

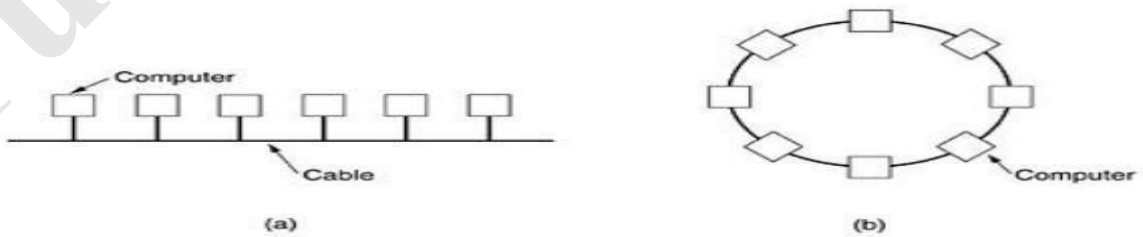


Fig.1: Two broadcast networks . (a) Bus. (b) Ring.

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):

Metropolitan Area Network:

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. The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on. But from their inception until the late 1990s, they were intended for television reception only. To a first approximation, a MAN might look something like the system shown in Fig. In this figure both television signals and Internet are fed into the centralized head end for subsequent distribution to people's homes. Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as IEEE 802.16.

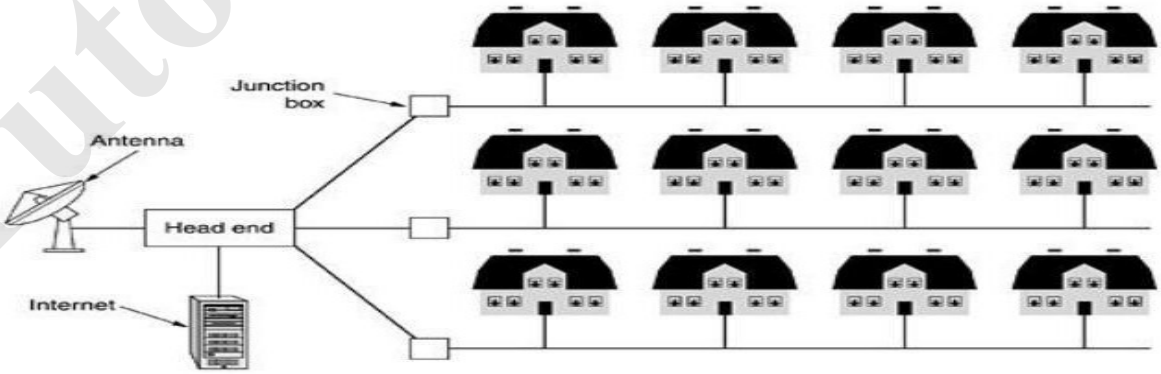


Fig.2: Metropolitan area network based on cable TV.

TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well

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).

Wide Area Network:

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. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.

Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design. In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers. If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers. When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded. A subnet organized according to this principle is called a store-and-forward or packet-switched subnet. 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.

The principle of a packet-switched WAN is so important. Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence. These packets are then injected into the network one at a time in quick succession. The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process. A stream of packets resulting from some initial message is illustrated in Fig.

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.

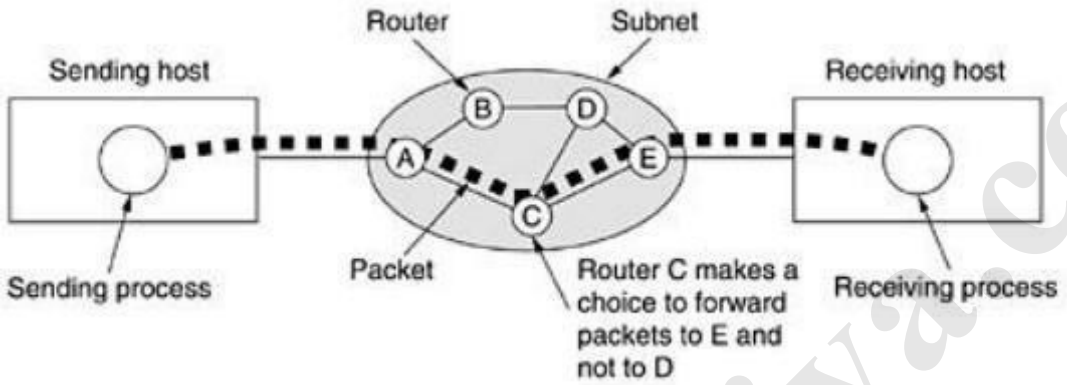


Fig.3.1: A stream of packets from sender to receiver.

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 Trekkie, 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.

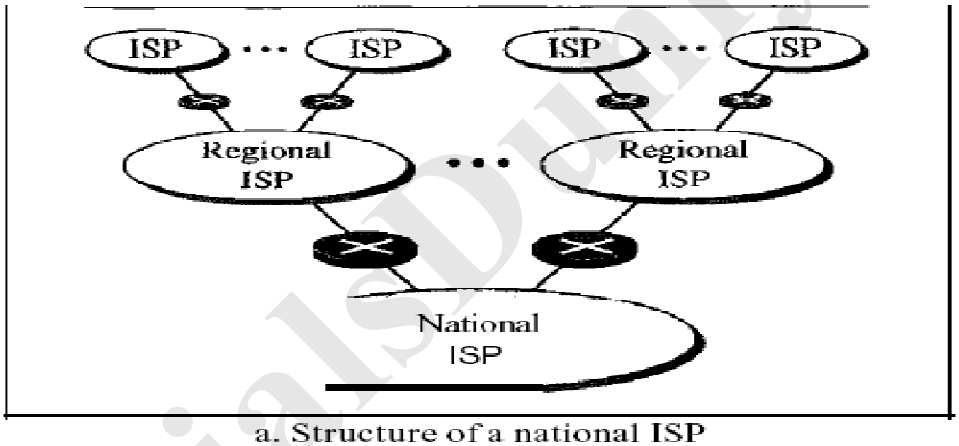
In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *inteiface message processor* (IMP). The IMPs, in tum, 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 *Internetting 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

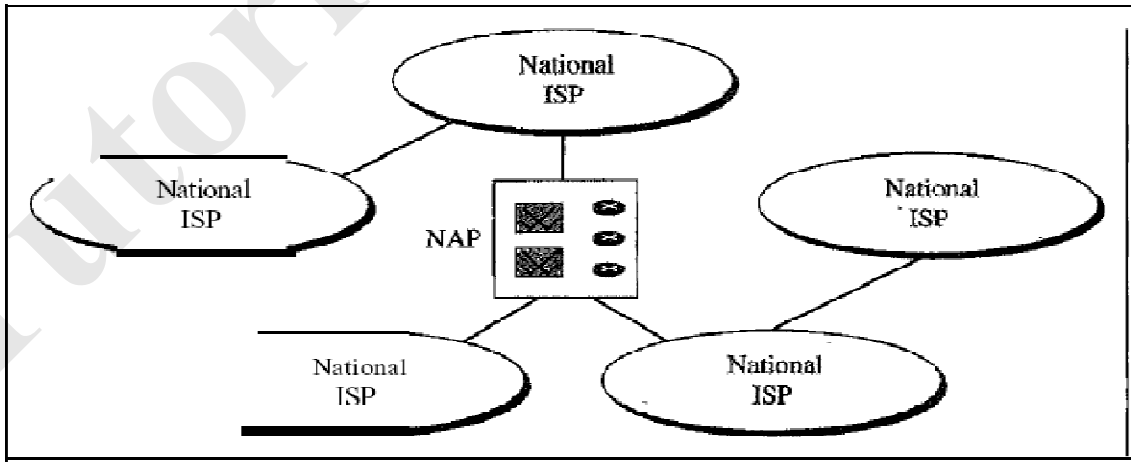
segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP.

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 (lSPs). 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.

1.4 PROTOCOLS AND STANDARDS

Protocols:

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

o Syntax. The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

o Semantics. The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

o Timing. The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

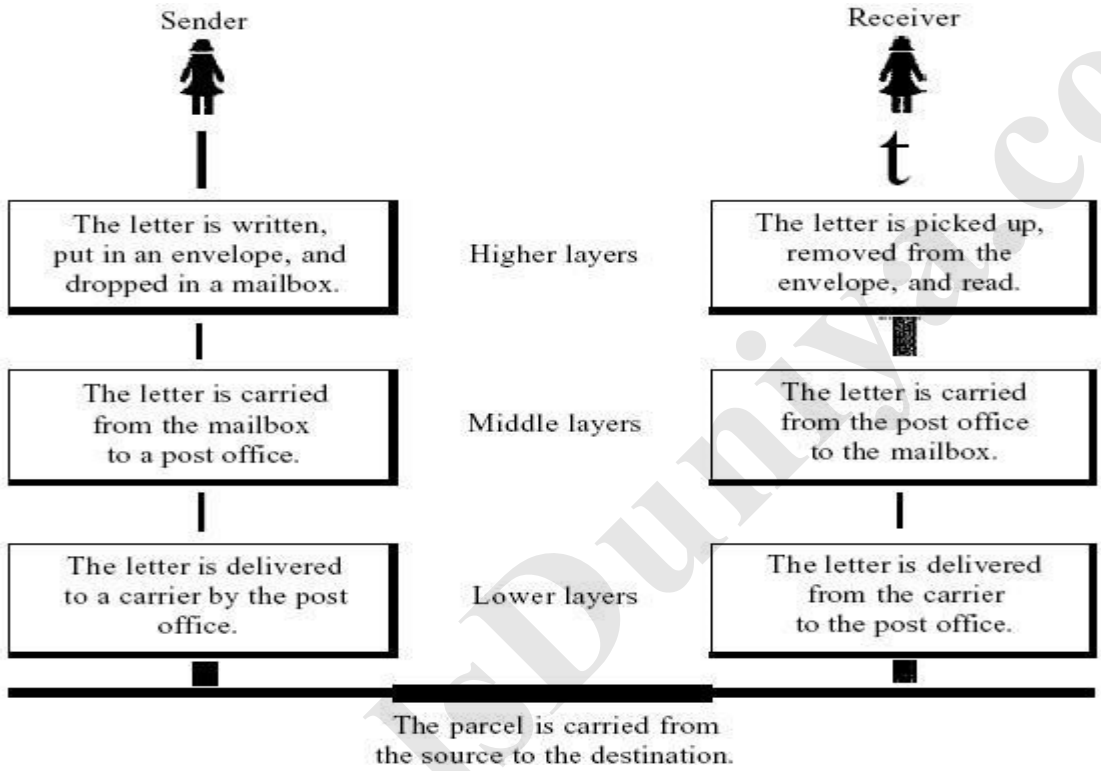
Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" or "by regulation").

o De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.

o De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

1.5 LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal maiL The process of sending a letter to a friend would be complex if there were no services available from the post office. Below Figure shows the steps in this task.



Sender, Receiver, and Carrier

In Figure we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sender Site

Let us first describe, in order, the activities that take place at the sender site.

- o Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.
- o Middle layer. The letter is picked up by a letter carrier and delivered to the post office.
- o Lower layer. The letter is sorted at the post office; a carrier transports the letter.

0n the Way: The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

- o Lower layer. The carrier transports the letter to the post office.
- o Middle layer. The letter is sorted and delivered to the recipient's mailbox.
- o Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

1.6 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.

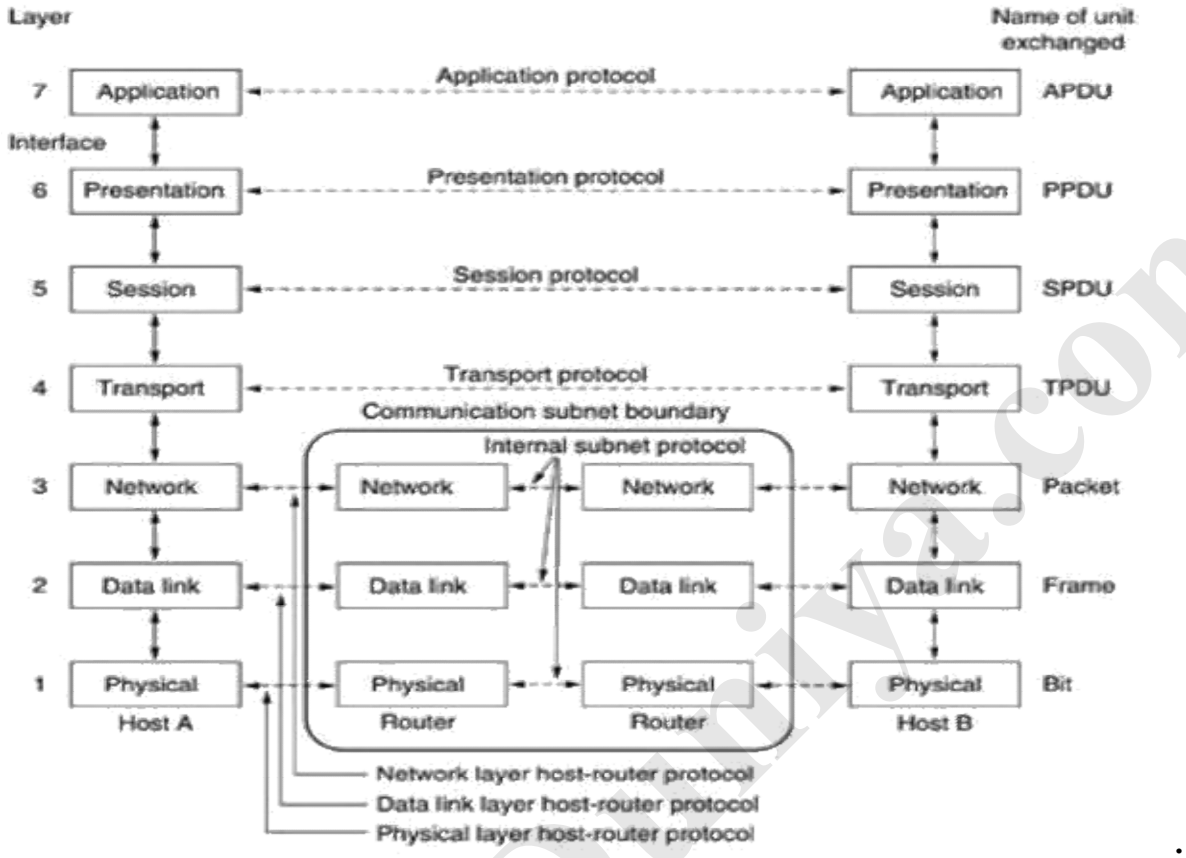


Fig.4: The OSI reference model

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 neighbours, 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

Application Layer

Transport Layer

Internet Layer Host-to-

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

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.

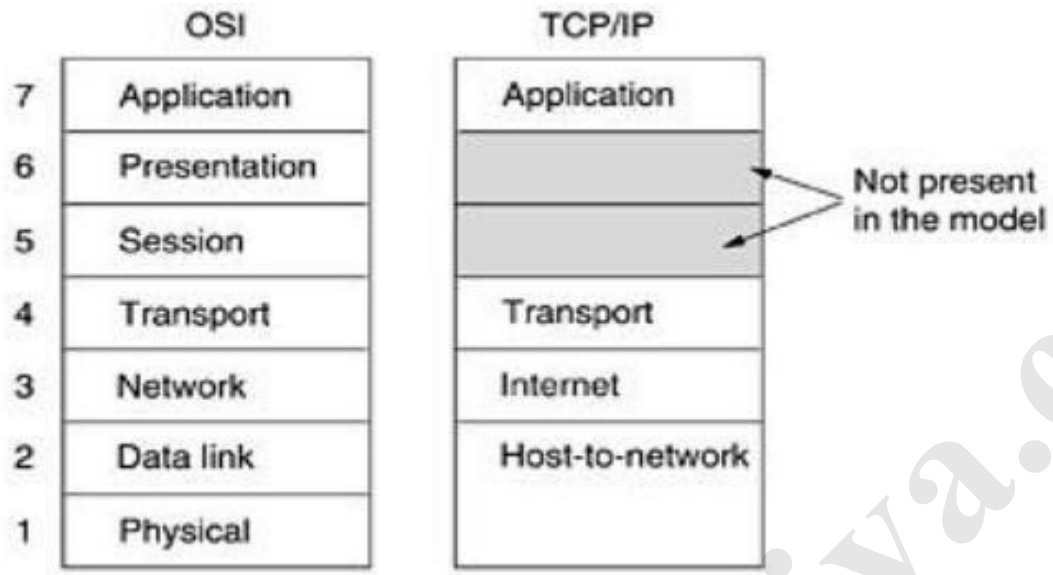


Fig.1: The TCP/IP reference model.

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.

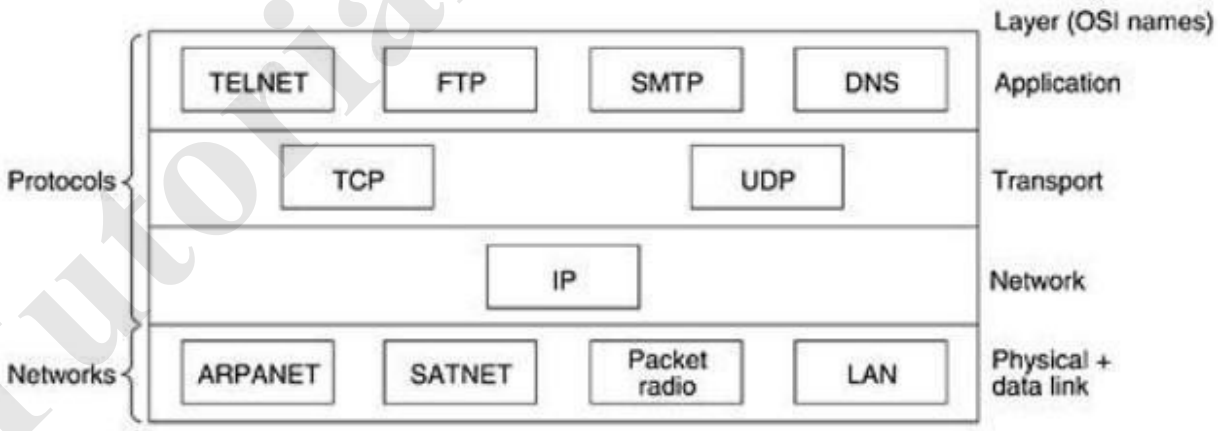


Fig.2: Protocols and networks in the TCP/IP model initially.

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.

TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well

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.

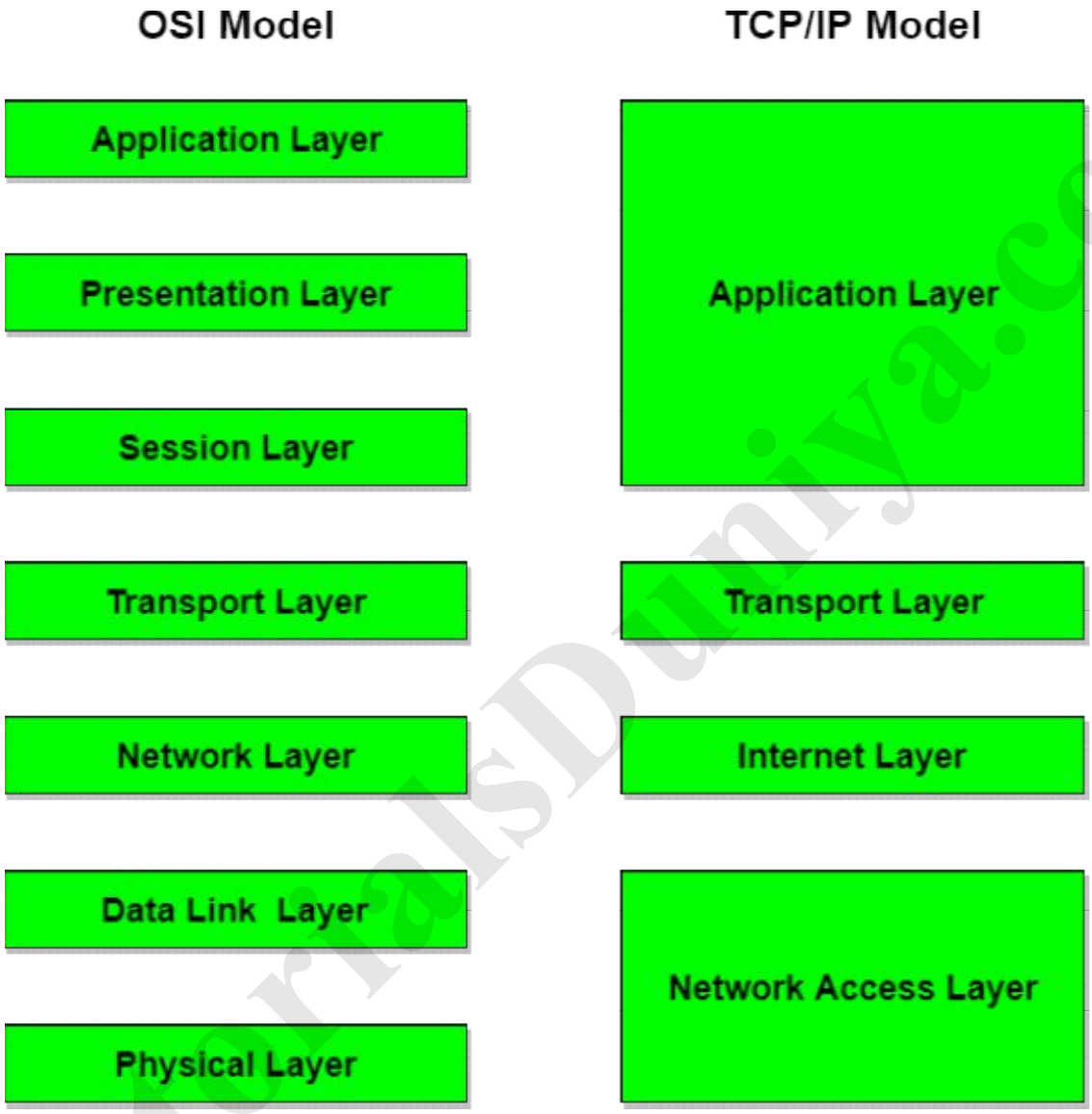
As a consequence, the protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes. Being able to make such changes is one of the main purposes of having layered protocols in the first place. The OSI reference model was devised before the corresponding protocols were invented. This ordering means that the model was not biased toward one particular set of protocols, a fact that made it quite general. The downside of this ordering is that the designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.

