Maximum efficiency = 18.4%	Maximum efficiency = 36.8%
Collision rate is high	Collision rate is reduced to half

Differences between persistent methods

I-persistent CSMA	**P - persistent CSMA**	**Non-persistent CSMA**
Transmits when channel is idle.	Transmits with probability of p when channel is idle.	Transmits when channel is idle.
Continuously senses the channel or carrier.	Waits for the time slot to sense the channel.	Waits for random time to check the channel or carrier.
Rate of collision is high	Rate of collision is less when compared with other methods	Rate of collision is less compared to I – persistent and more when compared to P – persistent.
Bandwidth utilization is good than ALOHA	Bandwidth utilization depends on probability P	Bandwidth utilization is more compared with I – persistent.
Delay is low when channel is idle.	Delay is low when P is small.	Delay is low when channel is idle.

3.5.4 Carrier sense multiple access – Collision detection (CSMA/CD)

1. This algorithm is used to handle the collision during transmission.
2. Here the station monitors the medium after the frame is sent for successful transmission.
3. Let us consider an example as shown in figure below. Here four stations using same medium for transmission of frames. Station A and Station C sense the medium is idle and transmits frames at time t_1 and t_4 respectively.
4. When station A begins to transmit a frame at t_1 and the first bit of this frame has not been sensed by station C, then station C executes its persistence methods and starts sending its frames at time t_4.
5. While propagating on the same line these two frames collide at time t_3 where the first bit of A’s frame is detected by station C.
6. Then station C immediately aborts transmission. Station A detects the collision at a time t_4 when it detects the first bit of station C, it also aborts transmission.

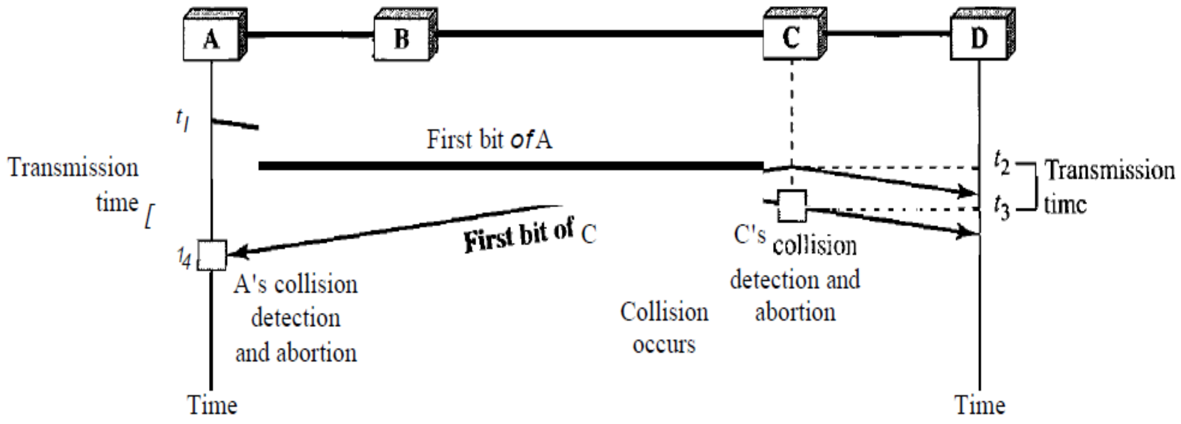


Fig.3.42. Collision of first bit in CSMA/CD.

7. From the above figure we can understand that station A transmits during $t_4 - t_1$ entry transmits between duration $t_3 - t_2$.
8. So there is a trade-off between the bit rate and the time durations in which the transmission has occurred.
9. The bit rate in this protocol must be more than either of these durations i.e., $t_4 - t_1$ and $t_3 - t_2$.

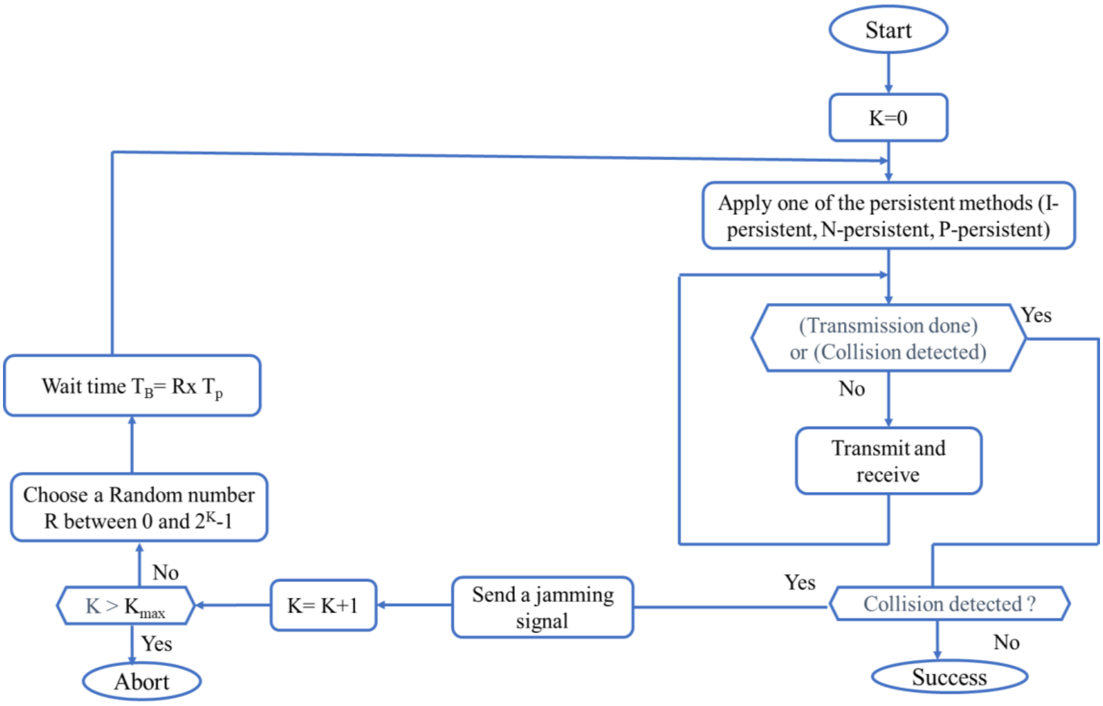

Start
K=0
Apply one of the persistent methods (I-persistent, N-persistent, P-persistent)
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Wait time T_B= Rx T_p
Choose a Random number R between 0 and 2^K-1
No
K > K_{max}
Yes
Abort
K= K+1
Send a jamming signal
Yes
Collision detected ?
No
Success

Fig. 3.43 .

Flow chart for CSMA/CD.

In the above figure K = number of attempts

T_p = Maximum propagation time

T_{fr} = Average transmission time

T_B = Back off time = Rx T_p

R = random number between 0 to 2^{K}-1
usually K_{max} = 15

3.5.5 Carrier sense multiple access – Collision avoidance (CSMA/CA)

1. Collision detection could be done when a station is able to receive during transmission.
2. When no collision has occurred then stations will receive their own signal.
3. When collision has occurred stations will receive two signals: its own signals and signal transmitted by a second station. The stations will distinguish signals by the amount of energy added to them due to collision.
4. In a wired network all the stations will transmit signal with same energy and repeaters are used to enhance the signal strength when required. So, the station could detect the collision.
5. In a wireless network the signal energy is lost in transmission and the energy added to the signal after collision will be helpful to detect the collision. In such case, carrier sense multiple access – collision avoidance is implemented.
6. In CSMA/CA we use interframe space, the contention window and acknowledgments.

Interframe space (IFS)

1. In CSMA/CA the station will not transmit even though it found the channel is idle.
2. The station will wait for interframe time IFS because any other station may be in the middle of the transmission and the signal has not reached the station which is ready for transmission.
3. So, after the completion of the IFS time the station once again detects the channel is idle and then starts transmitting the signals.
4.This IFS variable can be used to prioritize the stations or frame types. The station that has assigned a shorter IFS has a higher priority.

Contention window

1. In this window am amount of time is divided into slots. A station which is ready for transmission chooses a random number of slots as its wait time.
2. The number of slots in the window changes according to the exponential back-off strategy i.e 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.
3. The station needs to sense the channel once the contention window time is completed for each slot. The station finds channel is busy it does not restart the process.
4. It stops the timer and restarts it when the channel is sensed as idle.
5. This gives priority to the station with the longest waiting time.

Acknowledgment

1. A positive acknowledgment and the timeout timer can help generate the receiver has

received the frame.

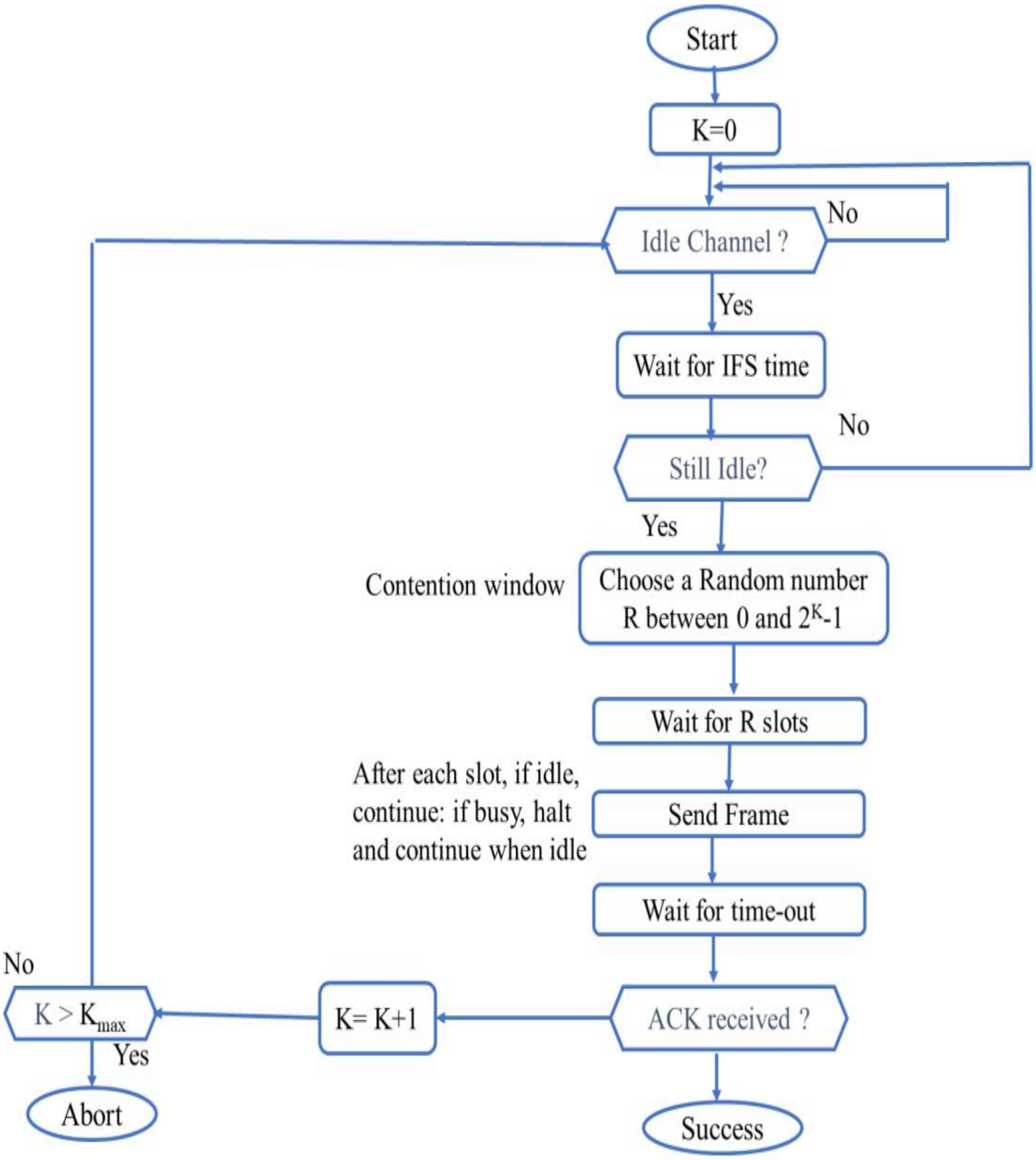


Fig.3.44. Flow chart for CSMA/CA.

Advantages of CSMA

1. Helps prevent data collisions.
2. No data is unnoticeably lost.
3. Efficiency is increased.
4. Simple protocol, flexible and cost effective to implement.

Disadvantages of CSMA

1. Longer waiting times.
2. Causes additional traffic.

3. Limited reliability and vulnerable to access

Difference between CSMA CA and CSMA CD

S. No	CSMA CD	CSMA CA
1.	It is the type of CSMA to detect the collision on a shared channel.	It is the type of CSMA to avoid collision on a shared channel.
2.	It is the collision detection protocol.	It is the collision avoidance protocol.
3.	It is used in 802.3 Ethernet network cable.	It is used in the 802.11 Ethernet network.
4.	It works in wired networks.	It works in wireless networks.
5.	It is effective after collision detection on a network.	It is effective before collision detection on a network.
6.	Whenever a data packet conflicts in a shared channel, it resends the data frame.	Whereas the CSMA CA waits until the channel is busy and does not recover after a collision.
7.	It minimizes the recovery time.	It minimizes the risk of collision.
8.	The efficiency of CSMA CD is high as compared to CSMA.	The efficiency of CSMA CA is similar to CSMA.
9.	It is more popular than the CSMA CA protocol.	It is less popular than CSMA CD.

