BUDDHA SERIES

(Unit Wise Solved Question & Answers)

Course – B.Tech. (CSE Allied-AIML/DS)

College – Buddha Institute of Technology

(AKTU CODE-525)

Department: Computer Science & Engineering Allied-AIML/DS

(Accredited by NBA 2024-27)

Subject: Computer Networks

(BCS 603)

Faculty Name: Mr. Shailesh Kumar Patel

Unit - 1

Q.1 What are the number of cable links required for n devices connected in mesh, ring, bus and star topology? **(AKTU 2014-15)**

Solution: The number of cables for each type of network is:

a. Mesh: n (n – 1) / 2

b. Star: n

c. Ring: n – 1

d. Bus: one backbone and n drop lines

Q2. Differentiate between bit rate and baud rate. State two reason for using layered protocols. **(AKTU 2014-15)**

Solution: Bit rate and Baud rate, these two terms are often used in data communication. Bit rate is simply the number of bits (i.e., 0's and 1's) transmitted in per unit time. While Baud rate is the number of signal units transmitted per unit time that is needed to represent those bits. There are two main reasons for using the layered protocols and these are:

1. Specialization and

2. Abstraction

- A neutral standard is created by a protocol which can be used by the rival companies for creating programs that are compatible.

- So many protocols are required in the field and that should also be organized properly and these protocols have to be directed to the specialists that can work up on these protocols.

- A network program can be created using the layered protocols by a software house if the guidelines of one layer are known.

- The services of the lower level protocols can be provided by the companies.

- This helps them to specialize.

- In abstraction, it is assumed that another protocol will provide the lower services.

- A conceptual framework is provided by the layered protocol architecture that divides the complex task of information exchange into much simpler tasks between the hosts.

- The responsibility for each of the protocols is narrowly defined.

- A protocol provides an interface for the successive higher layer protocol.

- As a result of this, it goes in to hiding the details of the higher protocol layers that underlies.

- **The advantage of using the layered protocols** is that the same application i.e., the user level program can be used by a number of diverse communication networks.

- For example, when you are connected to a dial up line or internet via LAN you can use the same browser.

- For simplifying the networking designs, one of the most common techniques used is the protocol layering.

- The networking designs are divided in to various functional layers and the protocols are assigned for carrying out the tasks of each layer.

- It is quite common to keep the functions of the data delivery separate from each other and separate layers for the connection management too.

- Therefore, we have one protocol for performing the data delivery tasks and second one for performing connection management.

- The second one is layered up on the first one.

- Since the connection management protocol is not concerned with the data delivery, it is also quite simple.
- The OSI seven layer model and the DoD model are one of the most important layered protocols ever designed.
- A fusion of both the models is represented by the modern internet.
- Simple protocols are produced by the protocol layering with some well defined tasks.
- These protocols then can be put together to be used as a new whole protocol.
- As required for some particular applications, the individual protocols can be either replaced or removed.
- Networking is such a field involving programmers, electricians, mathematicians, designers, electricians and so on.
- People from these various fields have very less in common and it is because of the layering that people with such varying skills to make an assumption or feel like others are carrying out their duty.
- This is what we call abstraction.
- Protocols at a level can be followed by an application programmer via abstraction assuming that network exists and similarly electricians assume and do their work.
- One layer can provide services to the succeeding layer and can get services in return too.
- Abstraction is thus the fundamental foundation for layering.
- Stack has been used for representing the networking protocols since the start of network engineering.
- Without stack, it would be unmanageable as well as overwhelming.
- Representing the layers of specialization for the first protocols derived from TCP/ IP.

Q3. Calculate the required bandwidth, if in a communication channel the signal power is 100 W and noise power is 10 W and the information transmission rate is 10kbps.

(AKTU 2014-15)

Solution:

Signal power is 100 W

Noise power is 10 W

Data rate of 10 kbps

Bandwidth?

Data rate = bandwidth * log (1 + (Signal power / Noise power))

10 = bandwidth * log (1 + (100 / 10)) {log (1 + (100 / 10)) = 3.4594 approx. equal to 4 is taken here}

10 = bandwidth * 4

Bandwidth = 2.5 KHz

Q4. It is required to transmit a data at a rate of 64kbps over a 3 kHz telephone channel. What is the minimum SNR required to accomplish this? **(AKTU 2014-15)**

Solution:

Given: Bit Rate = 64Kbps
W = 3KHz
$C = W \log_2 (1 + SNR)$, $C \geq C_{min} = 64$ kbps

$C_{min} = W \log_2 (1 + SNR_{min}) \Rightarrow$
$\log_2 (1 + SNR_{min}) = C_{min} / W = 64K / 3 \Rightarrow$
$1 + SNR_{min} = 2^{64K/3} \Rightarrow$
$SNR_{min} = 2.64 \times 10^6$
In dB: $SNR_{min} = 10 \log_{10} (2.64 \times 10^6) = 64.2$ dB

Q5. Discuss the devices of each layer of OSI reference model. **(AKTU 2014-15)**

Solution: Devices used in each layer are:

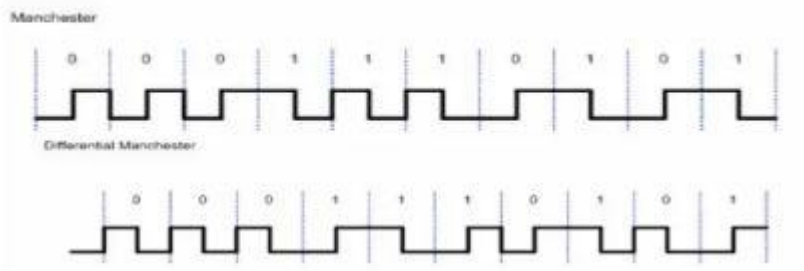
1. Physical layer or below: Hubs, Repeaters, Cables, Fibers, Wireless.
2. Data-link layer: Bridges, Modems, Network cards, 2-layer switches.
3. Network layer: Routers, Brouters, 3-layer switches.
4. Transport layer: Gateways, Firewalls.
5. Session layer:Gateways, Firewalls, PC's.
6. Presentation layer: Gateways, Firewalls, PC's.
7. Application layer: Gateways, Firewalls, all end devices like PC's, Phones, Servers.

Q6. Sketch the Manchester and differential Manchester encoding for the bit stream: 0001110101.

(AKTU 2014-15)

Solution:

The Manchester and differential Manchester encoding for the bit stream 0001110101:



Q7. What is OSI model? Explain the functions and protocols and services of each layer.

(AKTU 2015-16, 2017-18, 2018-19, 2021-22)

or

Explain functionalities of every layer in OSI model with neat block diagram.

(AKTU 2016-17, 2022-23)

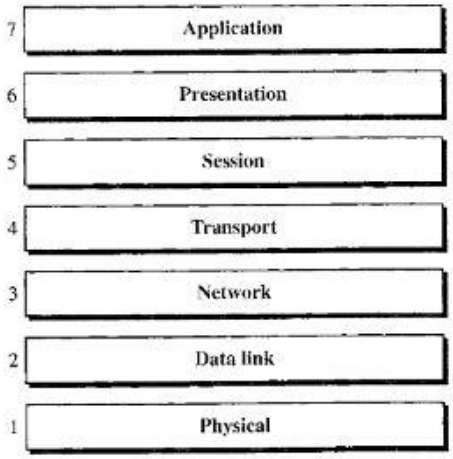
Solution:

THE OSI MODEL:

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

The OSI model is a layered framework for the design of network systems that allows communication

between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.



1) Physical Layer:

- Physical characteristics of interfaces and medium.
- Representation of bits.
- Data rate.
- Synchronization of bits.
- Line configuration.
- Physical topology.
- Transmission mode.

2) Data Link Layer:

- Framing.
- Physical addressing.
- Flow control.
- Error control.
- Access control.

3) Network Layer:

- Logical addressing.
- Routing.

4) Transport Layer:

- Service-point addressing
- Segmentation and reassembly.
- Connection control.
- Flow control.
- Error control.

5) Session Layer:

- Dialog control
- Synchronization

6) Presentation Layer:

- Translation.
- Encryption.
- Compression.

7) Application Layer:

- Network virtual terminal.
- File transfer, access, and management.
- Mail services.
- Directory services.

Q8. List the advantages and disadvantages of star topology. **(AKTU 2016-17, 2021-22)**

Solution:

Advantages of Star Topology:

1) As compared to Bus topology it gives far much better performance, signals don't necessarily get transmitted to all the workstations.

2) Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.

3) Centralized management. It helps in monitoring the network.

4) Failure of one node or link doesn't affect the rest of network. At the same time it's easy to detect the failure and troubleshoot it.

Disadvantages of Star Topology:

1) Too much dependency on central device has its own drawbacks. If it fails whole network goes down.

2) The use of hub, a router or a switch as central device increases the overall cost of the network.

3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device

Q9. List the advantages and disadvantages of ring topology. **(AKTU 2017-18, 2021-22)**

Solution: Advantages of ring topology:

1) Data can transfer between workstations at high speeds.

2) All data flows in one direction, reducing the chance of packet collisions.

Disadvantages of ring topology:

1) This topology is not very reliable, because when a link fails the entire ring connection is broken.

2) The entire network will be impacted if one workstation shuts down.

Q10. If a binary signal is sent over a 3 kHz channel whose signal to noise ratio is 20dB. What is the maximum achievable data rate? **(AKTU 2017-18)**

Solution:

According to Shannon theorem which specifies the maximum data rate in a noisy channel as B*log_2^(1+S/N) where B is the bandwidth, S/N is the signal-to-noise ratio. Usually, S/N is given in "decibel", not just a ratio. Decibel is calculated by dB=10log_10^(S/N)
Therefore, we get S/N first by 20dB=10log_10^(S/N) ==> S/N=10^2=100

Substitute S/N into Shannon's theorem, we get the maximum bps as
3k*log2^(1+S/N)=3log2^101kbps=19.97kbps.

However, the maximum data rate, assuming the channel is noise free, is only 6kbps, according to Nyquist rate. Therefore, the final answer should be 6kbps.

Q11. Explain network topological design with necessary diagram and brief the advantages and disadvantages of various topologies. **(AKTU 2017-18, 2022-23)**

or

Define topology and explain the advantage and disadvantage of Bus, Star and Ring topologies. **(AKTU 2018-19, 2021-22)**

Solution:

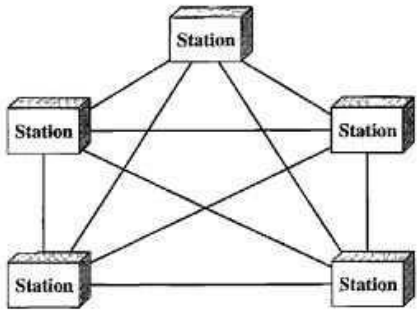
The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to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

Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries 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-1 nodes, node 2 must be connected to n-1nodes, 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. In this, connection is point-to-point.



Advantages:

(i) First, 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.

(ii) Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

(iii) Third, there is the advantage of privacy or security.

Disadvantages:

(i) The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

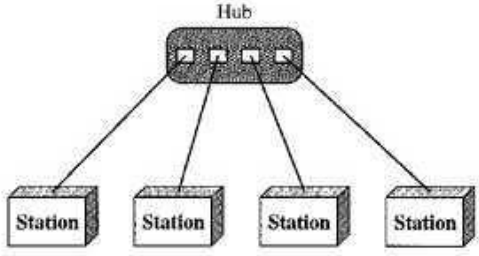
(ii) Every device must be connected to every other device, installation and reconnection are difficult.

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.

The star topology is used in local-area networks.



Advantages:

(i) 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.

(ii) It is robustness. If one link fails, only that link is affected. All other links remain active.

Disadvantages:

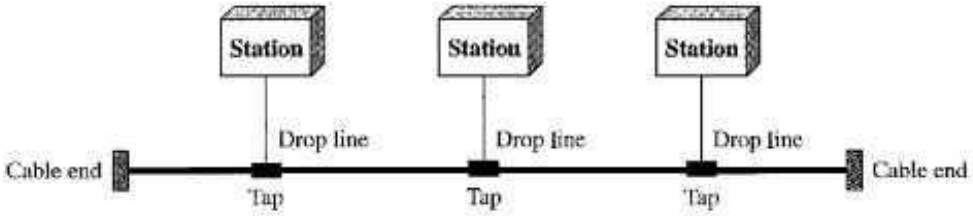
(i) The dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

Bus Topology:

A bus topology has multipoint connection. 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.

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.



Advantages:

(i) Advantages of a bus topology include ease of installation.

Disadvantages:

(i) Disadvantages include difficult reconnection and fault isolation.

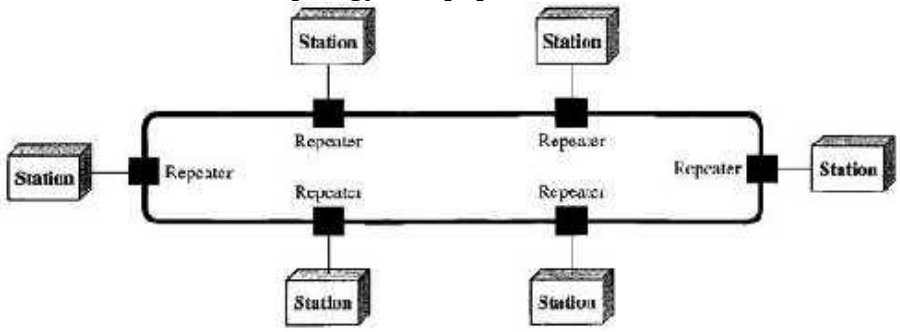
(ii) Difficult to add new devices.

(iii) A fault or break in the bus cable stops all transmission.

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.

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.



Advantages:

(i) A ring is relatively easy to install and reconfigure. To add or delete a device requires changing only two connections.

Disadvantages:

(i) Unidirectional traffic can be a disadvantage.

Q12. Use the network architecture knowledge to compare TCP/IP and OSI model.

(AKTU 2018-19, 2023-24)

Solution:

TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily inter dependent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.

i) Physical and Data Link Layers:

At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internet work can be a local-area network or a wide-area network.

ii) Network Layer:

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

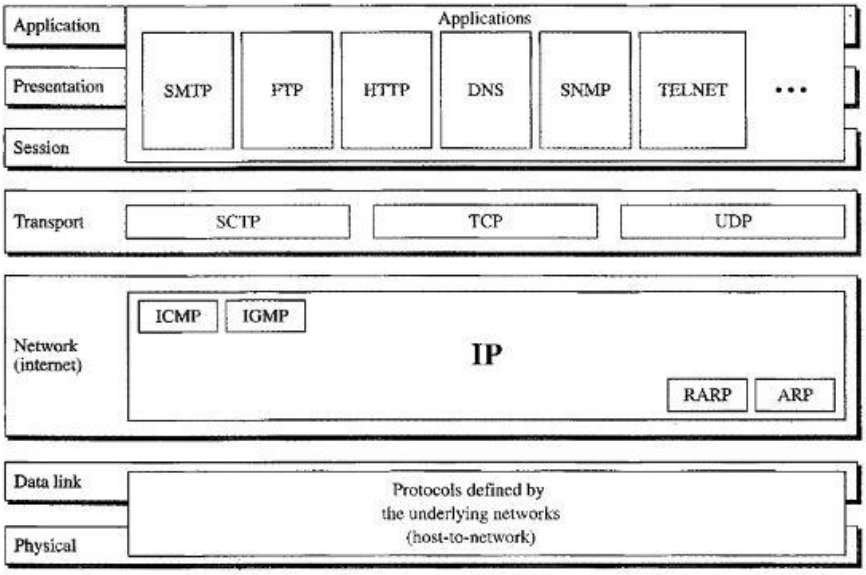
Internetworking Protocol (IP): The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Address Resolution Protocol: The Address Resolution Protocol (ARP) is used to associate a logical address with a physical address. ARP is used to find the physical address of the node when its Internet address is known.

Reverse Address Resolution Protocol: The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol: The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

Internet Group Message Protocol: The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.



iii) Transport Layer:

The transport layer was represented in TCP/IP by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol: It is a process-to-process protocol that adds only port addresses, check sum error control, and length information to the data from the upper layer.

Transmission Control Protocol: TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

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

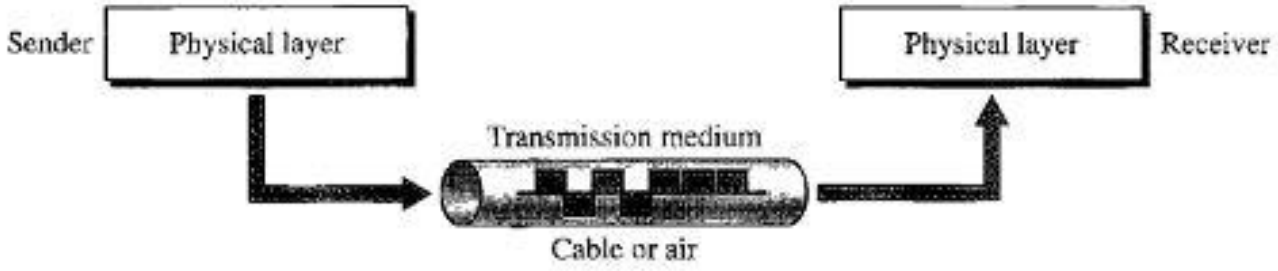
iv) Application Layer:

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.

Q 13. Define transmission media. Explain fibre optic cable in brief. Also explain the advantages of optical fibre over twisted pair and coaxial cable. **(AKTU 2017-18)**

Solution:

Transmission media are actually located below the physical layer and are directly controlled by the physical layer. A transmission medium can be broadly defined as anything that can carry information from a source to a destination. The transmission medium is usually free space, metallic cable,or fiber-optic cable.



For example, the transmission medium for two people having a dinner conversation is the air. For a written message, the transmission medium might be a mail carrier, a truck, or an airplane.

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Following figure shows how a ray of light changes direction when going from a more dense to a less dense substance.