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, giving the users a choice. This choice is especially important for simple request-response protocols.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology	10. In TCP/IP replacing protocol is not easy.

changes.	
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
12. It has 7 layers	12. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model

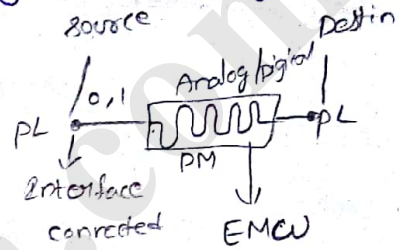


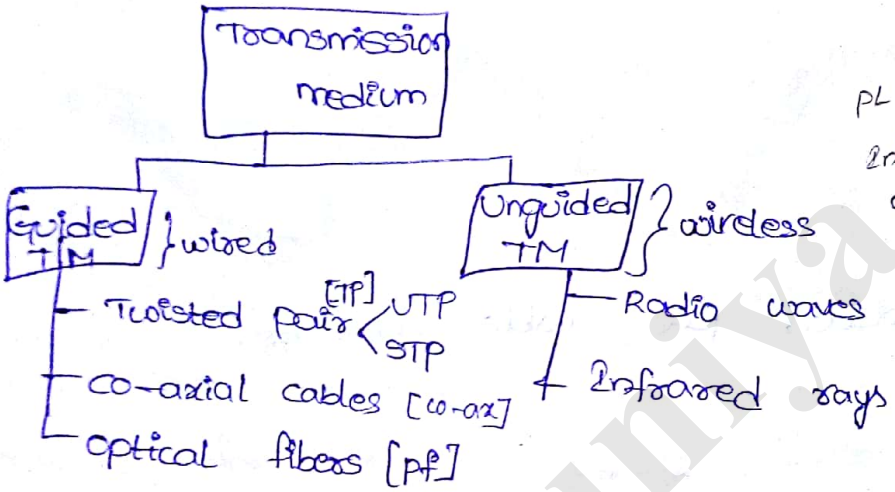
UNIT II

Physical Layer

Transmission Medium / physical Medium / Communication Medium:-

* Physical path blw transmitter and receiver.
* Repeaters or amplifiers may be used to extend the length of the medium. (capacity)
* Communication of electromagnetic wave is guided or unguided.





UTP - unshielded Twisted pair

STP - shielded Twisted pair

Digital Transmission Media Bit Rates:-

frequency is measured in terms of Hz

Digital Transmission (DTS) system	Bit rate	observations.
Telephone twisted pair	33.6 Kbps	4KHz telephone channel.
Ethernet over twisted pair	10 Mbps	100 meters over unshielded twisted pair.
Fast ethernet over twisted pair	100 Mbps	100 meters using several arrangements of unshielded twisted pair
Cable modem	500 Kbps to 4Mbps	shared CATV return channel.
ADSL (Asymetric Digital Subscriber Line) over twisted pair	64-640 Kbps in bound 1.536-6.144 Mbps outbound.	uses higher frequency band and coexists with conventional analog telephone signal, which occupies 0-4 KHz band.
Radio LAN in 2.4 GHz band	2Mbps	IEEE 802.11 wireless LAN.
Digital radio in 28 GHz band	1.5-45 Mbps	5Km multipoint radio link.

optical fiber transmission system	2.4 – 9.6 Gbps	Transmission using one wavelength
optical " " "	1600 Gbps and higher	multiple simultaneous wavelength using wavelength division multiplexing.

11/12/18

Twisted pair:-

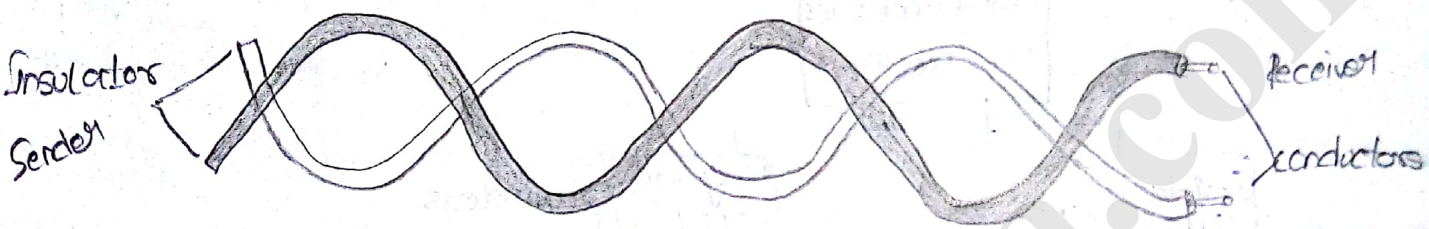


Fig:) Twisted pair cable structure.

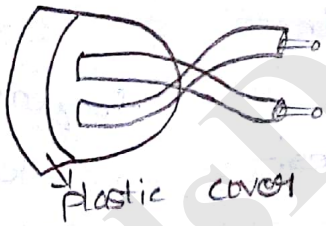


Fig: 1(a):- Unshielded Twisted pair (UTP).

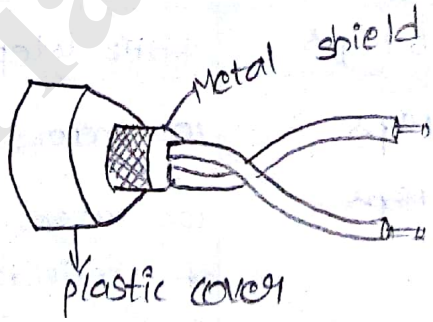


Fig: 1(b):- shielded Twisted pair (STP)

* A Twisted pair is provides a physical path between transmitter and receiver to carry signals physically.
* A Twisted pair is generally unshielded twisted pair.
* A Twisted pair cable is consisting two copper wires;

* one copper wire is using for signal transformation from sender to receiver where as another copper wire is used for the purpose of ground Reference.

* Basically a twisted pair one end is attached with insulator and other end is connected to conductor. Most frequently used twisted pair is unshielded twisted pair (UTP) in telephone lines and ethernet LAN. for voice and vedio signals transfotation.

* shielded twisted pair is another type of twisted pair which is designed by IBM and most specifically used in satilite communication where as STP connectors are more expensive than UTP connector.

* The examples for "RJ-45 Female" these are UTP connectors
"RJ-45 Male"

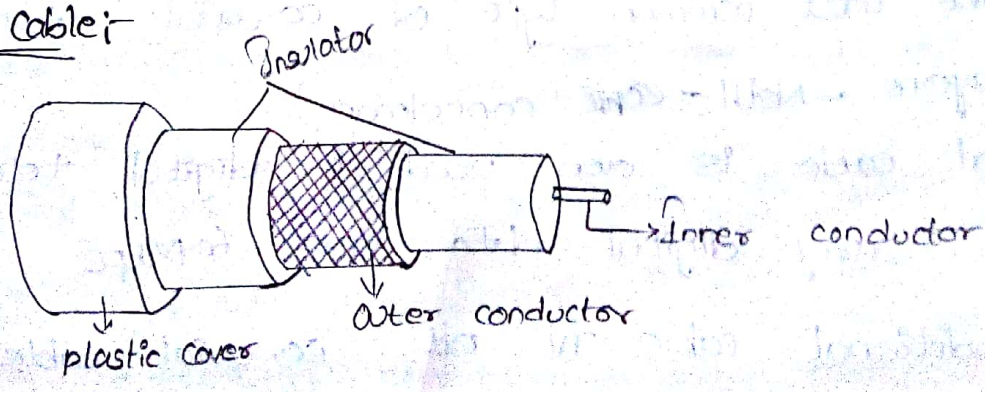
* In STP Transmission medium the Insulator of copper conductor covered by metal shield which is protected by plastic covers.

* In STP Metal shield (or) Metal foil (or) braided cover is protects signals without effecting noise &

* The twisted pair cables are twisted together to implement effecient communication path b/w transmitter & Receiver if the two wires of twisted pair are connected parallelly than there will be created noise and cross talks.

13/12/18

=> Co-axial Cable:-



* Co-axial cable is a specified type of transmission medium which is able to provide physical part between transmitor & receiver.

* Co-axial cable is consisting a copper conductor internally and out covered by another copper conductor which are insulated with plastic cover.

* These co-axial cables are designed to transport signals via analog telephone n/t which could carry 10,000 voice signals at a time.

* Co-axial cables are categoriesed into two types depending on capacity.

	category	Impedence	use
Type-1 →	RG-59	75 Ω	cable TV
Type-2 →	RG-58	50 Ω	thin Ethernet
	RG-11	50 Ω	thick Ethernet.

* As specified in the above table these are co-axial cables classified into two types 1. 75 Ω
2. 50 Ω.

* RG is expanded as Radio Government.

* connect co-axial cable devices we need co-axial cable converters. The most common type of co-axial cable connector is BNC. (Bayone - Neill - concelman)

* co-axial cable is even used in digital telephone n/t and i carry digital data upto 60Mbps

* In traditional cable TV n/t co-axial cables are

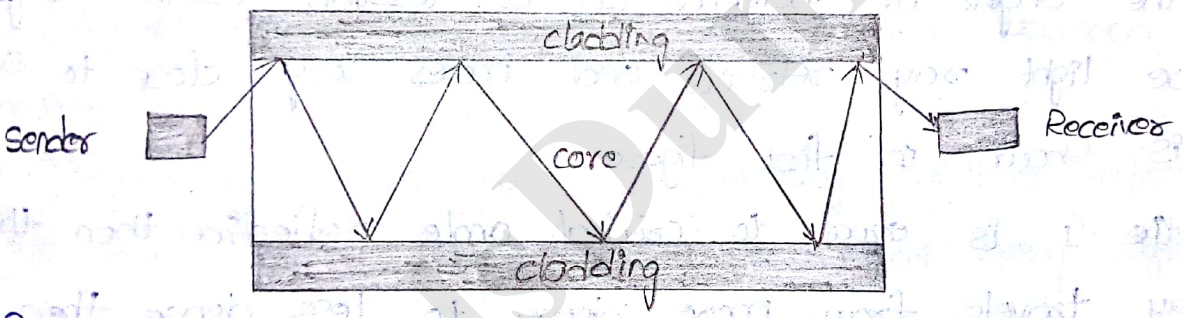
are replaced by fiber optic lines because of high speed data transfer.

* The another common application of co-axial cable is used in ethernet.

* Thin ethernet is supporting for digital transmission of data using 10 base 2 by RG-58 ; 50Ω co-axial cable. this can transmits the data at 10Mbps with a range of 185 mts.

* The Thick ethernet is supporting for digital transmission of data using 10 base 5 by RG-11 ; 50Ω co-axial cable and this can transmits the data at 10Mbps with a range of 500mts

fiber optic cables:-



* In the types of transmission medium of co-axial cable, twisted pair cable accepts and transports the signals in the form of electric current where as in optical fibers cables accepts and transports the signal in the form of light signal.

* An optical fiber cable is connected between the two physical layers of source and destination systems which can provides the physical path to carry the data in the form of light waves.

* An optical fiber is cable is made of glass (or) plastic which can be able to explore through various aspects of light. To understand the transmission medium of optical

fiber we need to understand first the light wave propagation mode and the incidence of critical angles.

* The optical fiber cable is consisting the outcover of cladding material and internally through the core the light waves are propagated internally using different propogation modes of core material.

* Optical fiber cables projects light ray dog which can travel at different density through the core by changing the ray directions in the below three figures there is explain how light ray direction changes from more dense to less dense of substance.

* If the angele of incidence (I) is less than critical angele then the light ray refracts and moves very close to surface which is shown in first figure.

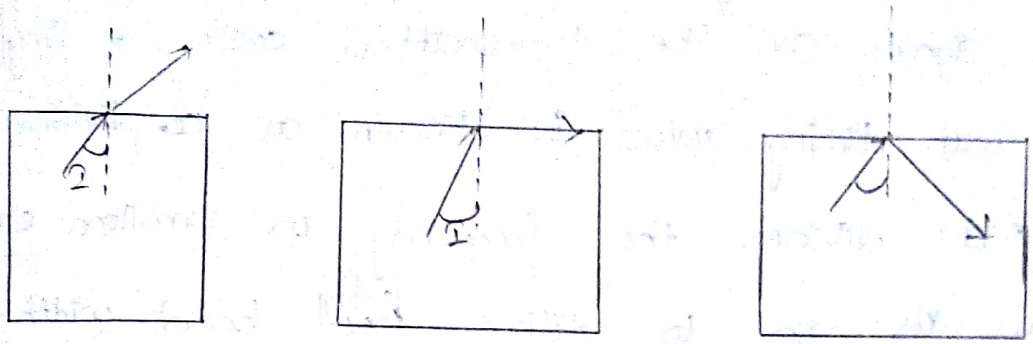
* If the I is equal to critical angle reflection then the light ray travels from more dense to less dense then the light ray bends along with the interface.

* If the I is greater than critical angle Reflection then the light ray travels from more dense to less dense then the light ray travels towards critical angle with reflection.

* Generally a critical angle Reflection (CAR) is a property of substance and it can changes depending on different substance

* The light ray through optical fiber is propogated depending on the type of mode. The mode is may be single mode (or) multi mode through this mode only the beam of light

space can be travel. Comparatively the all available types of transmission mediums the optical fibers are capable of high data transfers for long distances.



Multiplexing:-

* Multiplexing is a technique which is applied on physical medium to share physical path among multiple nodes to utilize band width efficiently. Multiplexing technique is used by many different analog and digital streams to share physical medium between multiple computers.

* Multiplexing devides the high capacity medium logically and assigns the acquire frequencies to each and every system simultaneously. Multiplexing mechanism are used at the side of multiple senders who are try to send over a single medium can be implemented by a device known as multiplexer and the signals received by demultiplexers at the other end of physical medium by receivers.

* The physical medium sharing can be done based on following parameters.

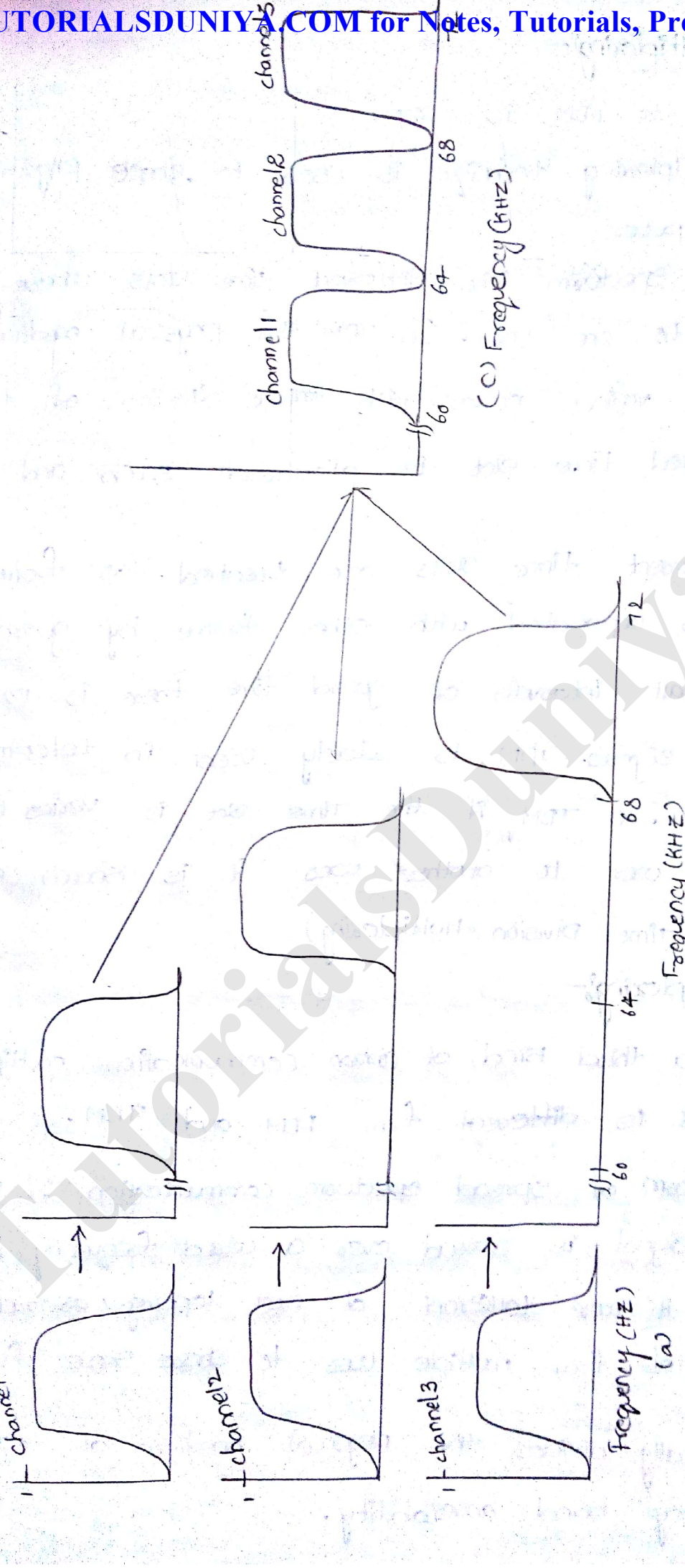
a. physical medium sharing is done based on frequencies among multiple users these known as frequency division multiplexing.

* the physical medium capacity is divided based on the timing values where as each and every time slot is assigned to a specific system is known as time division multiplexing).

* Multiple data signals can be transmitted over a single frequency along with timing values is known as co division multiplexing. FDM divides the frequency in smaller channel but CDM allow its user to utilize full band width. at all timing slot

Frequency Division Multiplexing:-

* Frequency division multiplexing is a pure analog technology which is introduced and use to the first generation of communication. FDM carries and divides the spectrum in two logical channels and allocates specific frequency each and every user independently and can provide exclusive access to the users. All channels are divided depending on frequency and binaries can be transmitted without over lapping with each other. channels are separated by guard bands. Guard band is a frequency which is not used by either channel; which can be logically separates each and every user channel frequency without interfering by others.



Time Division Multiplexing:-

* In alternative to FDM is TDM.
* TDM is multiplexing technique is used to share physical medium among computer.
* TDM divides spectrum into different time slots whose as each is assign to one user. In TDM the physical medium is shared among various nodes with logical division of total time and a fixed time slot is allocated each and every system.
* In TDM different time slots are treated as frames so each frame is separated with other frame by guards because of small intervals of guard time there is no overlapping b/w signals. TDM is widely used in telephone and cellular N/t. In TDM if the time slot is varies (Not fixed) from one user to another user it is known as STDM (Statistical Time Division Multiplexing)

Code-Division Multiplexing:-

* CDM means a third kind of common communication multiplexing mechanism. Ep it is different from FDM and TDM.
* CDM is a form of spread spectrum communication in which a narrow band signal is spread over a wired frequency band. This can make it more tollerant of over lapping, as well as allows multiple signals from multiple user to share same frequency bands.
* CDM is basically divides the physical medium at required time slot frequency band accessability.

TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well

* CDM allows to transfer each station over the entire frequency spectrum at all the time.
* In CDM multiple stations can transfer signals and utilize full band width at any allocated time slots.
* CDM is able to extract design signal effectively than TDM & FDM.
* CDM is used by cable n/t and satellite communication n/t.

Datalink layer design issue:- the purpose of introducing datalink layer. - Network layer services

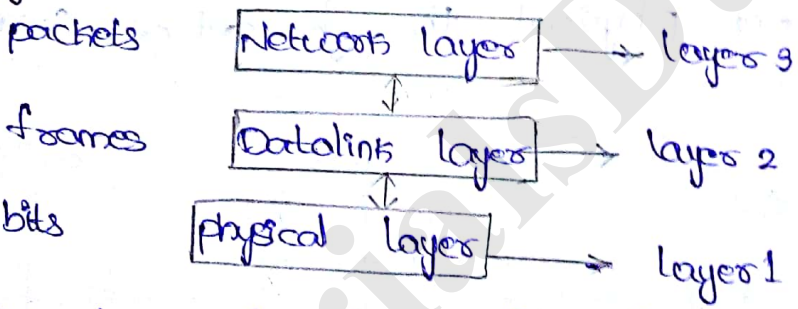
- framing
- Error control
- flow control

Network layer services implementation:-

* Data link layer data format is frame. Data link layer recives either packets (or) binarys from nt layer at the side of sender and from physical layer at the side of receiver.

* Framing a process of converting packets and binarys into frames.

Framing:-

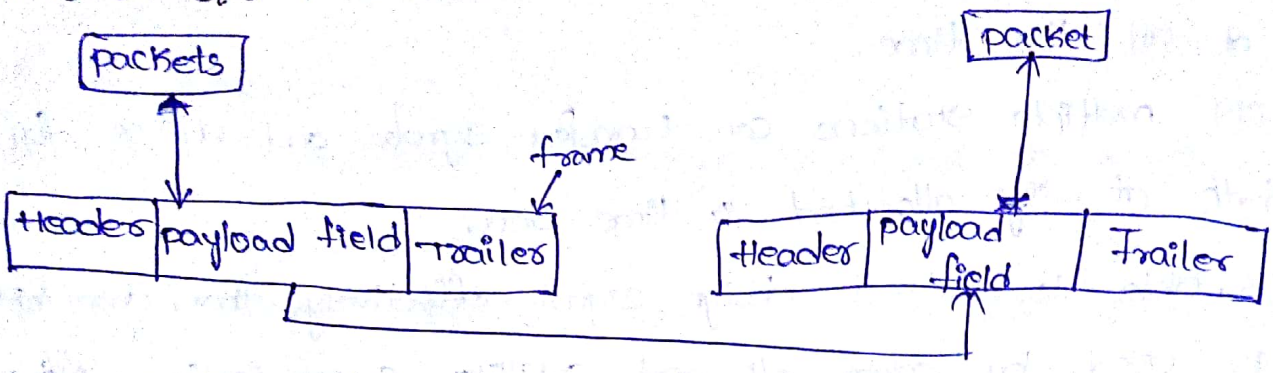


* Datalink layer is design with the primary purpose of achieving reliable and efficient communication b/w source & destination.

* Datalink layer accepting as well as offering the services to the network layer.

* Datalink layer frame is consisting frame header, payload field as well as trailer

Relation b/w packets and frame:-



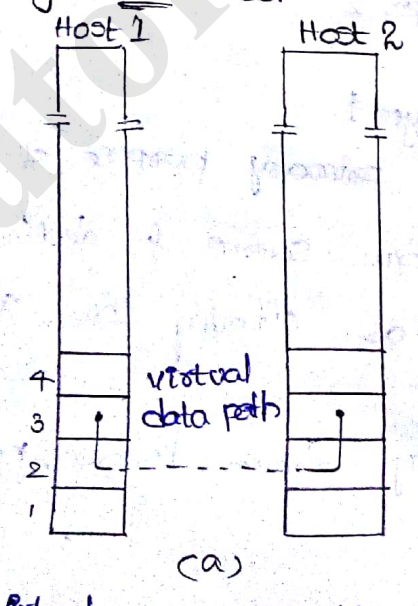
Header & trailer parts of a frame is representing the starting and ending sequences of a message which is to be transported

A message is contained in a payload field.

