COMPUTER NETWORK

(Day :-1)

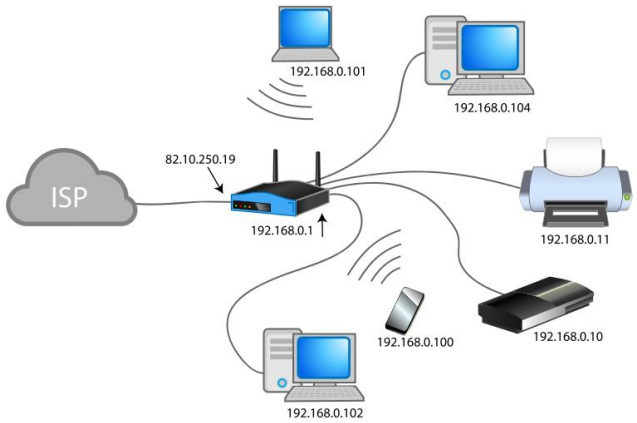
Question 1 :- What are network, node and link ?

A network consists of two or more separate devices linked together such that they can communicate. Networks can be classified according to different criteria such as size, type of connection, topology etc.

Nodes and Links:-

Nodes – Devices or data points on a more extensive network are known as nodes. They are individual parts of a larger data structure and contain data. They also link other nodes.

Links- A link is the physical and logical network component for interconnecting hosts or nodes in a network. It is a physical communication medium such as a coaxial cable or optical fiber.



Considering the size or span of a network, we can classify them as follows:

- **PAN (Personal Area Network)** – PAN is made up of devices used by a single person. It has a range of a few meters.
- **WPAN (Wireless Personal Area Network)** – It is a PAN network that uses wireless technologies as a medium.
- **LAN (Local Area Network)** – LAN is a network whose range is limited to a relatively small area, such as a room, a building, an airplane, etc.
- **WLAN (Wireless Local Area Network)** – WLAN is a LAN network that uses wireless means of communication. It is a widely used configuration due to its scalability and because it does not require the installation of cables.
- **CAN (Campus Area Network)** – A network of high-speed devices that connects LANs in a limited geographical area, such as a university campus, a military base, etc.
- **MAN (Metropolitan Area Network)** or metropolitan area network – It is a high-speed (broadband) network providing coverage in a larger geographic area than a campus, but still limited.

- **WAN (Wide Area Network)** – WAN extends over a large geographical area using unusual means of communication, such as satellites, interoceanic cables, fiber optics, etc. Use public media.
- **VLAN** – It is a type of logical or virtual LAN, mounted on a physical network, in order to increase security and performance.

Network vs Networking

The main difference between network and networking is that network is a collection of computing devices connected via a communication medium to exchange information and resources while networking is the practice of creating, maintaining, securing and troubleshooting the network.