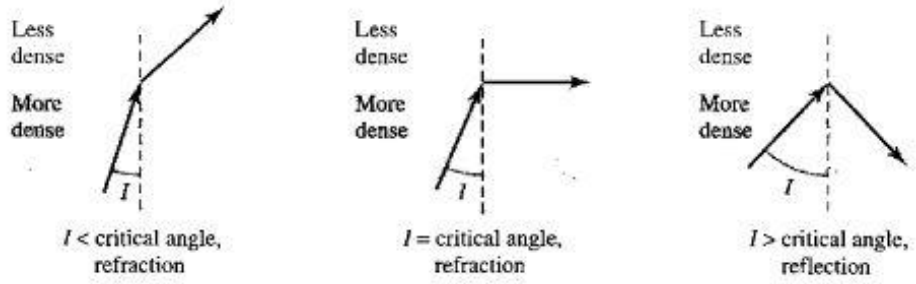


Figure: Bending of light ray

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

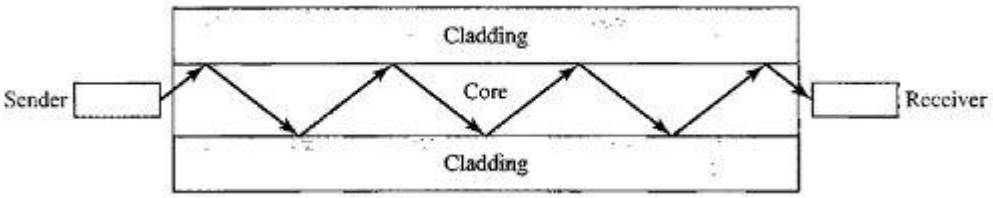


Figure: Optical fiber

Propagation Modes: It supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index.

Multimode: Multimode is so named because multiple beams from a light source move through the core in different paths. Multimode are two types:

i) **In multi mode step-index fiber**, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding.

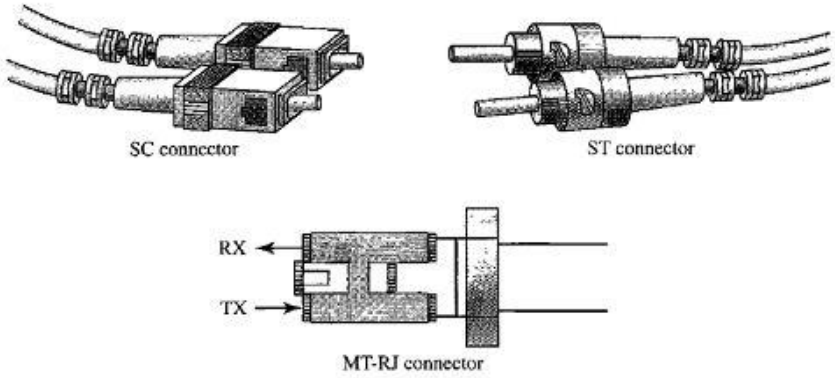
ii) A second type of fiber, called **multimode graded-index fiber**, decreases this distortion of the signal through the cable. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge.

Single-Mode: Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density.

Fiber Sizes: Optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

Fiber-Optic Cable Connectors: There are three types of connectors for fiber-optic cables.



The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system. The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.MT-RJ is a connector that is the same size as RJ45.

Performance: Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually 10 times less) repeaters when we use fiber-optic cable.

Applications: Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective. Today, with wavelength-division multiplexing (WDM), we can transfer at a rate of 1600 Gbps. Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Local-area networks such as 100Base-FX network (Fast Ethernet) and l000Base-Xalso use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber:

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

- ❖ Higher bandwidth.
- ❖ Less signal attenuation.
- ❖ Electromagnetic noise cannot affect fiber-optic cables.
- ❖ Glass is more resistant to corrosive materials than copper.
- ❖ Light weight.

Disadvantages: There are some disadvantages in the use of optical fiber-

- ❖ Installation and maintenance.
- ❖ Unidirectional light propagation.
- ❖ Cost.

Q 14. What is transmission impairment? Explain the three causes of transmission impairment.

(AKTU 2022-23)

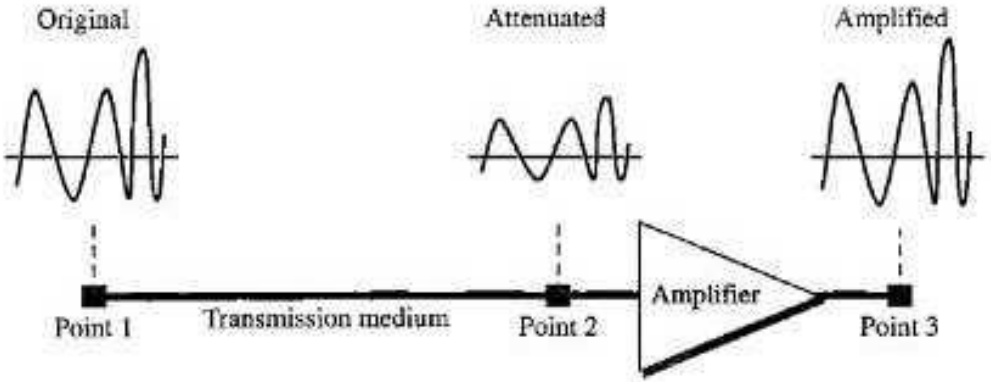
Solution:

Transmission Impairment:

Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received. Three causes of impairment are attenuation, distortion, and noise.

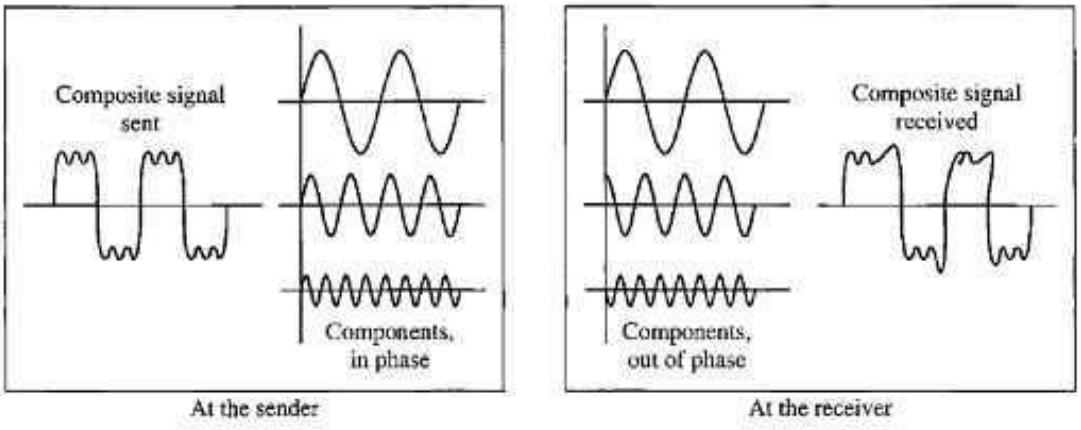
i) Attenuation:

Attenuation means a loss of energy. When a signal, simple or composite, travels through a medium, it loses some of its energy.



ii) Distortion:

Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of different frequencies. Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination. Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.



iii) Noise:

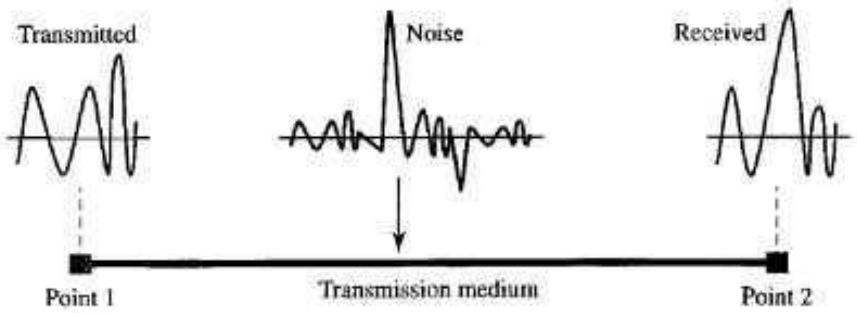
Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

Thermal noise is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

Induced noise comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

Crosstalk is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.

Impulse noise is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.



Q 15. How do guided media differ from unguided media? Explain co-axial cable in brief.

(AKTU 2018-19)

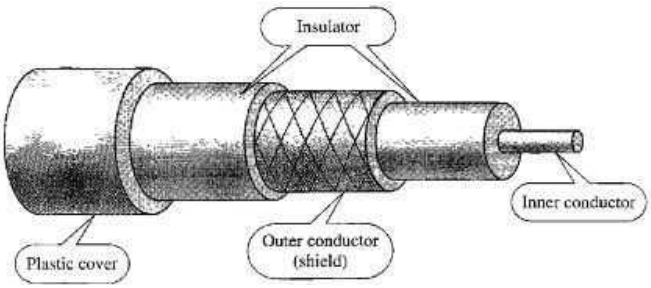
Solution:

In guided media, Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

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

Coaxial Cable:

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



Coaxial Cable Standards: Coaxial cables are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing.

Coaxial Cable Connectors: To connect coaxial cable to devices, we need coaxial connectors. The most common type of connector used today is the Bayone-Neill-Concelman (BNC), connector. Three popular types of these connectors: the BNC connector, the BNC T connector, and the BNC terminator.

Performance: the attenuation is much higher in coaxial cables than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth.

Applications: Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals. Later it was used in digital telephone networks where a single coaxial cable could carry digital data up to 600 Mbps. However, coaxial cable in telephone networks has largely been replaced today with fiber -optic cable. Cable TV networks also use coaxial cables.

Q 16. What is line coding? Explain different types of line coding scheme. **(AKTU 2018-19)**

Solution:

Line Coding: Line coding is the process of converting digital data to digital signals. We assume that data, in the form of text, numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits. Line coding converts a sequence of bits to a digital signal. At the sender, digital data are encoded into a digital signal; at the receiver, the digital data are recreated by decoding the digital signal.

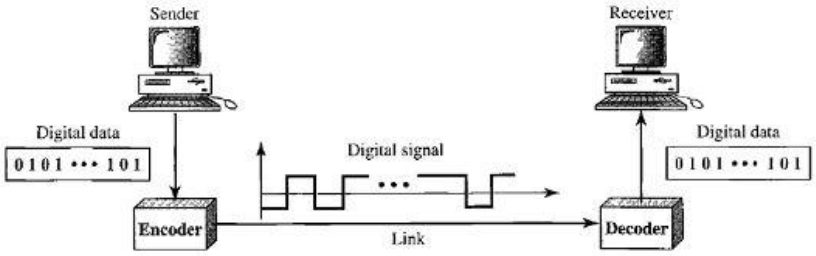


Figure: Line coding and decoding

Line Coding Schemes: We can roughly divide line coding schemes into five broad categories, as shown in Figure 1.54.

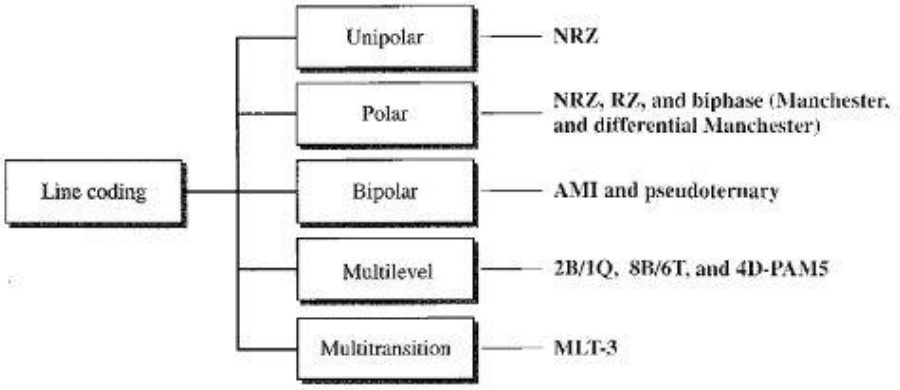


Figure: Line coding schemes

i) Unipolar Scheme: In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below.

NRZ (Non-Return-to-Zero): Traditionally, a unipolar scheme was designed as a non-return-to-zero (NRZ) scheme in which the positive voltage defines bit 1 and the zero voltage defines bit 0. It is called NRZ because the signal does not return to zero at the middle of the bit.

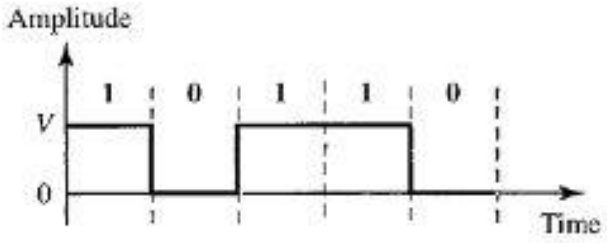


Figure: Unipolar NRZ scheme

ii) Polar Schemes: In polar schemes, the voltages are on the both sides of the time axis. For example, the voltage level for 0 can be positive and the voltage level for 1 can be negative.

Non-Return-to-Zero (NRZ): In polar NRZ encoding, we use two levels of voltage amplitude. We can have two versions of polar NRZ: NRZ-L and NRZ-I.

In the first variation, NRZ-L (NRZ-Level), the level of the voltage determines the value of the bit. In the second variation, NRZ-I (NRZ-Invert), the change or lack of change in the level of the voltage determines the value of the bit. If there is no change, the bit is 0; if there is a change, the bit is 1.

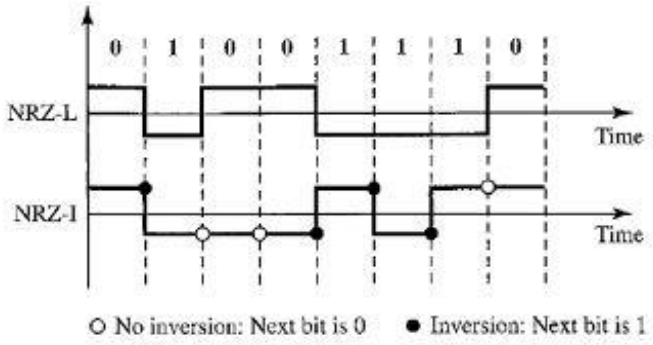


Figure: Polar NRZ-L and NRZ-I schemes

Return to Zero (RZ): The main problem with NRZ encoding occurs when the sender and receiver clocks are not synchronized. The receiver does not know when one bit has ended and the next bit is starting. One solution is the return-to-zero (RZ) scheme, which uses three values: positive, negative, and zero. In RZ, the signal changes not between bits but during the bit.

In Figure 1.57 we see that the signal goes to 0 in the middle of each bit. It remains there until the beginning of the next bit.

The main disadvantage of RZ encoding is that it requires two signal changes to encode a bit and therefore occupies greater bandwidth. Another problem is the complexity: RZ uses three levels of voltage, which is more complex.

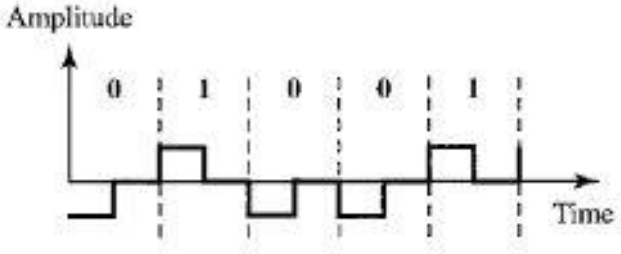


Figure: Polar RZ scheme

Biphase: Manchester and Differential Manchester The idea of RZ (transition at the middle of the bit) and the idea of NRZ-L are combined into the Manchester scheme.

In Manchester encoding, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization.

Differential Manchester, on the other hand, combines the ideas of RZ and NRZ-I. There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. If the next bit is 0, there is a transition; if the next bit is 1, there is none.

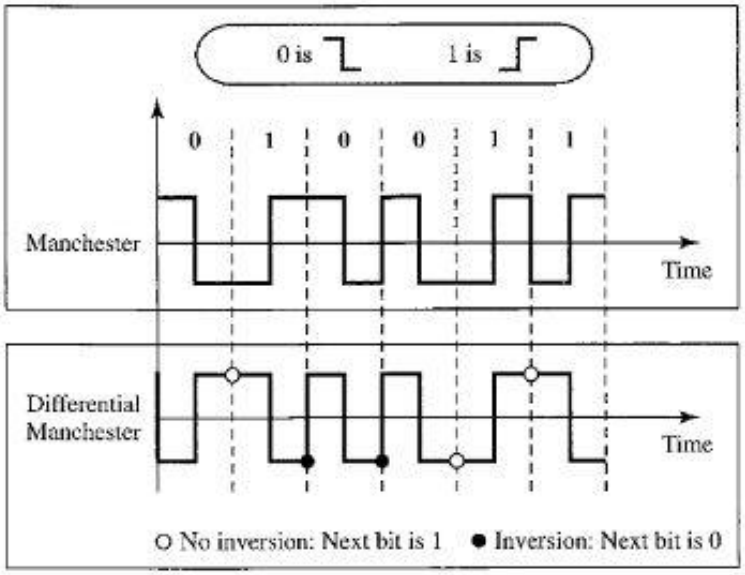


Figure: Polar biphase: Manchester and differential Manchester schemes

Q 17. What are transmission media? Explain Twisted-Pair Cable in brief. **(AKTU 2018-19)**

Solution:

A transmission medium can be broadly defined as anything that can carry information from a source to a destination. The transmission medium is usually free space, metallic cable, or fiber-optic cable.

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together. One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise)and crosstalk may affect both wires and create unwanted signals.

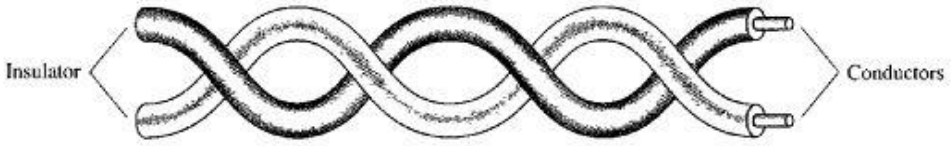


Figure: Twisted-pair cable

If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e.g., one is closer and the other is farther). This results in a difference at the receiver. By twisting the pairs, a balance is maintained. It is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

Unshielded Versus Shielded Twisted-Pair Cable: The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

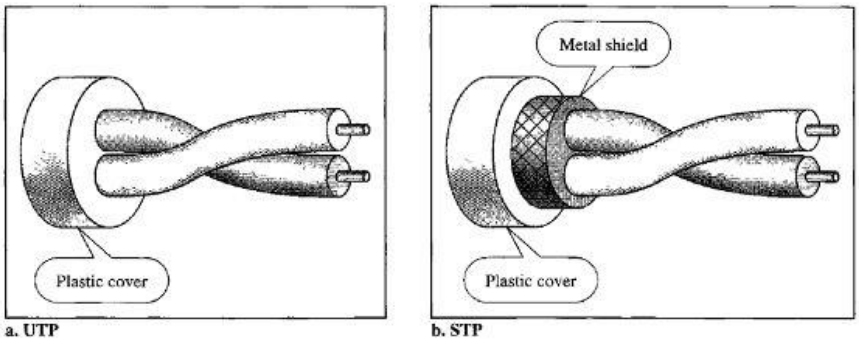


Figure: UTP and STP cables

Categories: The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories, as shown in below Table 1.1. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest.