The network layer service is forwarded to the datalink layer and the datalink layer principal service function is to transfer the data from the network layer on the source machine to network layer of distination machine logically.

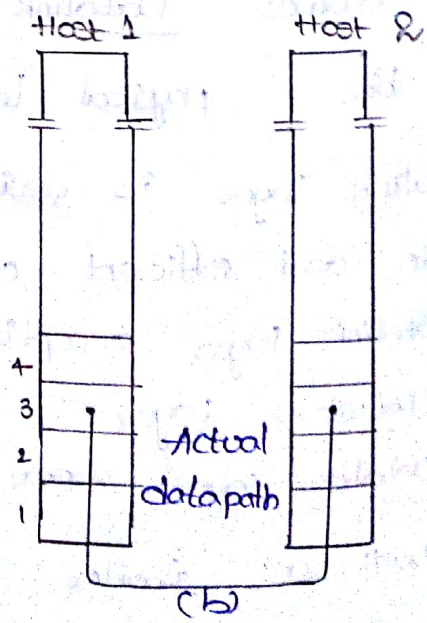
Datalink layer logically connected from source to datalink layer destination machine is through virtual communication layer the datalink layer accepts the packets converts into the frame data forword to physical layers. from physical layer of source machine to connect physical through actual communication path.

Network layer services:-



(a)

Virtual communication



(b)

Actual communication.

Datalink layer implement possible services offered:

1. Unacknowledged connectionless service
2. Acknowledged connectionless service
3. Acknowledged connection-oriented service.

Datalink layer implements even acknowledgement policy in connectionless services.

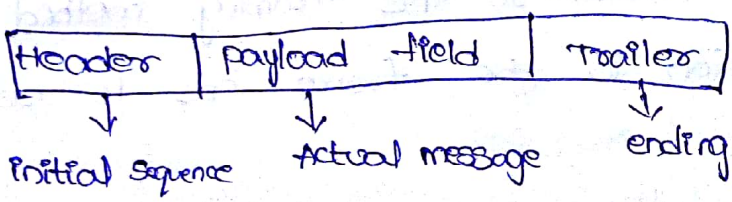
Unacknowledged connectionless Service:-

* It consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

Eg:-
Ethernet, voice over IP, etc. in all the communication channel where real-time operation is more important that quality of transmission.

Framing:- The process of converting packets at the sender side binaries at the receiver side into frames is known as framing.

* Actually framing process is too difficult to implement. Frame
* Framing is a specific functionality implemented by data link layer.
* the general frame structure is consisting three parts.



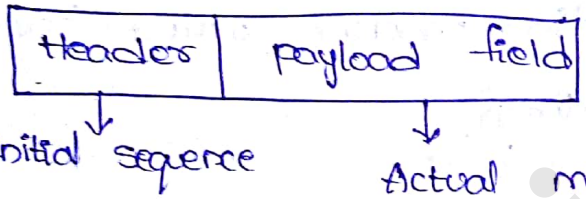
* Depending on the framing process the trailer sequence is optional.
* They has been proposed for various trailing method by

the datalink layer.

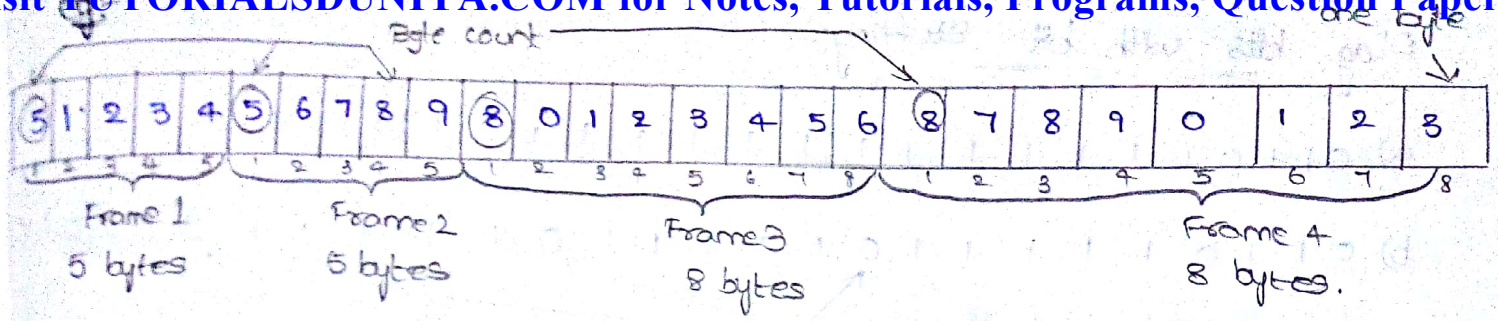
1. Byte count
2. Flag bytes with byte stuffing
3. Flag bits with bit stuffing
4. physical layer coding violations.

Byte count Framing Method:-

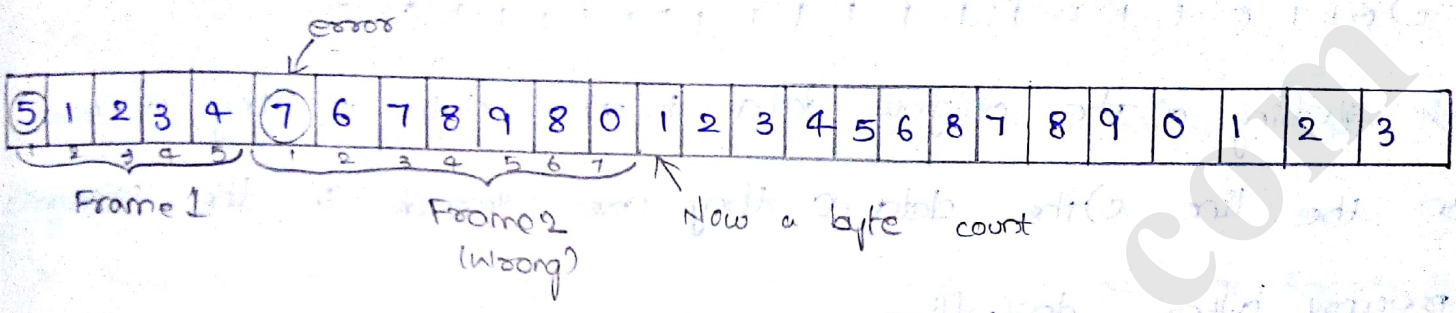
* Byte count framing method is a specific type of framing method which is implemented by data link layer.
* The frame structure in this framing method is generally two parts like



* In this framing method the header part of a frame structure is specifing byte count which gives the total count of bytes that are transported from source to destination.
* Once the header information is being received by receiver it will be used to determine the end of the frame.
* Problem with this framing method is when the header information (Byte count) is incorrect then it will be effected to lead wrong messages to the correct frame as well as to the other frames also. So, that the total message transmission get out of synchronization. In this framing method to avoid this problem this solution is the frame has to be entirely re-transmitted.



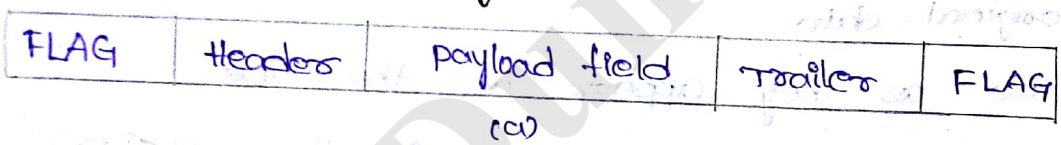
(a)



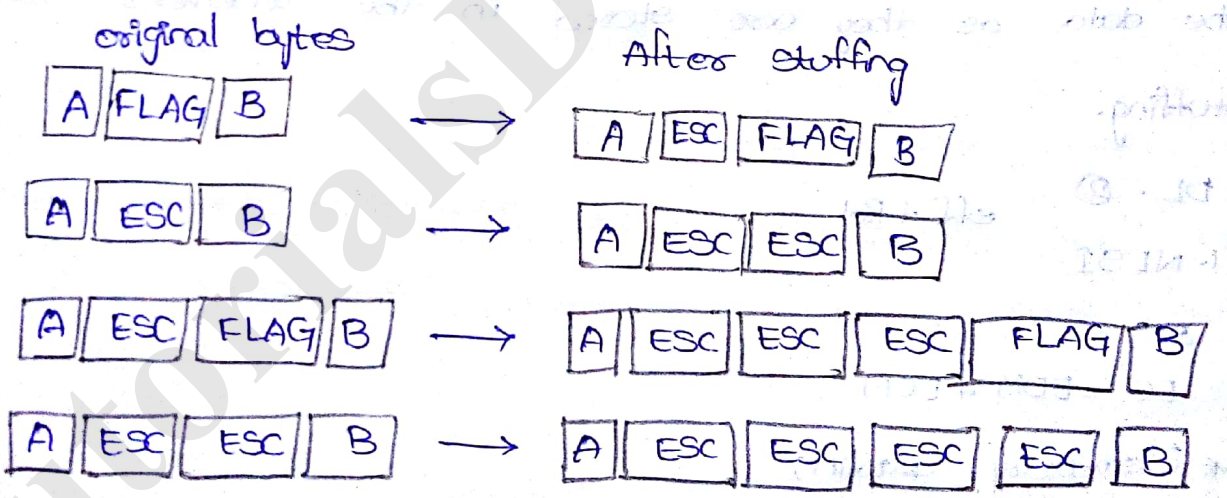
(b)

A byte stream a) without errors b) with one error.

2. Flag bytes with byte stuffing:-



(a)



(b)

a) A frame delimited by flag bytes

b) four examples of byte sequences before and after byte stuffing.

Flag bits with bit stuffing:-

a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

Stuffed bits

c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Bit stuffing a) the original data b) the data as they appear on the line c) the data as they are stored in the receiver's memory after destuffing.

Physical layer coding violations:-

Bit stuffing (a)

a) the original data

b) the data as they appear on the line

c) the data as they are stored in the receiver's memory after destuffing.

DL - ②

eff + Rel

1. NLSI

2.

EC = EDM + ECM

* Elementary datalink

* sliding window

Elementary data link protocol:-

- Utopian simplex protocol
- Simplex stop-and-wait protocol for Error-free channel.
- Simplex stop-and-wait protocol for Noisy channel.

Utopian simplex protocol:-

* this protocol is also known as protocol 1 of datalink layer. In this protocol it provides the data transmission (both sender and receiver) in one direction only.
* the communication channel is assumed to be error free channel and can quickly process infinite data frame.

problem with protocol (1):-

* Data loss because of simplex data transmission b/w sender and receiver.
* channel capacity will be wastage because of re-transmission

```
typedef enum {frame arrival} event type;
#include "protocol.h"
void Sender1(void)
{
 frame s;
 packet buffer;
 while (true){
 from network layer (&buffer);
 s.info = buffer;
 to physical layer (&s);
 }
}
....
void receive 1 (void)
{
 frame r;
 event type event;
 while(true){
  wait for event(&event);
```

from physical layer(&r);
to network layer(&r.info);
}
}

Simplex stop-and-wait protocol for Error free channel:

* This protocol is also known as protocol 2 of data link layer
* In this stop and wait protocol of data link layer to acheive error free data transmission the sender transmits data frames and stops the data frame transmission until as Receiver waits still the complete data frame transmission arrive to the receiver after that only a receiver can utilize the channel for data frames transmission.
* In this protocols also there is one direction data flow the sender and Receiver.
* Even though in this protocol also there is a possibility to occur errors because of simplex direction of data-frame transmission b/w sender and Receiver.
* The protocol 2 assumptions are 1) Finite Buffer capacity at receiver side to process finite no. of data frame.
2) Still in protocol 2 it is assume an error free channel b/w sender and receiver.
* problem with protocol 2 is data loss because of sender prolongs channel utilization time of data-frame transmission from sender to receiver.

protocol 2 is better in performance when comparatively with protocol 1 but still there is a possibility to miss the

data-frame because of practical implementation problem with stop-and-wait protocol.

```
#include "protocol.h"
void sender2(void)
{
 frame s;
 packet buffer;
 event type event;
 while (true) {
   from network layer (&buffer);
   s.info = buffer;
   to physical layer (&s);
   wait for event (&event);
 }
}
...

void receiver2(void)
{
frame r, s;
event type event;
 while (true) {
    wait for event (&event);
    from physical layer (&r);
    to network layer (&r.info);
    to physical layer (&s);
 }
}
```

Simplex Stop-and-wait protocol for Noisy channel :-

* protocol3 uses simplex direction data transfer b/w sender and receiver, still in protocol3 sender sends a data frames and waits for an acknowledgement from the receiver machine so that even though in physical layer binaries coded into signals with errors still protocol3 can attempt to minimize the rate of errors generated through the noisy channel.

* protocol1 is the least priority comparitively to implement with protocol2 and protocol3.

* protocol3 is highest priority for practical implementations between sender and Receiver for efficient frames transmission in simplex data flow.

Sliding (moving) Window Protocols :-

* Datalink layer implements sliding window (buffer) protocol for data frames transmission b/w sender and receiver by emplying windows at the side of sender and receiver and this protocol introduced to implement bidirectional data frame transmission b/w sender and receiver.

* Because of uni-direction (simplex protocol) protocols of datalink layer will results maximum data loss to reduce the data frames to the sliding window protocols are introduced

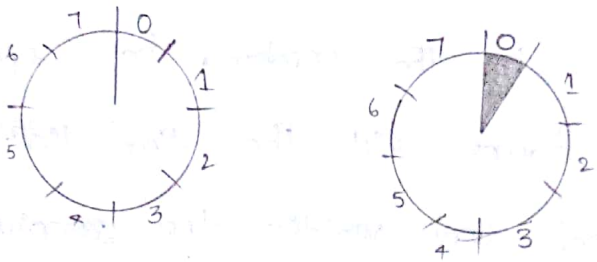
* Basically sliding window protocols are classified into 3 types. 1) 1-Bit sliding window protocol

2) Go-back-N sliding window protocol

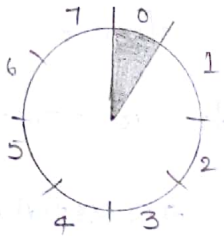
3) selective repeat sliding window protocol

1-bit sliding window protocol

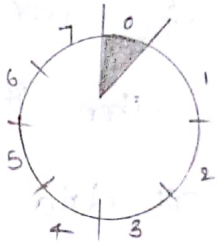
Sender



Receiver



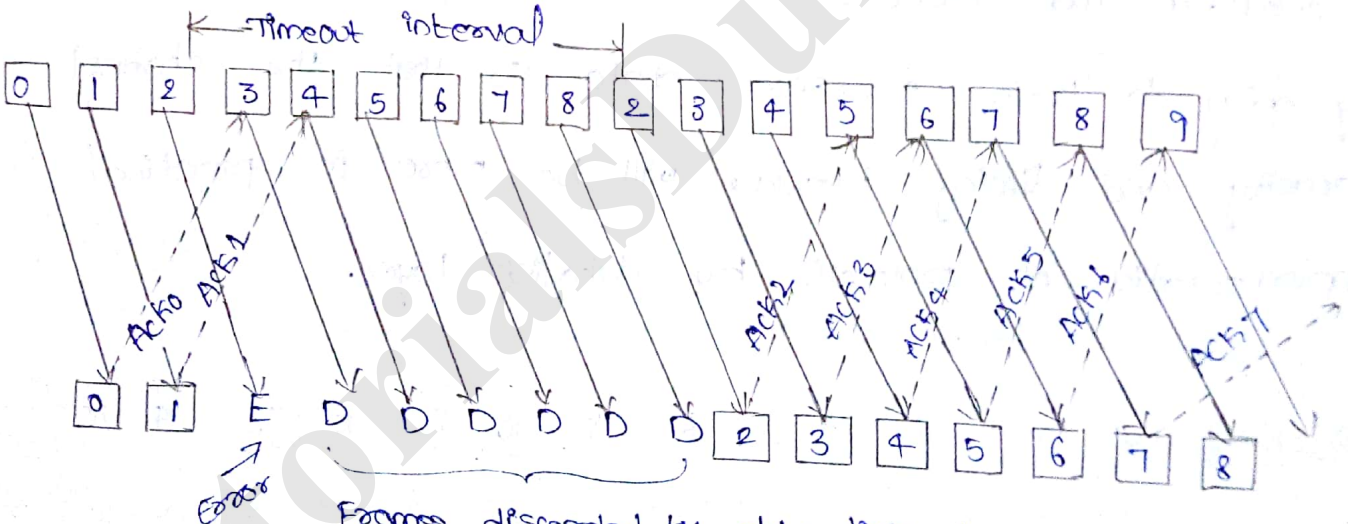
(a)



(b)

A sliding window of size 1, with a 3-bit sequence number.
a) Initially b) After the first frame has been sent.

Go-Back-N

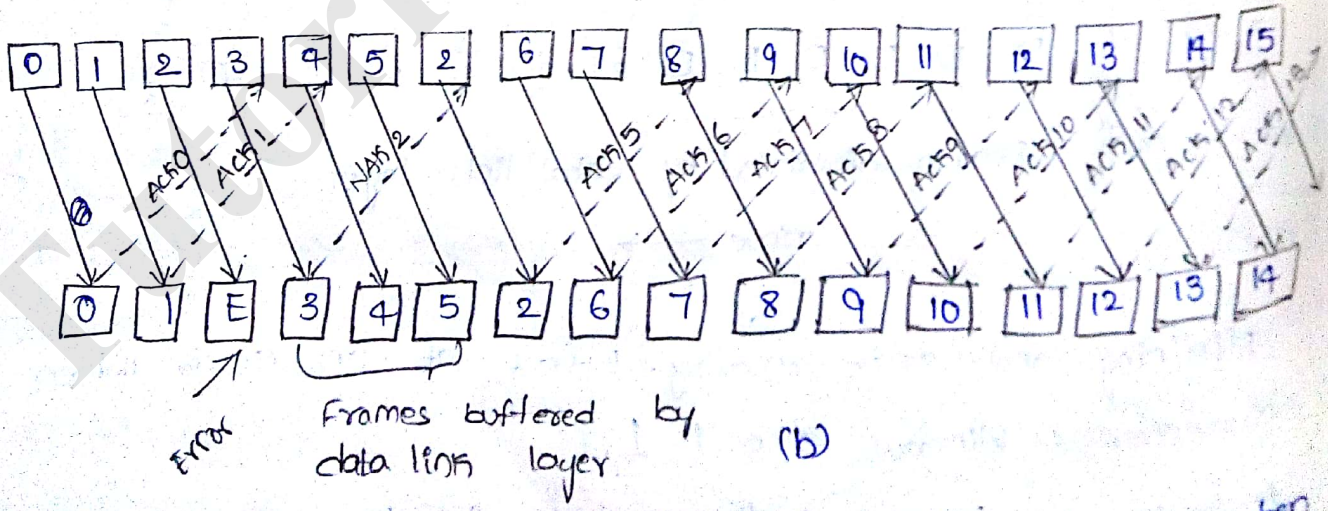


(a)

pipelining and error recovery. Effect of an error when receiver's window size is 1.

Go-Back-N sliding window protocol is known as protocol 5 of data link layer. In this protocol 5 the sender sends the list of data frames to the receiver upto the specified

Acknowledgement back to the sender. The sender continuously transporting data frames still the time limit expires once the time limit is expired and verifies the receiver status with all set of acknowledgements for the sent data frames i the acknowledgement for which data frame is not received by the senders window then it repeats retransmissions from sender to receiver all data frames successfully use go-back-N protocol will consider the error position at the receiver side and from that error position the remaining data frames are also discarded eventhough the sender transported data frames to the receiver. In this protocol5 the data transportation is repeated by going to Back erroreous state so that the channel capacity and timing intervals will be more in practical implementation of protocol5 by datalink layer.



pipelining and error recovery. Effect of an error when

b) receiver's window size is large

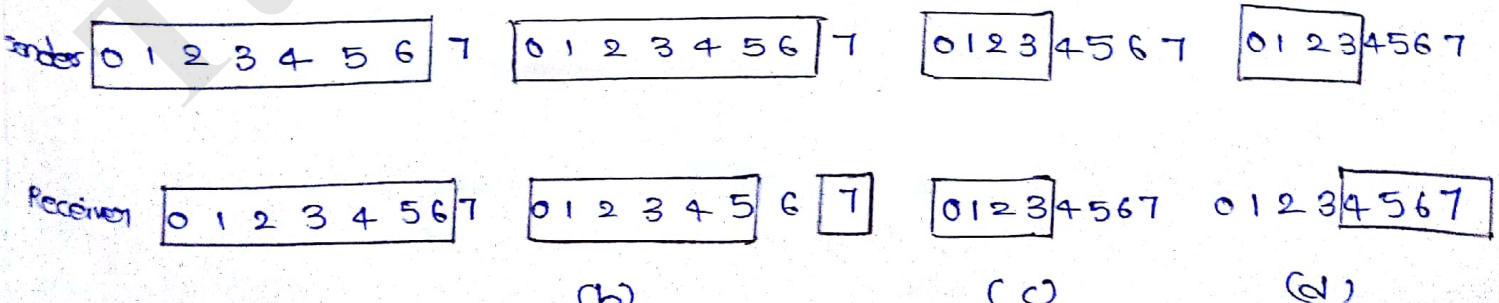
* In the above figure protocol using Go-Back-N in this case the sender is sending data frame to the receiver and the receiver will respond with ACK if receiver receives data frame without any errors; If the receiver is not received the data frame then it is an error (E) then the receiver responds NAK (Negative Acknowledgement) Back to the sender.

* The Error followed by remaining frames are generally buffer by datalink layer for error recovery. once the errored data frame is retransported by the sender then the buffer frames are sequentially attach to form an actual message and the remaining frames are transported in a regular fashion from sender to receiver.

* Comparitively in the above case (fig (a)) in this fig(b) the go-Back-N is reviced to minimize the member of data frames retransmission and also supports, only to re-transport the missed (Error) data frame.

* protocols allows to transport multiple outstanding frames upto Maximum Sequence frames without waiting for an Acknowledgement.

protocol using Selective Repeat (10)



a) Initial situation with a window of size 7

TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well

b) After 7 frames sent and received but not acknowledged

c) Initial situation with a window size of 4.

d) After 4 Frames send and received but not acknowledged.

Go-Back-N

Selective Repeat protocol (protocol 6) is selectively retransmit the dataframe to the sender and accordingly the window size is resize.

comparatively protocol 4 & 5; protocol 6 is able to transmit maximum no. of data frames and minimizes no. of re-transmissions of data frames.

5/1/18

Error control: Data link layer is implements error control

Error control service by using EDC (Error Detection codes) and ECC (Error correction codes).

* EDC & ECC are commonly implemented by data link layer to detect and correct the collected bit in the original message to implement reliability

* Datalink layer using error correcting codes is also refered as forward error correction (FEC) to correct single bit errors as well as Multiple bit errors

* Datalink layer to implement error control service there has been defined four different error correcting codes.