3.6 Physical addressing

1. MAC address is a physical address which uniquely identifies each device on a network.
2. To communicate between wo devices in a network we need MAC address.
3. It is assigned by the vendor to the network interface card (NIC) of every device.
4. It stands for media access control and also known as physical address, hardware address, burned in address (BIA). It is represented by a hexadecimal format on such as a1: 00: 2b: cd: 67:18.
5. It is a 12-digit and 48 bits long, out of which the first 24 bits are used OUI (organization unique identifier) and 24 bits are for NIC or vendor specific.
6. It is provided by the device vendor at the time of manufacturing and embedded with NIC which is ideally cannot be changed. It is used in the data link layer of the OSI model.
7. MAC addresses are expressed in hexadecimal notation. For example, "01-23-45-67-89-AB" in a 48-bit address or "01-23-45-67-89-AB-CD-EF" in a 64-bit address. Sometimes, colons

(:)

8. There are three types of MAC addresses. 1. Unicast address 2. Multicast address 3. Broadcast address.

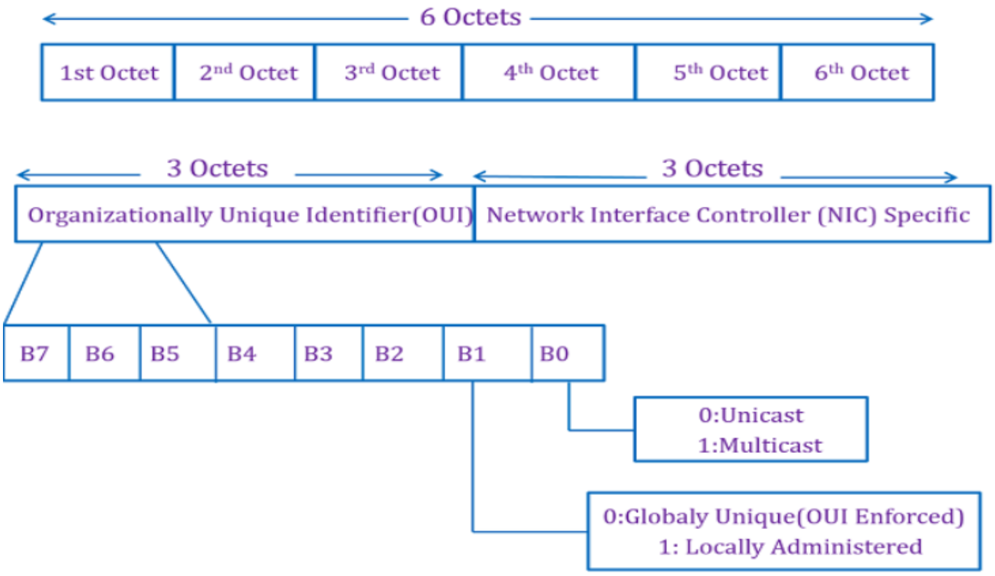


Fig.3.45. Structure of MAC address.

Unicast MAC address

The Unicast MAC address represents the specific NIC on the network. A Unicast MAC address frame is only sent out to the interface which is assigned to a specific NIC and hence transmitted to the single destination device. If the LSB (least significant bit) of the first octet of an address is set to zero, the frame is meant to reach only one destination NIC.

Multicast MAC address

Multicast addresses enables the source device to transmit a data frame to multiple devices or NICs. In Layer-2 (Ethernet) Multicast address, LSB (least significant bit) or first 3 bytes of the first octet of an address is set to one and reserved for the multicast addresses. The rest 24 bits are used by the device that wants to send the data in a group. The multicast address always starts with the prefix 01-00-5E.

Broadcast MAC address

It represents all devices within a Network. In broadcast MAC address, Ethernet frames with ones in all bits of the destination address (FF-FF-FF-FF-FF-FF) are known as a b**roadcast address**. All these bits are the reserved addresses for the broadcast. Frames that are destined with MAC address FF-FF-FF-FF-FF-FF will reach every computer belong to that LAN segment. Hence if a source device wants to send the data to all the devices within a network, that can use the broadcast address as the destination MAC address.

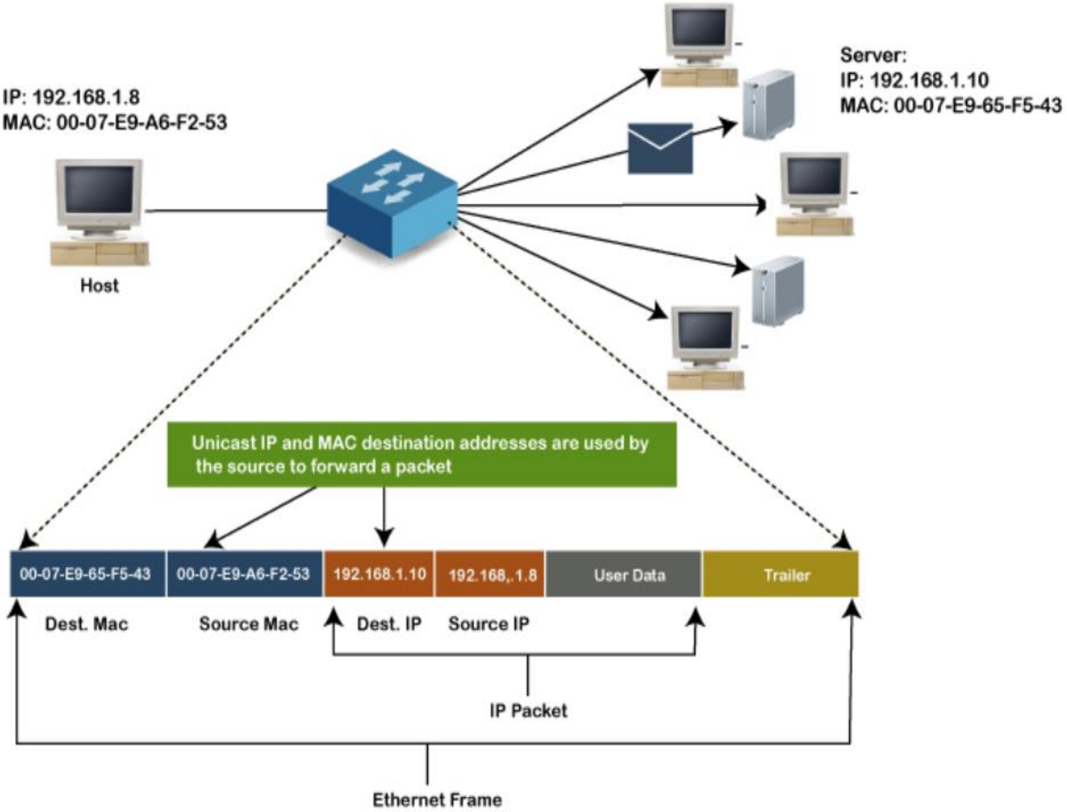


Fig.3.46. Structure of Unicast MAC address.

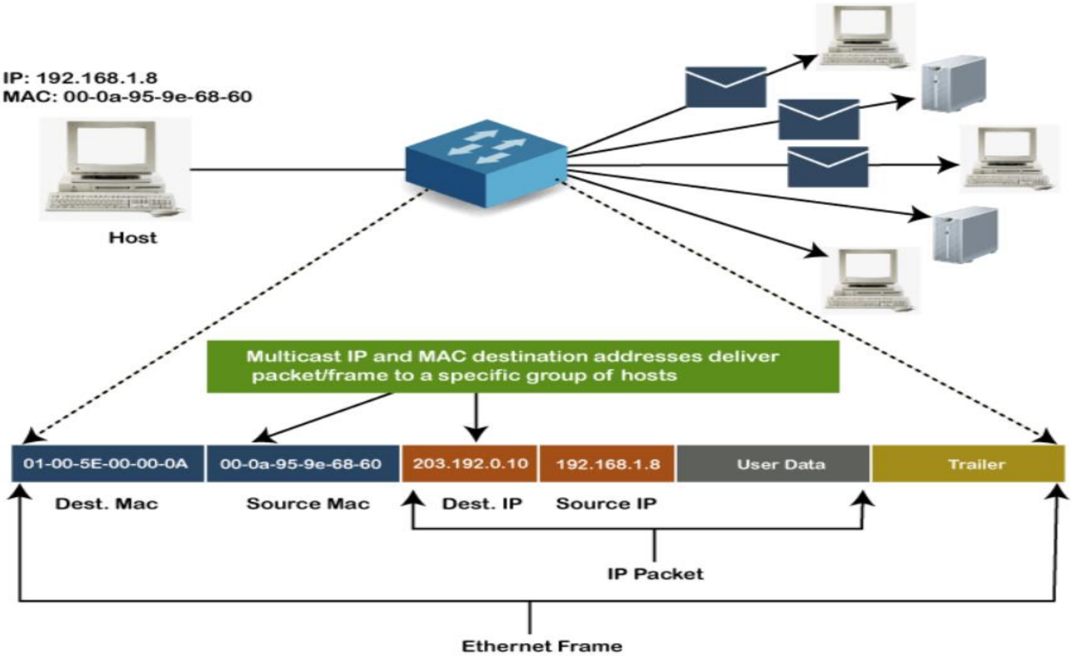


Fig.3.47. Structure of Multicast MAC address.

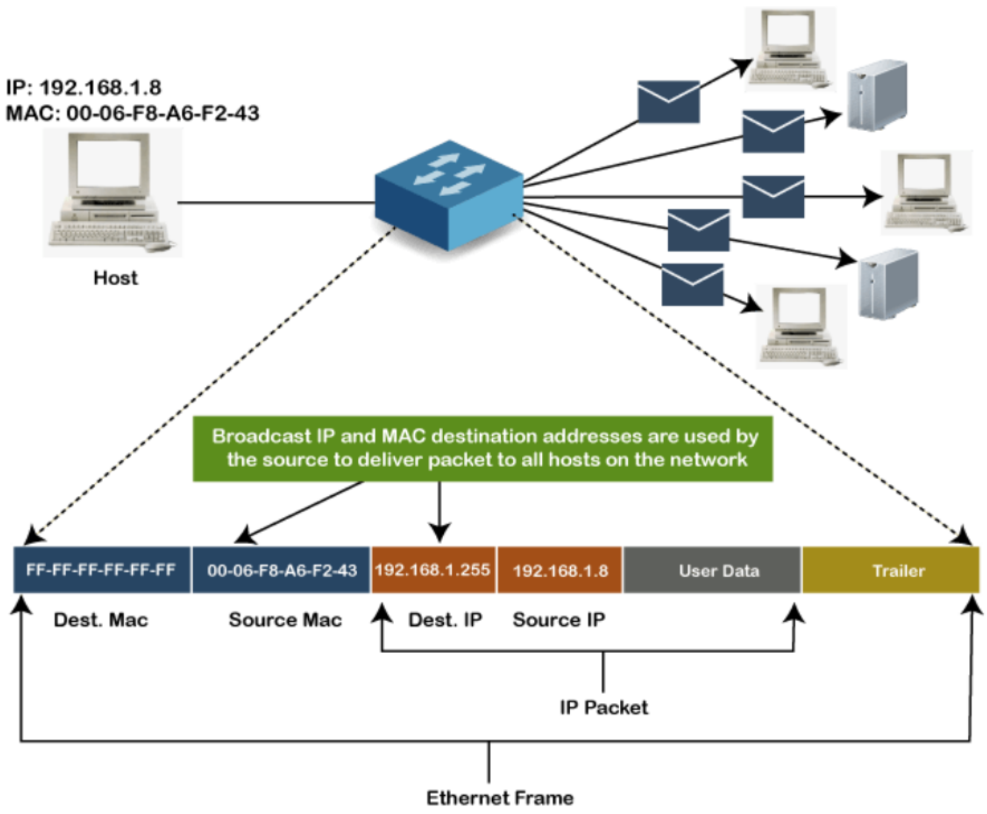


Fig.3.48. Structure of Broadcast MAC address.

3.7 Ethernet

1. The original Ethernet was created in 1976 at Xerox Palo Alto Research Centre (PARC).
2. From the time of its origin, Ethernet has been evolving and has gone through four generations named as standard Ethernet, Fast ethernet, Gigabit Ethernet and Ten-Gigabit Ethernet.

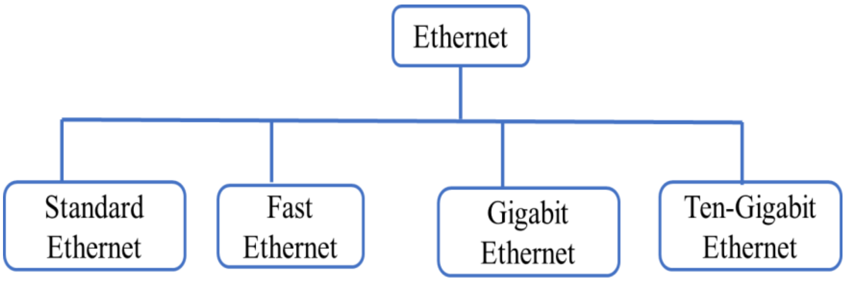


Fig.3.49. Evolution of Ethernet.

Standard Ethernet

1. Max sublayer governs the operation of stranded Ethernet It frames the data received from

the upper layer and passes them to the physical layer.

2. The Internet frame contains seven fields preamble, SFD, DA, SA, length or type of the protocol data unit (PDU), upper layer data and the CRE.
3. Ethernet does not provide any mechanism for acknowledging received frames, making it a unreliable medium.

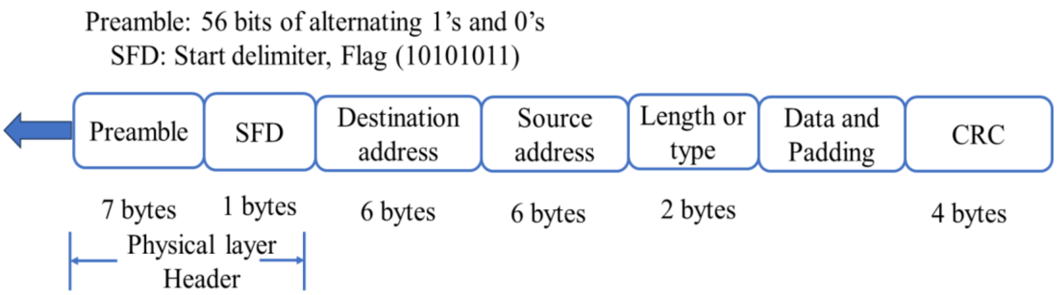


Fig.3.50. Frame format of standard Ethernet.

4. Preamble: The first field of eight nought 2.3 frame contains seven bytes of alternating zeros and ones that alerts the receiving system to the coming frame and enables it to synchronise its input timing. It is just alert and a timing pulse It allows the station to miss some bits of the beginning of the frame. It is added at the physical layer and not a part of a frame.
5. Start a frame delimiter (SFD) : The second field signals the beginning of the frame It wants the station or stations that it is the last chance of synchronisation The last two bits are 11, and See your that next field is the destination address.
6. Destination address: This field is of six bytes and contains physical letters of the destination station to receive the packet.
7. Source address: The source field is also six bytes and contain physical address of the sender of the packet.
8. Length or type: This field defined as type field or length field. Original Ethernet frame uses upper layer protocol number.
9. Data: This field carries data encapsulated from the upper layer protocols. It is minimum of 46. and maximum of 1500 bytes.
10. CRC: The last field contains error detection information.