Table 1.1: Categories of unshielded twisted-pair cables

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Connectors: The most common UTP connector is RJ45 (RJ stands for registered jack). The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.

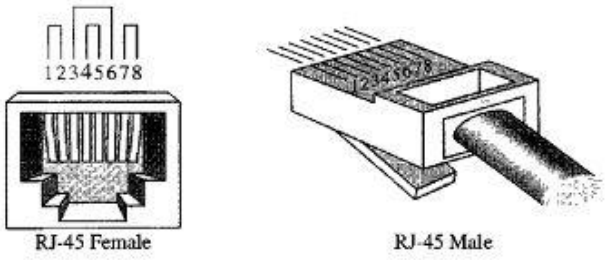


Figure: UTP connector

Performance: One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies.

Application: Twisted-pair cables are used in telephone lines to provide voice and data channels. The local loop-the line that connects subscribers to the central telephone office commonly consists of unshielded twisted-pair cables. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables. Local-area networks, such as l0Base-T and l00Base-T, also use twisted-pair cables.

Q 18. What is switching? Explain circuit switched network in brief. **(AKTU 2021-22)**

Solution:

A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example) and others are used only for routing.

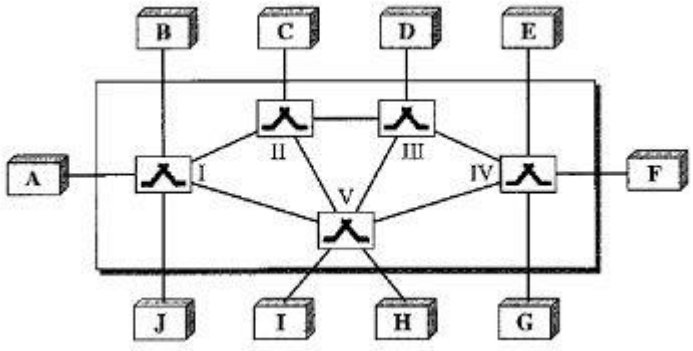


Figure: Switched network

The end systems (communicating devices) are labeled A, E, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

Three methods of switching: circuit switching, packet switching, and message switching. The first two are commonly used today. The third has been phased out in general communications but still has networking applications.

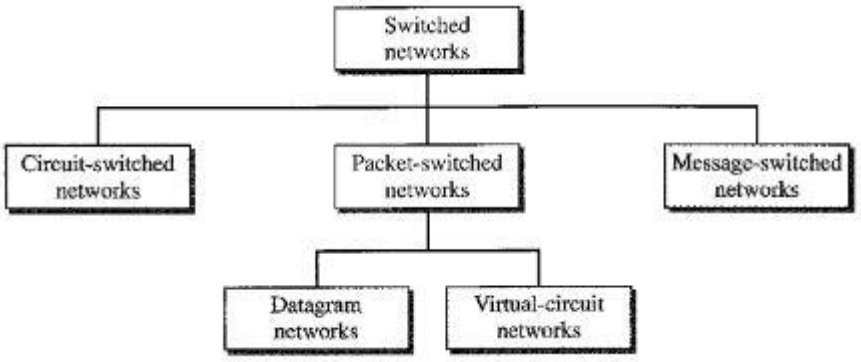


Figure: Taxonomy of switched networks

i) CIRCUIT-SWITCHED NETWORKS:

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. Each link is normally divided into n channels by using FDM or TDM.

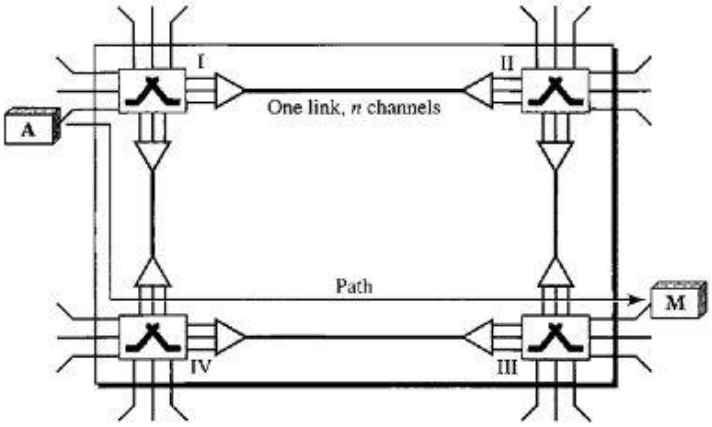


Figure: A circuit-switched network

The end systems, such as computers or telephones, are directly connected to a switch. When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels)is established, data transfer can take place. After all data have been transferred, the circuits are tear down.

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication.
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station.
- There is no addressing involved during data transfer.

In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase.

Three Phases: The actual communication in a circuit-switched network requires three phases: connection setup (request and acknowledgement), data transfer, and connection teardown.

Efficiency: Resources are allocated during the entire duration of the connection. These resources are

unavailable to other connections. In a telephone network, people normally terminate the communication when they have finished their conversation.

Delay: A circuit-switched network normally has low efficiency; the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection.

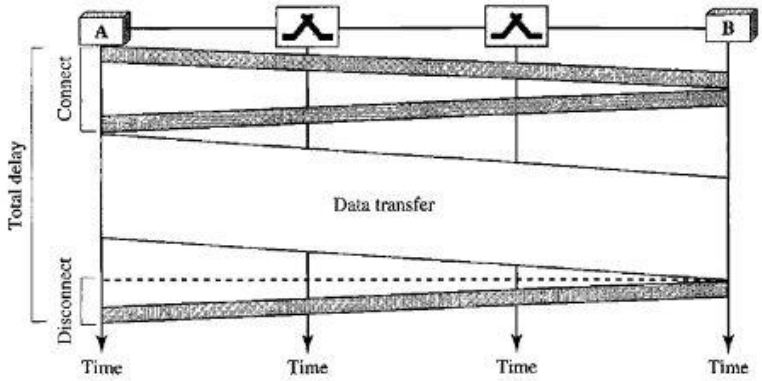


Figure: Delay in a circuit-switched network

Circuit switching today can use either of two technologies: the space-division switch or the time-division switch.

Space-Division Switch: In space-division switching, the paths in the circuit are separated from one another spatially. This technology was originally designed for use in analog networks but is used currently in both analog and digital networks. It is of two types: crossbar switch or matrix switch and multi-stage switch.

a) Crossbar Switch: A crossbar switch connects n inputs to m outputs in a grid, using electronic microswitches (transistors) at each crosspoint. The major limitation of this design is the number of crosspoints required. To connect n inputs tom outputs using a crossbar switch requires n x m crosspoints.

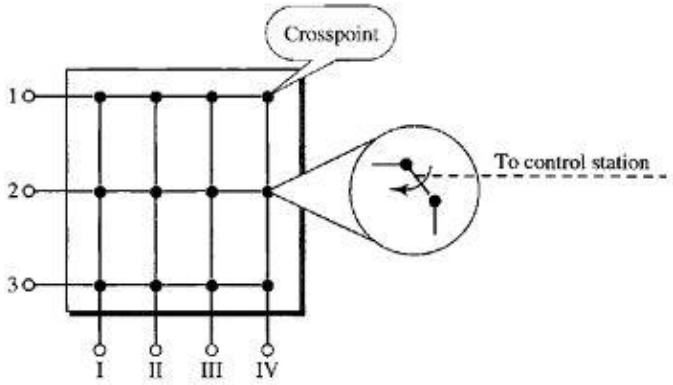


Figure: Crossbar switch with three inputs and four outputs

b) Multistage Switch: The solution to the limitations of the crossbar switch is the multistage switch, which combines crossbar switches in several (normally three) stages. The multistage switch has one drawback-blocking during periods of heavy traffic.

The advantage of space-division switching is that it is instantaneous. Its disadvantage is the number of crosspoints required to make space-division switching acceptable in terms of blocking.

Time-Division Switch: Time-division switching uses time-division multiplexing (TDM) inside a switch. The most popular technology is called the time-slot interchange (TSI).The advantage of time-division switching is that it needs no crosspoints. Its disadvantage, in the case of TSI, is that processing

each connection creates delays. Each timeslot must be stored by the RAM, then retrieved and passed on.

Virtual-circuit network:

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

- As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
- Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
- As in a datagram network, data are packetized and each packet carries an address in the header.
- As in a circuit-switched network, all packets follow the same path established during the connection.
- A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

Three Phases: As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

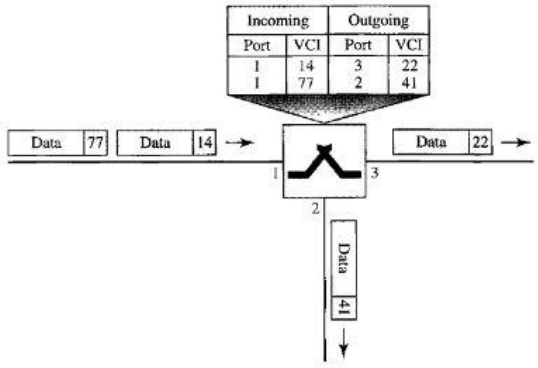


Figure: Switch and tables in a virtual-circuit network

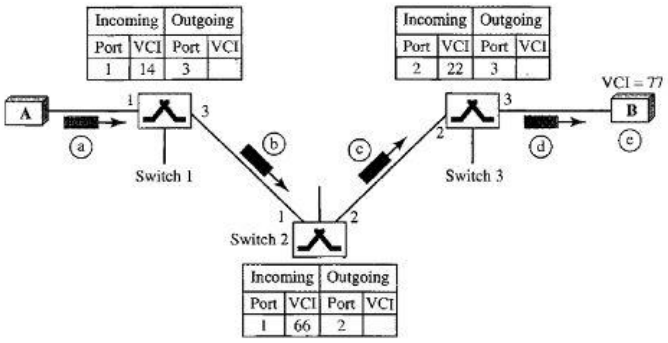


Figure: Setup request in a virtual-circuit network

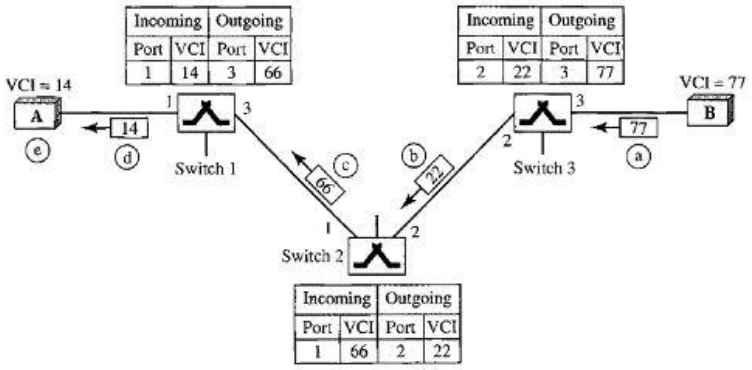


Figure: Setup acknowledgment in a virtual-circuit network

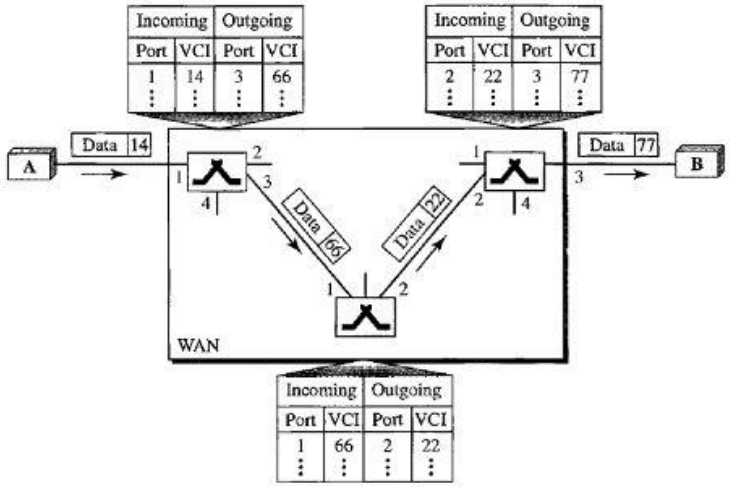


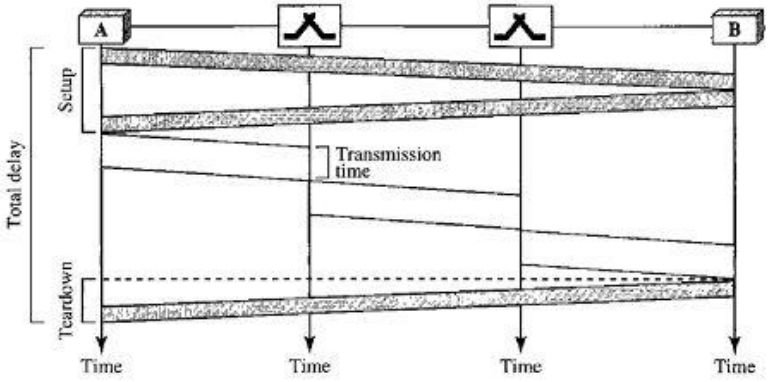
Figure: Source-to-destination data transfer in a virtual-circuit network

Teardown phase

In this, source A, after sending all frames to B, sends a special frame called a teardown request. Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Delay in Virtual-Circuit Networks: In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets.

Total delay = 3T + 3τ+ setup delay + teardown delay



Q 19. What are the design issues of network architecture? **(AKTU 2018-19)**

Solution:

Some design issues in computer network architecture include:

i) Security

The increasing number of internet-connected devices has made cyber-attacks more common and sophisticated.

ii) calability

The network should be able to accommodate future changes, such as more network traffic, new technologies, or business growth.

iii)Error control

Error control ensures that frames are delivered safely to their destination without being copied.

iv) Malfunctioning hardware

Network issues can be caused by malfunctioning hardware, such as routers, switches, firewalls, and wireless access points.

v) Addressing, packing, routing, and inter-networking

These are key design issues in the network layer.

BUDDHA SERIES

(Unit Wise Solved Question & Answers)

Course – B.Tech. (CSE Allied-AIML/DS)

College – Buddha Institute of Technology

(AKTU CODE-525)

Department: Computer Science & Engineering Allied-AIML/DS

(Accredited by NBA 2024-27)

Subject: Computer Networks

(BCS 603)

Faculty Name: Mr. Shailesh Kumar Patel

Unit - 2

Q 1. Explain Selective Repeat ARQ protocols. What are the advantages of Selective Repeat ARQ over Go-Back-N ARQ protocol? **(AKTU 2022-23)**

Solution:

Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link. In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called Selective Repeat ARQ.

Windows: The Selective Repeat Protocol also uses two windows: a send window and a receive window. However, there are differences between the windows in this protocol and the ones in Go-Back-N. First, the size of the send window is much smaller; it is 2^m-1. The reason for this will be discussed later. Second, the receive window is the same size as the send window.

The send window maximum size can be 2^m-1. For example, if m = 4, the sequence numbers go from 0 to 15, but the size of the window is just 8 (it is 15 in the Go-Back-N Protocol). The smaller window size means less efficiency in filling the pipe.

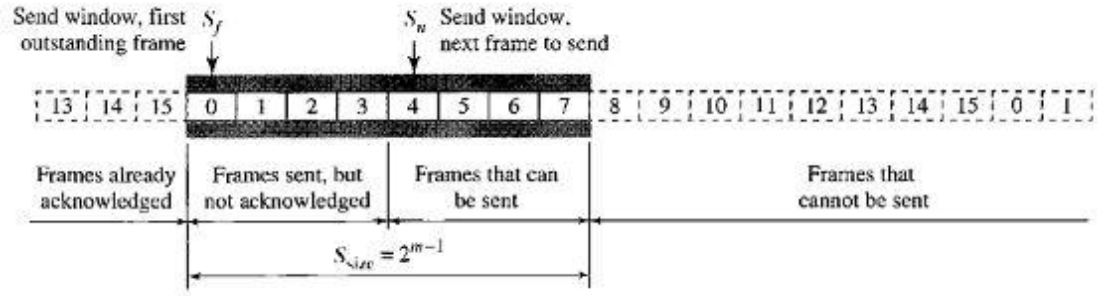


Figure: Send window for Selective Repeat ARQ

The receive window in Selective Repeat is totally different from the one in Go-Back-N. First, the size of the receive window is the same as the size of the send window(2^m-1). The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer. Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered.

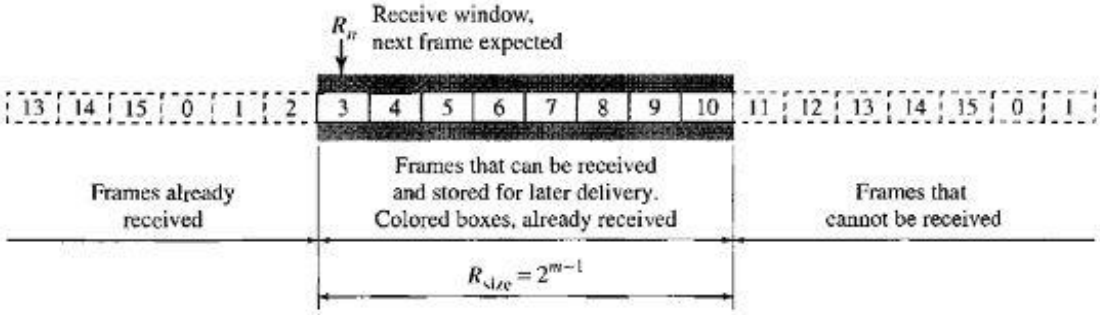


Figure: Receive window for Selective Repeat ARQ

Design The design in this case is to some extent similar to the one we described for the Go- Back-N, but more complicated.