*1. Hamming code

*2. Binary convolutional code

3. Reed - Solomon code

4. low - Density parity checks codes.

Hamming code

* Data link layer to implement error handling, it has to look at closely what the error has been a really occured along with the message.

* The senders message and receivers message binary representation is consider to be a codeword.

* For example sender sending a message - codeword is 10001001

* The senders message transmitted as it is but the receiver receives the message - codeword is 10110001

* To implement hamming code by the data link layer has to be consider by the above given two codewords.

* Codeword 1 - 10001001

  Codeword 2 - 10110001

  Hamming Distance → 00111000 (3)

(How many bits are differ from those two codewords then it is called as Hamming distance.)

"XOR"

0 0 → 0
0 1 → 1
1 0 → 1
1 1 → 0

* Hamming code applies "XOR" gate to handle the errors by finding out the hamming distance between the two given codewords.

* According to the hamming distance value the datalink layer identifies the error positions and applies 1's complement at the receivers codeword2. so that the message which is wrongly delivered will be get as codeword 1 10001001 is transmitted by the datalink layer to the network layer on receivers machine.

(and get corrected the receivers message)

* Senders message is 11110011 and receiver received the message as 00010001 apply

codeword1 : 1 1 1 1 0 0 1 1

codeword2 : 0 0 0 1 0 0 0 1 — XOR

1's complement: 1 1 1 0 0 0 1 0 → in this output where we are getting 1 that is error in codeword2

0 0 0 1 1 1 0 1

* Hamming code is used to identify single bit as well as multiple bit errors and also get correct the receive wrong message into actual message. So that hamming code is also known as error detection and correction code.

* the senders message is consisting 'm' no.of bits, the receivers message may be consisting all 'm' no.of error bits (or) n no.of error bits but still the hamming code is able to detect the error positions as well as able to correct receive wrong message.

* the implementation of hamming code on circuit by the datalink layer is easy and inexpensive. the problem with hamming code is the complex linear code when sent by the senders message and received wrongly by the receiver; in this case hamming code implementation on circuit of datalink layer is difficult and expensive.

Eg: codeword 1 : 1 1 1 1

codeword 2 : 1 0 1 1

0 1 0 0

* A single bit error at second position of receivers message at codeword2 and the hamming distance is 1.
* the codeword2 wrongly received message bit position is 2 and the bit is '0'. Now the hamming bit 0 has to be applied with 1's complement now the value is '1'.
* The corrected codeword2 is 1 1 1 1

NOTE:

* Data links layer uses error correcting code to acheive reliability by avoiding errors but for these error correcting codes add redundancy to the information which is send by the sender.
* Datalinks layer uses blocks code, system code and linear code to implement error contad service.
* Most of the networks are using hamming codes for error corrections which is valuble for understanding blocks codes.
* Still to avoid the errors of the data many of the network are using stronger codes than hamming code.

Binary convolutional Code (BCC):-

* The BCC code is stronger than hamming code and this codes are widely used in deployed networks like GSM (Global system for Mobile Communication) BCC code is not an Blocks code.
* In BCC an encoder processes a sequence of input bits and generates a sequence of output bits.
* There is no natural message size (or) encoding boundary like in blocks code.

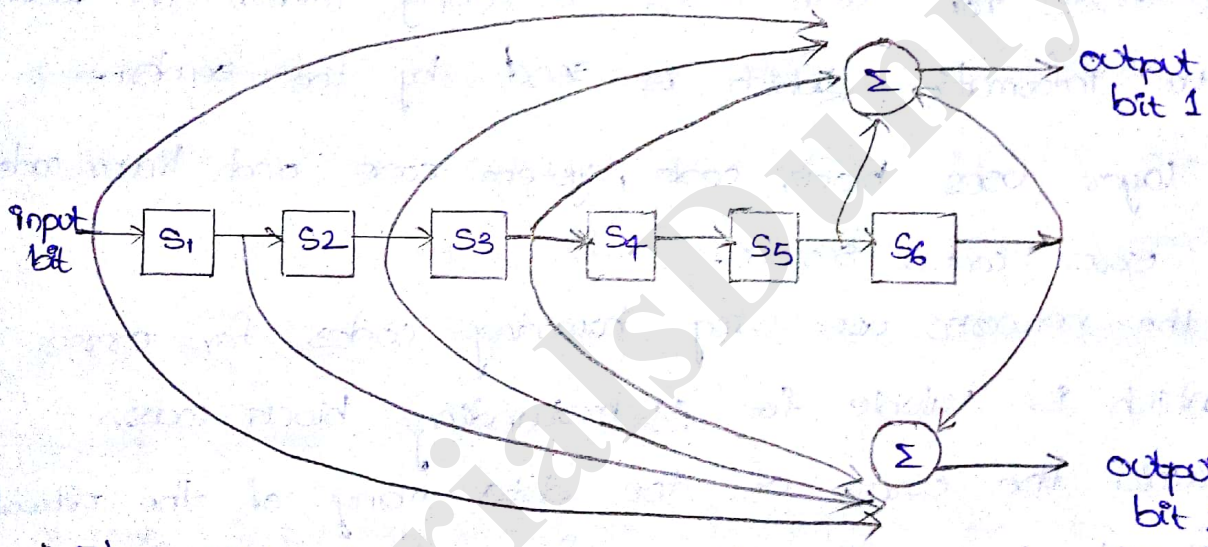
* In BCC the output depends on current and previous input bits i.e the encoder has enough memory space to store previous bits.

* The no. of previous bits on which the output depends is called the "constraint length" of the code.

* Convolutional codes are specify in terms of their rate and constraint length and these are most widely used in satellite communications, GSM and 802.11.

→ This code is also known as NASA binary convolutional code.

Error Detection code:-



* The NASA binary convolutional code used in 802.11

* In the above figure each input bit on left side produces two output bits on the right side that are "XOR" sums of input and internal state.

* Deals with bits and linear operations produce proper output at the side of datalink layer receiver.

* In the above figure each input produces two output bits and code rate is 1/2.

* The above circuit is implemented by the systems datalink layer along with gates and flipflops.

Reed-Solomon code:

* The third kind of error correction code is reed-Solomon code. Just like hamming code, this code is linear block code and are used as systematic circuit codes.

* These codes are implemented by datalink layer and involves lot of mathematical operations and are based on polynomial equations.

* These codes are actually defined as polynomials which are operate over finite f and widely used in DSL, Satellite communication, blue ray disks. and these codes are popularly known as strong error correction codes.

* For example a line having the form ax+b is determined by two points. Extra points on the same line are redundant which is helpfull for error correction.

* The two data points of the line and the two extra check points on the line are used for error correction.

Low density parity check:- (LDPC)

* LDPC is a linear block code invented by robert in 1962 for computing errors to acheive reliability by datalink layer.

* In LDPC each output bit is form from only a fraction of i/p bits. this leads a matrix representation of the code that has a low density of 1's hence the name given for that code.

* The receiver codes are decoded with an approximate algorithm which Iteratively improve the best fit data and corrects the errors.

* The LDPC are practically implemented for large block size

and have an excellent error correction abilities in practice.

* These are used in ethernet power line networks and later version of 802.11

5/11/19

Error Detecting codes (EDC):-

1) Parity bit Error Detecting code

2) checks sum Error Detecting code

3) Cyclic Redundancy Check (CRC) Error Detecting code.

* The above three EDC are implemented by datalink layer to detect the errors on actual message to implement error control service.

* Error detecting codes are used to find out single bit as well as multiple bit errors to achelve reliability.

Parity Bit Error Detecting codes (EDC):-

* parity Bit EDC is used on wireless links when the data is transported using co-axial cable from source to destination. The parity bit error detecting code is used to detect single data bit error in senders codeword.

* The parity bit is an extra appended bit in the given codeword and the system datalink layer will decide to implement either even parity error detecting mechanism (or) odd parity error detecting Mechanism.

* An even parity of code word should be carries the total no of 1 bits evenly.

* The odd parity of codeword will carries the total no. of on 1 bits is odd number.

* For example the given codeword is consisting total no. of 8 bits and apply even parity all the given codeword is

11111000

* Even parity 11111000 [1] ← extra bit

* If a datalink layer implements odd parity error detecting mechanism then the given codeword is 11111000

add parity 11111000 [0] ← extra bit

eg:- 11111111 eg:- 11111111

even parity 11111111 [0] ← extra bit odd parity 11111111 [1] ← extra bit

Check sum Error Detecting Code (EDC):-

* check sum EDC is implemented by data link layer to detect Multiple/Single bit errors. Whenever a sender sends a message which is consisting a group of bits, this block is received by receiver if the block is carrying morethan a single bit error then the data link layer is implementing check sum error detecting mechanism to acheive reliability.

* The error control service of datalink layer by using check sum EDC is "By adding check bits" either side of sender as well as receiver".

* The check sum error detecting code with check total no. of check bits of the Senders message as well as receivers message if both are same then there is no error. If a group of check bits calculated check sum is not similar Either side of the datalink layer then it seems to be there has been occur errors in the codeword.

* The 16-bit checks sum is commonly used in the internet packets of network communications.

* The checks sum is the sum of message bits will be divided individually and calculated the sum which is transfered to the datalink layer of receiver.

* The checks sum error detection codes is usually placed at the end of the message, as the compliment of the sum function.

* this wabg of detecting errors by summing the entire received codeword is with both data bits and checks sum.

eg:- N - 0 0 1
E - 1 0 0
T - 1 0 1
W - 1 1 1
O - 1 1 0
R - 1 1 1
S - 0 1 0
1 0 0 0 ← even parity

**

Cyclic Redundancy check (CRC):-

* CRC is an error detection Mechanism

* CRC is a stronger errors detecting Mechanism and also known as "polynomial code".

* CRC is implemented with help of checks sum calculated by "XOR" gate as well as polynomial equations.

* The polynomial generator circuit is generates the polynomial equation which is use to division the frames data.

$F(x) = x^4 + x + 1$

P.E

1001 φ

$G(x)$ = Frames data } Receiver's

I/p → CRC

CRC = $F(x)$ the polynomial equation has to be divide $G(x)$

* To implement CRC the $F(x)$ and $G(x)$ division has to be done along with "XOR" gate.
* consider $F(x)$ highest order value and add that many no. of 0's to the $G(x)$ value.

$F(x) = 10011$ ($2^4\ 2^3\ 2^2\ 2^1\ 2^0$) 19

```
                 1100001110
       10011 ) 11010111110000
               10011
               -----
               0 10011
                 10011
                 -----
                 0 00001
                   00000
                   -----
                   0 00011
                     00000
                     -----
                     0 00111
                       00000
                       -----
                       0 01111
                         00000
                         -----
                         0 11110
                           10011
                           -----
                           0 11010
                             10011
                             -----
                             0 10010
                               00000
                               -----
                               0 00100
                                 00000
                                 -----
                                 0 0100
```

$f(x) = x^3 + x + 1$

** $g(x) = 1110011$.

Illustrate cyclic Redundancy check (CRC) to find out the errors in the senders Message.

$F(x) = x^3 + x + 1$

1011

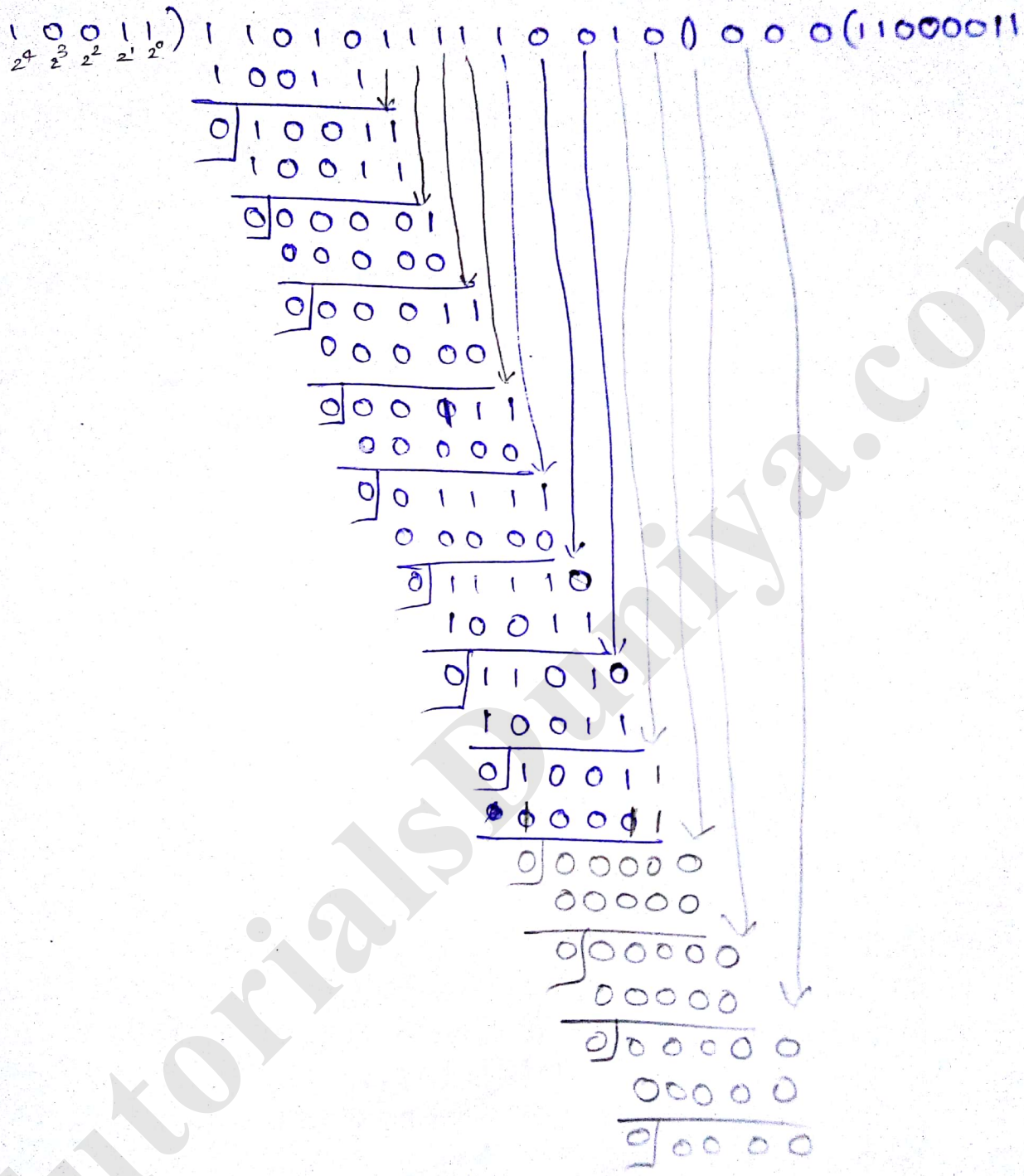
$G(x) = 1110011\boxed{000}$

```
1011 ) 1110011000 ( 1000010
       1011
       -----
        1010
        0000
        ----
         1010
         0000
         ----
          1010
          0000
          ----
           1011
           0000
           ----
            1011
            1011
            ----
               0000
               0000
               ----
                  0000
                  0000
                  ----
                     0000
                     0000
                     ----
                        000
```

G(x) is received by the receiver as it is there is no error from the sender's message.

F(x) = 10011

G(x) = 11010111110010



UNIT-IV

MEDIUM ACCESS CONTROL SUBLAYER (MAC)

Networks can be categories in to two ways

a) Point to point b) Broad cast channel

- In broadcast network, the key issue is how to share the channel among several users.

- Ex *a conference call with five people*

-Broadcast channels are also called as multi-access channels or random access channels.

-Multi-access channel belong to a sublayer at the DL layer called the MAC sublayer.

The Channel Allocation problem:

a) **Static channel allocation** in LANs & MANs

i) FDM ii) **TDM**

Drawbacks: -1) Channel is wasted if one or more stations do not send data.

2) If users increases this will not support.

b) Dynamic channel allocation

i) Pure **ALOHA** & Slotted **ALOHA**

CSMA/CD

ii) CSMA

CSMA/CA

Pure ALOHA

-1970's Norman Abramson end his colleagues devised this method, used ground –based radio broad costing. This is called the **ALOHA** system.

-The basic idea, many users are competing for the use of a single shared channel.

-There are two versions of ALOHA: **Pure and Slotted**.

-Pure ALOHA does not require global time synchronization, where as in slotted ALOHA the time is divided into discrete slots into which all frames must fit.

-Let users transmit whenever they have data to be sent.

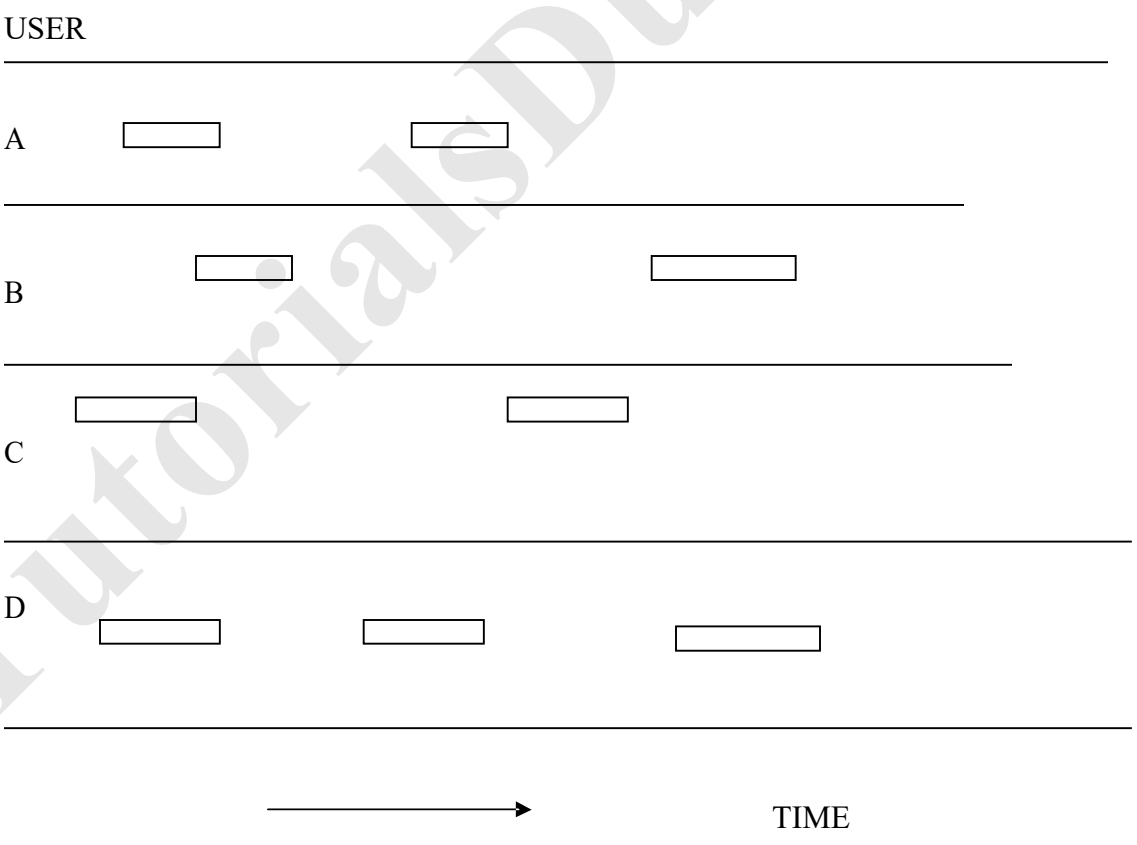
-There will be collisions and all collided frames will be damaged.

-Senders will know through feedback property whether the frame is destroyed or not by listening channel.

[-With a LAN it is immediate, with a satellite, it will take 270m sec.]

-If the frame was destroyed, the sender waits random amount of time and again sends the frame.

-The waiting time must be random otherwise the same frame will collide over and over.



TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well

Frames are transmitted at completely arbitrary times

-Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be destroyed.

-We have to find out what is the efficiency of an ALOHA channel?

-Let us consider an infinite collection of interactive users sitting at their systems (stations).

-A user will always in two states **typing or waiting**.

-Let the 'Frame time' denotes the time required to transmit one fixed length frame.

-Assume that infinite populations of users are generating new frames according to possion distribution with mean N frames per frame time.

-If N>1 users are generating frames at a higher rate than the channel can handle.

-For reasonable throughput 0<N<1.

-In addition to new frames, the station also generates retransmission of frames.

-Old and new frames are G per frame time.

-G≥ N

-At low load there will be few collisions, so G ~ N

-Under all loads, the throughput $S = GP_o$, where P_o is the probability that a frame does not suffer a collision.

-A frame will not suffer a collision if no other frames are sent with one frame time of its start.

-Let 't' be the time required to send a frame.

-If any other user has generated a frame between time t_o and t_o+t, the end of that frame will collide with the beginning of the shaded frame.

-Similarly, any other frame started b/w t_o+t and t_o+2t will bump into the end of the shaded frame.

-The probability that 'k' frames are generated during a given frame time is given by the possion distribution:

$$P_r[k] = \frac{G^k e^{-G}}{k!}$$

-The probability of zero frames is just e^{-G}

-In an interval two frame times long, the mean number at frames generated is 2G.