Network vs Internet

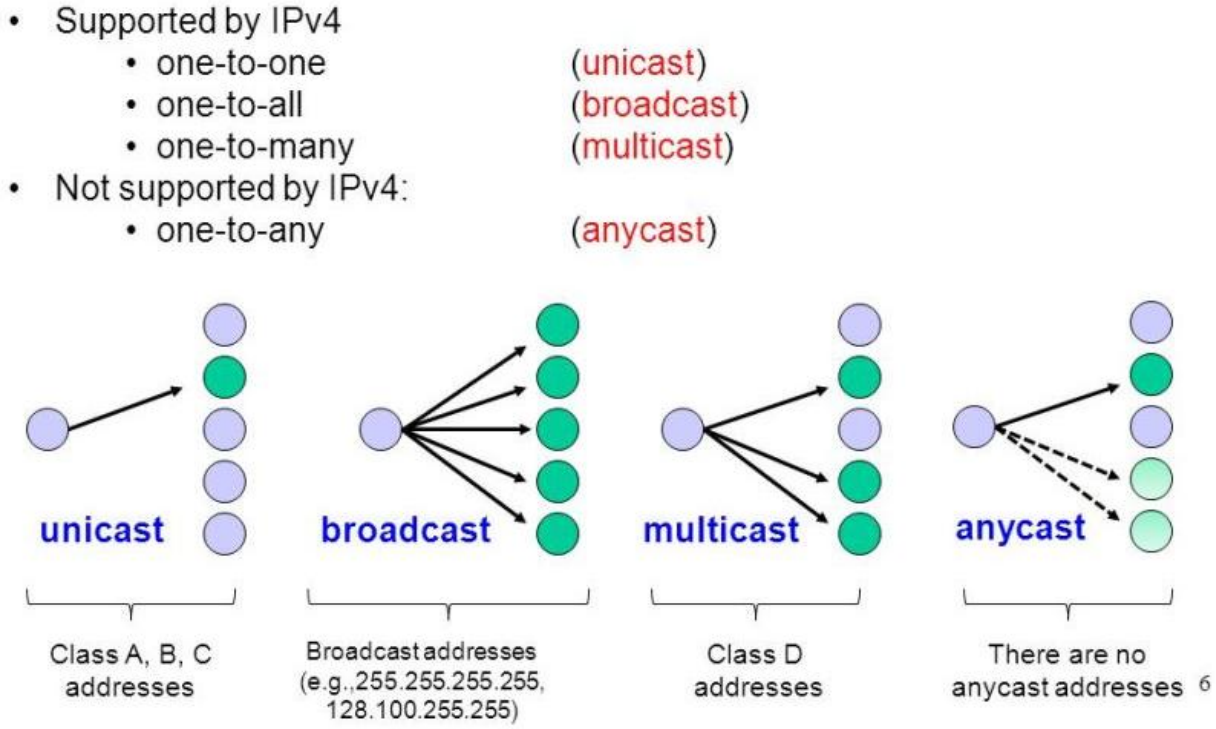
In simple words, the network is a collection of devices that can communicate with each other on the other hand the Internet is a collection of networks that can communicate with each other.

Question 2:- What is the difference between Communication and Transmission?

Transmission – A process of sending and receiving data between source and destination, in **only one way**. It is regarded as the physical movement of data.

Communication – A process of sending and receiving data between source and destination, in both ways.

Question3 :- What are Unicasting, Anycasting, Multicasting and Broadcasting?



If the message is sent from a source to a single destination node, it is called **Unicasting** . This is typically done in networks.

If the message is sent from a source to any of the given destination nodes, it is called **any casting**. This is used a lot in Content delivery Systems where we want to get content from any server.

If the message is sent to some subset of other nodes, it is called **Multicasting.** Used in the situation when there are multiple receivers of the same data. Like video conferencing, updating something on CDN servers which have a replica of same data.

If the message is sent to all the nodes in a network it is called **Broadcasting.** This is typically used in Local networks, for examples DHCP and ARP use broadcasting.

Question 4:- What are layers in OSI model?

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization of Standardization**', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform.

There are a total of 7 layers

Layer no	Layers	Data Units	Functions
7	Application Layer	Data	Mail Services,Directory Serices,FTAM
6	Presentation Layer	Data	Encryption/Decryption, Compression
5	Session Layer	Data	Session Establishment, Synchronization,Dialog Controller
4	Transport Layer	Segments,Datagram	Segementation
3	Network Layer	Packets	Traffic control,Fragmentation,Routing
2	Data Link Layer	Frames	Flow control,Error control,Access control
1	Physical Layer	Bits	Bit Synchronization,Bit rate control,Physical Topologies

OSI Model	DoD Model	Protocols	Devices / Apps
Layer 5, 6, 7	Application	DNS, DHCP, NTP, SNMP, HTTPS, FTP, SSH, TELNET, HTTP, POP3...etc.	Web server, Mail server, Browser, Mail client ...etc.
Layer 4	Host to Host	TCP | UDP	Gateway
Layer 3	Internet	IP, ICMP, IGMP	Router, Firewall layer 3, Switch
Layer 2	Network access	ARP (MAC), RARP`	Bridge, Layer 2 switch
Layer 1		Ethernet, Token ring	Hub

Question :- 5 Differences between Hub, Switch and Router?