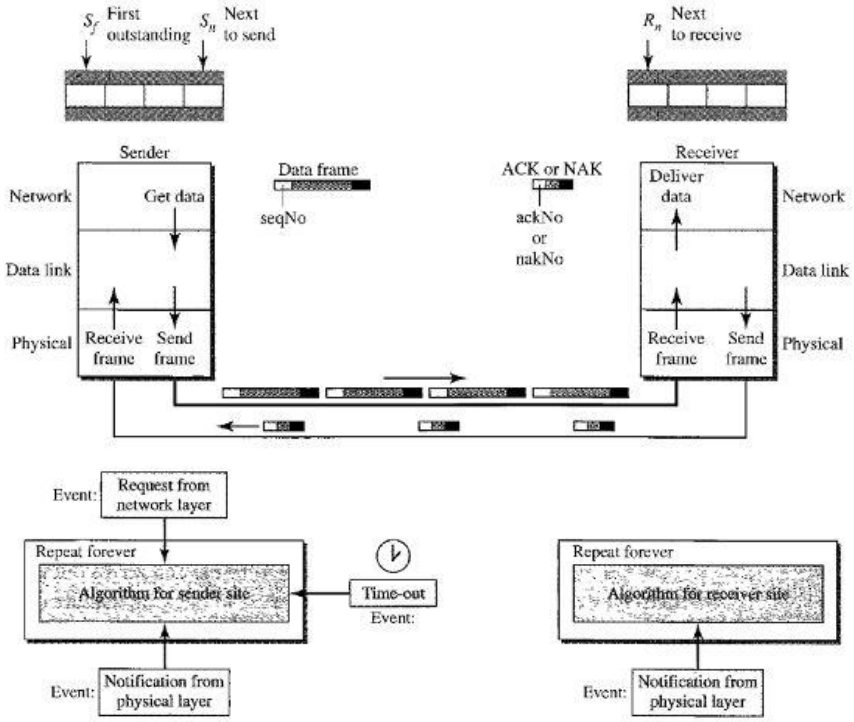


Figure: Design of Selective Repeat ARQ

Window Sizes the size of the sender and receiver windows must be at most one half of 2^m.

If the rate of error is high, then Go-Back-N will consume a lot of bandwidth. Selective Repeat is a better option if you have to be considering bandwidth requirement, as it would resend only the defective or missing packets and not the entire windows.

The basic difference between go-back-n protocol and selective repeat protocol is that the "go-back-n protocol" retransmits all the frames that lie after the frame which is damaged or lost. The "selective repeat protocol" retransmits only that frame which is damaged or lost.

Q 2. What is piggybacking? **(AKTU 2017-18)**

Solution:

In a real-life network, the data link protocols are implemented as bidirectional; data flow in both directions. In these protocols the flow and error control information such as ACKs and NAKs is included in the data frames in a technique called piggybacking.

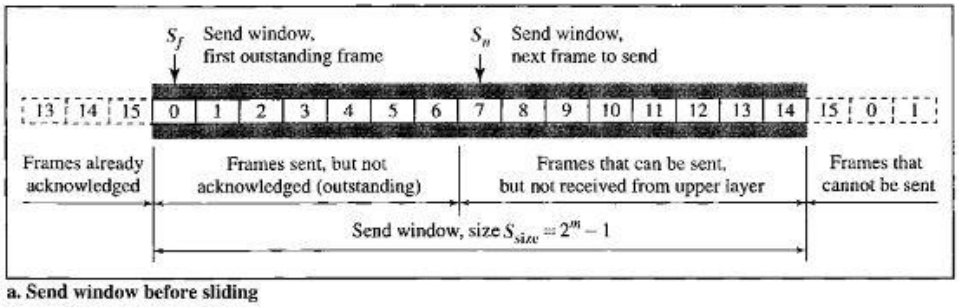
Q 3. Explain Sliding window protocol for Go-Back-N ARQ. How selective repeat ARQ is different from GO-BACK-N. **(AKTU 2022-23)**

Solution:

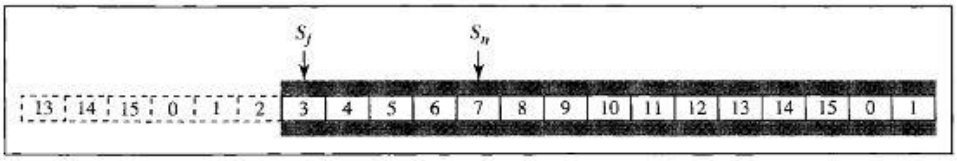
Go-Back-N Automatic Repeat Request: To improve the efficiency of transmission (filling the pipe), multiple frames must be in transition while waiting for acknowledgment. In this protocol we can send several frames before receiving acknowledgments; we keep a copy of these frames until the acknowledgments arrive.

Sequence Numbers Frames from a sending station are numbered sequentially. If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to 2^m- 1. For example, if m is 4, the only sequence numbers are 0 through 15 inclusive.

Sliding Window The sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receiver is called the receive sliding window.
The send window is an imaginary box covering the sequence numbers of the data frames which can be in transit. In each window position, some of these sequence numbers define the frames that have been sent; others define those that can be sent. The maximum size of the window is $2^m - 1$.
Figure shows a sliding window of size 15 (m = 4). The window at any time divides the possible sequence numbers into four regions. The first region, from the far left to the left wall of the window, defines the sequence numbers belonging to frames that are already acknowledged.
The sender does not worry about these frames and keeps no copies of them.

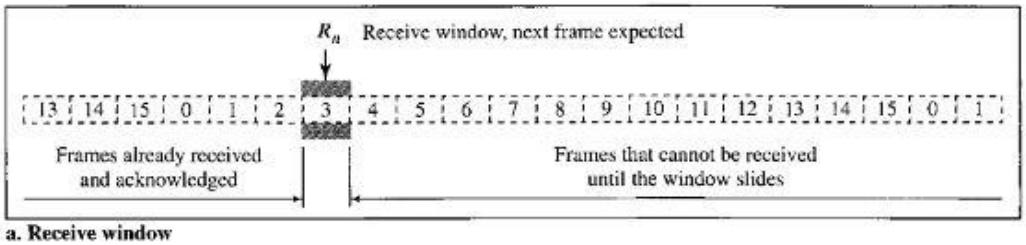


a. Send window before sliding

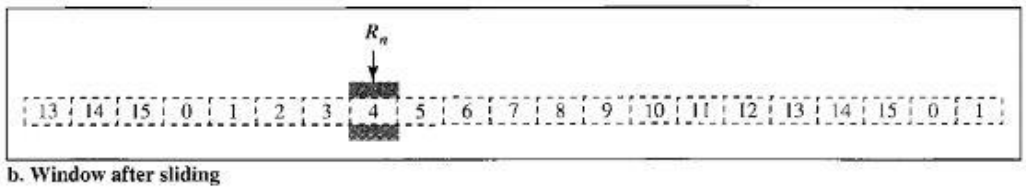


b. Send window after sliding

The second region, colored in Figure (a), defines the range of sequence numbers belonging to the frames that are sent and have an unknown status. The sender needs to wait to find out if these frames have been received or were lost. We call these outstanding frames. The third range, white in the figure, defines the range of sequence numbers for frames that can be sent; however, the corresponding data packets have not yet been received from the network layer. Finally, the fourth region defines sequence numbers that cannot be used until the window slides.
The send window is an abstract concept defining an imaginarybox of size 2^m -1 with three variables: S_f,S_n, and S_{size}.
We call these variables S_f(send window, the first outstanding frame), S_n (sendwindow, the next frame to be sent), and S_{size} (send window, size). The variable S_f definesthe sequence number of the first (oldest) outstanding frame. The variable S_n holds thesequence number that will be assigned to the next frame to be sent. Finally, the variableS_{size} defines the size of the window, which is fixed in our protocol.
Figure (b) shows how a send window can slide one or more slots to the right when an acknowledgment arrives from the other end. In this figure, frames 0, 1, and 2 are acknowledged,so the window has slid to the right three slots. Note that the value of S_f is 3 because frame 3is now the first outstanding frame.
The receive window makes sure that the correct data frames are received and thatthe correct acknowledgments are sent. The size of the receive window is always 1. Thereceiver is always looking for the arrival of a specific frame. Any frame arriving out oforder is discarded and needs to be resent. Following figure shows the receive window.



a. Receive window



b. Window after sliding

We need only one variable R_n (receive window, next frame expected) todefine this abstraction. The sequence numbers to the left of the window belong to theframes already received and acknowledged; the sequence numbers to the right of thiswindow define the frames that cannot be received. Any received frame with a sequencenumber in these two regions is discarded. Only a frame with a sequence number matchingthe value of R_n is accepted and acknowledged.The receive window also slides, but only one slot at a time. When a correct frameis received (and a frame is received only one at a time), the window slides.

Timers There can be a timer for each frame that is sent; in our protocol we use only one. The reason is that the timer for the first outstanding frame always expires first; we send all outstanding frames when this timer expires.

Acknowledgment The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting.

Resending a Frame When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4,5, and 6 again. That is why the protocol is called Go-Back-N ARQ.

Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link. In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. **This mechanism is called Selective Repeat ARQ. It is more efficient for noisy links**, but the processing at the receiver is more complex.

Q 4. Given the dataword 1010011010 and the divisor 10111. **(AKTU 2021-22, 2022-23)**

i) Show the generation of the codeword at the sender site (using binary division).

ii) Show the checking of the codeword at the receiver site (assume no error).

Solution:

Dataword = 1010011010

Divisor = 10111

i) Generation of the codeword at the sender site

dataword is augmented by adding 4 zeros

```
          10011010111
      ____________________
10111 | 10100110100000
        10111
        -----
        00111
        00000
        -----
        01111
        00000
        -----
        11110
        10111
        -----
        10011
        10111
        -----
        01000
        00000
        -----
        10000
        10111
        -----
        01110
        00000
        -----
        11100
        10111
        -----
        10110
        10111
        -----
        00001   <- Remainder
```

codeword = dataword & Remainder

= 10100110100001

checking of the codeword at the receiver site

```
          10011010111
      ____________________
10111 | 10100110100001
        10111
        -----
        00111
        00000
        -----
        01111
        00000
        -----
        11110
        10111
        -----
        10011
        10111
        -----
        01000
        00000
        -----
        10000
        10111
        -----
        01110
        00000
        -----
        11100
        10111
        -----
        10111
        10111
        -----
        00000   <- Syndrome
```

The remainder of the division is the syndrome. If the syndrome is all 0s, there is no error. The dataword is separated from the received codeword and accepted.

The received data word = 1010011010

Q 5.

If the 7-bit Hamming codeword received by a receiver is 1110101. Assuming the even parity, state whether the received codeword is correct or incorrect. If incorrect, locate the position of error. What will be the correct code? **(AKTU 2022-23)**

Solution:

D7	D6	D5	P4	D3	P2	P1
1	0	1	1	0	1	1

{ 1011→ to convert in 7 bit, add parity bits…….location of parity bits should be 2^n, Where n=0, 1, 2, 3, ……}

Selection of parity bits:

i) Selection of P1-
P1 is adjusted 0 or 1, to set even parity over bits 1, 3, 5, 7

ii) Selection of P2-
P2 is adjusted 0 or 1, to set even parity over bits 2, 3, 6, 7

iii) Selection of P3-
P3 is adjusted 0 or 1, to set even parity over bits 4, 5, 6, 7

For P1:
P1, D3, D5, D7
1, 0, 1, 1
This show odd parity means error exists.

For P2:
P2, D3, D6, D7
1, 0, 0, 1
This show even parity means no error.

For P4:
P4, D5, D6, D7
1, 1, 0, 1
This show odd parity means error exists.

Therefore, position of error:
P1, P2, P4

P4	P2	P1
1	0	1

5^{th} position is having error i.e. D5
Therefore, correct message is:

1	0	0	1	0	1	1

Q 6. Explain the working of pure ALOHA and slotted ALOHA protocols. How slotted ALOHA improve the performance of pure ALOHA? **(AKTU 2018-19)**

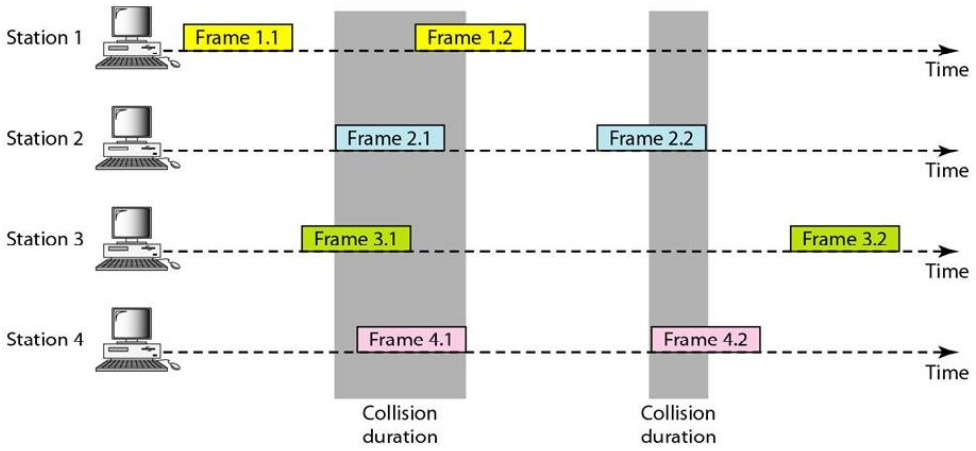
Solution:

ALOHA, the earliest random-access method, was developed at the University of Hawaii in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any shared medium. It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

- **Pure ALOHA**

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one

channel to share, there is the possibility of collision between frames from different stations. Fig shows an example of frame collisions in pure ALOHA.



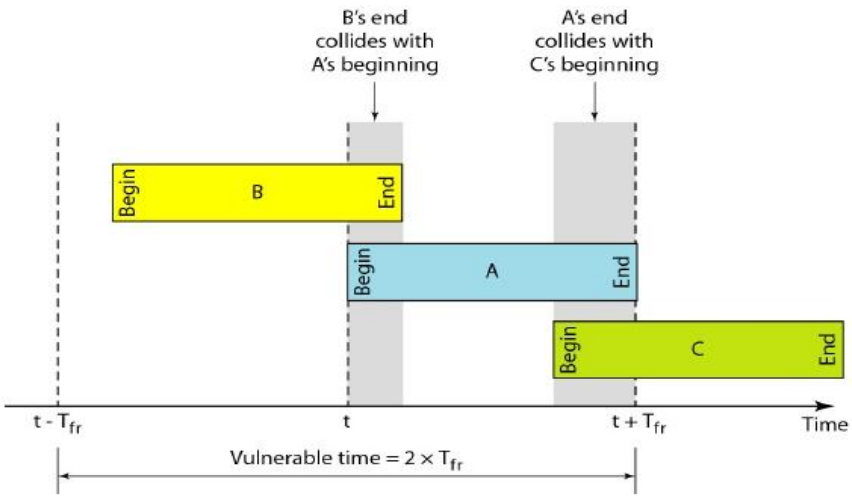
There are four stations (unrealistic assumption) that contend with one another for access to the shared channel. The figure shows that each station sends two frames; there are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Fig.3 shows that only two frames survive: frame 1.1 from station 1 and frame 3.2 from station 3. We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed. It is obvious that we need to resend the frames that have been destroyed during transmission. The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame. A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time TB.

Vulnerable time Let us find the length of time, the vulnerable time, in which there is a possibility of collision. We assume that the stations send fixed-length frames with each frame taking Tfr S to send. Fig.4 shows the vulnerable time for station A.

Station A sends a frame at time t. Now imagine station B has already sent a frame between t - Tfr and t. This leads to a collision between the frames from station A and station B. The end of B's frame collides with the beginning of A's frame. On the other hand, suppose that station C sends a frame between t and t + Tfr. Here, there is a collision between frames from station A and station C. The beginning of C's frame collides with the end of A's frame.

Looking at following Fig., we see that the vulnerable time, during which a collision may occur in pure ALOHA, is 2 times the frame transmission time.

Pure ALOHA vulnerable time = 2 x Tfr



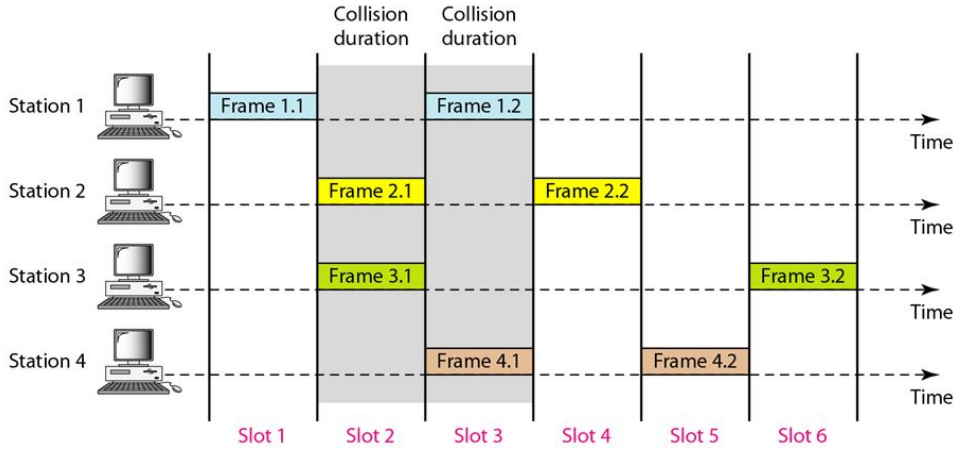
Throughput Let us call G the average number of frames generated by the system during one frame transmission time. Then it can be proved that the average number of successful transmissions for pure ALOHA is S = G x e-2G. The maximum throughput Smax is 0.184, for G = ½ . In other words, if one-half a frame is generated during one frame transmission time (in other words, one frame during two frame transmission times), then 18.4 percent of these frames reach their destination successfully. This is an expected result because the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.

The throughput for pure ALOHA is S =G x e-2G.

The maximum throughput Smax =0.184 when G =(1/2).