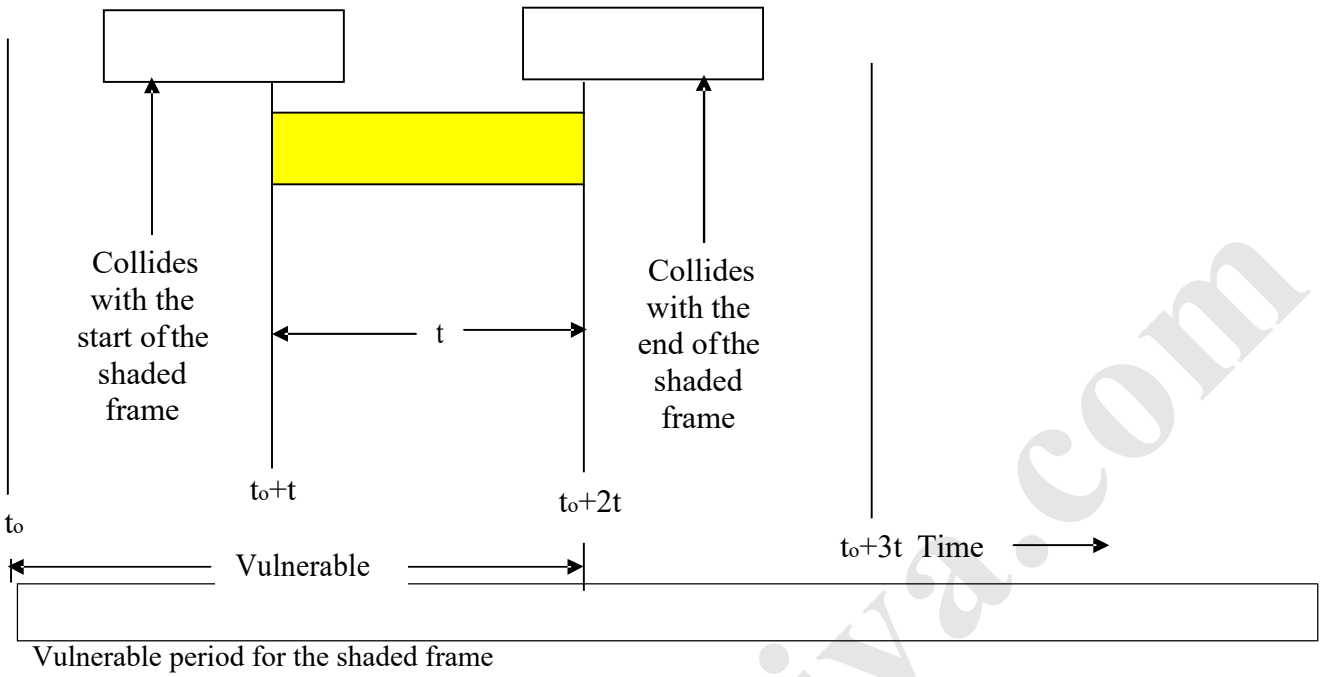
-The probability at no other traffic being initiated during the entire vulnerable period is given by

$$P_o = e^{-2G}$$

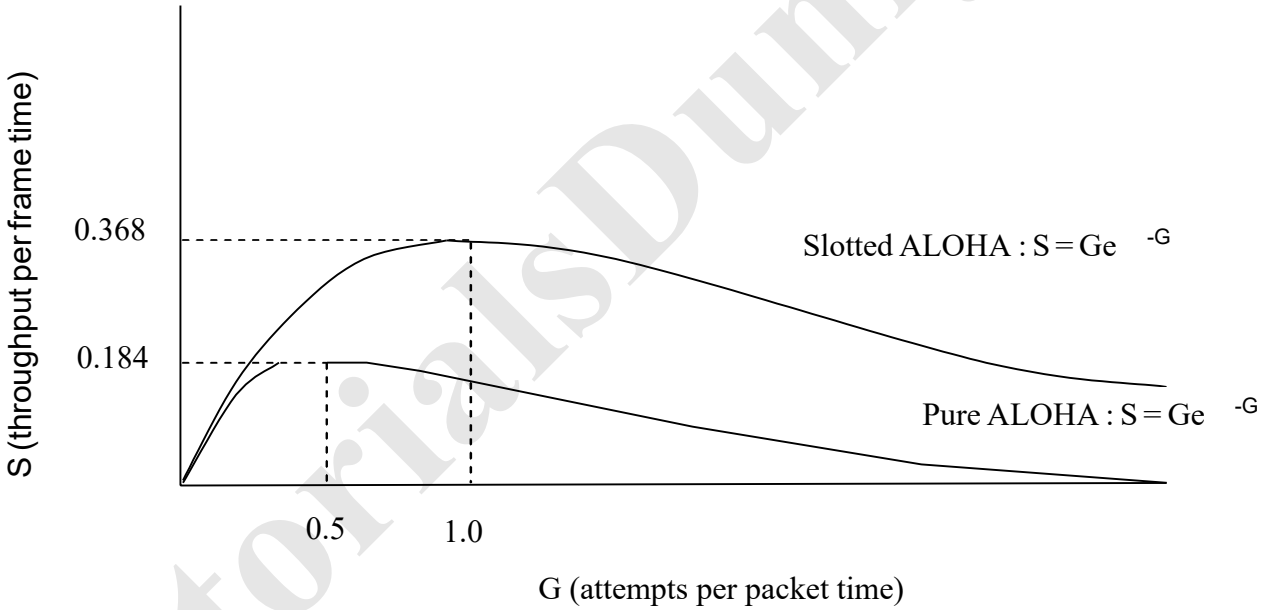
$$S = Ge^{-2G} \qquad [S=GP_o]$$

The Maximum through put occurs at G=0.5 with S=1/2e = 0.184

The channel utilization at pure ALOHA =18%.



Vulnerable period for the shaded frame



Throughput versus offered traffic for ALOHA systems

Slotted ALOHA

-In 1972, Roberts' devised a method for doubling the capacity of ALOHA system.

-In this system the time is divided into discrete intervals, each interval corresponding to one frame.

-One way to achieve synchronization would be to have one special station emit a pip at the start of each interval, like a clock.

-In Roberts' method, which has come to be known as slotted ALOHA, in contrast to Abramson's pure ALOHA; a computer is not permitted to send whenever a carriage return is typed.

-Instead, it is required to wait for the beginning of the next slot.

-Thus the continuous pure ALOHA is turned into a discrete one.

-Since the vulnerable period is now halved, the of no other traffic during the same slot as our test frame is e^{-G} which leads to

$S = Ge^{-G}$

- At G=1, slotted ALOHA will have maximum throughput.

- So S=1/e or about 0.368, twice that of pure ALOHA.

- The channel utilization is 37% in slotted ALOHA.

Carrier Sense Multiple Access Protocols

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

Persistent CSMA

When a station has data to send, it first listens to the channel to see if any one else is transmitting at that moment. If the channel is busy, the station waits until it become idle. When the station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1-persistent also because the station transmits with a probability of 1 when it finds the channel idle.

The propagation delay has an important effect on the performance of the protocol. The longer the propagation delay the worse the performance of the protocol.

Even if the propagation delay is zero, there will be collisions. If two stations listen the channel, that is idle at the same, both will send frame and there will be collision.

Non persistent CSMA

In this, before sending, a station sense the channel. If no one else is sending, the station begins doing so it self. However, if the channel is busy, the station does not continually sense it but it waits a random amount of time and repeats the process.

This algorithms leads to better channel utilization but longer delays then 1-persistent CSMA.

With persistent CSMA, what happens if two stations become active when a third station is busy? Both wait for the active station to finish, then simultaneously launch a packet, resulting a collision. There are two ways to handle thisproblem.

a) P-persistent CSMA b) exponential backoff.

P-persistent CSMA

The first technique is for a waiting station not to launch a packet immediately when the channel becomes idle, but first toss a coin, and send a packet only if the coin comes up heads. If the coin comes up tails, the station waits for some time (one slot for slotted CSMA), then repeats the process. The idea is that if two stations are both waiting for the medium, this reduces the chance of a collision from 100% to 25%. A simple generalization of the scheme is to use a biased coin, so that the probability of sending a packet when the medium becomes idle is not 0.5, but p, where $0< p < 1$. We call such a scheme **P-persistent CSMA**. The original scheme, where p=1, is thus called 1-persitent CSMA.

Exponential backoff

The key idea is that each station, after transmitting a packet, checks whether the packet transmission was successful. Successful transmission is indicated either by an explicit acknowledgement from the receiver or the absence of a signal from a collision detection circuit. If the transmission is successful, the station is done. Otherwise, the station retransmits the packet, simultaneously realizing that at least one other station is also contending for the medium. To prevent its retransmission from colliding with the other station's retransmission, each station backs off (that is, idles) for a random time chosen from the interval

[0,2*max-propagation_delay] before retransmitting its packet. If the retransmission also fails, then the station backs off for a random time in the interval [0,4* max_propagation_delay], and tries again. Each subsequent collision doubles the backoff interval length, until the retransmission finally succeeds. On a successful transmission, the backoff interval is reset to the initial value. We call this type of backoff exponential backoff.

CSMA/CA

In many wireless LANS, unlike wired LANS, the station has no idea whether the packet collided with another packet or not until it receives an acknowledgement from receiver. In this situation, collisions have a greater effect on performance than with CSMA/CD, where colliding packets can be quickly detected and aborted. Thus, it makes sense to try to avoid collisions, if possible. CSMA/CA is basically p-persistence, with the twist that when the medium becomes idle, a station must wait for a time called the interframe spacing or IFS before contending for a slot. A station gets a higher priority if it is allocated smaller inter frame spacing.

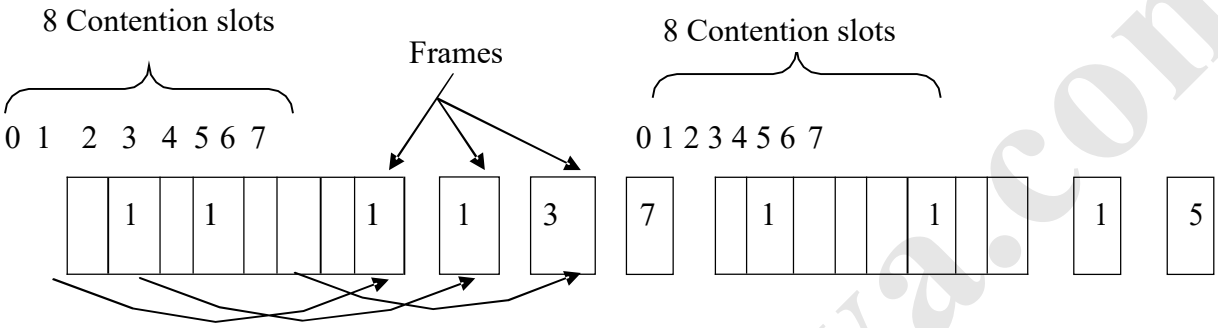
When a station wants to transmit data, it first checks if the medium is busy. If it is, it continuously senses the medium, waiting for it to become idle. When the medium becomes idle, the station first waits for an interframe spacing corresponding to its priority level, then sets a contention timer to a time interval randomly selected in the range [0,CW], where CW is a predefined contention window length. When this timer expires, it transmits a packet and waits for the receiver to send an ack. If no ack is received, the packet is assumed lost to collision, and the source tries again, choosing a contention timer at random from an interval twice as long as the one before(binary exponential backoff). If the station senses that another station has begun transmission while it was waiting for the expiration of the contention timer, it does not reset its timer, but merely freezer it, and restarts the countdown when the packet completes transmission. In this way, stations that happen to choose a longer timer value get higher priority in the next round of contention.

Collision-Free Protocols

A Bit-Map Protocol

In the basic bit-map method, each contention period consists of exactly N slots. If station 0 has a frame to send, it transmits a 1 bit during the zeroth slot. No other station is allowed to transmit during this slot. Regardless of what station 0 does, station 1 gets the

opportunity to transmit a 1during slot 1, but only if it has a frame queued. In general, station j may announce the fact that it has a frame to send by inserting a 1 bit into slot j. after all N slots have passed by, each station has complete knowledge of which stations with to transmit.



The basic bit-map protocol

Since everyone agrees on who goes next, there will never be any collisions. After the last ready station has transmitted its frame, an event all stations can easily monitor, another N bit contention period is begun. If a station becomes ready just after its bit slot has passed by, it is out of luck and must remain silent until every station has had a chance and the bit map has come around again. Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols.

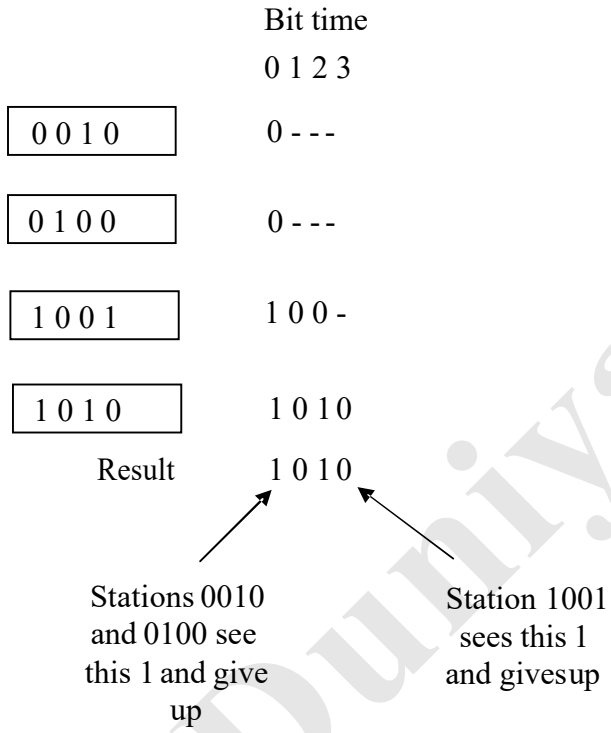
Binary Countdown

A problem with the basic bit-map protocol is that the overhead is 1 bit per station. A station wanting to use the channel now broadcasts its address as a binary bit string, starting with the high-order bit. All addresses are assumed to be the same length. The bits in each address position from different stations are BOOLEAN ORed together. We will call this protocol binary countdown. It is used in Datakit.

As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up. For example, if station 0010,0100,1001, and 1010 are all trying to get the channel, in the first bit time the stations transmit 0,0,1, and 1, respectively. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue.

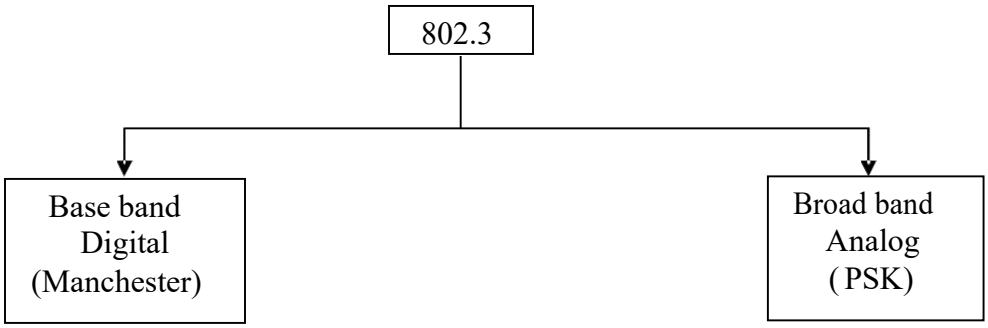
The next bit is 0, and both stations continue. The next bit is 1, so station 1001 gives up. The winner is station 1010, because it has the highest address. After winning the bidding, it may now transmit a frame, after which another bidding cycle starts.

The binary countdown protocol. A dash indicates silence



IEEE Standard 802 for LANS and MANS

The IEEE 802.3 is for a 1-persistent CSMA/CD LAN. Xerox built a 2.94 Mbps CSMA/CD system to connect over 100 personal workstations on 1-Km cable. This system was called Ethernet through which electromagnetic radiation was once thought to propagate. Xerox DEC and Intel came with another standard for 100 Mbps Ethernet. This differs from old one that it runs at speeds from 1 to 10 Mbps on various media. The second difference between these two is in one header (802.3 length field is used for packet type in Ethernet).



10Base5, 10Base2

10Base-T, 1Base5

100 Base-T

10 Broad 36

802.3 Cabling

Five types of cabling are commonly used, 10Base5 cabling called thick Ethernet, came first. It resembles a yellow garden hose, with markings every 2.5 m to show where the taps go. Connections to it are generally made using **vampire taps**, in which a pin is carefully forced halfway into the coaxial cable's core. The notation 10Base5 means that it operates at 10 Mbps, uses baseband signaling, and can support segments of up to 500m.

Name	Cable	Max. segment	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Good for backbones
10Base2	Thin coax	200 m	30	Cheapest system
10Base-T	Twisted pair	100 m	1024	Easy maintenance
10Base-F	Fiber optics	2000 m	1024	Best between buildings

The second cable type was **10Base2** or thin Ethernet, which, in contrast to the garden-hose-like thick Ethernet, bends easily. Connections to it are made using industry standard BNC connectors to form T-junctions, rather than using vampire taps. These are easier to use and more reliable. Thin Ethernet is much cheaper and easier to install, but it can run for only 200m and can handle only 30 machines per cable segment.

Cable breaks, bad taps, or loose connectors can be detected by a devise called time domain reflectometry.

For 10Base5, a transceiver is clamped securely around the cable so that its tap makes contact with the inner core. The transceiver contains the electronics that handle carrier detection and collision detection. When a collision is detected, the transceiver also puts a

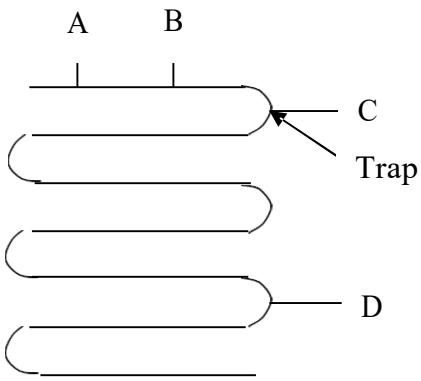
special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred.

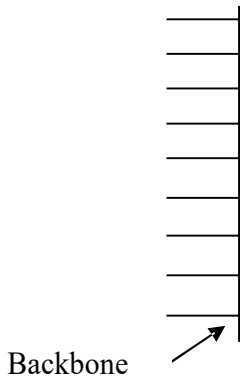
The transceiver cable terminates on an interface board inside the computer. The interface board contains a controller chip that transmits frames to, and receives frames from, the transceiver. The controller is responsible for assembling the data into the proper frame format, as well as computing checksums on outgoing frames and verifying them on incoming frames.

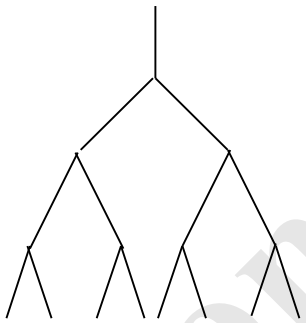
With 10Base2, the connection to the cable is just a passive BNC T-junction connector. The transceiver electronics are on the controller board, and each station always has its own transceiver.

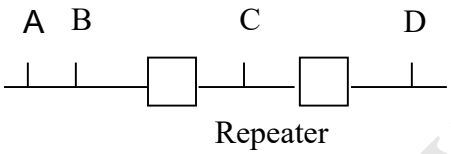
With 10Base-T, there is no cable at all, just the hub (a box full of electronics). Adding or removing a station is simple in this configuration, and cable breaks can be detected easily. The disadvantage of 10Base-T is that the maximum cable run from the hub is only 100m, may be 150m if high-quality (category 5) twisted pairs are used. 10Base-Tis becoming steadily more popular due to the ease of maintenance. 10Base-F, which uses fiber optics. This alternative is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between buildings or widely separated hubs.

Each version of 802.3 has a maximum cable length per segment. To allow larger networks, multiple cables can be connected by repeaters. A repeater is a physical layer device. It receives, amplifies, and retransmits signals in both directions. As far as the software is concerned, a series of cable segments connected by repeaters is no different than a single cable (except for some delay introduced by the repeater). A system may contain multiple cable segments and multiple repeaters, but no two transceivers may be more than 2.5km apart and no path between any two transceivers any traverse more than four repeaters.

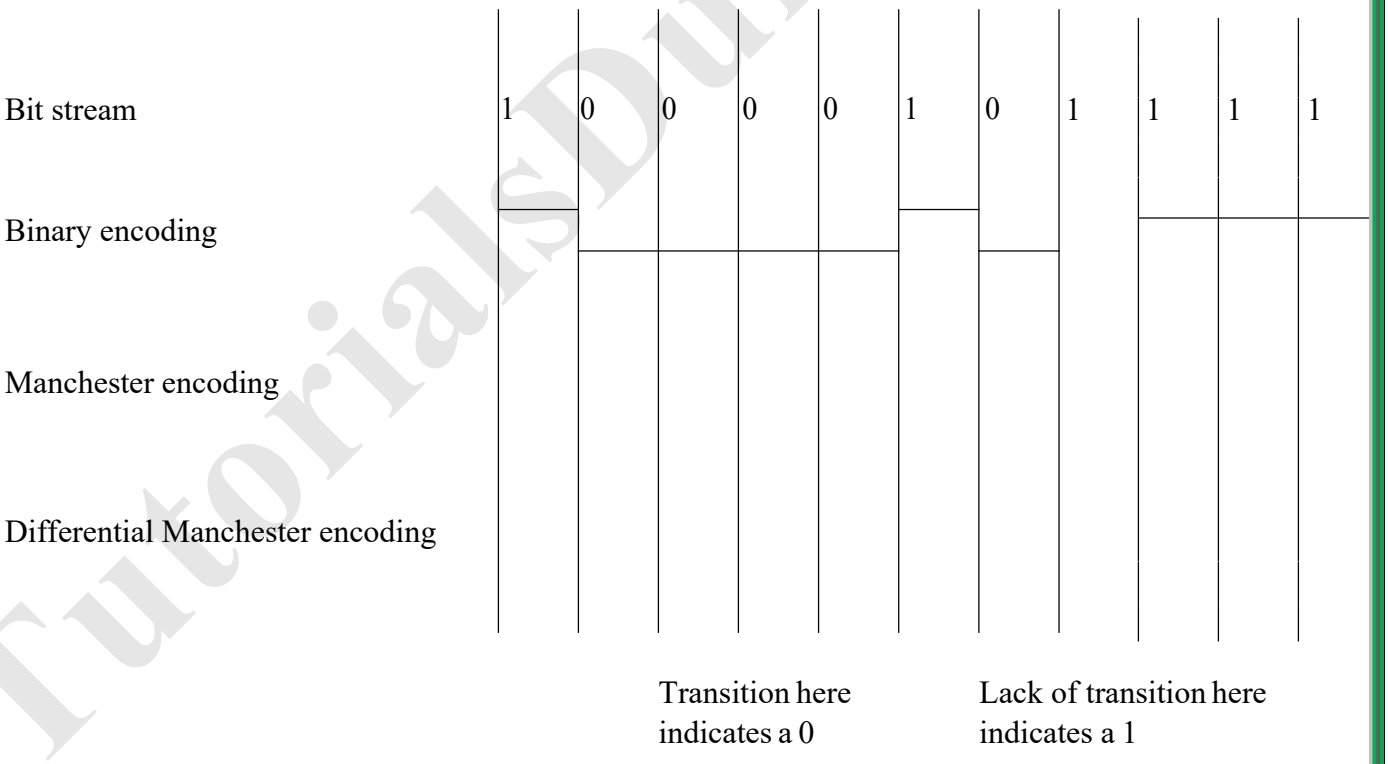


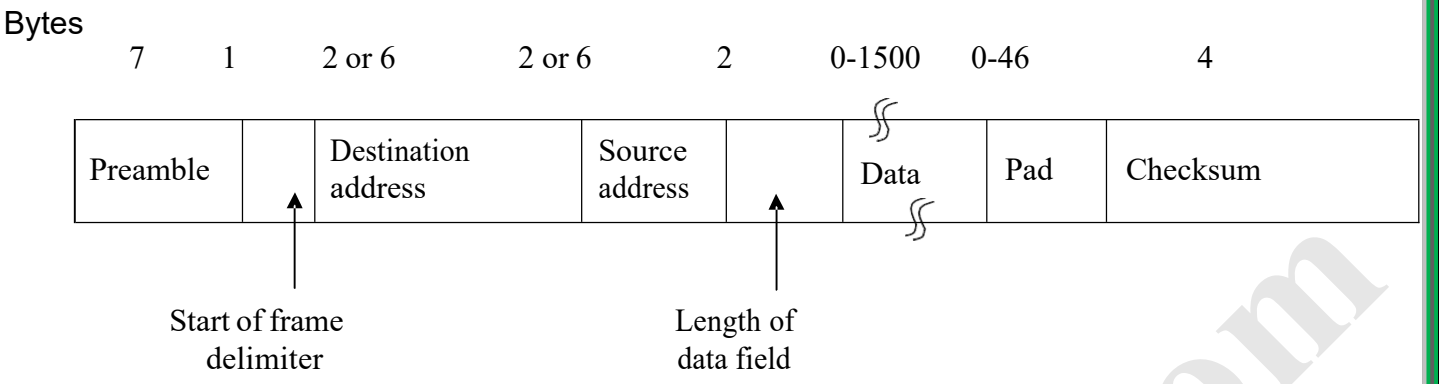






802.3 uses Manchester Encoding and differential Manchester Encoding





The 802.3 MAC sub layer protocol:

I) Preamble:

Each frame start with a preamble of 7 bytes each containing a bit pattern 10101010.