Hub	Switch	Router
Physical Layer Device	Data Link Layer Device	Network Layer Device
Simply repeats signal to all ports	Doesn't simply repeat, but filters content by MAC or LAN address	Routes data based on IP address
Connects devices within a single LAN	Can connect multiple sub-LANs within a single LAN	Connect multiple LANS and WANS together.

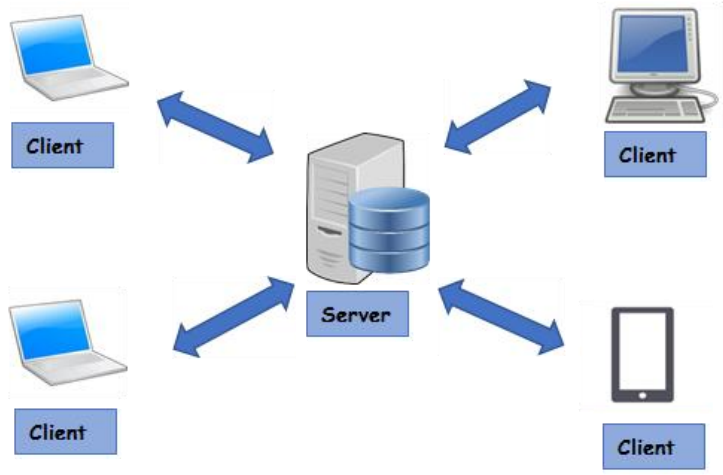
Question :- 6 What are 'client' and 'server' in a network?

Ans. Clients and servers are separate logical entities that work together over a network to accomplish a task.

A client application is the element of communication that requests or requests a network service, for example, accessing a web page, or downloading a file, or sending an email.

A server application is the element of communication that responds to customer requests, providing the required service, that is, sending the web page or the requested file or email.

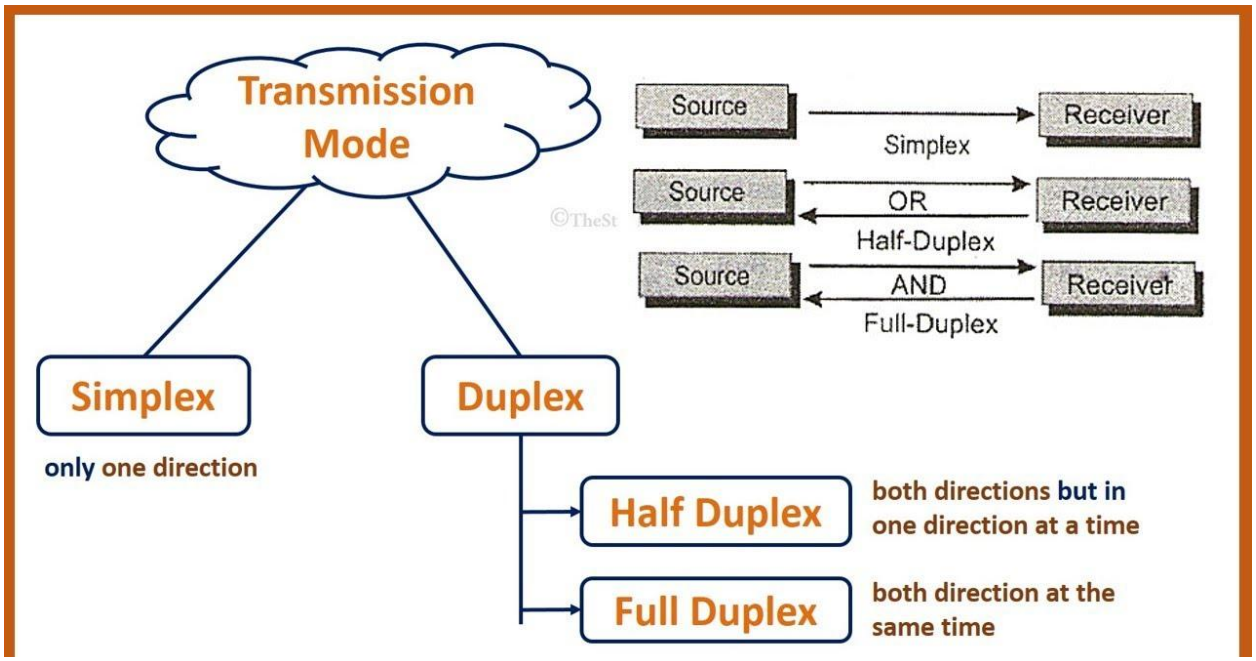
The client-server model is used by computer applications such as email, the worldwide web, and network printing.