- **Slotted ALOHA**

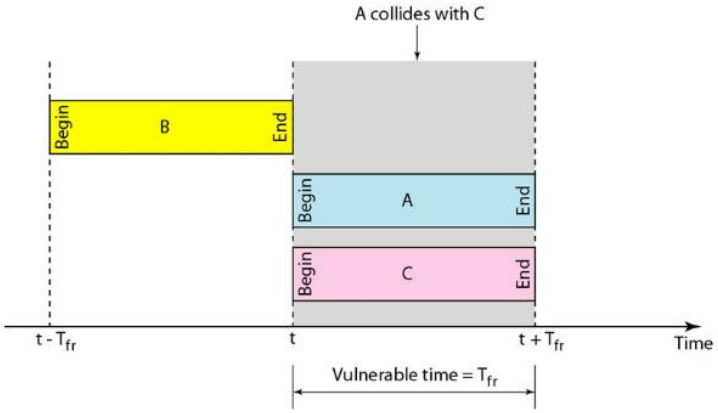
Pure ALOHA has a vulnerable time of 2 x Tfr. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of Tfr s and force the station to send only at the beginning of the time slot. Fig. shows an example of frame collisions in slotted ALOHA.



Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame. Of course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to Tfr following Fig. shows

the situation. Fig. shows that the vulnerable time for slotted ALOHA is one-half that of pure ALOHA.

Slotted ALOHA vulnerable time = Tfr



Throughput It can be proved that the average number of successful transmissions for slotted ALOHA is S = G x e-G. The maximum throughput Smax is 0.368, when G = 1. In other words, if a frame is generated during one frame transmission time, then 36.8 percent of these frames reach their destination successfully. This result can be expected because the vulnerable time is equal to the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other station generates a frame during this time), the frame will reach its destination successfully.

The throughput for slotted ALOHA is S =: G x e-G.

The maximum throughput Smax == 0.368 when G =1.

Slotted ALOHA improves the performance of pure ALOHA by reducing the chances of collisions and increasing network efficiency.

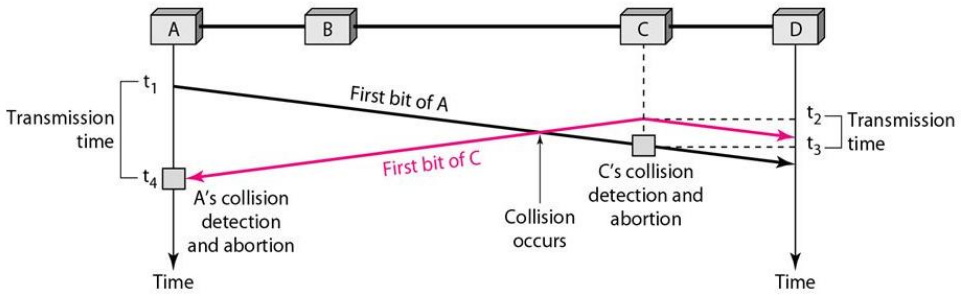
Q 7. How CSMA/CD protocol is different from CSMA/CA protocol? Explain.

(AKTU2021-22, 2022-23)

Solution:

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again. To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision. Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide. In the following Fig., stations A and C are involved in the collision.



At time t 1, station A has executed its persistence procedure and starts sending the bits of its frame. At

time t2, station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time t2 Station C detects a collision at time t3 when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time t4 when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration t4 - tl; C transmits for the duration t3 - t2. Later we show that, for the protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time t4, the transmission of A:s frame, though incomplete, is aborted; at time t3, the transmission of B's frame, though incomplete, is aborted.

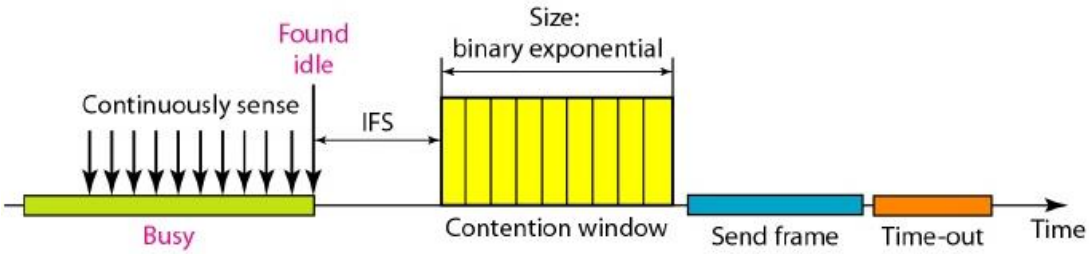
Minimum Frame Size

For CSMA/CD to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time Tfr must be at least two times the maximum propagation time Tp. To understand the reason, let us think about the worst-case scenario. If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time Tp to reach the second, and the effect of the collision takes another time Tp to reach the first. So the requirement is that the first station must still be transmitting after 2Tp .

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

The basic idea behind CSMA/CD is that a station needs to be able to receive while transmitting to detect a collision. When there is no collision, the station receives one signal: its own signal. When there is a collision, the station receives two signals: its own signal and the signal transmitted by a second station. To distinguish between these two cases, the received signals in these two cases must be significantly different. In other words, the signal from the second station needs to add a significant amount of energy to the one created by the first station.

In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles. However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection. We need to avoid collisions on wireless networks because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMA/CA) was invented for this network. Collisions are avoided through the use of CSMA/CA's three strategies: the inter-frame space, the contention window, and acknowledgments, as shown in Fig.



- Interframe Space (IFS)

First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS. Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this station. The

IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time (described next). The IFS variable can also be used to prioritize stations or frame types. For example, a station that is assigned a shorter IFS has a higher priority.

In CSMA/CA, the IFS can also be used to define the priority of a station or a frame.

- Contention Window

The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station. One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

In CSMA/CA, if the station finds the channel busy, it does not restart the timer of the contention window; it stops the timer and restarts it when the channel becomes idle.

- Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

Procedure Note that the channel needs to be sensed before and after the IFS. The channel also needs to be sensed during the contention time. For each time slot of the contention window, the channel is sensed. If it is found idle, the timer continues; if the channel is found busy, the timer is stopped and continues after the timer becomes idle again.

Q 8. A slotted ALOHA network transmits 200-bit frames using a shared channel with a 200-kbps bandwidth. Find the throughput if the system (all stations together) produces

a. 1000 frames per second
b. 500 frames per second
c. 250 frames per second **(AKTU 2018-19)**

Solution:

This situation is similar to the previous exercise except that the network is using slotted ALOHA instead of pure ALOHA. The frame transmission time is 200/200 kbps or 1 ms.

a. In this case G is 1. So S =G x e-G or S =0.368 (36.8 percent). This means that the throughput is 1000 x 0.0368 =368 frames. Only 368 out of 1000 frames will probably survive. Note that this is the maximum throughput case, percentagewise.

b. Here G is ½ . In this case S =G x e-G or S =0.303 (30.3 percent). This means that the throughput is 500 x 0.0303 =151. Only 151 frames out of 500 will probably survive.

c. Now G is ¼ . In this case S =G x e-G or S =0.195 (19.5 percent). This means that the throughput is 250 x 0.195 = 49. Only 49 frames out of 250 will probably survive.

Q 9. State the requirements of CRC. **(AKTU 2013-14)**

Solution:

Reliability: CRC ensures accurate data delivery by identifying transmission errors.

Efficiency: The method is computationally efficient, suitable for high-speed data transmission.

Versatility: CRC is used in various communication protocols, including Ethernet, USB, and Bluetooth.

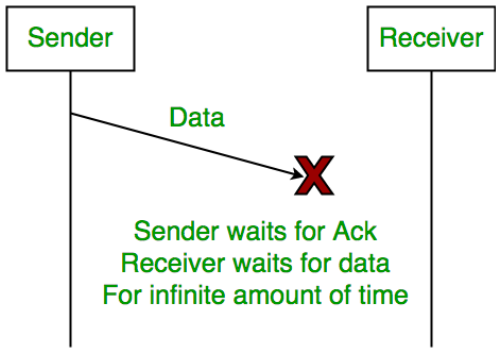
Q 10. List out discuss the disadvantages in stop and wait protocol. **(AKTU 2021-22)**

Solution:

The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

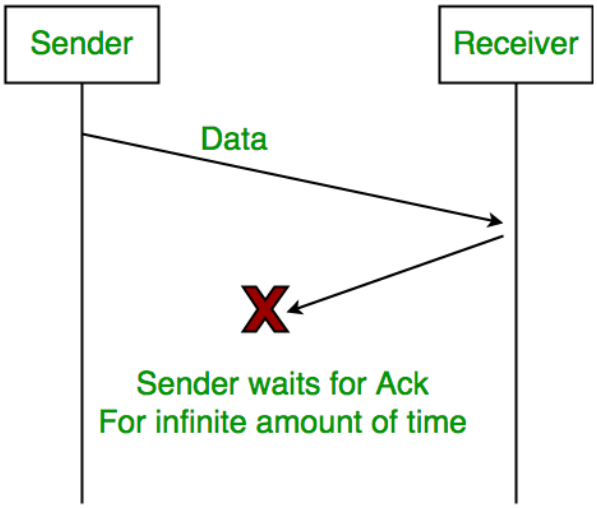
1. Lost Data

Assume the sender transmits the data packet and it is lost. The receiver has been waiting for the data for a long time. Because the data is not received by the receiver, it does not transmit an acknowledgment. The sender does not receive an acknowledgment, it will not send the next packet. This problem is caused by a loss of data.



2. Lost Acknowledgement

Assume the sender sends the data, which is also received by the receiver. The receiver sends an acknowledgment after receiving the packet. In this situation, the acknowledgment is lost in the network. The sender does not send the next data packet because it does not receive acknowledgement, under the stop and wait protocol, the next packet cannot be transmitted until the preceding packet's acknowledgment is received.



3. Delayed Acknowledgement/Data

Assume the sender sends the data, which is also received by the receiver. The receiver then transmits the acknowledgment, which is received after the sender's timeout period. After a timeout on the sender side, a long-delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

BUDDHA SERIES

(Unit Wise Solved Question & Answers)

Course – B.Tech. (CSE Allied-AIML/DS)

College – Buddha Institute of Technology

(AKTU CODE-525)

Department: Computer Science & Engineering Allied-AIML/DS

(Accredited by NBA 2024-27)

Subject: Computer Networks

(BCS 603)

Faculty Name: Mr. Shailesh Kumar Patel

Unit - 3

Q1. Explain ICMP BGP protocol and its application in real-world scenarios. **(AKTU 2022-23)**

Solution:

"ICMP BGP" refers to the combination of two network protocols: ICMP (Internet Control Message Protocol), which is used for error reporting and network diagnostics, and BGP (Border Gateway Protocol), which is responsible for routing information exchange between different autonomous systems (AS) on the internet; essentially, ICMP can be used to troubleshoot issues related to BGP routing by sending diagnostic messages when BGP encounters problems connecting to a network or exchanging routing information.

Key points about ICMP and BGP:

ICMP Function:

ICMP primarily sends error messages back to the source when a packet encounters an issue during transmission, like an unreachable host, time exceeded, or a network issue. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. As different types of errors can exist in the network layer, so ICMP can be used to report these errors and to debug those errors.

BGP Function:

BGP is a path vector routing protocol that allows different autonomous systems to exchange routing information, determining the best path to reach a specific network.

How they work together:

BGP Path Issues:

When a BGP router encounters a problem while attempting to establish a routing path, it can use ICMP messages to notify the sending router about the issue.

Troubleshooting with ICMP:

Network administrators can use ICMP "ping" messages to test connectivity between different network segments and identify potential issues with BGP routing.

Example scenarios:

Unreachable Network:

If a BGP router tries to establish a route to a network that is unreachable, it might send an ICMP "Destination Unreachable" message back to the originating router, indicating the problem.

Route Flap Detection:

If a BGP router detects rapid changes in routing information (route flapping), it can use ICMP messages to notify other routers about the instability.

For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data. A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminals utilities trace route and ping both operate using ICMP.

Q2. Illustrate the difference between IPv4 and IPv6. **(AKTU 2022-23)**

Solution:

Difference between IPv4 and IPv6:

S. No.	IPv4	IPv6
1	IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
2	It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
3	In IPv4 end to end, connection integrity is Unachievable	In IPv6 end-to-end, connection integrity is Achievable
4	It can generate 4.29×10^9 address space	The address space of IPv6 is quite large it can produce 3.4×10^{38} address space
5	The Security feature is dependent on the application	IPSEC is an inbuilt security feature in the IPv6 protocol

6	Address representation of IPv4 is in decimal	Address representation of IPv6 is in hexadecimal
7	Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation is performed only by the sender
8	In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are available and uses the flow label field in the header
9	In IPv4 checksum field is available	In IPv6 checksum field is not available
10	It has a broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
11	In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
12	IPv4 has a header of 20-60 bytes.	IPv6 has a header of 40 bytes fixed
13	IPv4 can be converted to IPv6	Not all IPv6 can be converted to IPv4
14	IPv4 consists of 4 fields which are separated by addresses dot (.)	IPv6 consists of 8 fields, which are separated by a colon (:)
15	IPv4's IP addresses are divided into five different classes. Class A , Class B, Class C, Class D , Class E.	IPv6 does not have any classes of the IP address.
16	IPv4 supports VLSM (Variable Length subnet mask).	IPv6 does not support VLSM.
17	Example of IPv4: 66.94.29.13	Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB

Q3. Write advantages of Next-generation IPV6 over IPV4. **(AKTU 2018-19)**

Solution:

Advantages:

The next-generation IP, or IPv6, has some advantages over IPv4 that can be summarized as follows:

Larger address space An IPv6 address is 128 bits long, compared with the 32-bit address of IPv4, this is a huge (2^{96}) increase in the address space.

Better header format IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

New options IPv6 has new options to allow for additional functionalities.

Allowance for extension IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

Support for resource allocation In IPv6, the type-of-service field has been removed, but a mechanism (called flow label) has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

Support for more security The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Q4. How is the BOOTP different from DHCP? **(AKTU 2018-19)**

Solution:

BOOTP is a network protocol for assigning an IP address to every piece of networking equipment and providing all the major configuration information, such as the default gateway and the subnet mask. It was

previously invented for the diskless workstations that needed to download their operating systems from a network server.

DHCP refers to Dynamic Host Configuration Protocol. This is a network protocol used for automating the process of assigning IP addresses and other network configurations to devices on a network. Devices request and obtain an IP address and configuration information from the DHCP server; hence, in this case, managing the network becomes easy and efficient.

Difference between BOOTP and DHCP:

S. No.	BOOTP	DHCP
1	BOOTP stands for Bootstrap Protocol.	While DHCP stands for Dynamic host configuration protocol.
2	BOOTP does not provide temporary IP addressing.	While DHCP provides temporary IP addressing for only limited amount of time.
3	BOOTP does not support DHCP clients.	While it support BOOTP clients.
4	In BOOTP, manual-configuration takes place.	While in DHCP, auto-configuration takes place.
5	BOOTP does not support mobile machines.	Whereas DHCP supports mobile machines.
6	BOOTP can have errors due to manual-configuration.	Whereas in DHCP errors do not occur mostly due to auto-configuration.

Q5. What is IP Addressing? How it is classified? How subnet addressing is performed? **(AKTU 2021-22)**

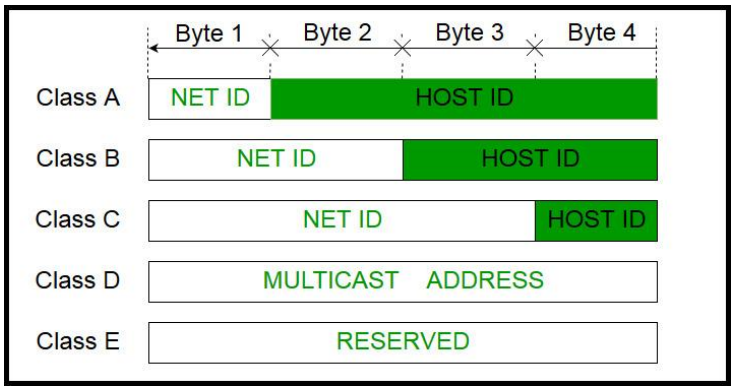
Solution:

An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the internet. An IP address definition is a numeric label assigned to devices that use the internet to communicate.

An IP address, or Internet Protocol address, is a unique string of numbers assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves as an identifier that allows devices to send and receive data over the network, ensuring that this data reaches the correct destination.

The 32-bit IP address is divided into five sub-classes. These are given below:

- Class A
- Class B
- Class C
- Class D
- Class E



A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs.

A subnet is like a smaller group within a large network. It is a way to split a large network into smaller networks so that devices present in one network can transmits data more easily.

How Does Subnetting Work?

The working of subnets starts in such a way that firstly it divides the subnets into smaller subnets. For communicating between subnets, routers are used. Each subnet allows its linked devices to communicate with each other. Subnetting for a network should be done in such a way that it does not affect the network bits.

An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets. The rest of the world still sees the organization as one entity; however, internally there are several subnets. All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets. The organization, however, needs to create small sub-blocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.

As an example, suppose an organization is given the block 17.12.40.0/26, which contains 64 addresses. The organization has three offices and needs to divide the addresses into three sub-blocks of 32, 16, and 16 addresses. We can find the new masks by using the following arguments:

- Suppose the mask for the first subnet is nl, then 2^{32-n1} must be 32, which means that n1 = 27.
- Suppose the mask for the second subnet is n2, then 2^{32-n2}must be 16, which means that n2 = 28.
- Suppose the mask for the third subnet is n3, then 2^{32-n3} must be 16, which means that n3 = 28.

This means that we have the masks 27, 28, 28 with the organization mask being 26. Following figure shows one configuration for the above scenario.