II) Start of frame byte:

It denotes the start of the frame itself. It contains 10101011.

III) Destination address:

This gives the destination address. The higher order bit is zero for ordinary address and 1for group address (Multi casting). All bits are 1s in the destination field frame will be delivered to all stations (Broad casting).

The 46 thbit (adjacent to the high-order bit) is used to distinguish local from global addresses.

IV) Length field:

This tells how many bytes are present in the data field from 0 to 1500.

V) Data field:

This contains the actual data that the frame contains.

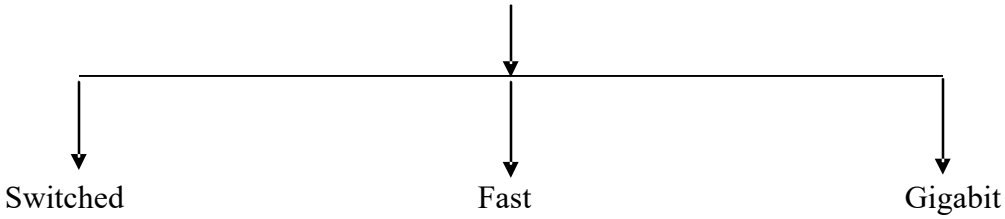
VI) Pad:

Valid frame must have 64 bytes long from destination to checksum. If the frame size less than 64 bytes pad field is used to fill out the frame to the minimum size.

VII) Checksum:

It is used to find out the receiver frame is correct or not. CRC will be used here.

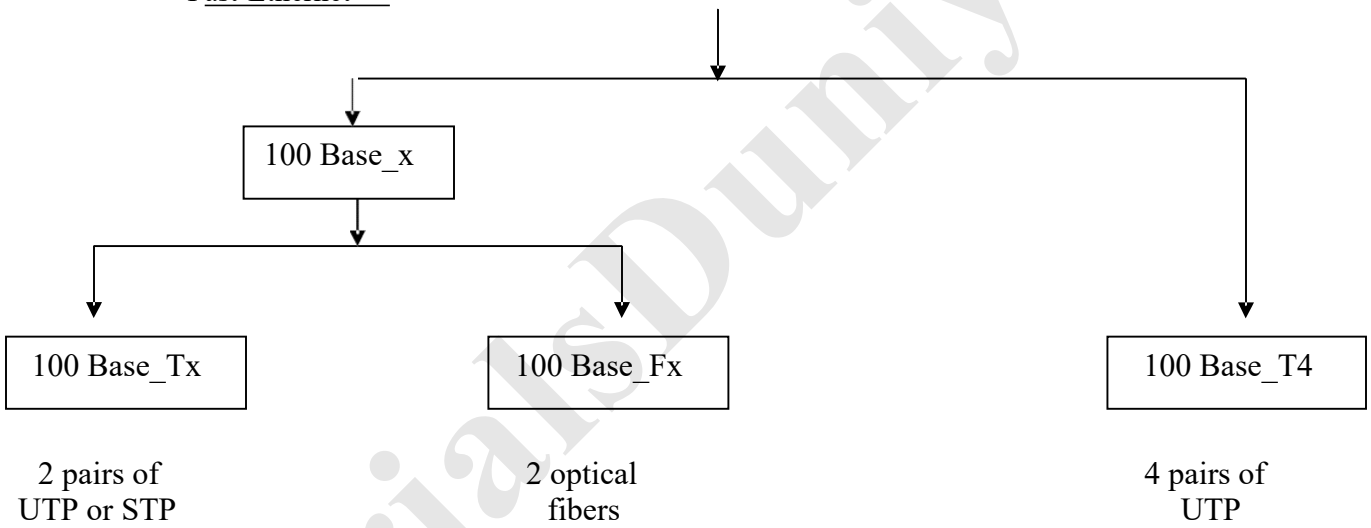
Other Ethernet Networks



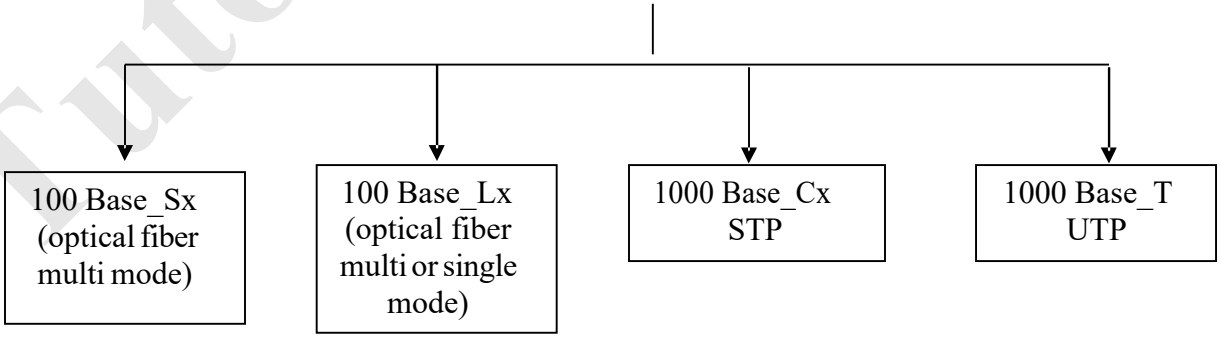
Switched Ethernet:

- 10 Base-T Ethernet is a shared media network.
- The entire media is involved in each transmission.
- The HUB used in this network is a passive device. (not intelligent).
- In switched Ethernet the HUB is replaced with switch. Which is a active device (intelligent)

Fast Ethernet

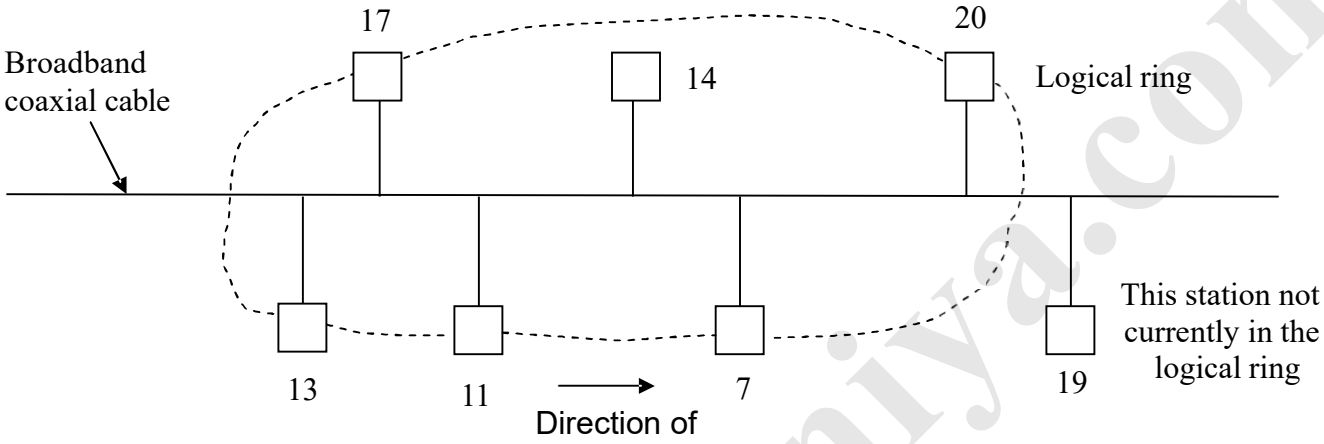


Gigabit Ethernet



IEEE 802.4 (Token Bus)

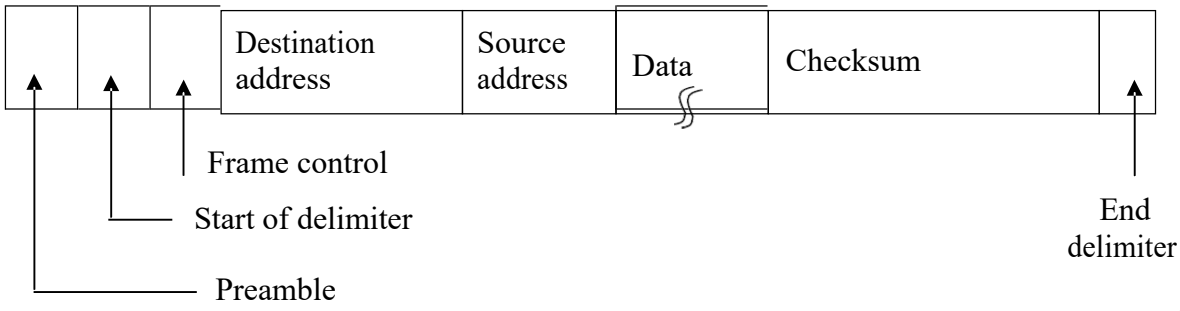
802.3 frames do not have priorities, making them unsuited for real-time systems in which important frames should not be held up waiting for unimportant frames. A simple system with a known worst case is a ring in which the stations take turns sending frames. If there are n stations and it takes T sec to send a frame, no frame will ever have to wait more than nT sec to be sent.



This standard, 802.4, describes a LAN called a token bus. Physically, the token bus is a linear or tree-shaped cable onto which the stations are attached. Logically, the stations are organized into a ring, with each station knowing the address of the station to its "left" and "right." When the logical ring is initialized, the highest numbered station may send the first frame. After it is done, it passes permission to its immediate neighbor by sending the neighbor a special control frame called a token. The token propagates around the logical ring, with only the token holder being permitted to transmit frames. Since only one station at a time holds the token, collisions do not occur.

Since the cable is inherently a broadcast medium, each station receives each frame, discarding those not addressed to it. When a station passes the token, it sends a token frame specifically addressed to its logical neighbor in the ring, irrespective of where that station is physically located on the cable. It is also worth noting that when stations are first powered on, they will not be in the ring, so the MAC protocol has provisions for adding stations to, and deleting stations from, the ring. For the physical layer, the token bus uses the 75-ohm broadband coaxial cable used for cable television. Both single and dual-cable systems are allowed, with or without head-ends.

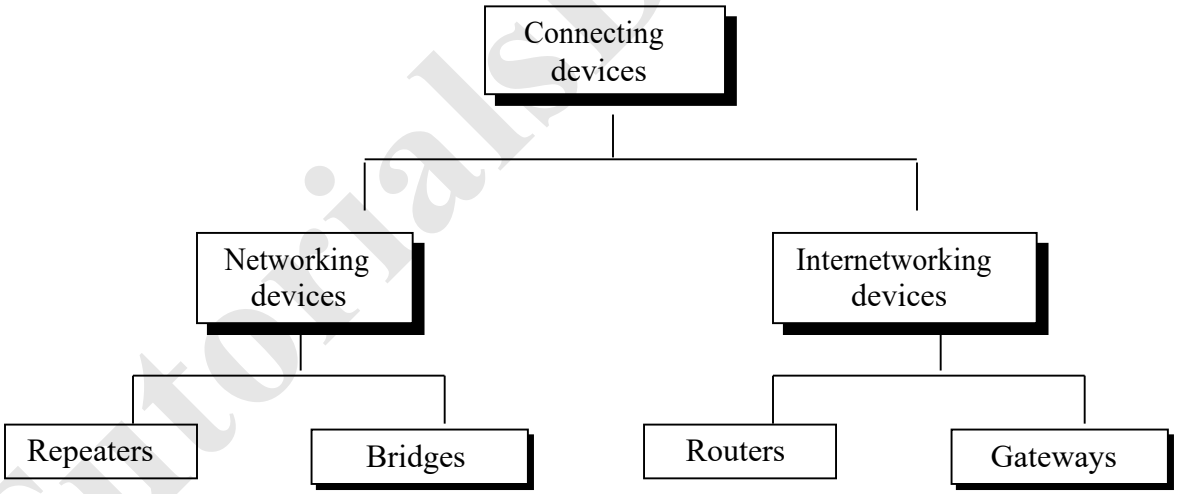
Bytes ≥	1	1	1	2 or 6	2 or 6	0-8182	4	1



The frame control field is used to distinguish data frames from control frames. Fro data frames, it carries the frame's priority. It can also carry an indicator requiring the destination station to acknowledge correct or incorrect receipt of the frame.

For control frames, the frame control field is used to specify the frame type. The allowed types include token passing and various ring maintenance frames, including the mechanism for letting new stations enter the ring, the mechanism for allowing stations to leave the ring, and so on.

Connecting devices



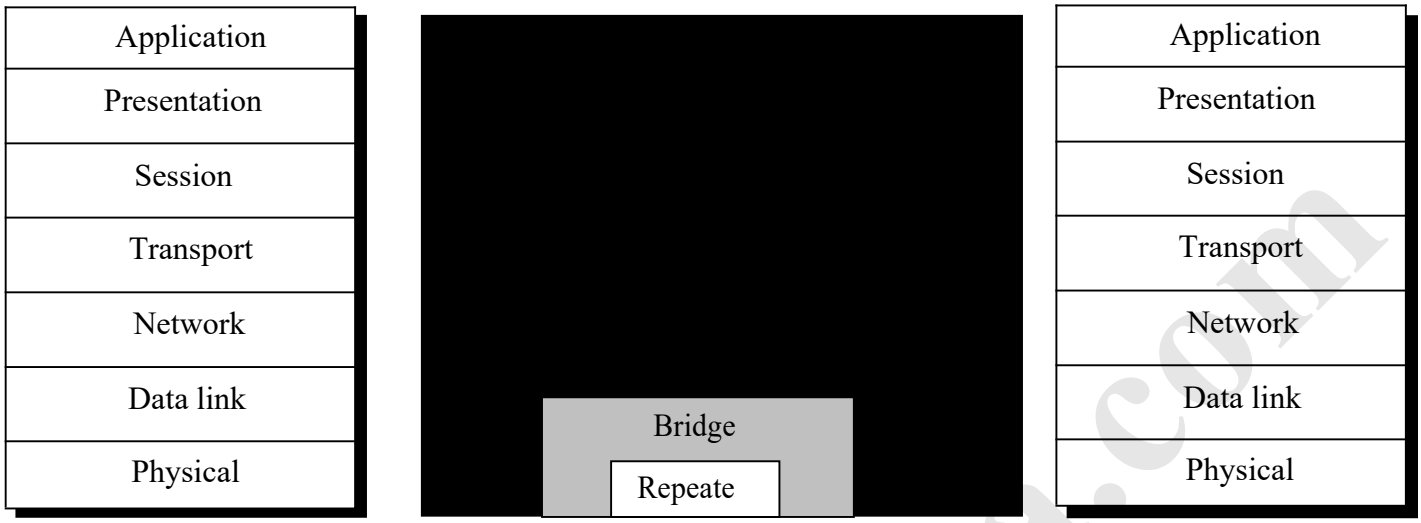
Connecting devices and the OSI model

TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well



Bridges

LANS can be connected by devices called bridges, which operate in the data link layer. Bridges do not examine the network layer header and can thus copy IP, IPX, and OSI packets equally well.

The various reasons why the bridges are used.

1) Many university and corporate departments have their own LANS, primarily to connect their own personal computers, workstations, and servers. Since the goals of the various departments differ, different departments choose different LANS, without regard to what other departments are doing. Sooner or later, there is a need for interaction, so bridges are needed.

2) The organization may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANS in each building and connect them with bridges and infrared links than to run a single coaxial cable over the entire site.

3) It may be necessary to split what is logically a single LAN into separate LANS to accommodate the load. Putting all the workstations on a single LAN- the total bandwidth needed is far too high. Instead multiple LANS connected by bridges are used.

4) In some situations, a single LAN would be adequate in terms of the load, but the physical distance between the most distant machines is too great (e.g., more than 2.5km for 802.3). Even if laying the cable is easy to do, the network would not work due to the

excessively long round-trip delay. Only solution is to partition the LAN and install bridges between the segments.

5) There is the matter of reliability. On a single LAN, a defective node that keeps outputting a continuous stream of garbage will cripple the LAN. Bridges can be inserted at critical places, to prevent a single node which has gone berserk from bringing down the entire system.

6) And last, bridges can contribute to the organization's security. By inserting bridges at various places and being careful not to forward sensitive traffic, it is possible to isolate parts of the network so that its traffic cannot escape and fall into the wrong hands.

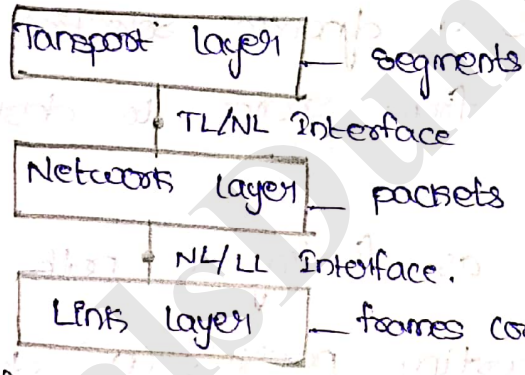
Network Layer

Network Layer:-

Network layer is a mandatory layer a N/t architecture which implements an important service of routing.

Network Layer Design Issues(or) Functionality (or) services:-

* N/t Layer provide accessibility to the above and below layers N/t layer is accessing the services from transport layer and provides the services to the link layer at the side of source system where as N/t Layer is accessing the services from link layer and provide services to the transport layer at the side of destination system.
* N/t layer Data format is packets.



Design Issue (2):-

Implementation of connection oriented Service:-

* N/t layer uses two types of services. One is connection oriented service (COS). N/t layer uses cos for efficient packet transmission. In this type of service (TOS) N/t layer implements and setup a connection, establishes a routing path before packet transportation.
* Generally a packet is prefered as datagram so that the datagram transportation in a N/t through a subnet is known as datagram circuit
* N/t layer while transporting a packet through cos

is implemented reliability.

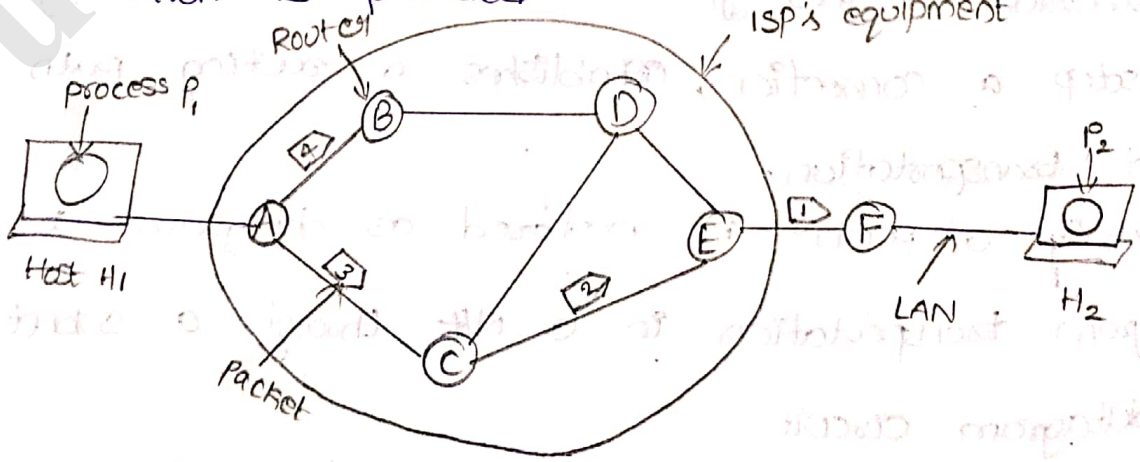
③ Implementation of connection less services:- (CLS)

* N/t layer uses two types of services; where as the second type of service defined by N/t layer is connection less service.
* In this type of service, N/t layer does not advanced setup a circuit for packet transportation. When a packet transported from the source system the N/t layer connection less service implement a dynamic path for packet transportation to the destination.
* CLS implements a virtual circuit path by the N/t layer for transporting a packet from source to destination.
* A virtual circuit is a dynamic selection of routing path to transport a packet from source to destination.

④ Routing:-

* Routing is defined as finding a path from source to destination for transporting packets (or) datagram.
* A packet is routed by using routing table information provided by routing algorithms in dynamic routing, routing tables are updated dynamically where as in static routing information is provided.

eg:- fig



A's table (initially)

Desti	Line
A	
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	
B	B
C	C
D	B
E	D
F	D

C's Table

A	A
B	A
C	
D	E
E	E
F	E

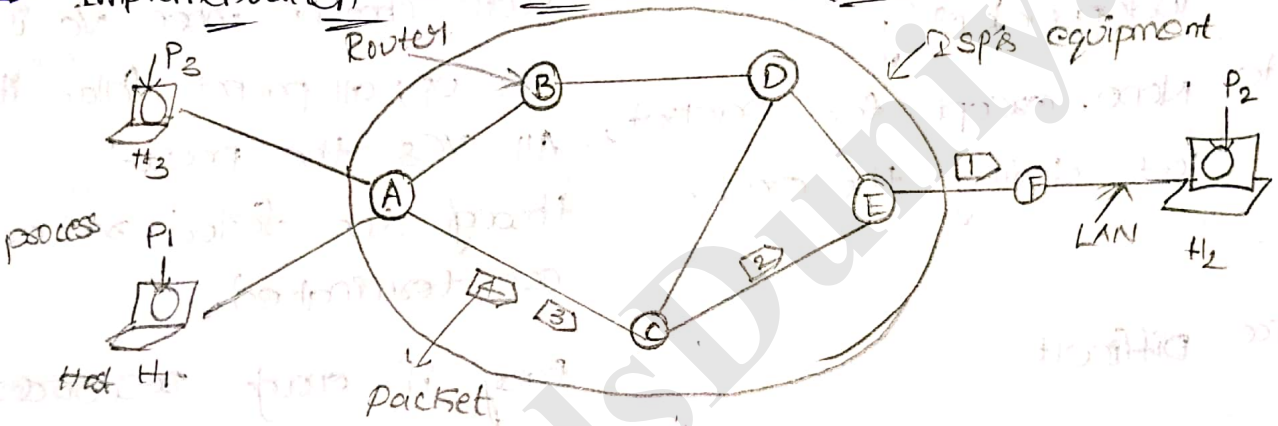
E's Table

A	C
B	D
C	C
D	D
E	
F	F

Routing within a datagram n/t.