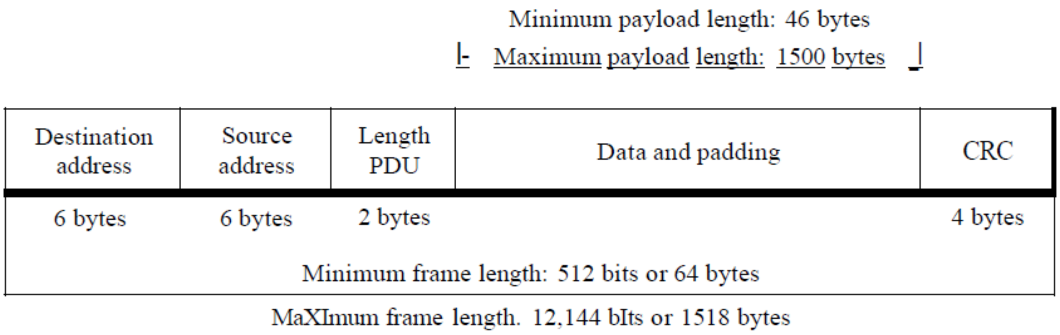

Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
MaXImum frame length. 12,144 bIts or 1518 bytes

Fig.3.51. Frame Length of standard Ethernet.

11. The minimum length restriction is required for current operation of CSMS/CD Ethernet frames needs to have a maximum length of 5 12 bits, or 64 bytes.
12. If upper layer packet is less than 46 bytes, padding is added to make up the difference.
13. The standard defines maximum length of the frame as 1518 bytes.
14. The standard Ethernet defines several physical layer implementations. Four most common are shown in the figure below.
15. All standard implementations use digital signalling at 10 Mbps. Data at the sender is converted into a digital signal using Manchester scheme.
16. At receiver, the received signal is interpreted and decoded into data. Manchester Encoding is self-synchronous, providing a transition of each bit interval.

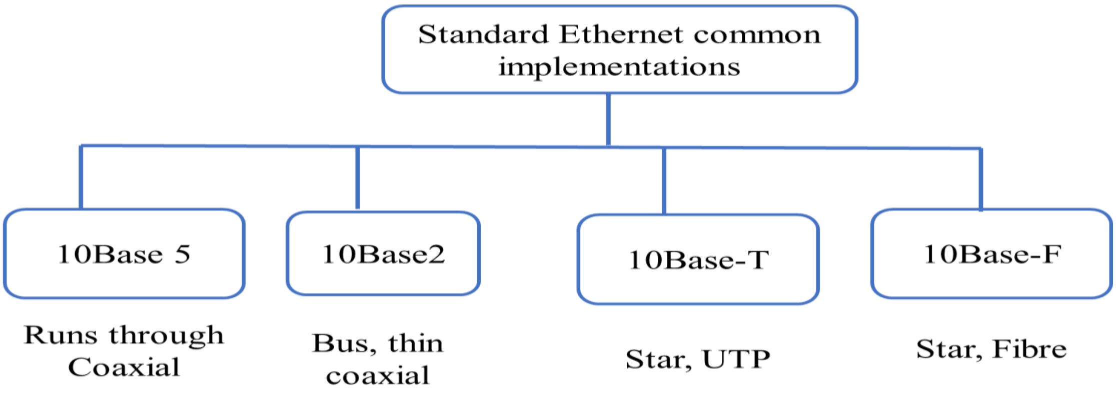


Fig.3.52. Standard Ethernet common implementations.

10Base5: Thick Ethernet

1. This is the first implementation of Ethernet also called as thick net. This is the first Ethernet specification using a bus topology with an external transceiver.
2. The transceiver is responsible for transmitting, receiving, and detecting collisions.
3. The transceiver is connected to the station via transceiver cable that provides separate paths for sending and receiving.
4. Maximum length of the coaxial cable must not exceed 500 metres. The length is more than 500 metres. Excessive degradation of the signal will happen.
5. If we have to connect the cable for more than 500 metres, up to five segments each of the maximum of 500 metres can be connected using repeaters.

10Base1: Thin Ethernet

1. This is the second implementation, and it is also called as thin net or cheaper net. It uses bus topology, but the cable is much thinner and more flexible.
2. The cable can pass very close to stations And the transceiver is normally a part of the network interface card (NIC).
3. Collision here occurs in the thin coaxial cable. This is a cost-effective implementation of

10base5 and tee connexions are much cheaper than tabs.

4. Installation of this is simple. And the length and length of each segment cannot exceed 185 metres due to high level of attenuation in thin coaxial cable.

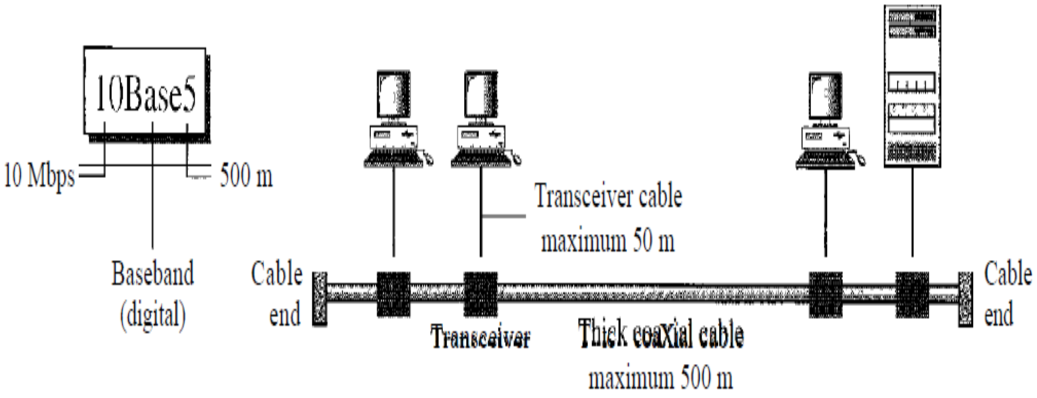


Fig.3.53. 10Base5 implementations.

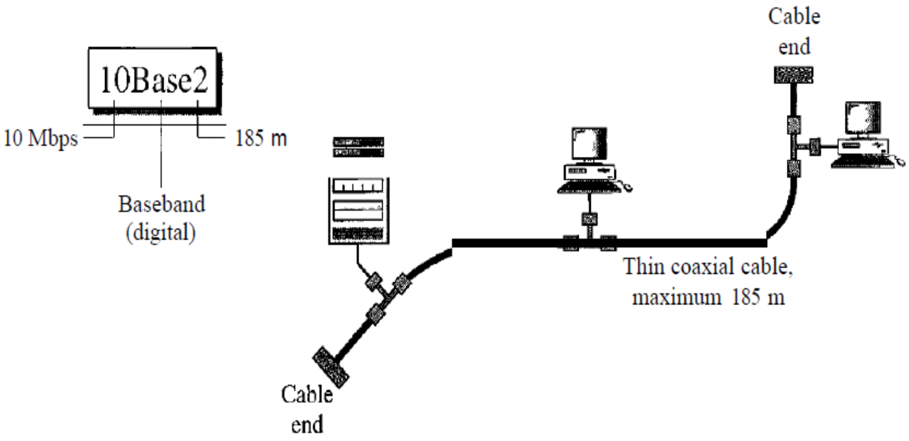


Fig.3.54. 10Base2 implementations.

10Base-T: Twisted -pair Ethernet

1. 10Base-T or twisted pair Ethernet uses a physical start topology. The connect the stations are connected to a hub via two pairs of twisted pair cable.
2. The two pairs of twisted pair cable create two parts between the station and the hub Any collisions happened in the club compared to 10Base5 or 10Base2.
3. The maximum length of twisted pair cable is defined as 100 metres.

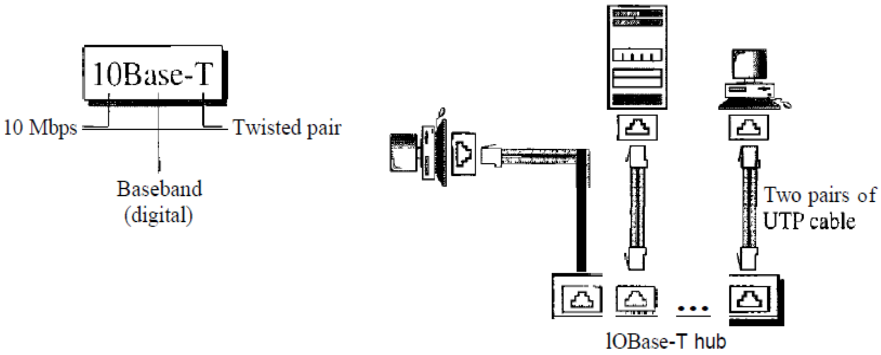


Fig.3.55. 10Base-T implementations.

10Base-F Fiber Ethernet

1. The most common fibre Internet is called 10Base-F. 10Base-F uses a star topology to connect stations to a hub.
2. The stations are connected to a hub using two fibre optic cables, as shown in the figure below.

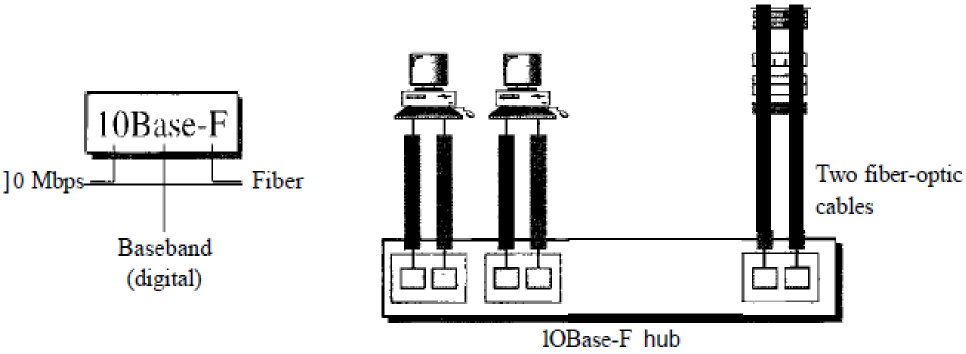


Fig.3.55. 10Base-F implementations.

Table 3.1: Summary of standard Ethernet implementations.

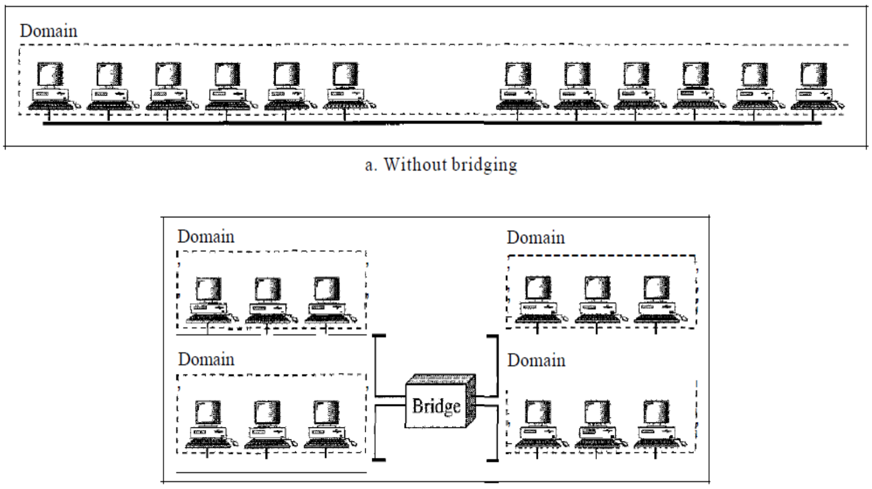
Characteristics	10Base5	10Base2	10Base-T	10Base-F
Media	Thick coaxial cable	Thin coaxial cable	2UTP	2Fiber
Maximum length	500m	185m	100m	2000m
Line encoding	Manchester	Manchester	Manchester	Manchester

3.7.1 Changes in standard ethernet

The standard Ethernet has gone through several changes which has opened a road to the revolution of Internet such that it became compatible with other high data rate LANs. The first step in the Internet evolution was of division of LANs by use of bridges. Bridges have two advantages: 1. Raise the bandwidth and 2. Separate collision domains.

In a unbridged Ethernet, the total capacity of the bandwidth is shared among all the stations. The total capacity is used by anyone station while sending the frames. If more than one station needs to use the network, the capacity is shared. Abridge divides the network into two or more networks. Bandwidth wise, each network is independent.

As shown in the figure below, the network of 12 stations is divided into two parts, each of six stations. Now both the stations have same capacity of bandwidth for example 10Mbps. In this network each station is offered 10/6 Mbps assuming that traffic is not going through the bridge. As the networks are divided the size of the collision domain are reduced and collision also are reduced.



a. Without bridging

b. With bridging

Fig.3.56. Example of network without and with bridges respectively.

The ethernet is then extend to a switched network where we can use network switches having N number of ports. Here the collision domain is divided into N number of domains. This evolution has opened a way to an faster ethernet. The limitation of 10Base5 and 10Base2 is that they are half-duplex networks where a station can either send or receive. The full duplex mode has increased the capacity of a switched network.

3.7.2 Fast ethernet

1. Designed to compete with land protocols such as FDDI.
2. IEEE created fast Internet under the name 802.3u.
3. Fast in the nut is backward compatible with standard Ethernet but can transmit data 10 times faster the rate of 100 Mbps.

4. Has the data rate of 100 Mbps.
5. Compatible with standard Ethernet.
6. Same frame format as of standard Internet.
7. Same minimum and maximum frame length as of standard Ethernet.
8. New feature added in the fast development is called auto negotiation. Auto negotiation helps the devices to negotiate the mode of data rate of operation.
9. It helps to allow incompatible devices to connect to one another.
10. Allow one device to have multiple capabilities.
11. Allow a station to cheque a hub’s capabilities.

Manchester Encoding needs 200Mbaurd bandwidth for a data rate of 100 Mbps. Past Ethernet designers alternative encoding and decoding scheme. They used three different encoding schemes. They use a different block coding and line coding techniques.

Characteristics	lOOBase- TX	lOOBase-FX	100Base-T4
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100m	100m	100m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

Common Fast ethernet implementations

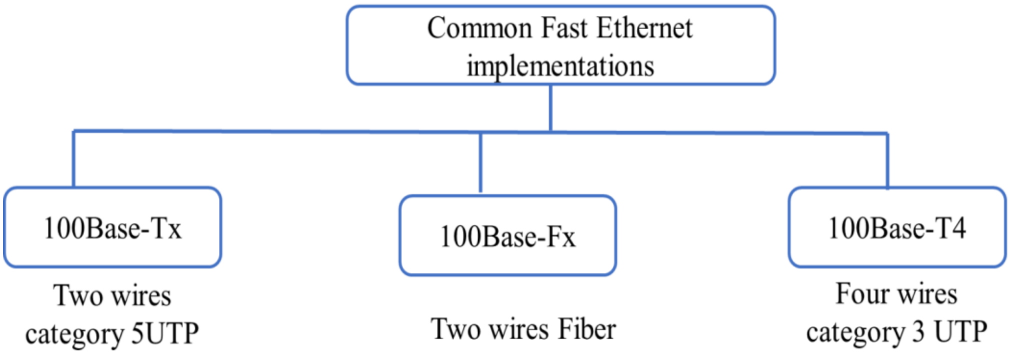


Fig.3.56. Common implementations of fast ethernet.