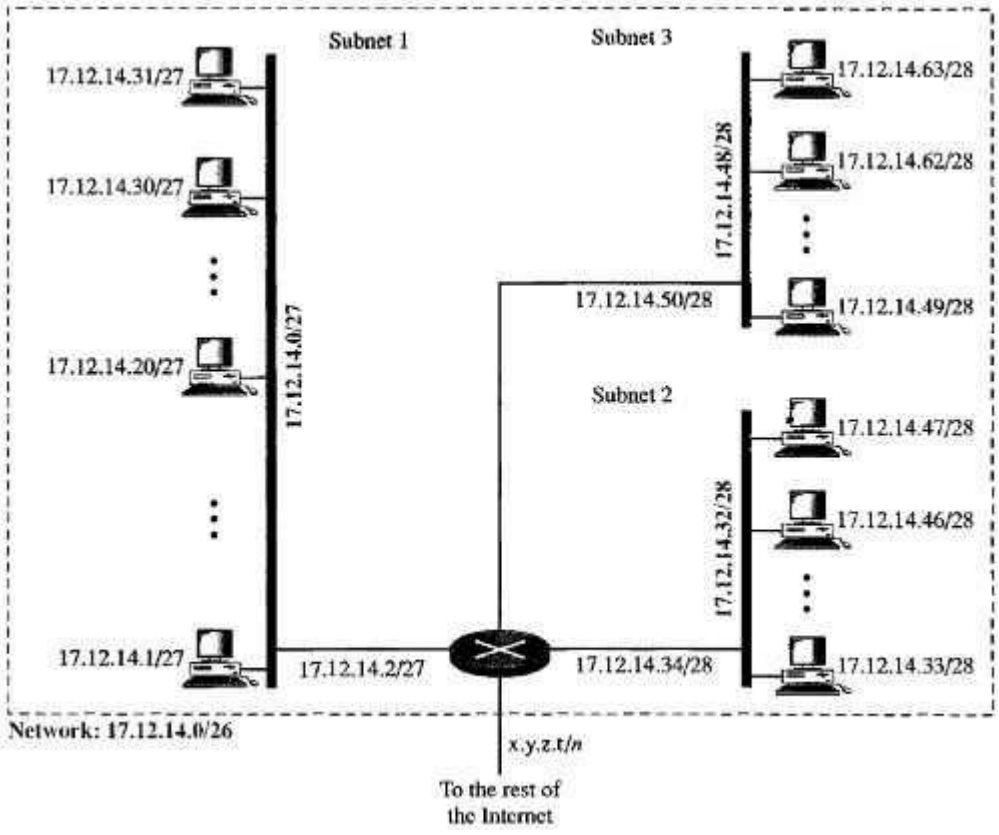


Figure: Configuration and addresses in a sub-netted network

a. In subnet 1, the address 17.12.14.29/27 can give us the subnet address if we use the mask /27 because
Host: 00010001 00001100 00001110 00011101
Mask: /27
Subnet: 00010001 00001100 00001110 00000000 → (17.12.14.0)
b. In subnet 2, the address 17.12.14.45/28 can give us the subnet address if we use the mask /28 because
Host: 00010001 00001100 00001110 00101101
Mask: /28
Subnet: 00010001 00001100 00001110 00100000 → (17.12.14.32)
c. In subnet 3, the address 17.12.14.50/28 can give us the subnet address if we use the mask /28 because
Host: 00010001 00001100 00001110 00110010
Mask: /28
Subnet: 00010001 00001100 00001110 00110000 → (17.12.14.48)

Q6. What is unicast routing? Discuss unicast routing protocols. **(AKTU 2018-19)**

Solution:

Unicast means the transmission from a single sender to a single receiver. It is a point-to-point communication between the sender and receiver. There are various unicast protocols such as TCP, HTTP, etc.

- TCP is the most commonly used unicast protocol. It is a connection-oriented protocol that relies on acknowledgment from the receiver side.
- HTTP stands for Hyper Text Transfer Protocol. It is an object-oriented protocol for communication.

Major Protocols of Unicast Routing

- **Distance Vector Routing:** Distance-Vector routers use a distributed algorithm to compute their routing tables.
- **Link-State Routing**: Link-State routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
- **Path-Vector Routing:** It is a routing protocol that maintains the path that is updated dynamically.

Distance Vector Routing:

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

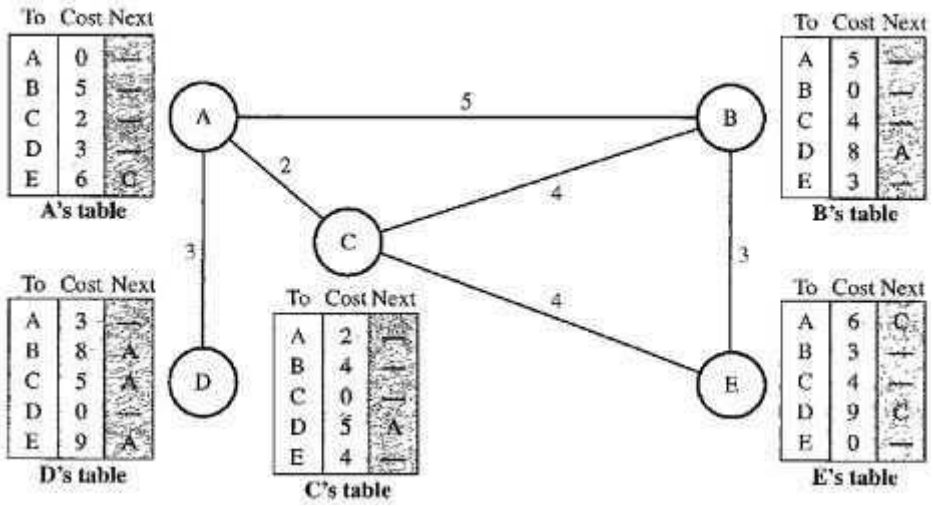


Figure A: Distance vector routing tables

We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities. In Figure, we show a system of five nodes with their corresponding tables. The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

Initialization: The tables in Figure A are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Figure B shows the initial tables for each node.

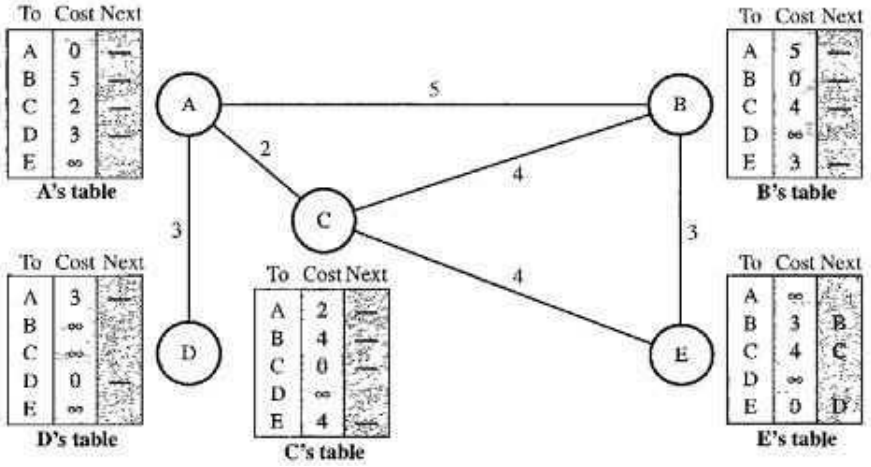


Figure B: Initialization of tables in distance vector routing

Sharing: The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to each node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

There is only one problem. How much of the table must be shared with each neighbor? A node is not aware of a neighbor's table. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbor. When the neighbor receives a table, this column needs

to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbor. In other words, sharing here means sharing only the first two columns.

Updating: When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

- The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is x mi, and the distance between A and C is y mi, then the distance between A and that destination, via C, is x + y mi.
- The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
- The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

1) If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
2) If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist anymore. The new route has a distance of infinity.

Figure C shows how node A updates its routing table after receiving the partial table from node C.

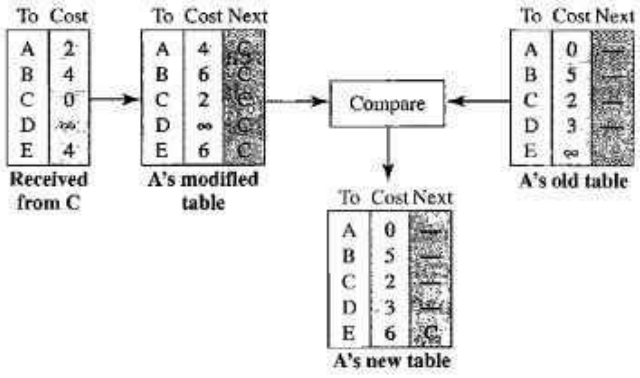


Figure C: Updating in distance vector routing

When to Share: The question now is, when does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.

Periodic Update: A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update: A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

- A node receives a table from a neighbor, resulting in changes in its own table after updating.
- A node detects some failure in the neighboring links which results in a distance change to infinity.

Q7. Describe the problem of count to infinity associated with distance vector routing technique.

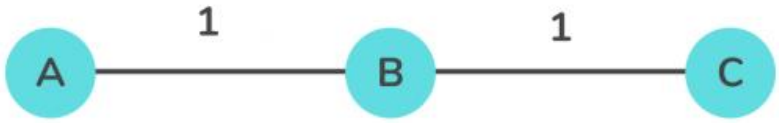
(AKTU 2016-17)

Solution:

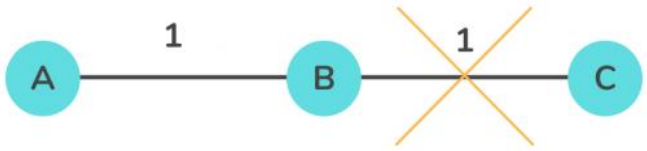
A Distance Vector Routing (DVR) requires that a router informs its neighbors of topology changes periodically. This algorithm is also well known in the Competitive Programming fraternity as the Bellman-Ford algorithm. The Distance Vector Routing (DVR) protocols have a major issue of Routing Loops because the Bellman-Ford algorithm cannot prevent loops. The Count to Infinity problem arises from the routing loop in this Distance Vector Routing (DVR) network. Such Routing Loops usually occurs when 2 routers send an update together at the same time or when an interface goes down.

The Count to Infinity Problem

The crux of the Count to Infinity problem is that if node A tells node B that it has a path somewhere, there is no way for node B to know if the path has node B as a part of it.



Consider the above diagram, for this setup, the Bellman-Ford algorithm will work such that for each router, they will have entries for each other. Router A will infer that it can reach B at a cost of 2 units, and B will infer that it can reach C at a cost of 1 unit.



Consider the case in the above diagram, where the connection between B and C gets disconnected. In this case, B will know that it cannot get to C at a cost of 1 anymore and update its table accordingly. However, it can be possible that A sends some information to B that it is possible to reach C from A at a cost of 2. Then, since B can reach A at a cost of 1, B will erroneously update its table that it can reach C via A at a cost of 1 + 2 = 3 units. A will then receive updates from B and update its costs to 4, and so on. Thus, the process enters into a loop of bad feedback and the cost shoots towards infinity. This entire situation is called the Count to Infinity problem.

Q8. What are different routing algorithms? Write the implementation of shortest path routing.

(AKTU 2002-3)

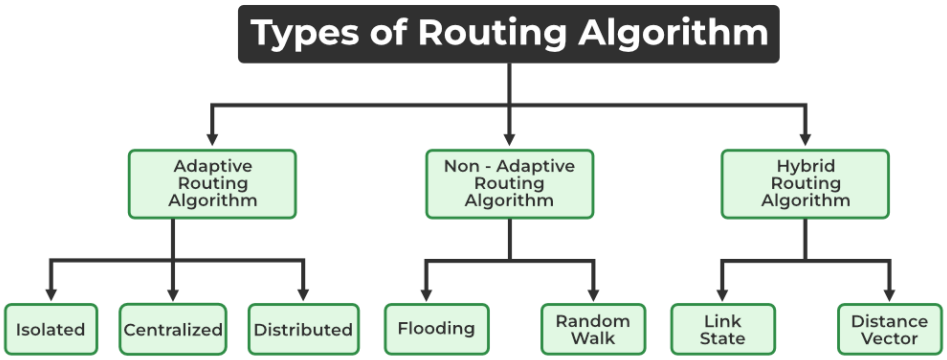
Solution:

Routing is the process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes that data packets follow. Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

Classification of Routing Algorithms

The routing algorithms can be classified as follows:

- Adaptive Algorithms
- Non-Adaptive Algorithms
- Hybrid Algorithms



In between sending and receiving data packets from the sender to the receiver, it will go through many routers and subnets. So as a part of increasing the efficiency in routing the data packets and decreasing the traffic, we must find the shortest path.

It refers to the algorithms that help to find the shortest path between a sender and receiver for routing the data packets through the network in terms of shortest distance, minimum cost, and minimum time.

- It is mainly for building a graph or subnet containing routers as nodes and edges as communication lines connecting the nodes.
- Hop count is one of the parameters that is used to measure the distance.
- Hop count: It is the number that indicates how many routers are covered. If the hop count is 6, there are 6 routers/nodes and the edges connecting them.
- Another metric is a geographic distance like kilometers.
- We can find the label on the arc as the function of bandwidth, average traffic, distance, communication cost, measured delay, mean queue length, etc.

Common Shortest Path Algorithms

- Dijkstra's Algorithm
- Bellman Ford's Algorithm
- Floyd Warshall's Algorithm

Dijkstra's Algorithm

The Dijkstra's Algorithm is a greedy algorithm that is used to find the minimum distance between a node and all other nodes in a given graph. Here we can consider node as a router and graph as a network. It uses weight of edge .ie, distance between the nodes to find a minimum distance route.

Algorithm:

1: Mark the source node current distance as 0 and all others as infinity.

2: Set the node with the smallest current distance among the non-visited nodes as the current node.

3: For each neighbor, N, of the current node:

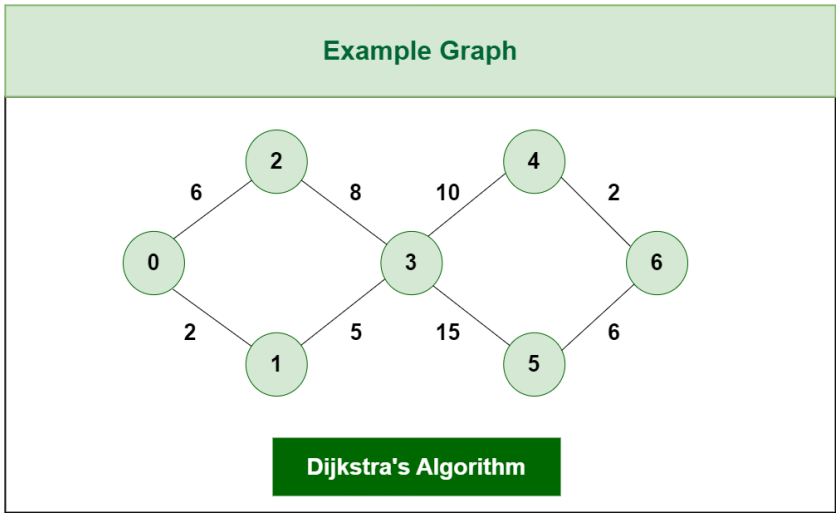
- Calculate the potential new distance by adding the current distance of the current node with the weight of the edge connecting the current node to N.
- If the potential new distance is smaller than the current distance of node N, update N's current distance with the new distance.

4: Make the current node as visited node.

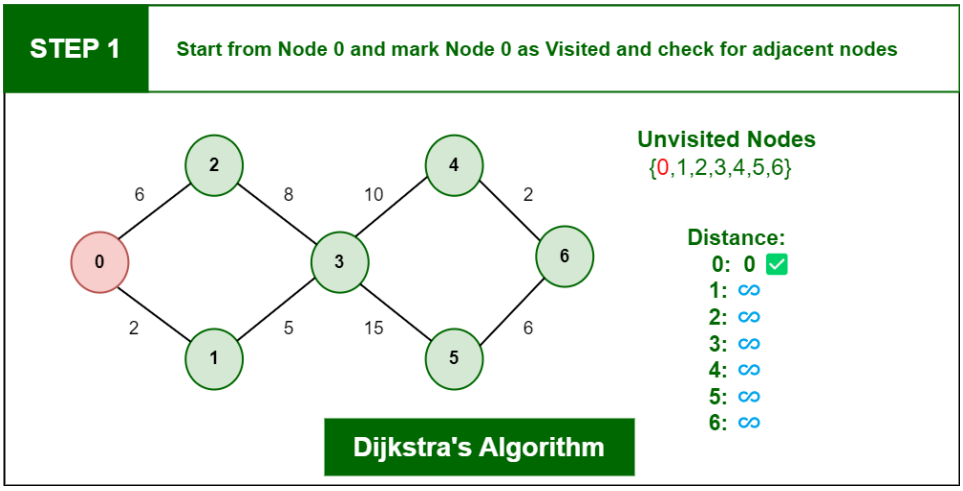
5: If we find any unvisited node, go to step 2 to find the next node which has the smallest current distance and continue this process.

Example:

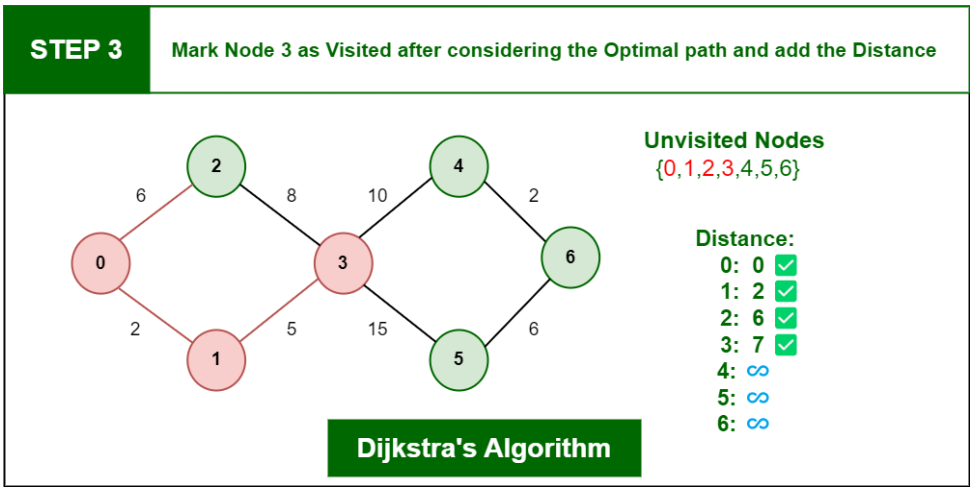
Consider the graph G:



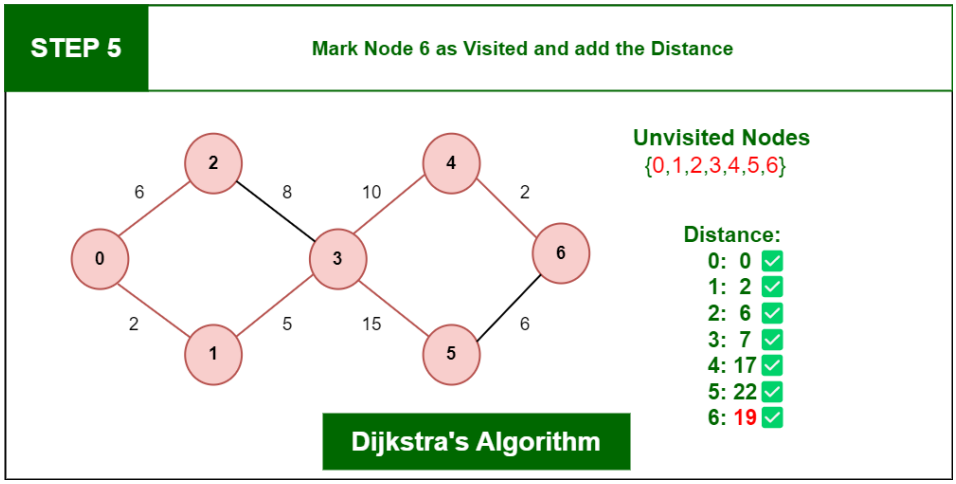
Now, we will start normalising graph one by one starting from node 0.