19/2/19

Implementation of connection-oriented service:-



A's Table

In	Out
H_1	1
H_3	1

In	Out
C	1
C	2

C's Table

In	Out
A	1
A	2

In	Out
E	1
E	2

E's Table

In	Out
C	1
C	2

In	Out
F	1
F	2

Routing with in a virtual-circuit n/t.

Comparision of

* Comparison of Virtual Circuit and Datagram:

Issue	Datagram N/t	virtual-circuit n/t.
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 the passed through the failed router are terminated.
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion / traffic control	Difficult	Easy if enough resources can be allocated in advance for each VC.

comparison of datagram and virtual-circuit networks.

20/2/19 Routing Algorithms :-

* N/t layer implements routing service using Routing algorithms. these algorithms are useful to findout a path b/w source & destination where the packets are cross many hops (routers).
* The calculation of Routing path is done according to the rules and regulations of routing algorithm.
* The various routing algorithms are applied based on wire, wireless n/t with respect to node ability.

* Some routing algorithms ... Question Papers

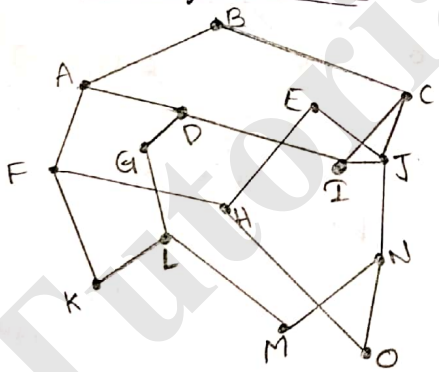
information dynamically in routing table where as some algorithms can specify static routing information in routing tables of the n/t routers. Some of the routing algorithms are listed below.

→ Optimality principle
→ shortest path algorithm (Non-adaptive)
→ Flooding
→ Distance vector Routing
→ Link state routing
→ Routing in ad hoc networks.

* The Routing algorithm finds a path for packet transportation from source to destination by considering the following parameters.

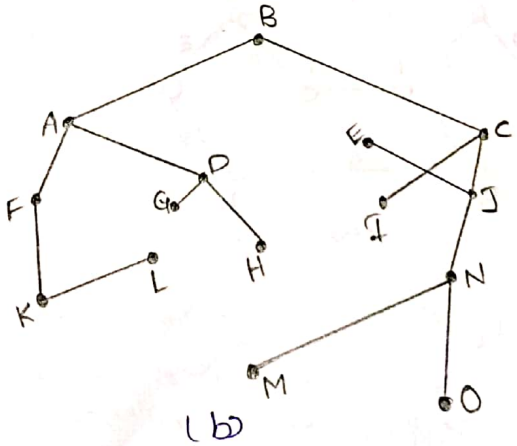
1. The type of n/t
2. Numbered hops
3. Minimizing cost
4. Networks provides interest.
5. Timing constraints
6. Delay

* Optimality principle :-



(a)

a Networks



(b)

A sink tree for router B

In optimality principle is

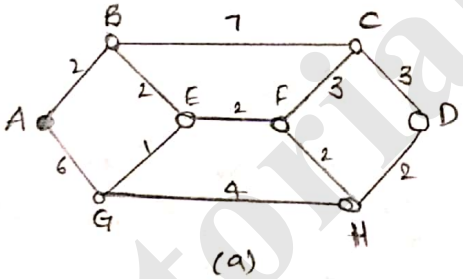
* An optimality principle is applied on networks to select an optimal route between set of source knows to a selected destination

* An optimality principle is used by networks to construct a sink tree to transport the packets efficiently between source to destination.

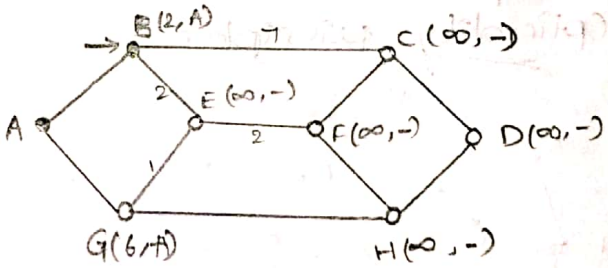
* An optimality principle is applied on networks for packet transportation with an optimal roots between source to destination by loops (∞) cycles in the network.

* An optimality principle can follows directly acyclic graph (DAG) so that a network can be formed sink trees without conjuctions

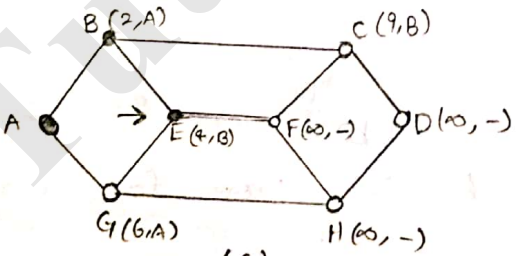
Shortest path algorithm:- Non-adaptive



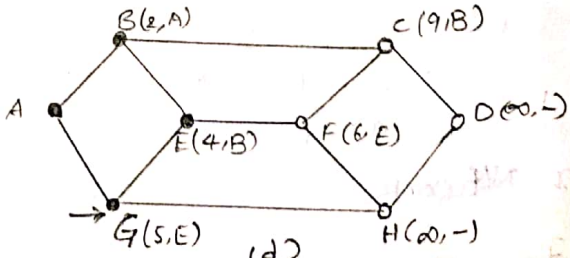
(a)



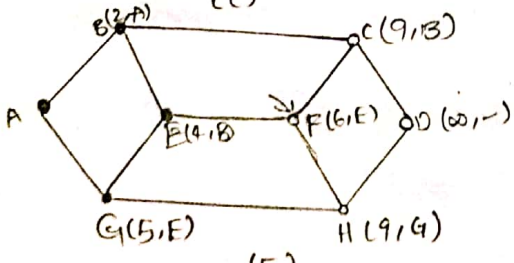
(b)



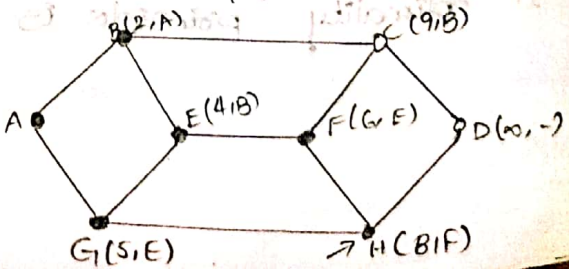
(c)



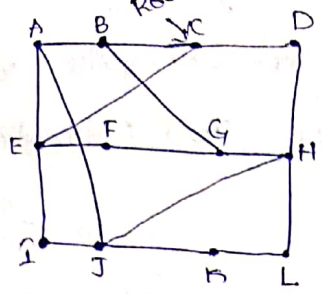
(d)



(E)



Distance vector routing algorithm



(a)

To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6

vectors received from J's four neighbours

New routing table for J (from J)

↓	Line
8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	—
6	K

(b)

JA = JA+AA =

JI = J

* Routing algorithms are use to find out an optimal path b/w sender and receiver in a n/t. the routing algorithm is responsible for deciding the outgoing path for each and every incoming packet in a n/t. which should be transmitted from source to destination.

* the routing algorithms can be grouped into two major classes one is 1) adaptive routing algorithms
2) Non - adaptive routing algorithms.

* Adaptive routing algorithms can change their routing decisions which reflects n/t topology where as non-adaptive routing algorithms do not depends on any measurement (or) Estimates of the current topology and topoby.

* In Non-adaptive routing algorithms the routing path b/w nodes of a n/t is available priorly. Based on this procedure only a non-adaptive routing algorithm is also known as static routing algorithm.

eg: shortest path routing algorithm.

In shortest path Routing algorithm a paths b/w nodes are available statically.

* A non adaptive routing algorithm example is distance vector routing algorithm which dynamically changes a routing paths along with desicions b/w nodes. which is generally apply on Mobile nodes of a n/t.

* Distance vector Routing can find out an optimal path b/w nodes of a n/t where each and every node maintain a table (Spectrum).

* This table is consisting two entries 1) The best node distance b/w nodes

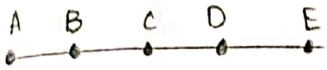
2) The line which is connecting the specify destination.

* If the distances changed b/w the nodes that will reflects an optimal path and n/t topology. for this reason the vectors (or) tables are dynamically updated depending on n/t nodes mobility (movement).

* The distance vector routing algorithm is introduced by Bellman ford in the year of 1962 with major revision.

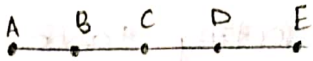
* this algorithm is practically applied on the ARPANET (Advance Research project Agency for Network)

the count-to-Infinity problem:



.	.	.	.	Initially
1	.	.	.	After 1 exchange
1	2	.	.	After 2 exchanges
1	2	3	.	After 3 exchanges
1	2	3	4	After 4 exchanges

(a)



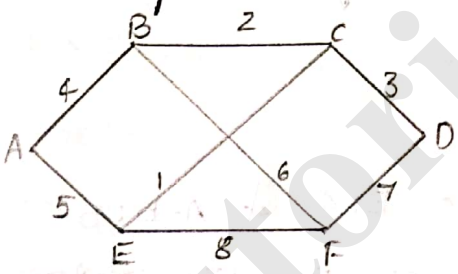
1	2	3	4	Initially
3	2	3	4	After 1 exchange
3	4	3	4	After 2 exchanges
5	4	5	4	After 3 exchanges
5	6	5	6	After 4 exchanges
7	6	7	6	After 5 exchanges
7	8	7	8	After 6 exchanges
:	:	:	:	
.	.	.	.	

(b)

Link State Routing

1. Discover neighbours, learn network addresses.
2. Set distance/cost metric to each neighbour.
3. Construct packet telling all learned.
4. Send packet to, receive packets from other routers.
5. compute shortest path to every other routing.

Building Link state packets:-



(a)

Link state packets

A	
Seq	
Age	
B	4
E	5

B	
Seq	
Age	
A	4
C	2
F	6

C	
Seq	
Age	
B	2
D	3
E	1

D	
Seq	
Age	
C	3
F	7

E	
Seq	
Age	
A	5
C	1
F	8

F	
Seq	
Age	
B	6
D	7
E	8

(b)

* problem with distance vector Routing Algorithm is count-to-Infinity. Because of this reason the distance vector routing algorithm is too for implementation specifically when the n/t topology has been changed.

* In this connection the distance vector Routing Algorithm

is replaced by link state routing algorithm.

* Link State Routing algorithm is uses various links to the state of the node which are maintained by each and every Routers routing table.
* Link state routing algorithm is most widely use routing algorithm inside of large n/t and in today's Internet.
* Link state routing algorithm is constructed fairly simple and can be stated as 5 points.

(all 5 points described in the above Section).

* In link state routing algorithm once the information is needed for exchange has been collected by the immediate router in the next step so that a ready build packet is consisting all the new data items.
* Each packet is specified with identity of the sender, followed by sequence number, age and list of neighbours.
* In the above example n/t it is consisting 6 no. of nodes with labels A, B, C, D, E, F, ~~G, H, S~~
* The neighbouring nodes for A are B & E.
* For each neighbour the label cost is A-B: 4 & A-E: 5
* The corresponding links state packet for all the six routers in a given n/t are describe in figure(b).
* A link specify the neighbouring node of a sender sequentially and the age also specify based on starting and ending timing values of each and every packet in a n/t node.
* All the neighbouring nodes states (or) specify based on senders links with neighbouring node sequence and age values

* the packets are constructed from sender to receiver computed shortest path. The computed shortest path will consist minimum values with respect to distance / cost metric.

* The link state routing algorithm defines over shortest path routing algorithm and DVR algorithm. while computing the best optimal route from sender to receiver in a n/t.

Congestion control:-

Congestion:- Too many packets arriving at a node in a n/t can decrease n/t performance and increases delay and packet loss. This situation is called congestion.

* Due to reason of n/t traphy congestion will lead to bottlenecks in a n/t which also degrades the n/t throughput.

* congestions has to be control to increase n/t data transfer rates b/w nodes.

* Cogestion control is a common responsibility for n/t layer and transport layer. When congestion is control by transport layer obviously there has been less traphy in the n/t layer.

* N/t layer and transport layer should work together for controlling congestions in a n/t. Still n/t layer will implement various approaches for congestion control where as transport layer can implement different approaches for congestion control.

* The congestion when occurs in a n/t the transport layer can apply congestion control algorithms and then only sends TPDU's to n/t layer. If still there is congestions the n/t layer implement its own congestion control algorithms to avoid congestions in a n/t.

* Basically n/t layer will provide the two existing soln to

address congestion issues.

1) N/t layer provides enough no.of n/t resources.

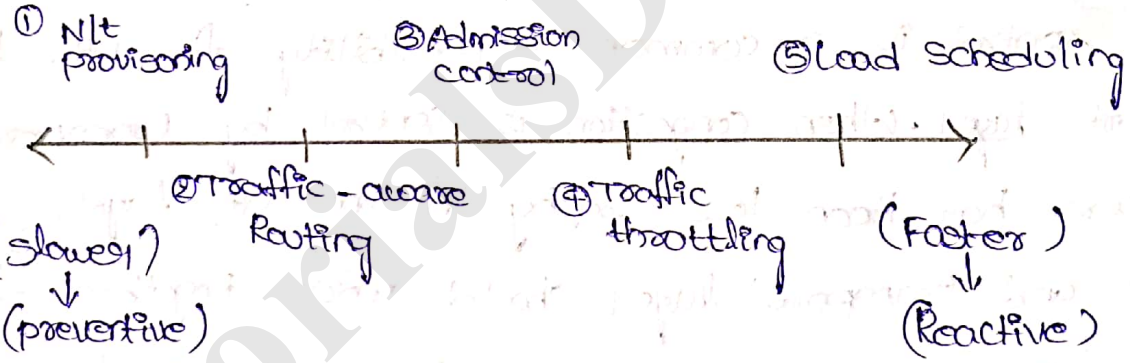
2) Transport layer TPDU's (N/t load) has to be decreased.

* these solutions are usually combine and applying on different schems with respect to the timing values.

* the most Basic way to avoid congestions is to build a n/t which is capable to carry the no.of generated packets, in a way by reducing traffic.

* the various approach for congestion contrd by n/t layer with different time scales has been pictured in the fatwing figures.

congestion contrd by n/t layer assigned to basic approaches not suitable in all cases in the n/t.



Network provisoning:

22/11/19

CN-6

Transport Layer

* Transport layer
* Application layer
    1. DNS Domain Name Server
    2. Resource Records
    3. Name servers
* E-Mail
    - E-Mail Architecture
    - Services
* User Agents, Message formats and Delivery

Application Layer:

* An application layer only interacting with sender and receiver system
* An application layer implements protocols like FTP, SMTP, HTTP, Telnet, SNMP and domain Name Servers (DNS).
* Application layer along with HTTP connects to World wide Web Servers to carry and forward message request and responses.
* An application layer in a n/t maintains Firewalls and application Gateways for secure message transfers.

**DNS :- Domain Name Server (or) System (or) Space

* Application layer of a computer N/t maintains domain name systems for providing services for the user queries.
* DNS is invented in the year of 1983 with support of a hierarchical, domain based Naming scheme and a distributed database system for implementing services to the end users in internet.
* A domain name system primarily used for mapping HostIp addresses and also used to address various resource records.

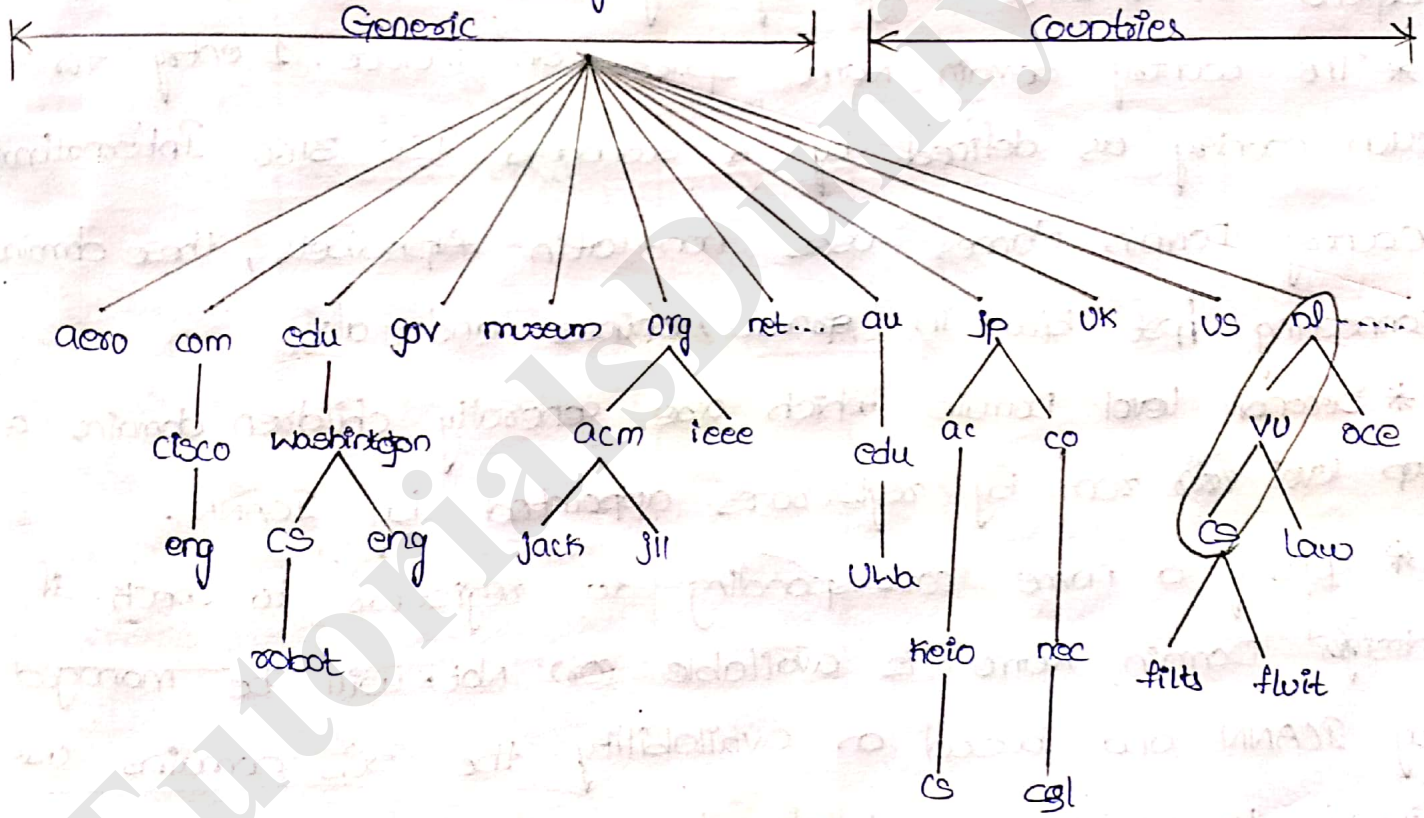
* Before 1983 handling a large databases which are connected to the internet is a non trivial problem.

* For the internet the naming hierarchy is managed by an organization called "ICANN" Internet corporation for Assigned Names and Numbers.

* ICANN were started in the year of 1998 as part of Internet world wide web for the purpose of domain names assignment and resource record allocation.

* Totally internet is consisting 250 top level domains, where each domain covers many hosts.

* Each domain is consisting sub domains again



A portion of the internet domain name space.

* DNS Represents all internet Root and children domains in tree structure which is represented in the above figure.

* In the above tree structure all domain names (top level domain) are directly connected to internet web server and the leaves of the tree represent sub domains where as sub domains

again creates further node divisions, or specific sub domains

have no further divisions they are directly link to the machines.

* A leaf domain may contain a single host (or) it may represent a company which is consisting thousands of host.

* The top-level domain of internet domain space is categorised into

→ Generic portion of Internet Domain Name space

→ Countries portion of Internet Domain Name space.

* The Generic portion of Domain Name space is consisting the general domains which can be added further in future depend on internet usage by organization.

* The country domain Name space can include 1 entry for each country as defined by a standard ISO 3166 Internationalize country Domain Names uses non-latin Alphabets, these domains connecting host blw in Arabic, chinese and also

* Second level Domain which are generally children domains of top level (are) run by registrars appointed by ICANN.

* Getting a name corresponding to registrar to check if desired Domain Name is available (or) Not, will be managed by ICANN and based on availability the sub domains are linked to registrars and also to the top-level domains.