3.7.3 Gigabit ethernet

1. The need for higher data rates has resulted in the design of Gigabit Ethernet protocol.
2. IEEE committee calls it as standard 802.3z.
3. Data rate is increased to 1Gbps.
4. It is compatible with standard or fast ethernet.
5. Use the same frame format.

6. Same minimum and maximum frame lengths.
7. Supports auto negotiation as defined in fast Internet.

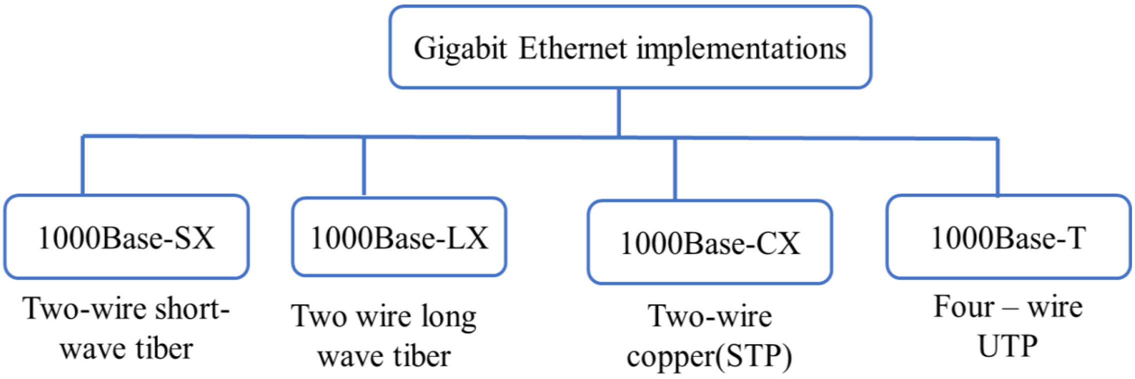


Fig.3.56. Common implementations of gigabit ethernet.

Characteristics	1000Base-SX	1000Base-LX	1000Base-CX	1000Base-T
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550m	5000m	25m	100m
Block encoding	8B/10B	8B/l0B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

3.7.4 Ten-Gigabit Ethernet

The IEEE committee created Ten-Gigabit Ethernet and called it Standard 802.3ae. The goals of the Ten-Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast, and Gigabit Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. Allow the interconnection of existing LANs into a metropolitan area network (MAN) or a wide area network (WAN).
7. Make Ethernet compatible with technologies such as Frame Relay and ATM.

Characteristics	10GBase-S	10GBase-L	10GBase-E
Media	Short-wave S50-nrn multi-mode	Long-wave 131O-nrn single mode	Extended 1550-mrn single mode
Maximum length	300m	10km	40km

3.8. Protocol Data Unit

Protocol data unit (PDU) is a term which represents a unit of inforamtion to be delivered among different peers in a network. It has information such as source and destination addresses, use data, and protocol-control information. For example, a bridge has a bridge protocol data unit (BPDU). These PDUs have different names in different layers of OSI model.

PDU in physical layer is called as bits. (smallest)
PDU in data link layer is called as frames.
PDU in network layer is called as packets.
PDU in transport layer is called as segments.
PDU in session, presentation and application layer is called data.(largest)

Summary

This chapter concentrates on the functions of data link layer. It addresses the framing, flow control, error detection and correction control mechanisms and access control protocols. All the protocols of flow and access control has been delt extensively to have good knowledge of link layer functions in OSI model. One of the important functions of link layer – node-to-node delivery is clearly explained in this chapter. Physical layer address or medium access address and its structure is also given here.

Self-assessment Questions

1. What is the primary purpose of data link layer?
a. Note to note delivery.
b. Device to device communication.
c. Communicate between different networks.

2. Differentiate between logical link layer (LLC) and media access control (MAC) sub layers.
3. What is the significance of fame delimiter in data frame?
4. What is the significance of flow control in data link layer?
5. State the purpose of frame cheque sequence (FCS) in data frame.
6. What is maximum transfer unit MTU? And how does it relate to the linked data link layer.
7. List the key responsibilities of data link layer?
8. Why is stop and weight protocol called as automatic repeat request?
9. Describe the concept of parity in error detection
10. Explain the concept of redundancy in error correction.
11. How is burst error correction different from random error correction?
12. What is the significance of receiver window in flow control.
13. How does selective repeat differ from Go-back-N flow control.
14. What are the differences between flow control and connexion oriented in connectionless

communication.
15. Describe the role of sliding window size in flow control.
16. Discuss the relationship between flow control and quality of service.
17. How do flow control mechanisms address the issue of out of order Packet delivery?
18. Explain the concept of channel access in MAC protocols.
19. Compare CSMA/CA and carrier sense multiple axis with CSMA/CD.
20. Differentiate between fixed and random access protocols.
21. Differentiate between Unicast Multicast and broadcast mac addresses.
22. What is interframe time and give its importance?
23. Explain the concept of dynamic channel location in MAC protocols.

24. Which of the following are 100BaseT cable types?
a) CAT 3 b) CAT 5 c) CAT5e d) 10Base FL

25. What is the physical limit for the number of ports on an Ethernet hub?
a) 24 b) 256 c) 512 d) 1024

26. When a network device can only send data or receive data, but not both at the same time, it is operating in what mode?
a) Duplex b) Fill-duplex c) Half-duplex

27. What important backbone technology is also known as Gigabit Ethernet?
a) 100BaseT b) 100BaseFL c) 100BaseFX d) 1000BaseT

28. What are the two major UTP variations of Fast Ethernet?
a) 100BaseTL b) 100BaseTX c) 100BaseFX d) 100BaseT4

29. What are the limitation of Fast Ethernet over UTP?
a) Distance is restricted to 100 meters from node to hub.
b) Shielding may be inadequate for some installations.
c) Intrusion from outsiders may be possible without detection.
d) The obsolete technology is insufficient for most networks.

30. Which standard defines Fast Ethernet using fiber cabling?
a) 10BaseFL b) 100BaseFX c) 100BaseT4 d) 100BaseTX

31. Which of the following are fiber connector types?
a) LC b) LS c) MR-RJ d) ST

32. What do you need to connect varying 10 GbE cable types to the same router?
a) SFF connectors on all cables
b) SC connectors on all cables
c) Multisource agreements on the router

d) This is not possible

33. Which standard defines Gigabit Ethernet over twisted-pair copper wire?
a) 802.3ab
b) 802.3e
c) 802.3GbUTP
d) 802.3z

34. You’ve lost the manual to your router. How can you tell the difference between a 1000BaseT port and a 100BaseT port on a router just by looking?
a) The 1000BaseT ports are noticeably larger.
b) The 100BaseT ports are green, whereas the 1000BaseT ports are gray.
c) 1000BaseT ports are reversed with the clip on the top.
D) You can’t tell the difference by looking. They look exactly the same.

35. Which statement about Ethernet is correct?
a) Only 10- and 100-megabit Ethernet may use a hub. Gigabit Ethernet must use a switch.
b)10- and 100-megabit Ethernet has a limit of 1024 nodes. Gigabit Ethernet has no limit.
c) Gigabit Ethernet that uses UTP cabling has a maximum distance between the node and switch of 250–400 meters, depending on the manufacturer.
d) All versions of 10 Gigabit Ethernet use the same cabling.

36. What will happen if you connect a 10BaseT NIC to an auto-sensing switch?
a) The switch will operate in hub mode.
b) The entire switch will operate at 10 megabits, even if 100-megabit devices are attached.
c) The 10BaseT NIC will operate at 10 megabits while connected 100-megabit devices will operate at their full speed of 100 megabits.
d) The 10BaseT NIC will overclock to run at 100 megabits.

37. What benefit does full-duplex offer?
a) It allows all NICs on a hub to send signals at the same time without collisions.
b) It doubles the bandwidth of the network.
c) It doubles the speed of the network.
d) It doubles both the bandwidth and the speed of the network.

38. What is the difference between the R and W designations in 10GBase standards, such as 10GBaseLR and 10GBaseLW, or 10GBaseER and 10GBaseEW?
a) The R indicates “regular," or half-duplex. The W indicates “wide mode," which is the 10 Gigabit Ethernet version of full-duplex.
b) The R indicates “read," or the ability to receive signals; the W indicates “write," or the ability to send signals.
c) The R and W indicate differences in the circuitry, with the W versions used to connect to SONET equipment.

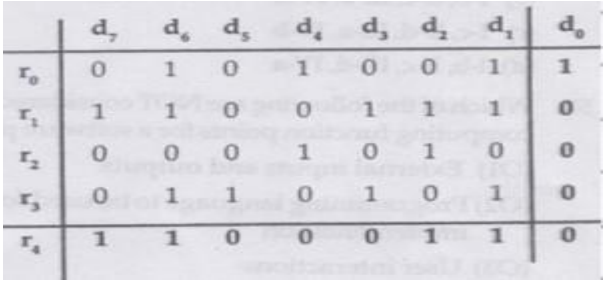
d) The R indicates the use of UTP, whereas the W indicates the use of fiber optics.

Terminal Questions.

1. What is the purpose of Network Interface Card?
2. What are Virtual LANs?
3. State the difference between Fast Ethernet and Gigabit Ethernet
4. What are the responsibilities of data link layer?
5. What are the functions of MAC?
6. What are the functions of LLC?
7. What is Ethernet?
8. Define Bluetooth.
9. Why Ethernet is said to be 1-persistent protocol?
10. Define flow control.
11. What is a buffer?
12. Mention the categories of flow control.
13. What is the function of stop and wait flow control?
14. Mention the advantage and disadvantage of stop and wait f low control.
15. Define ARQ.
16. Mention the function of go-back N-ARQ.
17. What is selective reject ARQ?
18. Define HDLC.
19. List the types of stations is HDLC.
20. What is meant by bit stuffing?
21. What is piggy backing?
22. What are the responsibilities of data link layer?
23. Mention the types of errors.
24. Define physical addressing.
25. Define Single bit error.
26. Define Burst error.
27. What is redundancy?

Problems:

1. Data transmitted on a link uses the following 2D parity scheme for error detection: Each sequence of 28 bits is arranged in a 4×7 matrix (rows r_0 through r_3, and columns d_7 through d_1) and is padded with a column d_0 and row r_4 of parity bits computed using the Even parity scheme. Each bit of column d_0 (respectively, row r_4) gives the parity of the corresponding row (respectively, column). These 40 bits are transmitted over the data link.



	d_7	d_6	d_5	d_4	d_3	d_2	d_1	d_0
r_0	0	1	0	1	0	0	1	1
r_1	1	1	0	0	1	1	1	0
r_2	0	0	0	1	0	1	0	0
r_3	0	1	1	0	1	0	1	0
r_4	1	1	0	0	0	1	1	0

2. Given below is a series of 7 7-bit items of data, with an additional bit each and an extra byte to account for parity.

1	1	1	0	1	1	0	
1	1	0	1	0	1	0	
0	1	1	1	1	1	0	
0	1	1	1	1	1	0	
1	1	0	0	0	1	0	
0	0	1	0	1	0	1	
1	1	0	0	0	0	0	

3. A bit stream 1101011011 is transmitted using the standard CRC method. The generator polynomial is x^4+x+1. What is the actual bit string transmitted?

4. A bit stream 10011101 is transmitted using the standard CRC method. The generator polynomial is x^3+1.

1. What is the actual bit string transmitted?
2. Suppose the third bit from the left is inverted during transmission. How will receiver detect this error?

5.Consider the message sender wants to send is 1010001101, and the generator polynomial is $x^5+x^4+x^2+1$. Find the message transmitted by the sender. If the receiver receives the message, check if the receiver receives the correct message or not.

6. Consider the cyclic redundancy check(CRC) based error detecting scheme having the generator polynomial x^3+x+1 Suppose the message $m_4m_3m_2m_1m_0$ = 11000 is to be transmitted. Check bits $c_2c_1c_0$ are appended at the end of the message by the transmitter using above CRC scheme. Find $m_4m_3m_2m_1m_0c_2c_1c_0$.

Chapter 4: Network layer and Inter-networking

The Network Layer is a critical component of the networking architecture, responsible for the efficient and reliable transportation of data across different networks. It operates at the third layer of the OSI model and plays a fundamental role in routing and forwarding data packets from the source to the destination, regardless of the underlying physical network infrastructure. At the Network Layer, data packets are encapsulated with logical addresses, such as IP (Internet Protocol) addresses, which uniquely identify devices within a network. These addresses facilitate the proper delivery of data across interconnected networks, allowing seamless communication between devices and hosts.
Inter-networking, often referred to as internetworking or simply "the internet," is the practice of connecting multiple individual networks into a larger, cohesive network infrastructure. It is a vital concept that has revolutionized modern communication, enabling seamless data exchange and collaboration on a global scale.Inter-networking brings together networks of various types, sizes, and geographical locations, allowing devices connected to these networks to communicate with each other, regardless of their physical location or underlying technology. The internet, as the most prominent example of inter-networking, enables users to access information, services, and resources from anywhere in the world.

Topic 1: Networking and Internetworking devices

Mainly focuses on networking and internetworking devices used in computer networks. Participants will gain an understanding of various devices such as routers, switches, hubs, and bridges, and their roles in network infrastructure. The session will cover the functions, features, and configurations of these devices, along with their advantages and limitations. Additionally, practical demonstrations and case studies will be presented to illustrate how these devices are used to create efficient and reliable network architectures. Participants will also learn about emerging trends and technologies in networking devices.

Internetworking

The word “internetworking,” which combines the words “inter” and “networking,” denotes a connection between completely distinct nodes/segments. Internetwork could be a collection of several networks that operate as a single large network and are connected by intermediate networking devices. The OSI-ISO model’s Layer 3 (Network Layer) enforces internetworking. The internet is the most prominent famous example of internetworking. Every network node or phase is built using a similar protocol or a communication logic, such as TCP (Transfer Control Protocol) or IP (Internet Protocol), to enable communication. It is referred to as “internetworking” when a network interacts with another network using ongoing communication protocols.