Question :-7 What are the different ways to exchange data?

Following are the different ways to exchange data:

- Simplex
- Half-duplex
- Full-duplex



Question :-8 How many layers does TCP/IP Model have?

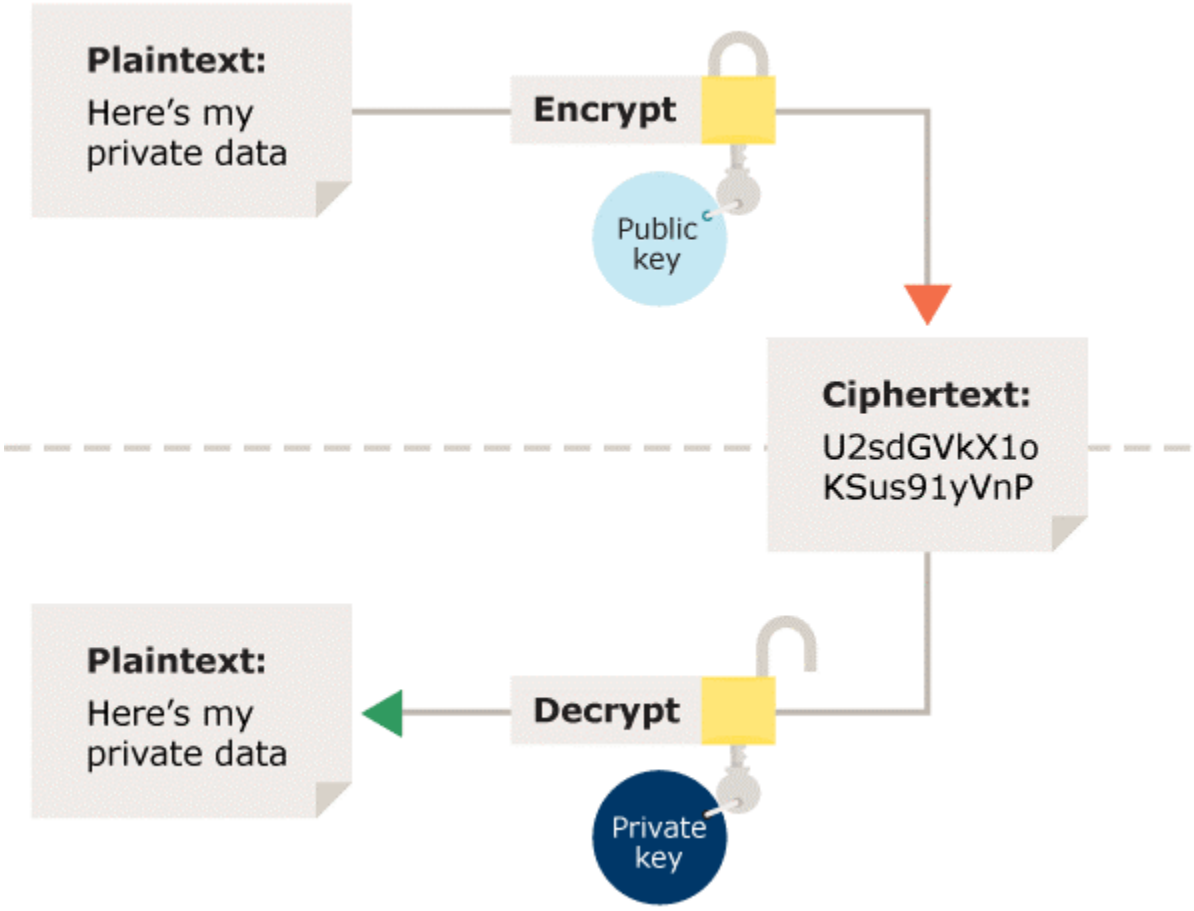
Ans. TCP/IP Model has four layers:

Layer	**Description**
Network Interface	Network Interface is also called a network access layer. It defines how data should be sent physically using the network.
Internet	It enables hosts to insert packets into the network and have them delivered to the destination, on the same network, or another remote network.
Transport	This layer permits devices on the source and destination hosts to carry on a conversation. It ensures reliability, flow control, and correction of data that is being sent over the network.
Application	It is the topmost layer of the TCP/IP model. It defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.

Question 9:- Why is encryption on a network necessary?

Ans. Encryption is the process of changing data from its original readable format to an unreadable format, thus ensuring network security. It requires the user to use a secret key or password to decrypt the data.

Encryption is not only useful for communications, but also in any case where you want to protect sensitive information. Thus, it is possible to encrypt the information contained in disks, folders or even individual files, to prevent unauthorized access. Then, in addition to the benefit of protecting the privacy of users, data encryption prevents other types of attacks such as identity theft, or bank fraud, in addition to providing a protection mechanism against the theft or loss of devices with sensitive information



Question 10:- What is difference between ARP and RARP?

The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver.

The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

Question 11:- What is the baud rate of the standard 10 Mbps 802.3 LAN?

AN uses Manchester Encoding Technique where-

Baud rate = 2 x Bit rate

For 10 Mbps,

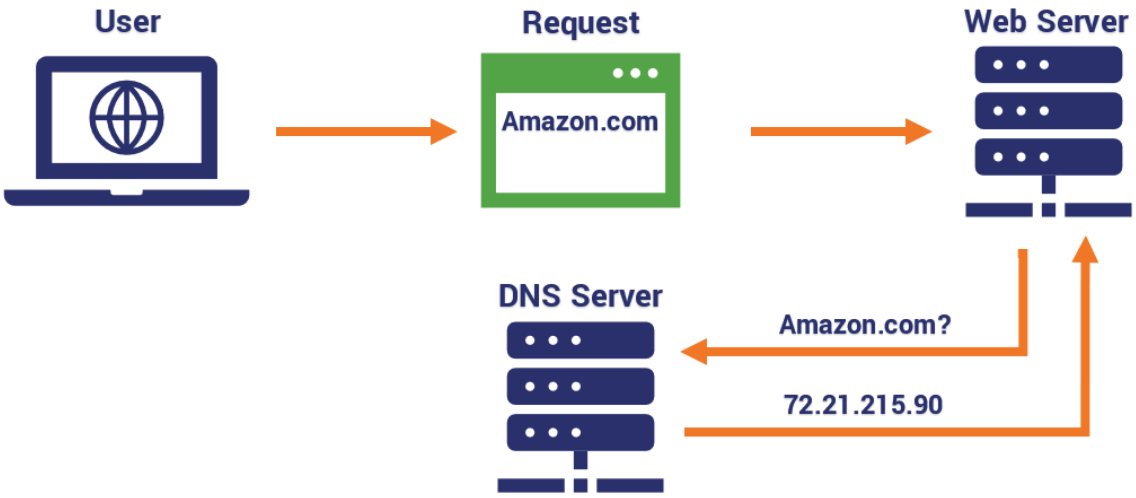
Baud rate

= 2 x 10 mega baud

= 20 mega baud

Question 12:- What is DNS? Differentiate between 'forward lookup' and 'reverse lookup' in DNS?