Nearest neighbour of 0 are 2 and 1 so we will normalize them first.



Similarly we will normalize other node considering it should not form a cycle and will keep track in visited nodes.



Q9. Discuss about the IP range of class A, B, C, and D. **(AKTU 2021-22)**

Solution:

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Q10. Explain distance vector routing with working example in detail. **(AKTU 2021-22)**

Solution:

Distance Vector Routing:

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

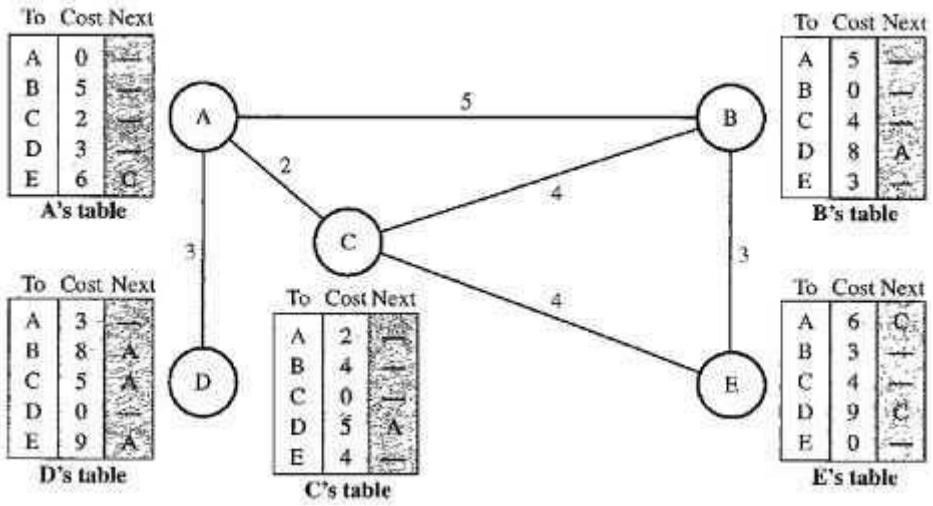


Figure A: Distance vector routing tables

We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities. In Figure, we show a system of five nodes with their corresponding tables. The table for node A shows how we can reach any node from this node. For example, our least cost to reach node E is 6. The route passes through C.

Initialization: The tables in Figure A are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Figure B shows the initial tables for each node.

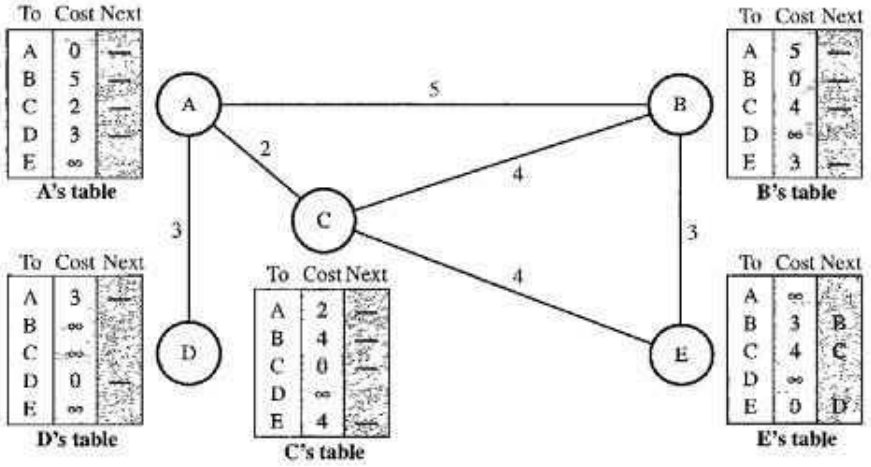


Figure B: Initialization of tables in distance vector routing

Sharing: The whole idea of distance vector routing is the sharing of information between neighbors. Although node A does not know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E. On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to each node D. In other words, nodes A and C, as immediate neighbors, can improve their routing tables if they help each other.

There is only one problem. How much of the table must be shared with each neighbor? A node is not aware of a neighbor's table. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbor. When the neighbor receives a table, this column needs

to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbor. In other words, sharing here means sharing only the first two columns.

Updating: When a node receives a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps:

- The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is x mi, and the distance between A and C is y mi, then the distance between A and that destination, via C, is x + y mi.
- The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
- The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

3) If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
4) If the next-node entry is the same, the receiving node chooses the new row. For example, suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller. The old route does not exist anymore. The new route has a distance of infinity.

Figure C shows how node A updates its routing table after receiving the partial table from node C.

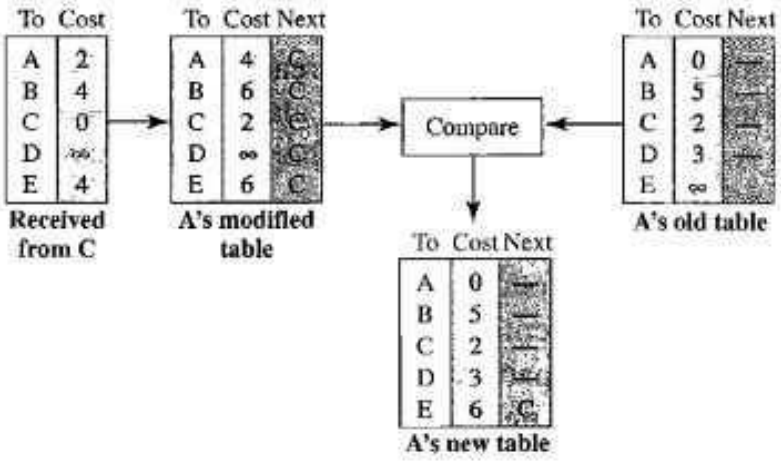


Figure C: Updating in distance vector routing

When to Share: The question now is, when does a node send its partial routing table (only two columns) to all its immediate neighbors? The table is sent both periodically and when there is a change in the table.

Periodic Update: A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

Triggered Update: A node sends its two-column routing table to its neighbors anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.

- A node receives a table from a neighbor, resulting in changes in its own table after updating.
- A node detects some failure in the neighboring links which results in a distance change to infinity.

Q11. Explain Routing Information protocol in brief. **(AKTU 2003-4)**

Solution:

Routing Information Protocol (RIP) is a routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network.

The Routing Information Protocol is a distance vector routing protocol that helps routers determine the best path to transfer data packets across the network. RIP works on the Network layer of the OSI model. It uses hop count as its metric for determining the best path, but the maximum hop count allowed in the RIP is 15. Routing Information Protocol is mostly used in small to medium-sized networks.

Hop count is the number of routers occurring between the source and destination network. The path with the lowest hop count is considered the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the hops allowed in a path from source to destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

Features of RIP

- Updates of the network are exchanged periodically.
- Updates (routing information) are always broadcast.
- Full routing tables are sent in updates.
- Routers always trust routing information received from neighbor routers. This is also known as routing on rumors.

How Routing Information Protocol Works?

Routing Information Protocol uses Distance Vector Routing to put the packets to its destination. In RIP, Each router maintains a routing table where the distance to each destination is mentioned. RIP shares its routing tables to neighboring routers at an interval of 30 seconds through broadcasting. Upon receiving the data, each router updates the table according to that. If a router receives a route and it is shorter than the previous one, then router simply updates the data in the table.

RIP has a limit of 15 hops, that is, if some route requires more than 15 hops, then that path in unreachable. It helps in limiting the size of network that a router can handle. In case, if a route is not updated in six successful cycles (180 seconds) in the routing table, the RIP will drop that route and inform rest of the network about the same.

Routing Information Protocol is simple to implement, but it is more efficient for smaller networks, for larger networks, protocols like OSPF or EIGRP are preferred.

Advantages of RIP

- **Simplicity:** RIP is a relatively simple protocol to configure and manage, making it an ideal choice for small to medium-sized networks with limited resources.
- **Easy implementation:** RIP is easy to implement, as it does not require much technical expertise to set up and maintain.
- **Convergence:** RIP is known for its fast convergence time, meaning that it can quickly adapt to changes in network topology and route packets efficiently.
- **Automatic updates:** RIP automatically updates routing tables at regular intervals, ensuring that the most up-to-date information is being used to route packets.
- **Low bandwidth overhead:** RIP uses a relatively low amount of bandwidth to exchange routing information, making it an ideal choice for networks with limited bandwidth.
- **Compatibility:** RIP is compatible with many different types of routers and network devices, making it easy to integrate into existing networks.

Disadvantages of RIP

- **Limited scalability:** RIP has limited scalability, and it may not be the best choice for larger networks with complex topologies. RIP can only support up to 15 hops, which may not be sufficient for larger networks.
- **Slow convergence:** While RIP is known for its fast convergence time, it can be slower to converge than other routing protocols. This can lead to delays and inefficiencies in network performance.
- **Routing loops:** RIP can sometimes create routing loops, which can cause network congestion and reduce overall network performance.
- **Limited support for load balancing:** RIP does not support sophisticated load balancing, which can result in suboptimal routing paths and uneven network traffic distribution.
- **Security vulnerabilities:** RIP does not provide any native security features, making it vulnerable to attacks such as spoofing and tampering.
- **Inefficient use of bandwidth:** RIP uses a lot of bandwidth for periodic updates, which can be inefficient in networks with limited bandwidth.

Limitations of RIP

On using RIP, there can be certain limitations. Some of them are mentioned below:

- **Increase in Network Traffic:** RIP increases traffic to the neighboring routers as it regularly performs updates on them.
- **Limitation of Hop Count:** Since, RIP has a maximum hop count of 15, therefore it is not suitable for large networks.
- **Difference in Closest Path and Shortest Path:** Since, RIP does not consider all factors while calculating shortest path, therefore, it creates a difference between closest path and shortest path.

BUDDHA SERIES

(Unit Wise Solved Question & Answers)

Course – B.Tech. (CSE Allied-AIML/DS)

College – Buddha Institute of Technology

(AKTU CODE-525)

Department: Computer Science & Engineering Allied-AIML/DS

(Accredited by NBA 2024-27)

Subject: Computer Networks

(BCS 603)

Faculty Name: Mr. Shailesh Kumar Patel

Unit - 4

Q1. Differentiate TCP and UDP in context of the header format. **(AKTU 2022-23)**

Solution:

User Datagram: UDP packets, called user datagrams, have a fixed-size header of 8 bytes.

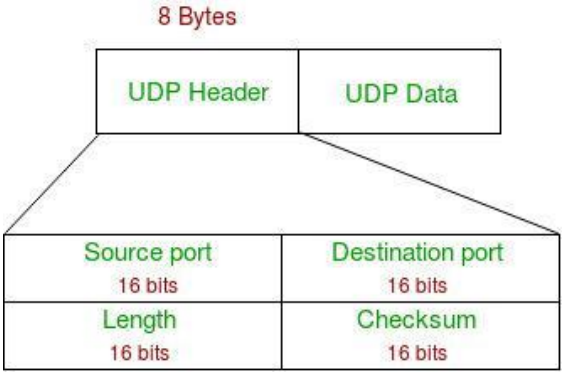


Figure 1: User datagram format

The fields are as follows:

Source port number This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535 (216-1). If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

Destination port number This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.

Length This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length.

UDP length = IP length - IP header's length

Checksum This field is used to detect errors over the entire user datagram (header plus data).

TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

TCP is called a connection-oriented, reliable transport protocol. It adds connection-oriented and reliability features to the services of IP.

Segment:

A packet in TCP is called a segment. Format The format of a segment is shown in Figure 2.

The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, a header is 20 bytes else it can be of upmost 60 bytes.

Header fields:

Source Port Address –

A 16-bit field that holds the port address of the application that is sending the data segment.

Destination Port Address –

A 16-bit field that holds the port address of the application in the host that is receiving the data segment.

Sequence Number –

A 32-bit field that holds the sequence number, i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end of the segments that are received out of order.

Acknowledgement Number –

A 32-bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

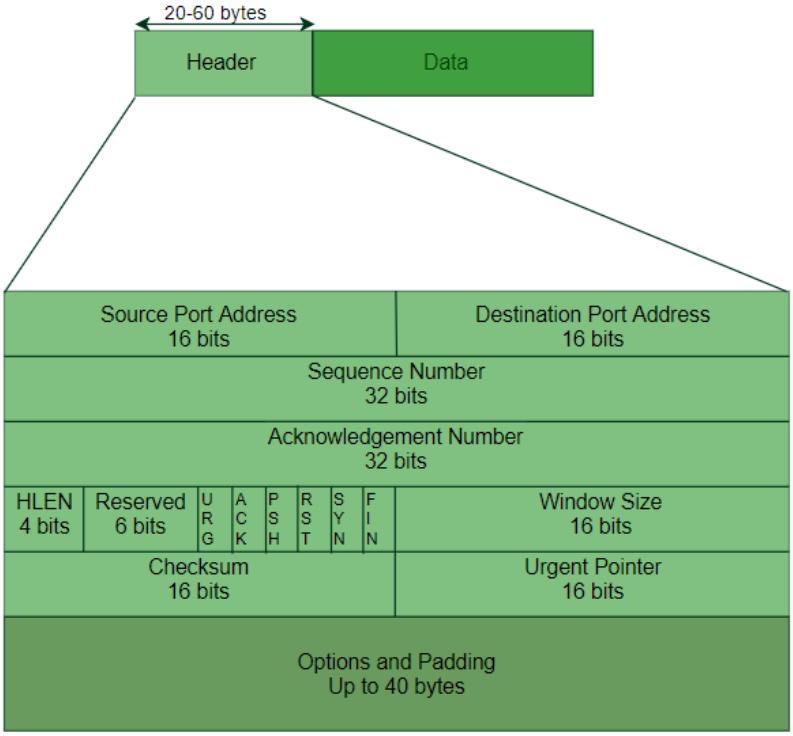


Figure 2: TCP segment format

Header Length (HLEN) –

This is a 4-bit field that indicates the length of the TCP header by a number of 4-byte words in the header, i.e if the header is 20 bytes (min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.

Control flags –

These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:

- URG: Urgent pointer is valid
- ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)
- PSH: Request for push
- RST: Reset the connection
- SYN: Synchronize sequence numbers
- FIN: Terminate the connection

Window size –

This field tells the window size of the sending TCP in bytes.

Checksum –

This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

Urgent pointer –

This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

Options -

There can be up to 40 bytes of optional information in the TCP header.

Q2. What do you understand by Quality of Service, parameters? List various Quality of Service parameters. **(AKTU 2018-19)**

Solution:

Quality of Service (QoS) is an important concept, particularly when working with multimedia applications. Multimedia applications, such as video conferencing, streaming services, and VoIP (Voice over IP), require certain bandwidth, latency, jitter, and packet loss parameters. QoS methods help ensure that these requirements are satisfied, allowing for seamless and reliable communication.

Quality-of-service (QoS) refers to traffic control mechanisms that seek to differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions, or traffic aggregates. The basic phenomenon for QoS is in terms of packet delay and losses of various kinds.

QoS Specification

- Delay
- Delay Variation(Jitter)
- Throughput
- Error Rate

Types of Quality of Service

- **Stateless Solutions** – Routers maintain no fine-grained state about traffic, one positive factor of it is that it is scalable and robust. But it has weak services as there is no guarantee about the kind of delay or performance in a particular application which we have to encounter.
- **Stateful Solutions –** Routers maintain a per-flow state as flow is very important in providing the Quality-of-Service i.e. providing powerful services such as guaranteed services and high resource utilization, providing protection, and is much less scalable and robust.

QoS Parameters

- **Packet loss:** This occurs when network connections get congested, and routers and switches begin losing packets.
- **Jitter:** This is the result of network congestion, time drift, and routing changes. Too much jitter can reduce the quality of voice and video communication.
- **Latency:** This is how long it takes a packet to travel from its source to its destination. The latency should be as near to zero as possible.
- **Bandwidth**: This is a network communications link's ability to transmit the majority of data from one place to another in a specific amount of time.
- **Mean opinion score:** This is a metric for rating voice quality that uses a five-point scale, with five representing the highest quality.

Q3. The following is the dump of a TCP header in hexadecimal format: **(AKTU 2018-19)**

05320017 00000001 00000000 500207FF 00000000

(i) What is the source port number?

(ii) What is the destination port number?
(iii) What is the sequence number?
(iv) What is the acknowledgment number?
(v) What is the length of the header?
(vi) What is the type of the segment?
(vii) What is the window size?