TYPES OF INTERNETWORKING

Internetworking primarily consists of three units:. Extranet, Internet, and Intranet

Extranet

It’s a network of the internetwork with a confined scope to one organisation or institution but with limited links to one or more other networks on occasion. It is the lowest degree of internet usage and is typically prohibited in extremely private areas. An extranet may also be referred to as a MAN, WAN, or another type of network, but it cannot include a single local area network; rather, it must make at least one mention of an external network.

Internet

Internet is a specific internetworking that connects governmental, academic, public, and private networks on a global scale. It is based on the ARPANET, which was created by the ARPA (Advanced Research Projects Agency) of the U.S. Defense Department. It is also the location of the World Wide Web (WWW) and is referred to as the "Internet" to distinguish it from other generic internetworking. Internet users and their service providers utilise IP addresses obtained from address registries that control assignments.

Intranet

This computer network can be a collection of interconnected networks that employ the Internet Protocol and IP-based software like web browsers as well as FTP tools, all of which are controlled by a single body entity. This body entity blocks access to the computer network for the rest of the world and only allows a select few users. This network most frequently refers to the internal network of a business or other enterprise. To provide users with browseable data, a large computer network can typically have its own internet server.

NETWORK DEVICES

Components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines. It is basically used to setup a Local Area Network (LAN). Some expels of Network Devices are Repeater, Hub, Bridge, Switch, Routers, Gateway, and NIC

Repeater –
A repeater operates at the physical layer.
Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.
An important point to be noted about repeaters is that they do not amplify the signal.
When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting if original strength.
It is a 2-port device.

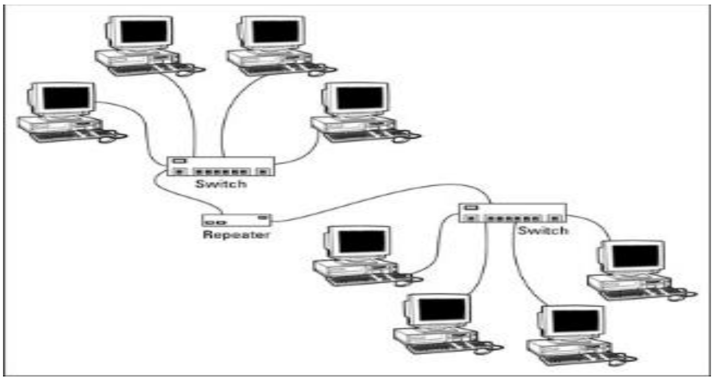


Fig 1.1 Connection with Repeater

Hub –

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

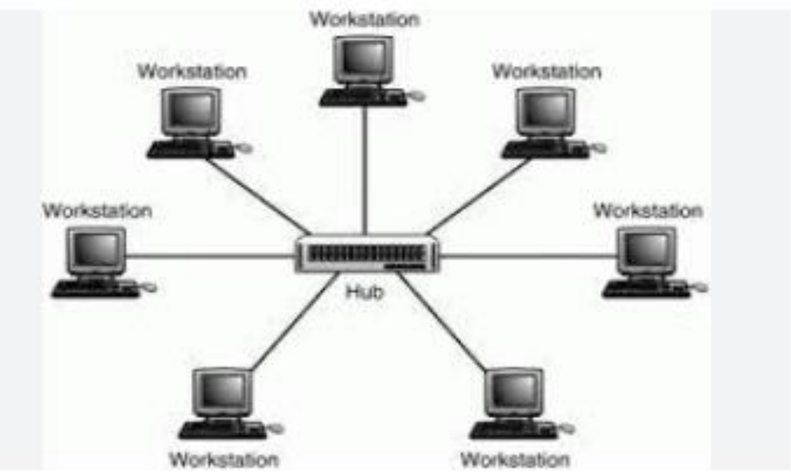


Fig 1.2 Connection with Hub

Types of Hubs

Active Hub:-
These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network.
It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

Passive Hub:-
These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.

Intelligent Hub:-
It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Bridge –
A bridge operates at the data link layer.
A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
It is also used for interconnecting two LANs working on the same protocol.
It has a single input and single output port, thus making it a 2 port device.

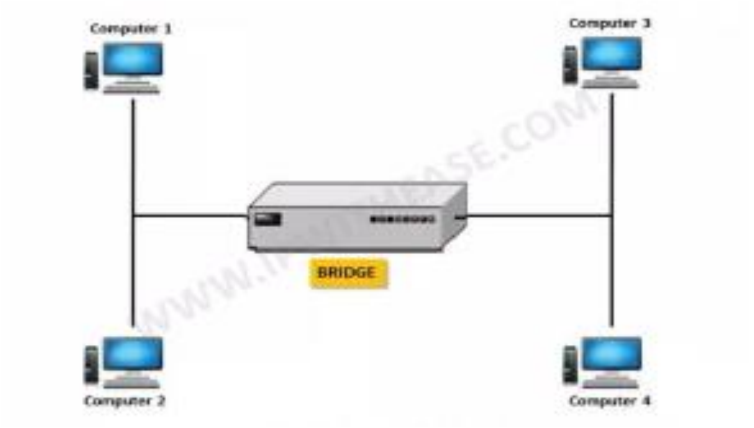


Fig 1.3 Connection with a Bridge

Types of Bridges
Transparent Bridges:-
These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary.
These bridges make use of two processes i.e. bridge forwarding and bridge learning.

Source Routing Bridges:-
In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Switch –
A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
A switch is a data link layer device.
The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.
In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

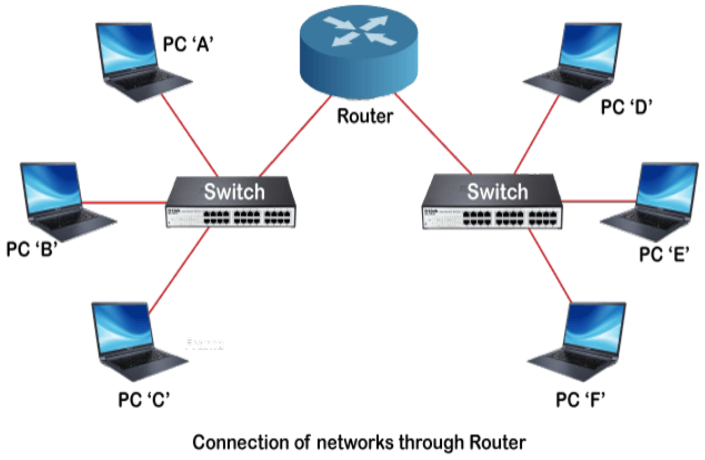


Fig 1.4 Connection with Switch

Routers –

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

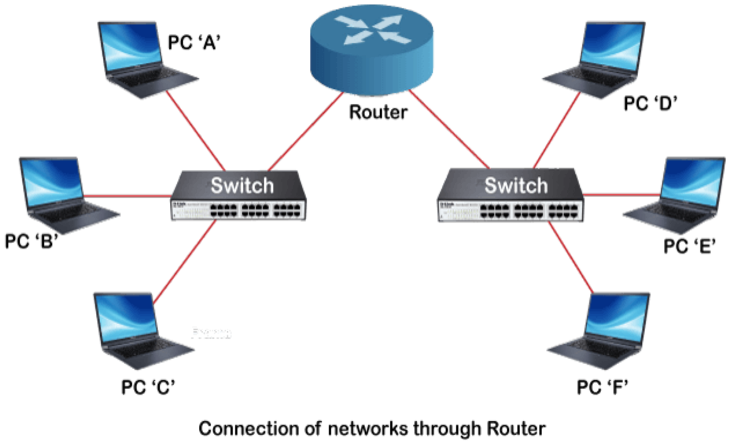


Fig 1.5 Connection with Router

Gateway –

A gateway, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

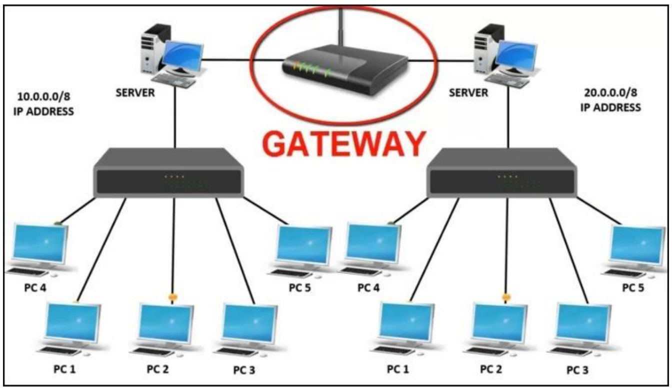


Fig 1.6 Connection with Gateway

NIC –

NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

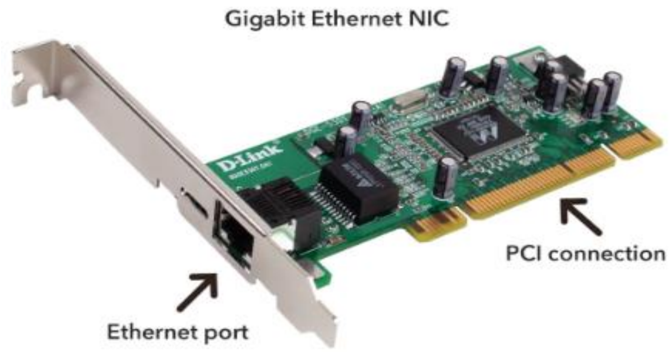


Fig 1.7 NIC Card

SAQ’s Self-Assessment Questions

What is the function of Network Interface Cards?
connects the clients, servers and peripherals to the network through a port
allows you to segment a large network into smaller, efficient networks
connects networks with different protocols like TCP/IP
boost the signal between two cable segments or wireless access points

A device that connects networks with different protocols –
Switch
Hub
Gateway
All of these

A device that is used to connect a number of LANs is?
Router
Repeater
Bridge
All of these

Which networking device connect one LAN to other LAN using same protocol?
Router
Switch
Bridge
Modem

5. Which device operates at the physical layer of the OSI model?
a) Hub
b) Switch
c) Router
d) Bridge

6. Which device operates at the data link layer of the OSI model?
a) Router
b) Modem
c) Bridge

d) Repeater

7. Which device is used to connect multiple network segments together?
a) Hub
b) Modem
c) Router
d) Switch

8. Which device examines the destination IP address of a packet to determine the best path for forwarding?
a) Hub
b) Router
c) Bridge
d) Switch

9. Which device operates at both the network layer and the data link layer of the OSI model?
a) Hub
b) Router
c) Modem
d) Switch

10. Which device is used to connect a local area network (LAN) to the internet?
a) Hub
b) Modem
c) Router
d) Bridge

11. Which device amplifies and regenerates signals to extend the length of a network segment?
a) Hub
b) Switch
c) Router
d) Repeater

12. Which device enables communication between different networks using different protocols?
a) Hub
b) Switch
c) Router
d) Bridge

13. Which device operates at the transport layer of the OSI model?
a) Modem
b) Switch
c) Router
d) Firewall

14. Which device is used to create a wireless network?
a) Hub
b) Switch

c) Router
d) Access point

15. Connecting two or more networks to form a single network is called :
a) Internetworking
b) Intranetworking
c) Interconnecting
d) Intraconnectivity

16. NIC stands for____.
network interface card
network identity card
network interface control
none of the above
17. ETHERNET card consists of ____bus.
PCI
DIP
MAC
NIC

18. Repeater is Amplifier?
true
false
19. Identify the correct statement.
statement-1: Hub is the unicasting device.
statement-2: Network switch is the broadcasting device.
statement-1 is true,statement-2 is true
statement-1 is true,statement-2 is false
statement-1 is false,statement-2 is true
statement-1 is false,statement-2 is false
20. Which router is created table automatically?
dynamic
static
simplex
None of the above

Terminal Questions

What is the difference between a router and a switch? Explain their respective functions in a computer network.
How does a firewall work, and what are its primary roles in network security?
List all the network interfaces currently active on your system.
Display the routing table of your system.
Check the MAC (Media Access Control) address of a specific network interface.
Describe the principles of working of a Hub
Explain the difference between Hub and Switch

Answer Keys:

1. a	2. c	3. a	4. b	5. d	6. c	7. d	8. b	9.	10. c

								b	
11. d	12. c	13. d	14. d	15. a	16. a	17. a	18. a	19. c	20. a

Summary:

The Network Layer is a critical part of the networking architecture, operating at the third layer of the OSI model. Its primary function is to ensure efficient and reliable data transportation across different networks. This layer is responsible for logical addressing, assigning unique IP addresses to devices on a network to enable end-to-end communication. It also handles routing, determining the best path for data packets to reach their destinations, and forwarding, transferring data packets from one network device to the next along the selected route. Additionally, the Network Layer performs fragmentation and reassembly, breaking large data packets into smaller fragments for transmission and reassembling them at the destination. Error handling mechanisms are also implemented to detect and manage errors that may occur during data transmission. The Network Layer plays a pivotal role in inter-network communication, enabling the seamless flow of data across various interconnected networks to create a vast global network, such as the internet. Inter-networking devices are fundamental components that facilitate the connection and communication between multiple individual networks, creating a cohesive network infrastructure.

Topic 2: IP Addressing

This module will provide a comprehensive overview of IP addressing in computer networks. Participants will learn about the structure and format of IP addresses, including IPv4 and IPv6. The session will cover topics such as IP address classes, subnetting, and supernetting. Participants will gain an understanding of how IP addresses are assigned, the role of subnet masks, and the concept of network and host addresses. The session will also discuss dynamic IP addressing, DHCP (Dynamic

Host Configuration Protocol), and NAT (Network Address Translation). Practical examples and hands-on activities will be included to reinforce the concepts and allow participants to practice IP addressing configuration. By the end of the session, participants will have a solid understanding of IP addressing and be equipped to design and manage IP-based networks effectively.

IP ADDRESS:
IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}.

VERSIONS:
There are basically 2 versions of IP Address such as IP version-4 (IPv4) and IP version-6 (IPv6)

ADDRESS SPACE:
A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses *N* bits to define an address, the address space is *2N* because each bit can have two different values (0 or 1) and *N* bits can have *2N* values. IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

NOTATIONS:
Generally, there are three notations in which IP address is written
Dotted decimal notation
Binary Notation
Hexadecimal notation.

Dotted-Decimal Notation
To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted-decimal notation of the above address:
117.149.29.2

As each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

Binary Notation
In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:
01110101 10010101 00011101 00000010

Figure below shows an IPv4 address in both binary and dotted-decimal notation.