Generic Top-level domains:— top-levels are run by registrars

Domain Name	Intended usage	started year	Restricted
.com	commercial	1985	No
.edu	educational Institutions	1985	Yes
.gov	government	1985	yes
.int	international organizati on	1988	yes
.mil	Military	1985	yes
.net	Internet providers	1985	No
.org	Non profit orgnization	1985	No
.aero	Aerospace	2001	yes
.biz	Bussiness	2001	No
.coop	co-operatives	2001	yes
.info	informational	2002	No
.museum	Museums	2002	yes
.name	people	2002	No
.pro	professionals	2002	yes
.cat	catalan	2005	yes
.jobs	employement	2005	yes
.mobi	Mobile devices	2005	yes
.tel	contact details	2005	yes
.travel	Travel Industry	2005	yes

6/2/19

* Each domain is named by path from leaves to root the components are separated by dots.

eg: cs.vu.nl

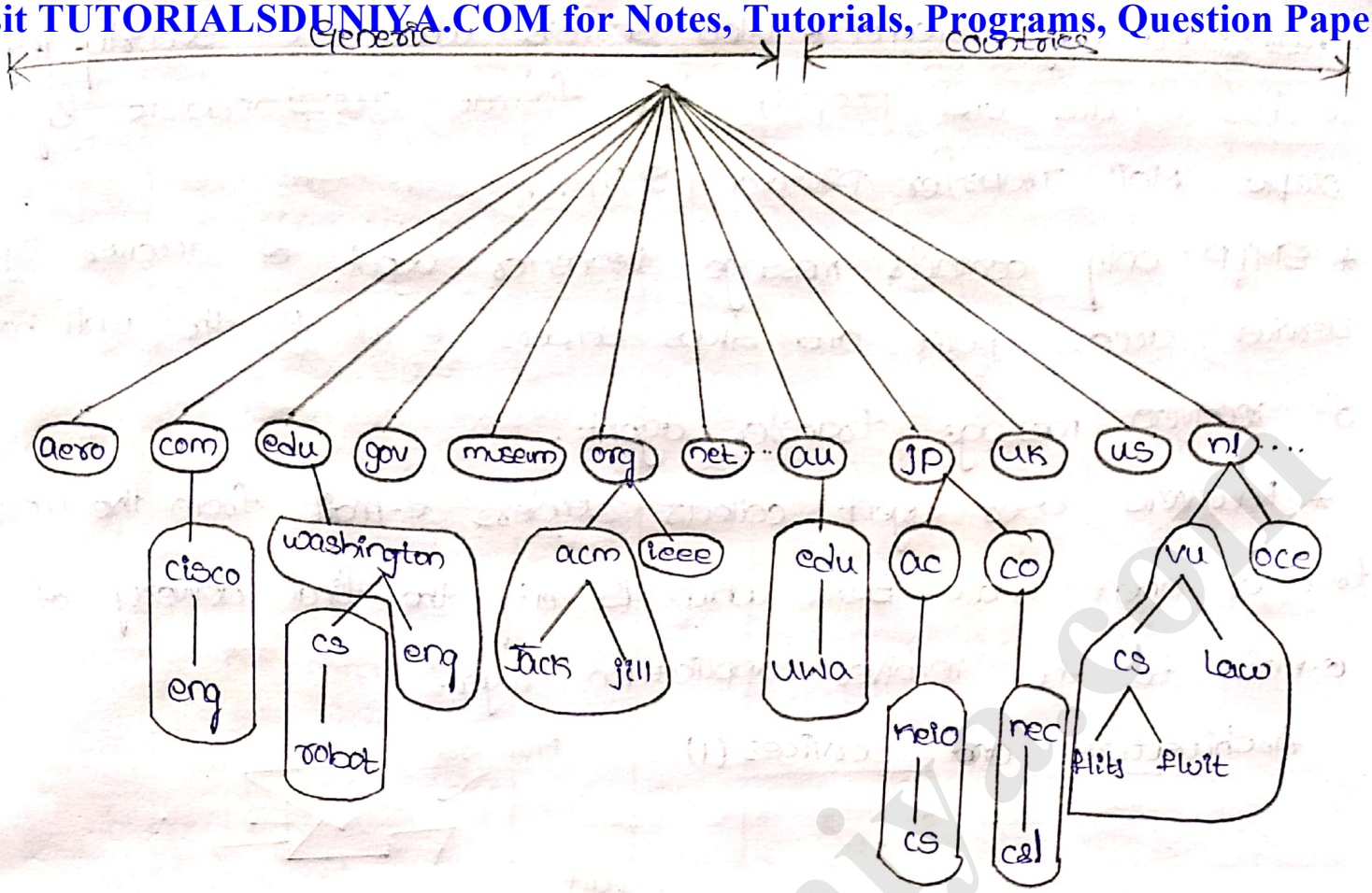
* The above statement is consisting the top level domain is "nl" (netherlands), "vu" is sub domain to 'nl' which is

beije university and 'cs' is a leaf to the bu third-level domain which is school of computer science.

* To create a new domain permission is required from the domain root, registrors, internet domain space availability should be conformed by related country and finally issued by ICANN.

Domain (Resource Records):- physically domain data stored

Type	Meaning	Value
SOA	start of authority	parameters for this zone
A	IPV4 address of a host	32-Bit integer
AAAA	IPV6 address of a host	128-Bit integer
MX	Mail exchange	priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	canonical name	Domain name
PTR	pointer	Alias for an Ip address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	service	host that provides it
TXT	Text	Descriptive ASCII text.



part of DNS Name space is divided into zones which are serviced by

7/2/19

E-mail:- (Electronic-Mail)

* E-mail are basically introduced with the purpose of file transfer and specifically for resource sharing.

* In Internet domains emails (or) Launched with the support of basic protocol FTP and SMTP.

* Emails are prepared and initiated at the side of sender source along with W3 World Wide Web with specific format.

E-mail Architecture:-

* At the side of senders system user agent are programs prepared for submission of senders data with the rules and regulations of SMTP. User agent application programs only interacts with senders host.

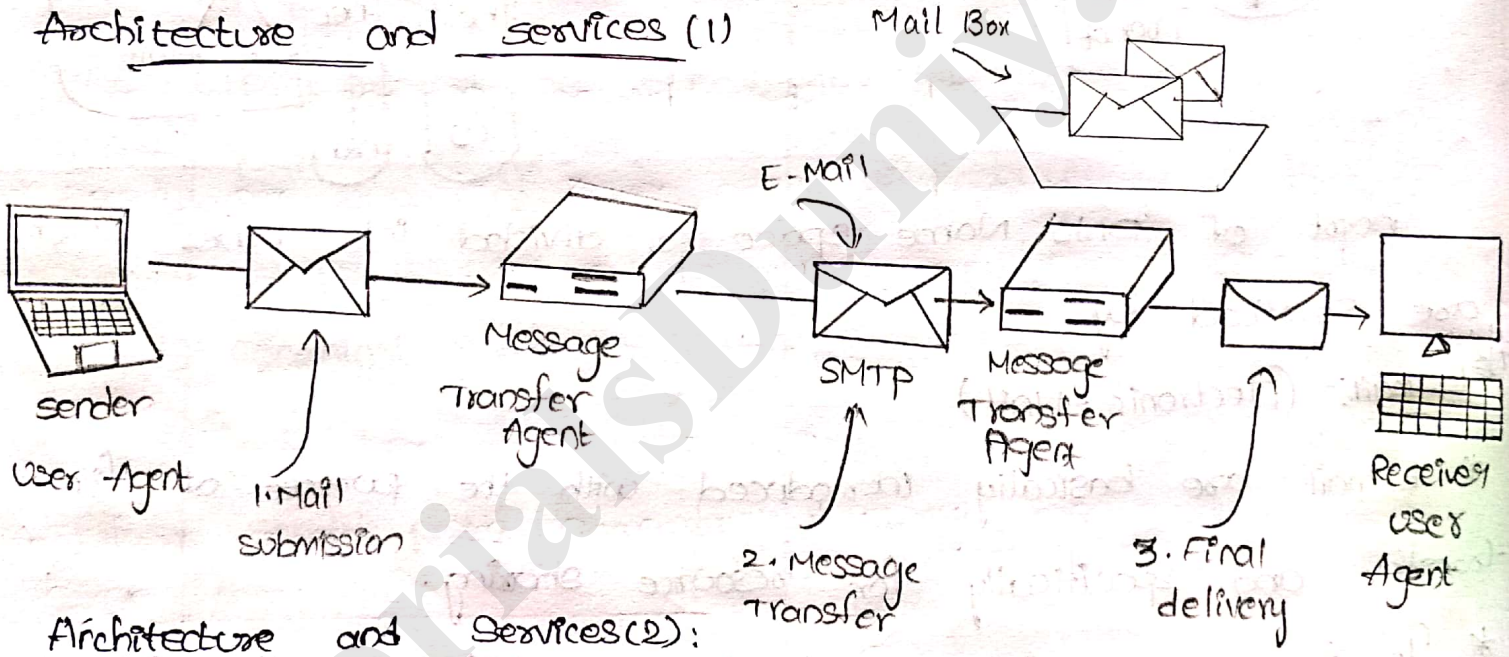
Message transfer agents are the application programs

maintained by internet - Web servers which are securly receive senders e-mails and prepares the format understandable by simple Mail Transfer protocol (SMTP).

* SMTP only contacts message transfer agent of receiver system service access point and drops senders e-mail in the mail box of receivers message transfer agent.

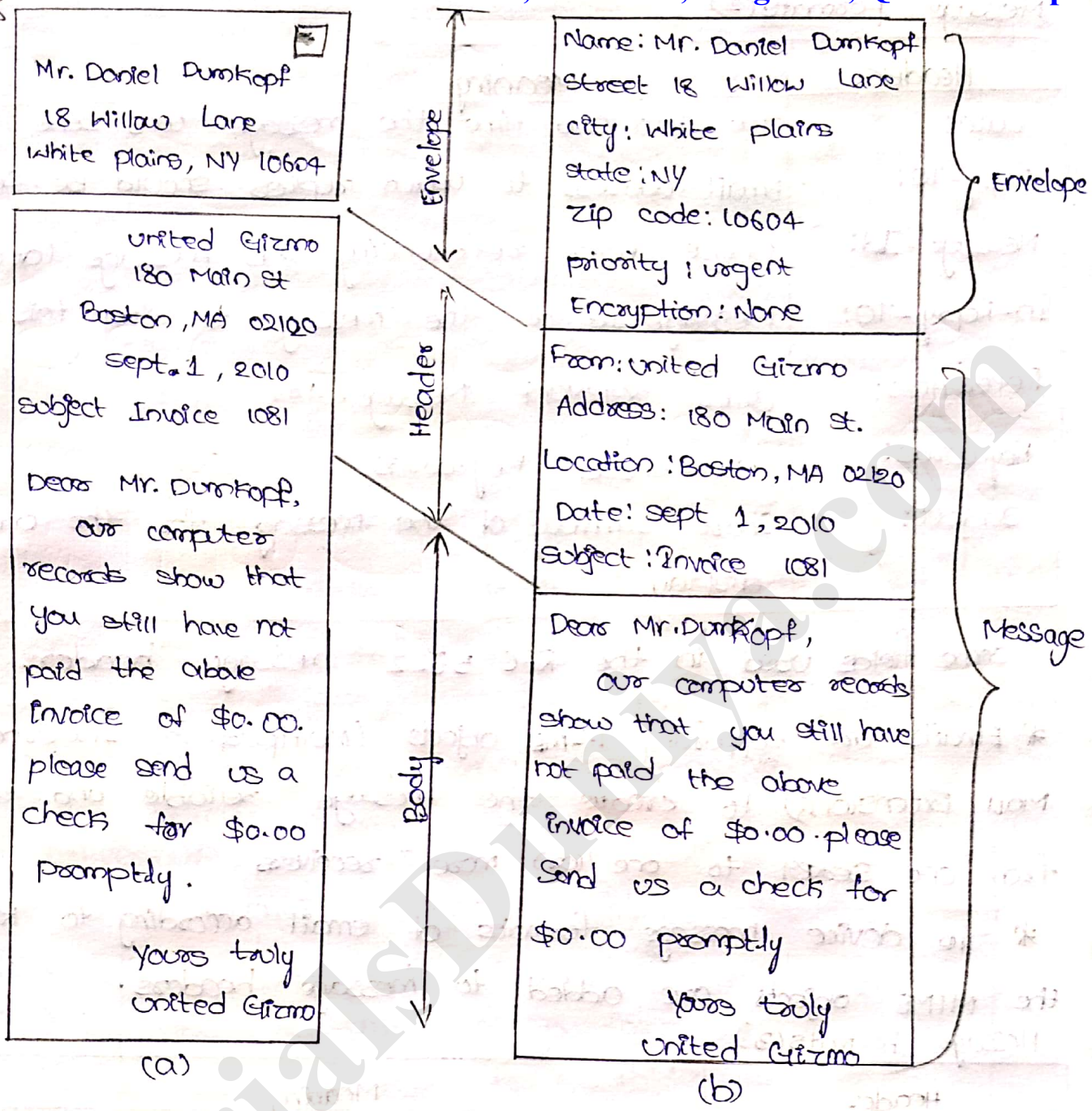
* Receivers user agent collects senders e-mail from the message transfer agent mail Box which is only the final delivery of e-mail to the receiver application layer.

Architecture and services (1)



Architecture and Services (2):

SAP - service Access point



Envelopes and messages. (a) paper mail (b) Electronic mail.

Message Formats

Header	Meaning
TO:	Email address(es) of primary recipient(s)
CC:	Email address(es) of secondary recipient(s)
Bcc:	Email address(es) for blind carbon copies
From:	person or people who created the message
Sender:	Email address the actual sender
Received:	Line added by each transfer agent along the route
Return-path:	can be used to identify a path back to the Sender.

Message Formats (2)

Header	Meaning
Date:	The data and time the message was sent
Reply-TO:	Email address to which replies should be sent
Message-Id:	Unique no. of referencing this message later
In-Reply-TO:	Message-Id of the message to which this is a reply
References:	Other relevant Message-Ids
Keywords:	User-chosen keywords
Subject:	Short summary of the message for the one-line display

Some fields used in the RFC 5322 message header.

* Emails are supporting MIME objects (Multipurpose Internet Mail Extensions) to create the message reliable and effectively from one sender to one (or) more receivers

* the device message formats of email according to RFC 5322 the MIME objects are added to message headers.

Message Formats (3)

Header	Meaning
MIME-version:	Identify the MIME version
content-Description:	Human-readable string telling what is in the msg.
content-Id:	Unique identifier
content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content.

Message headers added by MIME.

Command	Description.
CAPABILITY	List server capabilities
STARTTLS	Start secure transport (TLS; see chap. 8)
LOGIN	Log on the server
AUTHENTICATION	Log on with other method
SELECT	select a folder
EXAMINE (ready to send data)	select a read-only folder
CREATE	create a folder
DELETE	Delete a folder
RENAME	Rename a folder
SUBSCRIBE	Add folder to active set
UNSUBSCRIBE	Remove folder from active set.

IMAP (version 4) commands.

Final Delivery(2):-

LIST	List the available folders
LSUB	List the active folders.
STATUS	Get the status of a folder
APPEND	Add a message to a folder
CHECK	Get a checkpoint of a folder
FETCH	Get messages from a folder
SEARCH	Find messages in a folder
STORE	Alter message flags
COPY	Make a copy of a message in a folder
EXPUNGE	Remove messages flagged for deletion
UID	Issue commands using unique identifiers
NOOP	Do nothing
CLOSE	Remove flagged messages and close folder
LOGOUT	Log out and close connection.

* Final Delivery is ready to receive by receiver agent at the receiver system.

* Now a days the user agents on pc, Laptop (or) Mobile is lisely on the different machine rather than ISP.

* The final Delivery of message is almost receives the message by the receiver but still IMAP protocol has to be called by the receiver agents.

* IMAP is internet message access protocol define with RFC 5301 version (4) standard.

* IMAP is similar to SMTP, to use IMAP the mail server runs an IMAP server that listens to the pole 143 and the user agents runs as IMAP clients. The client can connects to the server by issuing commands.

* IMAP is an improvement to the pop 3. (post office protocol)

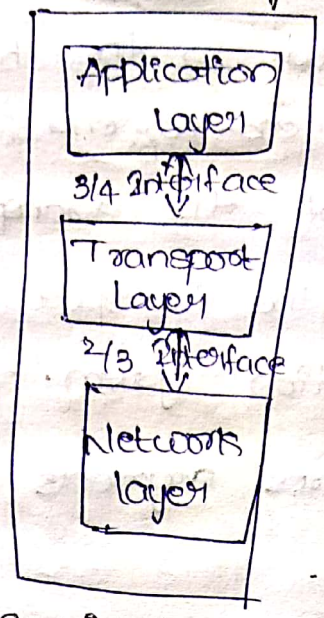
pop3 is an initial version for message transfers though emails according to RFC 1939.

12/2/19 Transport Layer:-

* Transport Layer is works along with N/t Layer and both together implements reliable packet transmission as part of protocol hierarchy in a computer Network. Transport layer lies b/w Application and Network layer of a N/t Architecture.

* Transport layer access the services using 3/4 interface from the application layer and forward segments to the N/t layer using 2/3 Interface.

Configuration of Transport Layer:-



Transport layer services:-

* Services provided to the upper layers

* Transport layer implements services to the above layer using application / transport interface and also provides services to the below layers by transport / Network interface.

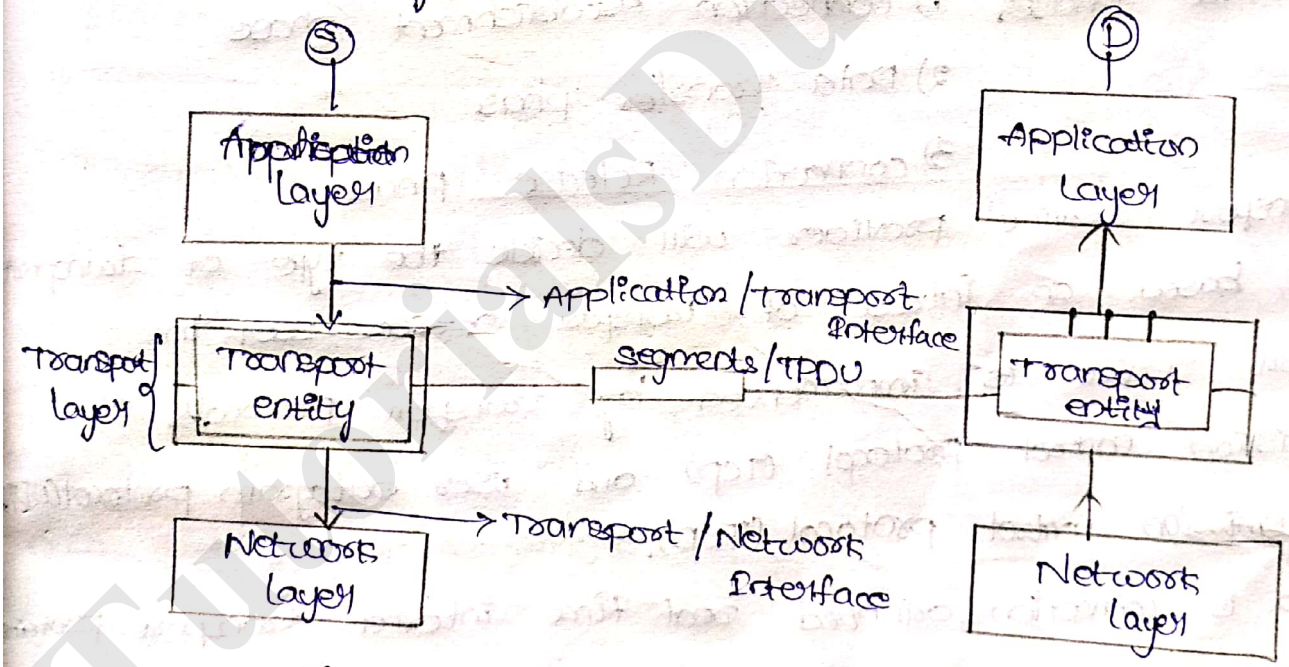


Fig:- N/t, Transport and application layer.

1) The ultimate goal of transport layer is to implement efficient, reliable and low cost effective data transmission to the user.

2) The S/W and oblic / H/W within transport layer is called

transport entity. Generally the transport entities is used by transport layer is located in the kernel of OS.

3) A transport layer provides end-to-end finctionality which needs the transport entity of the transport layer can be able to communicate with the transport entity of transport layer of source to Destination system. The transport layer transport entities only prepares segments which is the data format of transport layer.

4) There are two different types of transport services implemented by transport layer. Those are connection oriented transport service and connection less transport service.

5) In both cases of transport services are implemented by using three phases 1) connection establishment phase
2) Data Transfer phase
3) connection Release phase.

6) Transport service provider will decide the type of transport service based on intent of transport service user the transport service is implemented by transport protocals of transmission control protocol (TCP) and user datagram protocol(UDP)

** Transmission control protocol (TCP): (Telegram, Telephone)

* TCP is connection oriented real time internet transport protocol which is specifically designed to provide a reliable end to end byte stream protocol TCP was designed according to RFC 793 and in the year of 1981 which is designed to adopt properties dynamically of the internet.

* TCP is a reliable protocol, used to implement connection

of TCP. TCP connection has its own 32 bit sequence number in the ethernet and consisting 56 Kbps leased lines.

* The sending and receiving TCP entities exchange data in form of segments. The TCP segments consist a 20 byte header followed by 0 (or) more data bytes.

* Each segments include TCP header, must fit in the 65,515 byte IP payload and each link has an MTU (Maximum Transfer Unit).

* In TCP data transportation the receiver will send an acknowledgment back to the sender so that it guarentees the reliable data transportation.

* TCP specifies time stamp option so that the data is deliver from sender to receiver within specified timing values.

* TCP can manages effectivly congestion control and retransmissions, TCP timer and connection management

User Datagram protocol (UDP):- eg:- postcard

* UDP is used to implement connection less services and which is an important internet transport protocol.

* UDP protocol in a nlt will not give guarente regarding reliable data transmission in communications.

* UDP is a simple connection less protocol which runs in operating system and UDP typically runs in user space.

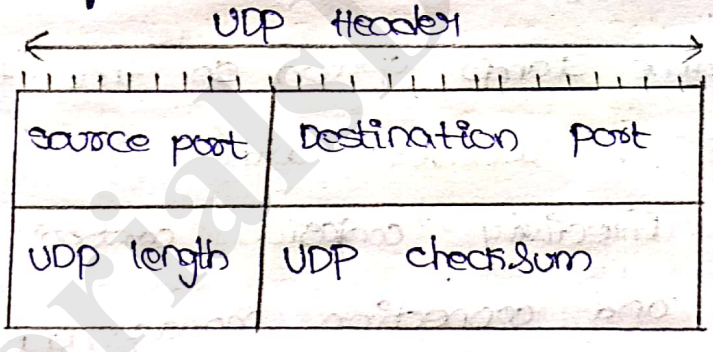
* UDP provides a way for application to send encapsulated IP datagrams without having to establish a connection.

* UDP is describe according to RFC 768

* UDP transmits segments consisting of an 8 byte header

followed by payload.

* The UDP header is consisting two ports to serve the communication end points within source and destination machine.
* The real time example for UDP is postal system.
* UDP header length includes 8 byte header and data. the minimum length is 8 bytes to cover the header and maximum length is 65515 bytes.
* In UDP header, UDP length field and checksum field is presented. UDP length field is includes 8 byte header and data. Checksum field is an optional field provided for extra reliability.



TutorialsDuniya.com

Download FREE Computer Science Notes, Programs, Projects, Books PDF for any university student of BCA, MCA, B.Sc, B.Tech CSE, M.Sc, M.Tech at https://www.tutorialsduniya.com

- Algorithms Notes
- Artificial Intelligence
- Android Programming
- C & C++ Programming
- Combinatorial Optimization
- Computer Graphics
- Computer Networks
- Computer System Architecture
- DBMS & SQL Notes
- Data Analysis & Visualization
- Data Mining
- Data Science
- Data Structures
- Deep Learning
- Digital Image Processing
- Discrete Mathematics
- Information Security
- Internet Technologies
- Java Programming
- JavaScript & jQuery
- Machine Learning
- Microprocessor
- Operating System
- Operational Research
- PHP Notes
- Python Programming
- R Programming
- Software Engineering
- System Programming
- Theory of Computation
- Unix Network Programming
- Web Design & Development

Please Share these Notes with your Friends as well