Solution: The following is the dump of a TCP header in hexadecimal format:
05320017 00000001 00000000 500207FF 00000000

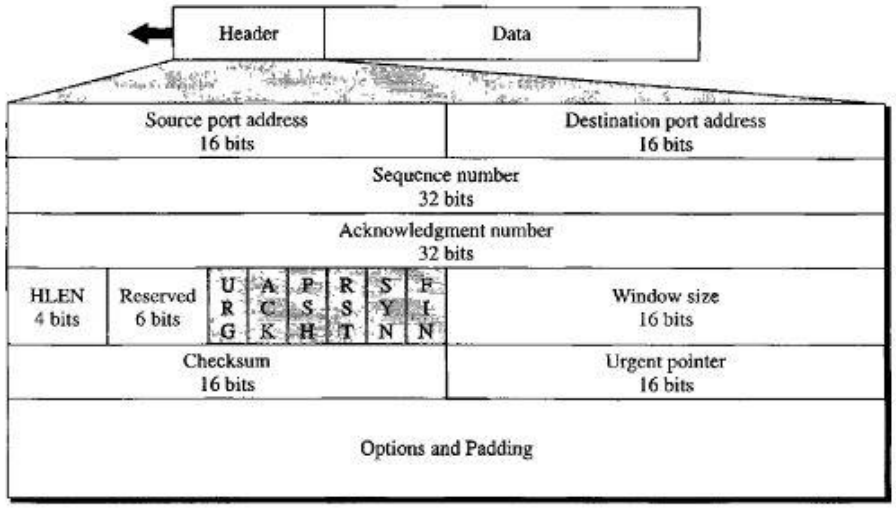


Figure:TCP segment format

(i) The source port number: source port is 2 bytes take =0532
$= (0000010100110010)_2$
0532
$= (1330)_{10}$
(ii) The destination on port number is 2 bytes as destination address = 0017
$= (0000000000010111)_2$
$= (23)_{10}$ (default TCP port)
(iii) The sequence number is 4 bytes as sequence number = 00000001
$= (00000000000000000000000000000001)_2$
$= (1)_{10}$
(iv) The acknowledgment number is next 4 bytes as ask = 00000000
$= (00000000000000000000000000000000)_2$
$= (0)_{10}$
(v) The length of the header is 4 bits as HLEN = 5
$= (0101)_2$
$= (5)_{10}$
This indicates number of sets of 4 bytes which makes the header length = 5*4 20 bytes
(vi) The type of the segment is 6 bits are reserved i.e.0 = 0000 and 2 bits from next 0 (0000) i.e. 00. Remaining two bits i.e. 00 and 4 bits of next 2 i. e. 0010.
Total 6 bits of control field = last two bits of 0 and 4 bits of 2

= 000010

=	U R G	A C K	P S H	R S T	S Y N	F I N

i.e. type of segment is SYN.

(vii) The window size is 2 bytes indicate the window length = 07FF

$= (0000011111111111)_2$

$= (2047)_{10}$

Q4. What is congestion? Briefly describe the techniques that prevent congestion. **(AKTU 2017-18)**

Solution:

Congestion in a network may occur if the load on the network-the number of packets sent to the network-is greater than the capacity of the network-the number of packets a network can handle.

Congestion in a computer network happens when there is too much data being sent at the same time, causing the network to slow down. Just like traffic congestion on a busy road, network congestion leads to delays and sometimes data loss.

Congestion Control techniques in Computer Networks:

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:

- Open Loop Congestion Control
- Closed Loop Congestion Control

1) Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control –

- **Retransmission Policy:** It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.

  To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

- **Window Policy:** The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.

  Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

- **Discarding Policy:** A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.

  In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

- **Acknowledgment Policy:** Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.

  The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send an acknowledgment only if it has to send a packet or

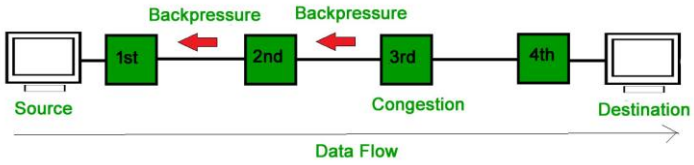
a timer expires.

- **Admission Policy:** In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of congestion or there is congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

2) Closed Loop Congestion Control

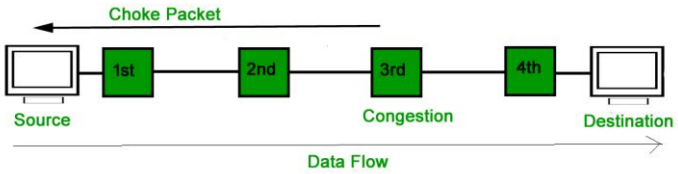
Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

- **Backpressure:** It is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagates in the opposite direction of data flow. The backpressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

- **Choke Packet Technique:** Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets have traveled are not warned about congestion.



- **Implicit Signaling:** In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is congestion.
- **Explicit Signaling:** In explicit signaling, if a node experiences congestion it can explicitly send a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique. Explicit signaling can occur in either forward or backward direction.
    - **Forward Signaling:** In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopts policies to prevent further congestion.
    - **Backward Signaling:** In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

Q5. Enumerate on TCP header and working of TCP and differentiate TCP and UDP with frame format.

(AKTU 2017-18)

Solution:

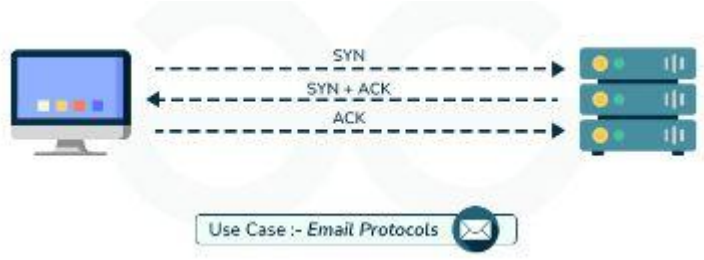
A TCP header consists of the following fields:

- **Source Port:** A 16-bit number identifying the sending application on the source host.
- **Destination Port:** A 16-bit number identifying the receiving application on the destination host.
- **Sequence Number:** A 32-bit number that indicates the order of the first byte of data in the segment, used for reliable data delivery.
- **Acknowledgement Number:** A 32-bit number that acknowledges the next byte the sender expects to receive from the receiver.
- **Data Offset (Header Length):** A 4-bit field specifying the length of the TCP header in 32-bit words.
- **Reserved Flags:** 6 reserved bits that must be set to zero
- **Control Flags:** Several flags like SYN (synchronize), ACK (acknowledge), FIN (finish), RST (reset), URG (urgent) used to control connection establishment and data flow.
- **Window Size:** A 16-bit field indicating how much data the receiver is willing to accept before needing to send another acknowledgement
- **Checksum:** A 16-bit field used for error detection in the TCP header and payload
- **Urgent Pointer (optional):** A 16-bit field used to indicate the position of urgent data within the segment

Working of Transmission Control Protocol (TCP):

Transmission Control Protocol (TCP) model breaks down the data into small bundles and afterward reassembles the bundles into the original message on the opposite end to make sure that each message reaches its target location intact. Sending the information in little bundles of information makes it simpler to maintain efficiency as opposed to sending everything in one go.

After a particular message is broken down into bundles, these bundles may travel along multiple routes if one route is jammed but the destination remains the same.



For Example: When a user requests a web page on the internet, somewhere in the world, the server process that request and sends back an HTML Page to that user. The server makes use of a protocol called the HTTP Protocol. The HTTP then requests the TCP layer to set the required connection and send the HTML file.

Now, the TCP breaks the data into small packets and forwards it toward the Internet Protocol (IP) layer. The packets are then sent to the destination through different routes.

The TCP layer in the user's system waits for the transmission to get finished and acknowledges once all packets have been received.

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented	UDP is the Datagram-oriented

	protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). This means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet .	UDP is used by DNS, DHCP, TFTP, SNMP , RIP , and VoIP .
Stream Type	The TCP connection is a byte stream.	UDP connection is a message stream.
Overhead	Low but higher than UDP.	Very low.
Applications	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.	This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc.

Q6. Explain the three-way handshaking protocol to establish the transport level connection. **(AKTU 2017-18)**

Solution:

TCP Connection:

In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.

Connection Establishment: TCP transmits data in full-duplex mode.

Three-Way Handshaking: The connection establishment in TCP is called three-way handshaking. The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a passive open.

The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown in following figure.

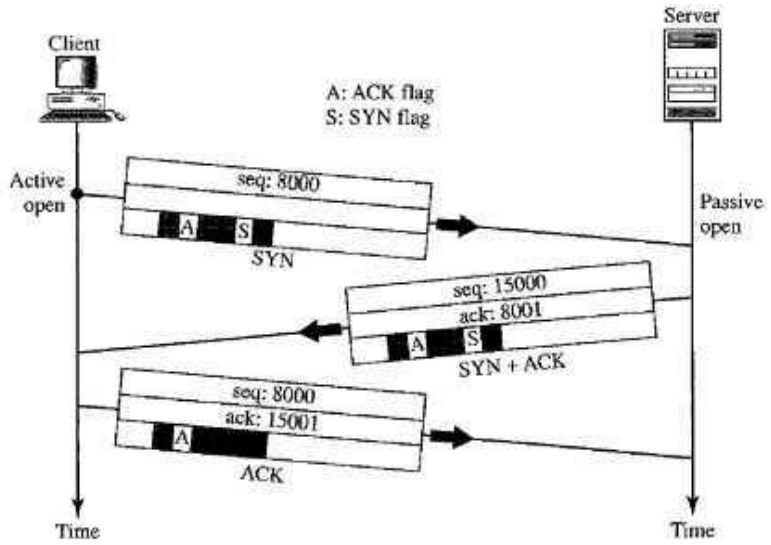


Figure: Connection establishment using three-way handshaking

The three steps in this phase are as follows:

- A SYN segment cannot carry data, but it consumes one sequence number.
- A SYN + ACK segment cannot carry data, but does consume one sequence number.
- An ACK segment, if carrying no data, consumes no sequence number.

Simultaneous Open A rare situation, called a simultaneous open, may occur when both processes issue an active open.

SYN Flooding Attack The connection establishment procedure in TCP is susceptible to a serious security problem called the SYN flooding attack. This happens when a malicious attacker sends a large number of SYN segments to a server, pretending that each of them is coming from a different client by faking the source IP addresses in the datagrams.

The server, assuming that the clients are issuing an active open, allocates the necessary resources, such as creating communication tables and setting timers. This SYN flooding attack belongs to a type of security attack known as a denial-of-service attack, in which an attacker monopolizes a system with so many service requests that the system collapses and denies service to every request.

Q7. Enumerate how the transport layer unsure that the complete message arrives at the destination and in the proper order. **(AKTU 2017-18)**

Solution:

The transport layer ensures a complete message arrives at the destination in the proper order by: dividing

the message into segments, assigning sequence numbers to each segment, and using acknowledgment mechanisms to verify receipt of each segment, allowing the receiver to reassemble the message correctly and re-request any missing segments if needed; this process is primarily implemented through protocols like TCP (Transmission Control Protocol) which utilize a sliding window mechanism for efficient data flow.

The transport layer ensures that all the fragments of a transmission arrive at the destination, not some of them. On the sending end, all the fragments of transmission are given sequence numbers by a transport layer. These sequence numbers allow the receiver's transport layer to identify the missing segment.

The transport layer achieves reliable delivery by using:

- Segmentation
- Sequence Numbers
- Acknowledgment (ACK)
- Retransmission
- Sliding Window

Q8. What is congestion? Explain leaky bucket algorithm. **(AKTU 2003-4)**

Solution:

Congestion in a network may occur if the load on the network-the number of packets sent to the network-is greater than the capacity of the network-the number of packets a network can handle.

Congestion in a computer network happens when there is too much data being sent at the same time, causing the network to slow down. Just like traffic congestion on a busy road, network congestion leads to delays and sometimes data loss.

Leaky Bucket: If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

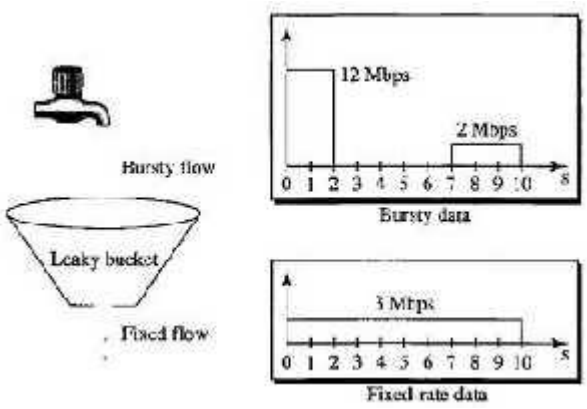


Figure: Leaky bucket

In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In figure the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbps of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbps of data. In all, the host has sent 30 Mbps of data in l0s. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10s.

A simple leaky bucket implementation is shown in following figure. A FIFO queue holds the packets. If the traffic consists of fixed-size packets, the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based

on the number of bytes or bits. The following is an algorithm for variable-length packets:

- Initialize a counter to n at the tick of the clock.
- If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
- Reset the counter and go to step 1.

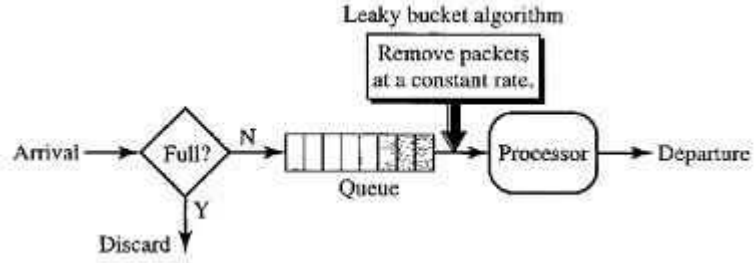


Figure: Leaky bucket implementation

Q9. Discuss TCP window management in detail. Also explain silly window syndrome and their solution.

(AKTU 2018-19)

Solution:

TCP window management, also known as the "sliding window" mechanism, is a crucial feature of the Transmission Control Protocol (TCP) that allows the sender to control the amount of data it can send to the receiver before needing an acknowledgment, effectively regulating data flow and preventing the receiver from being overwhelmed by a rapid influx of data, especially on networks with varying bandwidths or latency; it dynamically adjusts the sending window size based on the receiver's available buffer space and network conditions, ensuring efficient data transmission.

In TCP window management:

- **Sliding Window Concept:** Imagine a window that slides along the data stream, representing the range of data that the sender can currently transmit without waiting for an acknowledgment. As the receiver acknowledges received data, the window slides forward, allowing the sender to send more data.
- **Window Size:** The size of the window determines the maximum amount of data the sender can send before needing an acknowledgment. This size is communicated by the receiver through the TCP header, allowing the sender to adjust its sending rate based on the network conditions and receiver's capacity.
- **Acknowledgement (ACK):** When the receiver successfully receives a segment of data, it sends an acknowledgment packet back to the sender, indicating that it is ready to receive more data and updating the window size accordingly.
- **Flow Control:** TCP window management acts as a flow control mechanism, preventing the sender from sending data faster than the receiver can process it.

How TCP window management works:

- **Initial Window Size:** When a TCP connection is established, the receiver advertises its initial window size to the sender.
- **Data Transmission:** The sender transmits data within the specified window size.
- **Acknowledgment:** Upon receiving data, the receiver sends an acknowledgment packet with a new window size, indicating how much more data it is ready to receive.
- **Sliding Window:** As the sender receives acknowledgments, the window slides forward, allowing it to send new data segments.
- **Congestion Control:** In case of network congestion, the sender may need to decrease its window

size to avoid overwhelming the network, and gradually increase it again when congestion subsides.

Silly Window Syndrome:

Silly Window Syndrome is a problem that arises due to poor implementation of TCP. It degrades the TCP performance and makes the data transmission extremely inefficient. The problem is called so because:

- It causes the sender window size to shrink to a silly value.
- The window size shrinks to such an extent that the data being transmitted is smaller than TCP Header.

The two major causes of this syndrome are as follows:

- Sender window transmitting one byte of data repeatedly.
- Receiver window accepting one byte of data repeatedly.

Cause-1: Sender window transmitting one byte of data repeatedly –

Suppose only one byte of data is generated by an application. The poor implementation of TCP leads to transmit this small segment of data. Every time the application generates a byte of data, the window transmits it. This makes the transmission process slow and inefficient. The problem is solved by Nagle's algorithm.

Nagle's algorithm suggests:

- Sender should send only the first byte on receiving one byte data from the application.
- Sender should buffer all the rest bytes until the outstanding byte gets acknowledged.
- In other words, sender should wait for 1 RTT(Round Trip Time).

After receiving the acknowledgement, sender should send the buffered data in one TCP segment. Then, sender should buffer the data again until the previously sent data gets acknowledged.

Cause-2: Receiver window accepting one byte of data repeatedly –

Suppose consider the case when the receiver is unable to process all the incoming data. In such a case, the receiver will advertise a small window size. The process continues and the window size becomes smaller and smaller. A stage arrives when it repeatedly advertises window size of 1 byte. This makes receiving process slow and inefficient. The solution to this problem is Clark's Solution.

Clark's solution suggests:

- Receiver should not send a window update for 1 byte.
- Receiver should wait until it has a decent amount of space available.
- Receiver should then advertise that window size to the sender.

Nagle's algorithm is turned off for those applications that require data to be immediately send. Nagle's algorithm can introduce delay as it sends only one data segment per round trip.

Both Nagle's as well as Clark's algorithm can work together. Both are complementary.

Q10. What is TCP? Connection termination in TCP is symmetric, whereas connection establishment is not. Why? **(AKTU 2012-13)**

Solution:

TCP (Transmission Control Protocol) is one of the main protocols of the TCP/IP suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. Transmission Control Protocol (TCP) ensures reliable and efficient data transmission over the internet.

Transmission Control Protocol (TCP) is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

The position of TCP is at the transport layer of the OSI model. TCP also helps in ensuring that information is transmitted accurately by establishing a virtual connection between the sender and receiver.

Yes, connection termination in TCP is considered "symmetric" because both sides of the connection must actively participate in the closing process by sending FIN (Finish) segments and acknowledging them, ensuring that neither side can fully close the connection without the other's cooperation; essentially, both parties need to agree to end the communication before it is truly terminated.

TCP connection termination symmetry:

- **Four-way handshake:** Unlike the three-way handshake for connection establishment, terminating a TCP connection requires a four-way handshake where each side sends a FIN segment and acknowledges the other's FIN to properly close the connection.
- **Half-close possibility:** While the process is symmetric, one side can initiate the close by sending its FIN first, creating a "half-closed" state where one side can still receive data while no longer sending any.
- **Importance of symmetry:** This symmetry ensures that no data is lost during closure, as both sides need to confirm that they have received all outstanding data before fully shutting down.

The connection establishment process itself is considered asymmetric because one side (typically the client) initiates the connection by actively sending a SYN packet, while the other side (the server) passively waits for the connection request and responds with a SYN-ACK packet, making the initial connection setup not perfectly balanced between the two parties.

TCP connection establishment asymmetry:

- **Active Open vs. Passive Open:** The client performs an "active open" by sending the initial SYN packet, while the server performs a "passive open" by listening for incoming connection requests on a specific port.
- **Three-Way Handshake:** Even though the connection establishment involves a three-way handshake (SYN, SYN-ACK, ACK), the initiation of the handshake is clearly driven by the client.