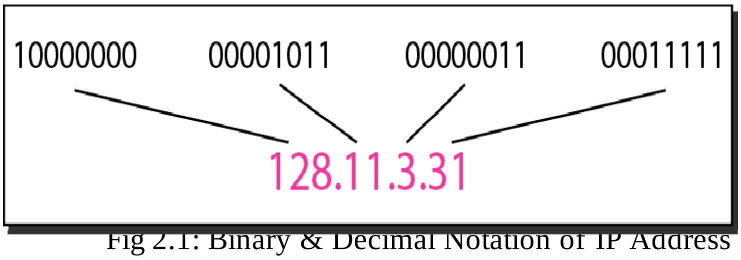


Fig 2.1: Binary & Decimal Notation of IP Address

Hexadecimal Notation
Sometimes an IPv4 address can be denoted in hexadecimal notation. Each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits. This notation is

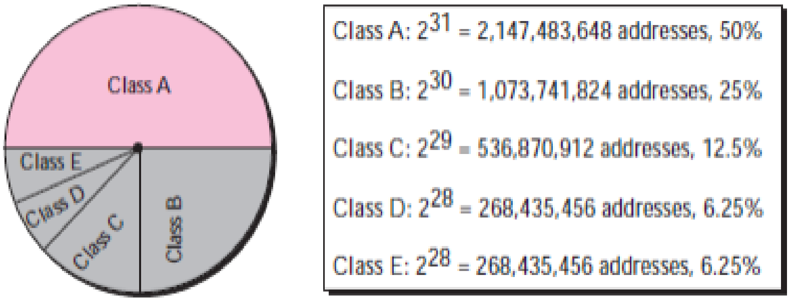
often used in network programming.
Example: 10000001 00001011 00001011 11101111
Hexadecimal notation is: $810B0BEF_{16}$

CLASSFUL ADDRESSING:

IP addresses, when started a few decades ago, used the concept of classes. This architecture is called classful addressing. In the mid-1990s, a new architecture, called classless addressing, was introduced that supersedes the original architecture. Now we introduce classful addressing because it paves the way for understanding classless addressing and justifies the rationale for moving to the new architecture.

Classes

In classful addressing, the IP address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the whole address space. Figure below shows the class occupation of the address space.



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

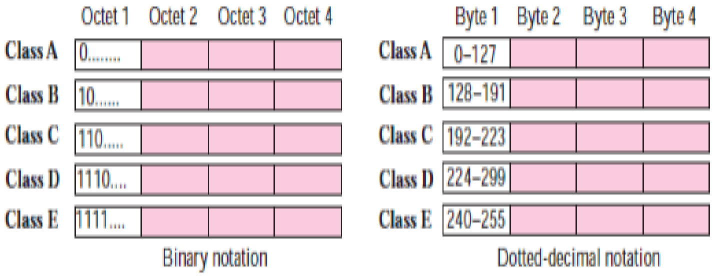
Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Fig 2.2: Address Space for each Class of IP Address

Recognizing Classes

We can find the class of an address when the address is given either in binary or dotted-decimal notation. In the binary notation, the first few bits can immediately tell us the class of the address; in the dotted-decimal notation, the value of the first byte can give the class of an address



	Octet 1	Octet 2	Octet 3	Octet 4
Class A	0........			
Class B	10......			
Class C	110.....			
Class D	1110....			
Class E	1111....			

Binary notation

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–299			
Class E	240–255			

Dotted-decimal notation

Fig 2.3: Recognizing IP Address from both Binary and Decimal Notation

Netid and Hostid

In classful addressing, an IP address in classes A, B, and C is divided into netid and hostid. These parts are of varying lengths, depending on the class of the address. Figure below shows the netid and hostid bytes. But classes D and E are not divided into netid and hostid, for reasons that we will discuss later.

In class A, 1 byte defines the netid and 3 bytes define the hostid. In class B, 2 bytes define the netid and 2 bytes define the hostid. In class C, 3 bytes define the netid and 1 byte defines the hostid.

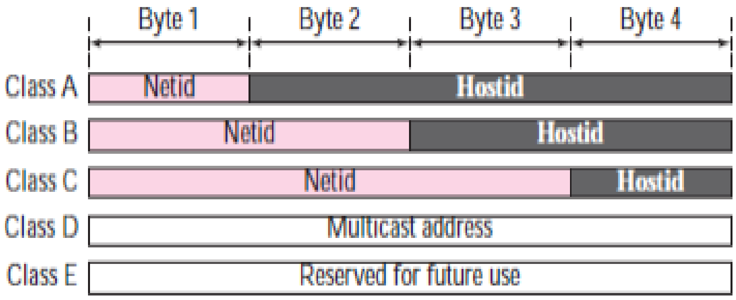


Fig 2.4: Net ID & Host ID in IP Address

Casting

Transmitting the data in the form of packets over the internet is called casting.

Types of Castings

The different types of casting are as follows –

Unicast – Transmitting data from one host to another host (one-one)

Broad cast – Transmitting data from one host to many host (one-all)

Multicast – Transmitting data from one host to a particular group of host (one-many).

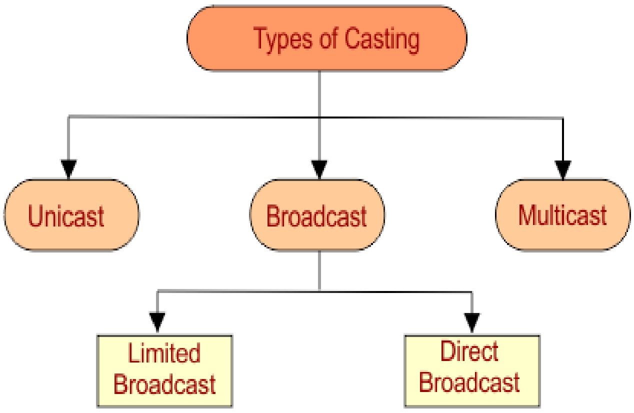


Fig 2.5: Types of Casting

Unicast

Transmitting data from one source host to one destination host is called a unicast. It is called as a one to one transmission

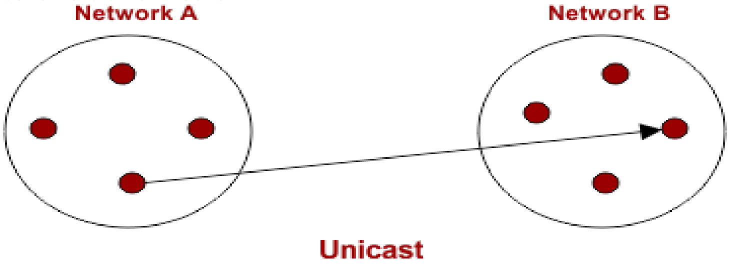


Fig 2.6: Unicasting

For example – source Host IP Address 192.168.20.1 sending data to destination Host having IP Address 192.122.140.34

Broadcast

Transmitting data from one source host to all other hosts present in the same or other network is called broadcast. It is called a one to all transmission.

Broadcast is classified into two types, which are as follows −

Limited Broadcast − Transmitting data from one source host to all other hosts present in the same network is called a limited broadcast.

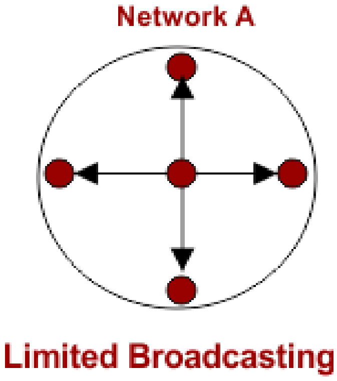


Fig 2.7: Broadcasting

In Limited Broad casting if the destination address is 255.255.255.255 then the packet will be sent to all the hosts in the network.
Limited Broadcast address of any network
=255.255.255.255
= 11111111.11111111.11111111.11111111
For example − If the source IP address is 12.23.2.5 sending data to all other hosts present in the same network, then the destination address is 255.255.255.255.

Direct Broadcast − Transmitting data from source host to all other hosts present in different networks then it is called as direct broadcast.

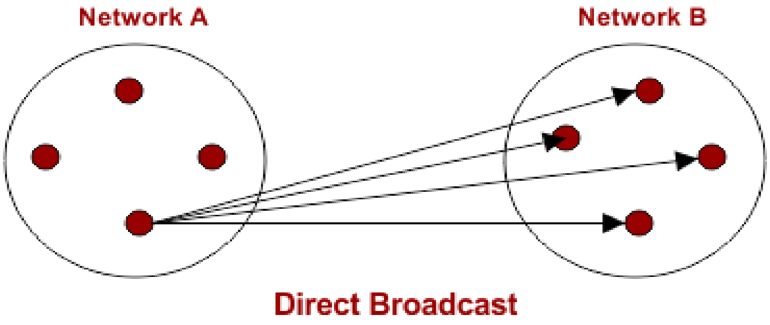


Fig 2.7.1: Direct Broadcasting

In direct broadcast Host ID bits are all set to 1, Network ID is the IP address where all destination hosts are present.
For example − Source IP address is 12.34.5.6 sending data to all other nodes present at different network having IP address 24.0.0.0
Therefore source address= 12.34.5.6
Destination address= 24.255.255.255.
Multicast
Transmitting data from one source host to a particular group of hosts that are interested in receiving the data is called Multicast. It is also called one to many transmissions.

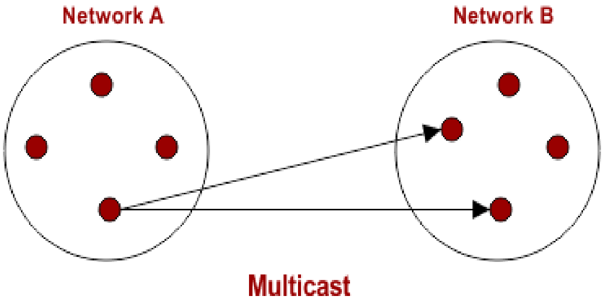
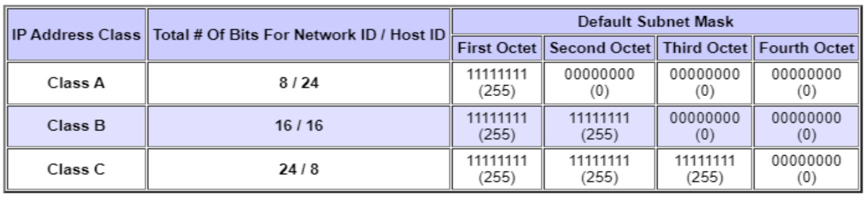


Fig 2.8: Multicasting

For example – Sending messages on whatsapp to particular groups, video conferences, and sending email to groups of people.

MASK

A mask is a four-octet number used to identify the network ID portion of a 32-bit IP address. It is made of contiguous 1's followed by contiguous 0's. A default mask is based on the IP address classes.
As for Class A, 1st octet is for Net-ID and rest 3 octets are for the host ID. So the default mask for Class A will be 255.0.0.0
As for Class B, 1st 2 octets are for Net-ID and rest 2 octets are for the host ID. So the default mask for Class B will be 255.255.0.0
As for Class C, 1st 3 octets are for Net-ID and rest 1 octet is for the host ID. So the default mask for Class C will be 255.255.255.0



IP Address Class	Total # Of Bits For Network ID / Host ID	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8 / 24	11111111 (255)	00000000 (0)	00000000 (0)	00000000 (0)
Class B	16 / 16	11111111 (255)	11111111 (255)	00000000 (0)	00000000 (0)
Class C	24 / 8	11111111 (255)	11111111 (255)	11111111 (255)	00000000 (0)

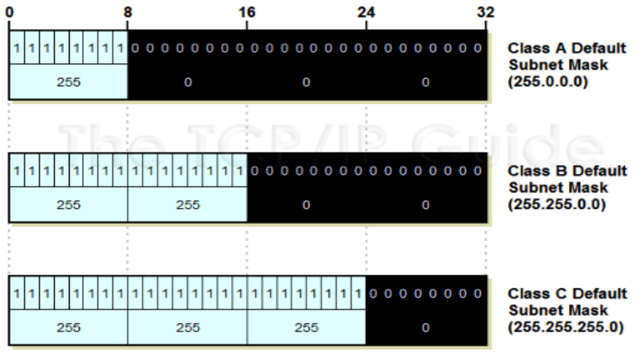

0
8
16
24
32
255
0
0
0
Class A Default Subnet Mask (255.0.0.0)
255
255
0
0
Class B Default Subnet Mask (255.255.0.0)
255
255
255
0
Class C Default Subnet Mask (255.255.255.0)
The TCP/IP Guide

Fig 2.9: Subnet Masks for each Class

CLASSLESS ADDRESSING

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. Here are no classes, but the addresses are still granted in blocks.

Address Blocks

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity.
Restriction: To simplify the handling of addresses, the Internet authorities impose three restrictions on

classless address blocks:
The addresses in a block must be contiguous, one after another.
The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ...).
The first address must be evenly divisible by the number of addresses.

Mask

A better way to define a block of addresses is to select any address in the block and the mask. A mask is a 32-bit number in which the *n* leftmost bits are I's and the 32 - *n* rightmost bits are 0's. However, in classless addressing the mask for a block can take any value from 0 to 32. It is very convenient to give just the value of *n* preceded by a slash (CIDR notation). There are 2 concepts for the CIDR notations.
Prefix Length: The prefix length denotes the number of bits are being used for Net-ID. If the IP address in classless addressing is P.Q.R.S/n then n is the prefix length
Suffix Length: The sufffix length denotes the number of bits are being used for Host-ID. If the IP address in classless addressing is P.Q.R.S/(32-n) then (32-n) is the sufffix length

IP VERSION 6 ADDRESSING

IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2^{128}, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:) .
For example, Below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:
0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011
Each block is then converted into Hexadecimal and separated by ':' symbol:
2001:0000:3238:DFE1:0063:0000:0000:FEFB
Even after converting into Hexadecimal format we can see, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:
Rule.1: Discard leading Zero(es):
In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):
2001:0000:3238:DFE1:63:0000:0000:FEFB
Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):
2001:0000:3238:DFE1:63::FEFB
Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):
2001:0:3238:DFE1:63::FEFB

Need for IPv6:
The primary driver for IPv6 adoption was address depletion as the demand for electronic devices increased rapidly with the advent of the Internet of Things (IOT) after the 1980s. Additional drivers included the need for new options, support for multimedia, and an urgent need for security. The IPv6 protocol addresses the aforementioned problems by making the following key modifications:

1. Large address space

An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.

2. 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.

3. New options

IPv6 has new options to allow for additional functionalities.

4. Support for resource allocation

In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

5. Support for more security

The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Interface ID

IPv6 has three different types of Unicast Address scheme. The second half of the address (last 64 bits) is always used for Interface ID. The MAC address of a system is composed of 48-bits and represented in Hexadecimal. MAC addresses are considered to be uniquely assigned worldwide. Interface ID takes advantage of this uniqueness of MAC addresses. A host can auto-configure its Interface ID by using IEEE's Extended Unique Identifier (EUI-64) format. First, a host divides its own MAC address into two 24-bits halves. Then 16-bit Hex value 0xFFFE is sandwiched into those two halves of MAC address, resulting in EUI-64 Interface ID.

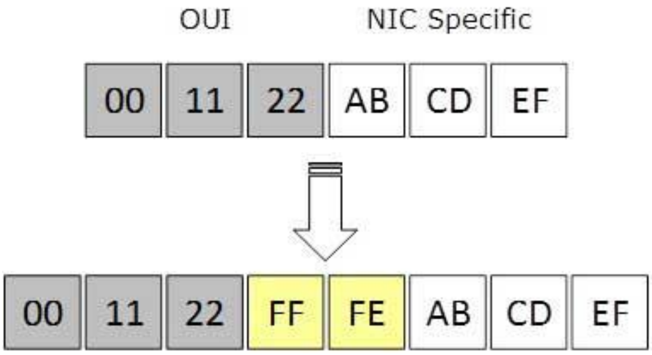


Fig 2.10: Interface ID

Conversion of EUI-64 ID into IPv6 Interface Identifier

To convert EUI-64 ID into IPv6 Interface Identifier, the most significant 7th bit of EUI-64 ID is complemented. For example:

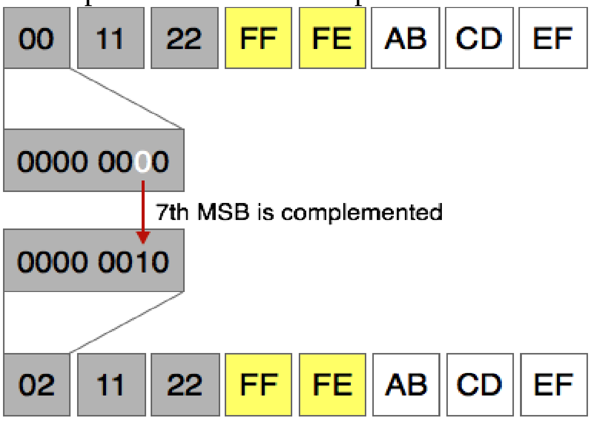


Fig 2.11: Conversion of EUI-64 ID into IPv6 Interface Identifier

Global Unicast Address

This address type is equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.

Global Routing Prefix: The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific autonomous system. The three most significant bits of Global Routing Prefix is always set to 001.

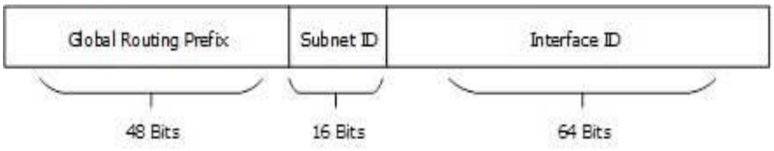


Fig 2.12: Global Unicast Address

Link-Local Address

Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0, thus:

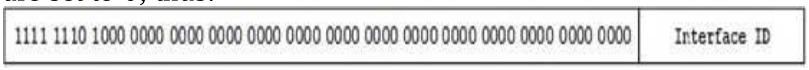


Fig 2.13: Linl-Local Address

Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable, so a Router never forwards these addresses outside the link.

Unique-Local Address

This type of IPv6 address is globally unique, but it should be used in local communication. The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.

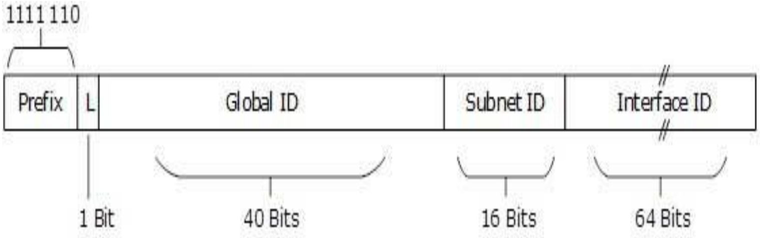


Fig 2.14: Unique-Local Address

Prefix is always set to 1111 110. L bit, is set to 1 if the address is locally assigned. So far, the meaning of L bit to 0 is not defined. Therefore, Unique Local IPv6 address always starts with ‘FD’.

SAQ’s Self-Assessment Questions

What is the format of IP address?
34 bit
64 bit
16 bit
32 bit
The last address of IP address represents?
Unicast address
Network address
Broadcast address
None of the above
What is the size of Host bits in Class B of IP address?
04
08

14
16
What is the usable size of Network bits in Class B of IP address?
04
08
14
16
Which of the following is correct regarding Class A address of IP address?
Network bit – 8, Host bit - 24
Network bit – 7, Host bit - 24
Network bit – 7, Host bit - 23
Network bit – 8, Host bit - 23
Select the wrong class.
CLASS A =1 to 126
CLASS C =192 to 220
CLASS B =128 to 191
CLASS D =224 to 239
Choose the address of class D is
Unicast
Reserved
Multicast
None of the above
Which of the following can be the beginning address of a block that contains 256 addresses?
205.16.37.32
190.16.42.0
17.17.32.0
123.45.24.52
9. Which class of IP address is reserved for multicasting?
a) Class A
b) Class B
c) Class C
d) Class D
10. How many unique IP addresses are possible in IPv6?
a) 2^32
b) 2^64
c) 2^128
d) 2^256
11. Which IPv6 address type is used for link-local communication?
a) Global Unicast Address
b) Link-Local Address
c) Multicast Address
d) Anycast Address
12. What is the loopback address in IPv4?
a) 127.0.0.1
b) 192.168.0.1
c) 172.16.0.1
d) 10.0.0.1

13. What is the purpose of an IP address in a network?
a) To uniquely identify a device on a network
b) To provide access to the internet
c) To determine the physical location of a device
d) To establish secure connections
14. Which subnet mask is associated with a Class C IP address?

a) 255.0.0.0
b) 255.255.0.0
c) 255.255.255.0
d) 255.255.255.255
15. What is the purpose of a default gateway in IP networking?
a) To translate IP addresses into domain names
b) To assign IP addresses dynamically
c) To connect different networks together
d) To resolve MAC addresses to IP addresses
16. Which protocol is used to dynamically assign IP addresses in a network?
a) DNS
b) DHCP
c) ARP
d) TCP
17. IPv6 does not use _________ type of address.
a) broadcast
b) multicast
c) anycast
d) unicast
18. The size of an IP address in IPv6 is _________
a) 4 bytes
b) 128 bits
c) 8 bytes
d) 100 bits
19. Which among the following features is present in IPv6 but not in IPv4?
a) Fragmentation
b) Header checksum
c) Options
d) Anycast address
20. Suppose two IPv6 nodes want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers. The best solution here is ________
a) Use dual-stack approach
b) Tunneling
c) No solution
d) Replace the system

Terminal Questions:

In a block of addresses, we know IP address of one host is 25.34.12.56/16. What is the first address (network address) and the last address (limited broadcast address) in this block?
An ISP is granted a block of addresses starting with 190.100.0.0/16 (65526 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:
The first group has 64 customers; each needs 256 addresses.
The second group has 128 customers; each needs 128 addresses
The third group has 128 customers; each needs 64 addresses.
Design the subblocks and find out how many addresses are still available after these allocations.
Find the block if one of the addresses is 190.87.140.202/29
In a network the address of one computer is 201.78.24.56 and the address of another computer is 201.78.120. 202. How many addresses are in between?
What is the main difference between IPv4 and IPv6?
What are the key advantages of IPv6 over IPv4?
How many bits are used to represent an IPv4 address, and how does that compare to an IPv6 address?

Summary:

IP Addressing is a fundamental concept in computer networking that serves as a unique identifier for devices connected to a network. The Internet Protocol (IP) is the underlying protocol used for communication within the internet and most local area networks (LANs). An IP address consists of a series of numerical values separated by periods and is divided into two parts: the network portion and the host portion. IP Addressing is a cornerstone of modern networking, allowing devices to communicate and exchange data across the internet and local networks. As the number of connected devices continues to grow, the adoption of IPv6 and efficient IP address management practices become crucial to sustain the expansion and evolution of the interconnected world.

Answer Keys:

1. d	2. c	3. d	4. c	5. b	6. d	7. c	8. b,c	9. d	10. c
11. b	12. a	13. a	14. c	15. c	16. b	17. a	18. b	19. d	20. b

Topic 3: Virtual Local Area Network (VLAN)

VLAN

Virtual LAN (VLAN) is a concept where we can logically divide devices into layer 2 (data layer). Generally, Layer 3 devices share a network point, but the network point can be shared by switches using the VLAN concept.

A broadcast domain is a network segment where when a device sends a packet, it is received by all devices in the same broadcast domain. Devices in the same coverage area receive all broadcast packets, but this is limited to switches only, as routers do not forward the broadcast packet. VLAN routing is required to forward packets to different VLANs (from one VLAN to another) or coverage area. A VLAN creates various small-sized subnets that are relatively easy to manipulate.

Benefits of Virtual Local Area Networks (VLANs):

Enhanced Network Security: VLANs allow for logical segmentation of a network, enabling administrators to isolate sensitive data or systems from unauthorized access. By separating network traffic into different VLANs, VLANs provide a layer of security by preventing unauthorized users from gaining access to critical resources.

Improved Network Performance: VLANs help reduce network congestion by limiting broadcast traffic. By dividing a large broadcast domain into smaller VLANs, broadcast storms are contained within a VLAN, preventing them from affecting the entire network. This improves overall network performance and bandwidth utilization.

Simplified Network Management: VLANs provide administrative flexibility by allowing network administrators to manage logical groups of devices based on their function or location. This simplifies network management tasks such as adding, moving, or changing devices within a VLAN, as well as implementing security policies specific to each VLAN.

Scalability and Flexibility: VLANs enable network scalability by accommodating the addition of new devices or users without the need to reconfigure the entire network infrastructure. New devices can be easily assigned to a specific VLAN, and VLANs can be extended across multiple switches or routed to other VLANs as needed.

Improved Resource Sharing: VLANs facilitate resource sharing within specific groups or departments. Devices within the same VLAN can communicate directly with each other without the need for routing, promoting collaboration and efficient sharing of resources such as printers, servers, and applications.

Guest Network Isolation: VLANs allow for the creation of separate guest networks, which are isolated from the main network. This ensures that guest devices have restricted access and cannot interfere with or access internal resources, improving security and maintaining network integrity.

Efficient Troubleshooting: VLANs simplify troubleshooting by isolating network issues to specific VLANs. Network administrators can focus on diagnosing and resolving issues within the affected VLAN without impacting the entire network, leading to quicker problem resolution and reduced downtime.

Quality of Service (QoS) Optimization: VLANs can be used to prioritize network traffic by assigning different QoS policies to specific VLANs. This enables administrators to allocate network resources based on the importance or sensitivity of the traffic, ensuring optimal performance for critical applications and services.

Easy Virtualization Support: VLANs are widely used in virtualized environments, where virtual machines (VMs) can be associated with specific VLANs. This allows for the creation of isolated virtual networks, enabling seamless integration of virtualized resources with the physical network infrastructure.

TYPES OF PORTS IN VLAN

There are two different types of ports in a switched environment.

Access Ports

Trunk Ports.

Access Ports

An *access port* belongs to and carries the traffic of only one VLAN

Traffic is both received and sent in native formats with no VLAN information (tagging) whatsoever.

Anything arriving on an access port is simply assumed to belong to the VLAN assigned to the port.

Because an access port doesn’t look at the source address, tagged traffic

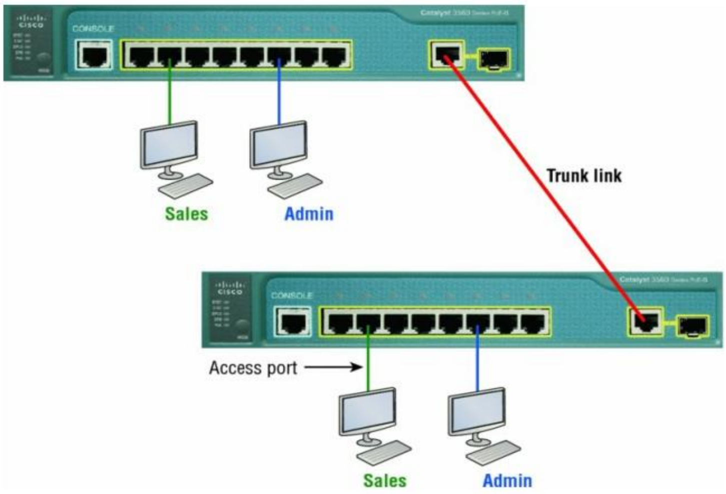
Switches remove any VLAN information from the frame before it’s forwarded out to an access-link device

Access-link devices can’t communicate with devices outside their VLAN unless the packet is routed

Trunk Ports

The term *trunk port* was inspired by the telephone system trunks, which carry multiple telephone conversations at a time. So it follows that trunk ports can similarly carry multiple VLANs at a time as well.

A *trunk link* is a 100, 1,000, or 10,000 Mbps point-to-point link between two switches, between a switch and router, or even between a switch and server, and it carries the traffic of multiple VLANs—from 1 to 4,094 VLANs at a time



VLANs can span across multiple switches by using trunk links, which carry traffic for multiple VLANs

Frame Tagging

Frame tagging in VLANs is a mechanism used to identify and differentiate VLAN traffic within a network. It involves adding additional information to Ethernet frames to indicate the VLAN to which the frame belongs. This tagging is crucial for switches to correctly identify and forward frames to the appropriate VLANs.

The two most commonly used frame tagging standards are IEEE 802.1Q and ISL (Inter-Switch Link).

IEEE 802.1Q Frame Tagging:

IEEE 802.1Q is the industry-standard frame tagging protocol for VLANs.

It adds a 4-byte VLAN tag to the Ethernet frame header.

The VLAN tag contains information such as the VLAN ID (VID), priority, and a few control bits.

The VID is a 12-bit field that represents the VLAN to which the frame belongs.

Switches use the VLAN tag to distinguish between different VLANs and forward frames accordingly.

VLAN tags are added and removed by switches as frames traverse through VLAN-aware network devices.

ISL (Inter-Switch Link) Frame Tagging:

ISL was a proprietary frame tagging protocol developed by Cisco Systems.

It adds a 26-byte ISL header to the Ethernet frame, encapsulating the original frame along with VLAN information.

The VLAN ID is represented by a 10-bit field in the ISL header.

ISL tagging is primarily used in Cisco networking environments, but it has been largely replaced by IEEE 802.1Q due to its standardization and wider industry support.

Frame tagging allows switches to identify frames belonging to specific VLANs, even when multiple VLANs are carried over a single physical link or trunk. When a frame is received by a switch port, the VLAN tag is examined to determine the VLAN membership of the frame. The switch then uses this information to forward the frame to the appropriate ports associated with the corresponding VLAN.

It's important to note that frame tagging is typically used on trunk links that interconnect switches. Access ports, which connect end devices (e.g., computers, printers) to a switch,

typically do not require frame tagging because the connected devices are typically unaware of VLANs and do not include VLAN tags in their frames.
Frame tagging is a fundamental aspect of VLAN implementation, enabling switches to effectively handle traffic separation and VLAN-based network segmentation.

SAQ's-Self Assessment Questions

1. What does VLAN stand for?
   a) Virtual Local Area Network
   b) Very Large Area Network
   c) Virtual LAN
   d) Variable Local Area Network
2. Which layer of the OSI model is associated with VLANs?
   a) Physical layer
   b) Data Link layer
   c) Network layer
   d) Transport layer
3. What is the primary purpose of VLANs?
   a) To increase network speed
   b) To improve network security
   c) To reduce network costs
   d) To segment a large network into smaller logical networks
4. Which device is commonly used to assign VLAN membership?
   a) Switch
   b) Router
   c) Hub
   d) Modem
5. Which protocol is commonly used for VLAN trunking?
   a) VLAN Tagging Protocol (VTP)
   b) Spanning Tree Protocol (STP)
   c) Border Gateway Protocol (BGP)
   d) Internet Protocol (IP)
6. How does VLAN tagging work?
   a) It adds a VLAN identifier to each Ethernet frame.
   b) It encrypts the VLAN traffic for security.
   c) It compresses the VLAN packets for efficient transmission.
   d) It assigns IP addresses to VLAN members.
7. What is a VLAN trunk?
   a) A high-speed connection between VLANs
   b) A physical cable used for VLAN communication
   c) A virtual link between VLANs
   d) A security feature for VLANs
8. Which VLAN type allows a single VLAN to span multiple switches?
   a) Access VLAN
   b) Native VLAN
   c) Trunk VLAN
   d) Extended VLAN
9. Which VLAN type is used to carry management traffic for a specific VLAN across a network?
   a) Access VLAN
   b) Native VLAN
   c) Management VLAN
   d) Voice VLAN
10. Which command is used to assign a port to a VLAN on a switch?
    a) assign vlan

b) set vlan
c) configure vlan
d) switchport access vlan

11. Which VLAN ID is reserved for native VLAN traffic?
a) VLAN 1
b) VLAN 10
c) VLAN 100
d) VLAN 1000

12. Which VLAN type is used to separate voice traffic in a network?
a) Access VLAN
b) Native VLAN
c) Data VLAN
d) Voice VLAN

13. Which spanning tree protocol can be used to prevent loops in a VLAN environment?
a) Rapid Spanning Tree Protocol (RSTP)
b) Border Gateway Protocol (BGP)
c) Open Shortest Path First (OSPF)
d) Dynamic Trunking Protocol (DTP)

14. Which VLAN type is used for untagged traffic on a trunk port?
a) Access VLAN
b) Native VLAN
c) Management VLAN
d) Voice VLAN

15. Which protocol allows VLAN information to be automatically propagated across switches?
a) VLAN Trunking Protocol (VTP)
b) Spanning Tree Protocol (STP)
c) Link Aggregation Control Protocol (LACP)
d) Dynamic Host Configuration Protocol (DHCP)

16. What is the maximum number of VLANs supported in IEEE 802.1Q?
a) 64
b) 128
c) 256
d) 4096

17. Which command is used to configure VLAN trunking on a switch port?
a) configure trunk
b) switchport trunk
c) enable trunking
d) switchport mode trunk

18. Which VLAN type is used to carry traffic from multiple VLANs over a single physical link?
a) Access VLAN
b) Native VLAN
c) Trunk VLAN
d) Extended VLAN

19. Which VLAN type is used for end devices to connect to a switch port?
a) Access VLAN
b) Native VLAN
c) Trunk VLAN
d) Extended VLAN

20. What is the purpose of the native VLAN on a trunk port?
a) To carry untagged traffic
b) To carry voice traffic
c) To prioritize traffic over other VLANs
d) To establish a management connection

Terminal Questions

What is a VLAN (Virtual Local Area Network), and what is its purpose in network infrastructure?
Describe the benefits of implementing VLANs in a network environment.
How does VLAN tagging work, and why is it necessary for inter-switch communication?
Explain the difference between access ports and trunk ports in relation to VLANs.
What are the common methods for VLAN membership assignment on a switch port?
How does VLAN segmentation enhance network security and isolate network traffic?

Summary

A Virtual Local Area Network (VLAN) is a technology used in computer networking to logically segment a single physical network into multiple virtual networks. VLANs enable the isolation and separation of network traffic based on criteria such as port, MAC address, or IP address, even though the devices may physically connect to the same network switch. VLANs are extensively used in modern networking environments to improve network performance, security, and management. By creating virtual segmentation, VLANs help optimize network resources and provide greater control over the flow of data, making them a valuable tool for network administrators in building efficient and secure networks.

Answer Keys:

1. a	2. b	3. d	4. a	5. a	6. a	7. c	8. c	9. c	10. d
11. a	12. d	13. a	14. b	15. a	16. d	17. d	18. c	19. a	20. a

Topic 4: Wired Router, Wireless Router, Gateway, CSU/DSU

Router

The router is a networking device responsible for routing the data packets from source to destination over a network. *It distributes or routes the internet connection from the modem to all the networking devices, either wired or wireless, such as PC, Laptop, Mobile phone, tablet, etc.* It also enables multiple devices to communicate with each other over the same network.

The routers are mainly two types: **Wired and Wireless.**

In a wired router, we need an ethernet cable to connect with it for the internet connection. Whereas, in a wireless router, we don't need any cable, and with the help of Wi-fi technology, we can connect our networking devices with it.

It also provides us the security features and makes our devices secure over the given network form any threat.

The function of a Router

The main function of a router is to keep the network up & to run smoothly.

To do this, they connect computers and other networking devices such as Mobile, tablets, printers, etc., to communicate with each other.

Types of Router

There are different types of the router; some popular types are given below:

1. Wireless Router

Wireless routers are the most used routers in offices and homes as they don't need any wire or cable to connect with networking devices.

It provides a secure connection, and only authenticated users can access the network using the id & password.

It can be accessed by the n number of users within the specified range.

Fig 4.1: Wireless Router

2. Wired Router/Broadband Router

As its name suggests, it requires a wire or cable to connect to the network devices.

Such routers are used mostly in schools or small offices to connect the PCs with the Ethernet cable.

It also has a Wi-fi access point, and a mobile phone can be connected to it using the VOIP (Voice-over-Internet Protocol) technology.

It is connected to the ADSL modems to take the transmission data from the modem and distribute it to a further network.

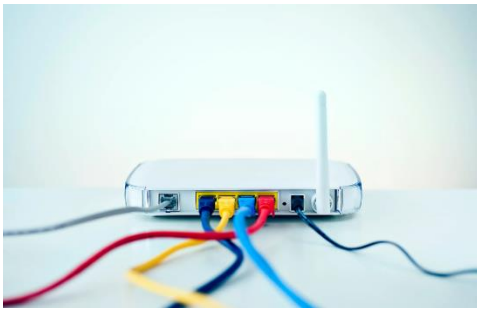


Fig 4.2: Wired Router

Gateway

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

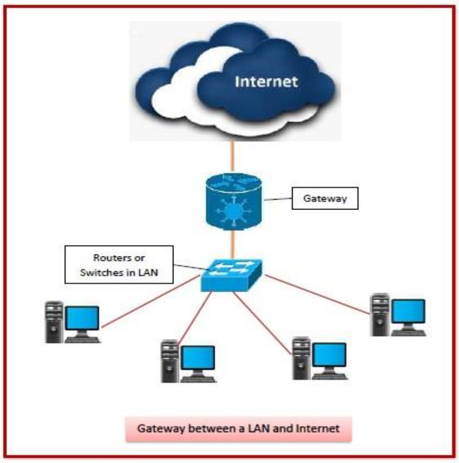

Internet
Gateway
Routers or Switches in LAN
Gateway between a LAN and Internet

Fig 4.3: Gateway

Features of Gateways

Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.

It forms a passage between two different networks operating with different transmission protocols.

A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.

The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.

It also stores information about the routing paths of the communicating networks.

When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.

A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.

It uses packet switching technique to transmit data across the networks.

Types of Gateways

On basis of direction of data flow, gateways are broadly divided into two categories −

Unidirectional Gateways − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.

Bidirectional Gateways − They allow data to flow in both directions. They can be used as synchronization tools.

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows −

Network Gateway − This is the most common type of gateway that provides as interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.

Cloud Storage Gateway − It is a network node or server that translates storage requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.

Internet-To-Orbit Gateway (I2O) − It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO).

IoT Gateway − IoT gateways assimilates sensor data from IoT (Internet of Things) devices in the field and translates between sensor protocols before sending it to the cloud network. They connect IoT devices, cloud network and user applications.

VoiP Trunk Gateway − It facilitates data transmission between plain old telephone service (POTS) devices like landline phones and fax machines, with VoIP (voice over Internet Protocol) network.

CSU/DSU

CSU/DSU stands for Channel Service Unit/Data Service Unit, is a digital communications device that combines the functions of both a Channel Service Unit (CSU) and a Data Service Unit (DSU).

These devices lie between the telephone company network and the customer network at the demarcation point and are the local interfaces between the data terminal equipment (DTE) at the customer premises and the telco’s digital communications line (such as a T1 line).

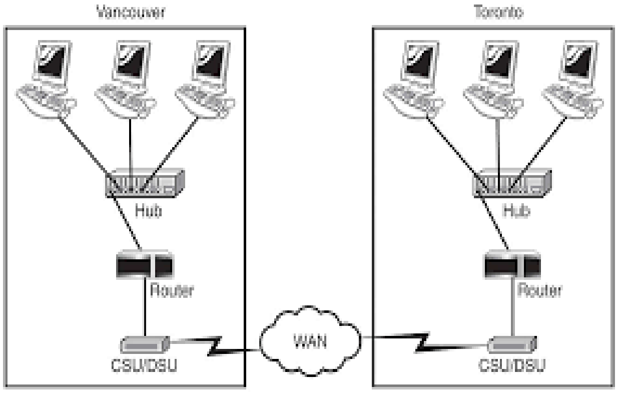


Fig 4.4: CSU/DSU

Digital Service Unit

A Digital Service Unit (DSU) is a piece of hardware that connects a Local Area Network (LAN) to an external communication carrier service via a Channel Service Unit (CSU).

A DSU is a device with two or more ports, one designated as the *WAN port* and the other as the *DTE port.*

The device translates bipolar digital signals from a digital circuit and a CSU that is compatible with the data terminal equipment to which the data is transferred.

When information is sent from the DTE to the circuit, the DSU performs a similar operation in reverse.

The telecommunications service that a DSU supports can be a point-to-point or multipoint operation in a digital environment.

DSU Applications

DSUs are typically incorporated with Channel Service Units to save customers the trouble of installing them individually. They make customer operations incredibly convenient and simple. The CSU is responsible for the majority of signal reception and relaying to and from the WAN line.

The DSU is in charge of line control as well as input and output conversion between frames. It handles signal regeneration and timing issues. It serves as a conduit for communication between the computer or desktop, as the case may be, and the CSU.

Pros and Cons of DSU

There are numerous advantages to using a DSU, including its ease of usage and access when in use. It handles responsibilities such as line control, timing problems, and signal regeneration.

Some disadvantages are that they are highly pricey and inefficient to use. Because it is highly sophisticated, there will be a delay in the setup. If the CSU and the DSU are incompatible, the consumer may experience issues. Digital service units come in a variety of shapes and sizes, which are quite different and varied. They're offered as a chip, a board, or a module. Some of the forms can be stacked on top of each other. When selecting a digital service unit, it is necessary to consider these factors.

SAQ's-Self Assessment Questions

1. Which device connects multiple networks and directs network traffic between them?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) Modem

2. Which device serves as an entry or exit point for a network, connecting it to another network?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) Switch

3. Which device converts digital signals into appropriate signals for transmission over a leased line?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) Modem

4. Which device provides functions like network address translation (NAT) and firewall capabilities?
   a) Router
   b) Gateway
   c) CSU/DSU
   d) Switch

5. What is the primary function of a CSU/DSU device?
   a) Packet forwarding
   b) Data encryption
   c) Signal regeneration
   d) IP address assignment

6. Which device is responsible for determining the best path for data packets between networks?
   a) Router

b) Gateway
c) CSU/DSU
d) Modem

7. What is the purpose of NAT (Network Address Translation) in a router?
a) It encrypts data packets for secure transmission.
b) It assigns unique IP addresses to devices on a network.
c) It filters network traffic based on predefined rules.
d) It translates private IP addresses to public IP addresses.

8. Which device provides services like DHCP and proxy services?
a) Router
b) Gateway
c) CSU/DSU
d) Switch

9. What does a CSU/DSU device do to ensure reliable data transmission?
a) Converts analog signals to digital signals.
b) Provides error correction for transmitted data.
c) Assigns IP addresses to network devices.
d) Routes network traffic based on IP addresses.

10. Which device is commonly used to connect a local network to the internet?
a) Router
b) Gateway
c) CSU/DSU
d) Switch

11. What is the purpose of a routing table in a router?
a) It translates IP addresses to domain names.
b) It determines the best path for data packet forwarding.
c) It assigns IP addresses to network devices.
d) It filters network traffic based on predefined rules.

12. Which device is responsible for maintaining clock synchronization in a data transmission?
a) Router
b) Gateway
c) CSU/DSU
d) Modem

13. What does QoS stand for in relation to routers?
a) Quality of Switching
b) Quick Operational Support
c) Quality of Service
d) Quantitative Operating System

14. What is the purpose of a firewall in a router or gateway?
a) It encrypts network traffic for secure transmission.
b) It assigns IP addresses to network devices.
c) It filters network traffic based on predefined rules.
d) It converts digital signals into analog signals.