The Domain Name System (DNS) is a central part of the internet, providing a way to match names (a website you're seeking) to numbers (the address for the website).

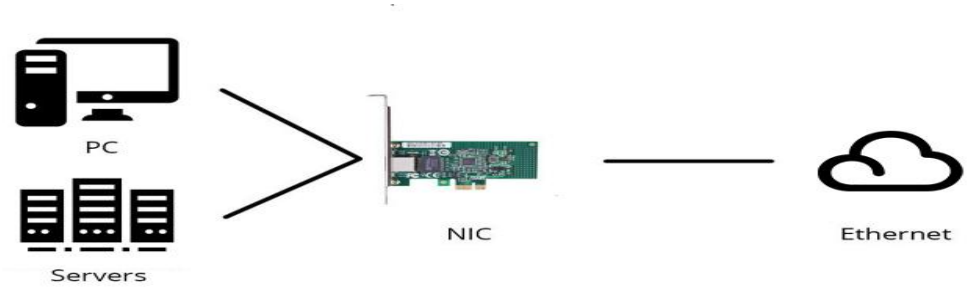


The major differences between a forward lookup and reverse lookup in DNS are –

Forward DNS lookup	Reverse DNS lookup
Converts a human input or a domain name to an IP address	Converts an IP address into a domain name
Has a mapping between hostnames and IP addresses	Has a mapping that relates IP addresses to hostnames
Used for a website or other server access	Used for network troubleshooting
Utilizes different servers with different IP addresses	Resolves reverse lookup queries where a client requests a hostname by providing an IP address
Uses A Records (basic) to identify any IP address for a particular hostname	Uses DNS pointer record to identify a hostname for a given IP address

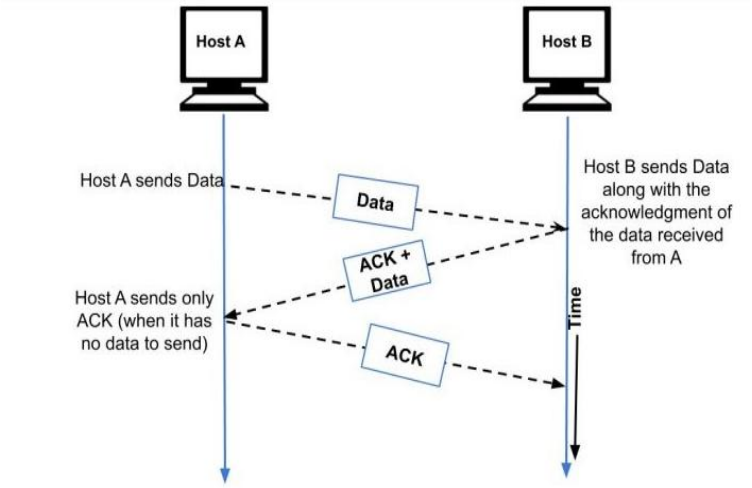
Question 13:- What is NIC

NIC is the abbreviation for Network Interface Card. It is a peripheral card with electronic circuitry. It is attached to a PC and connects it to a network. NIC has its own MAC address and this identifies a PC on the network



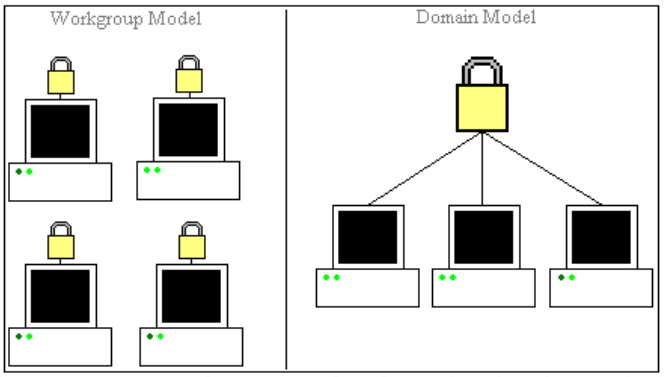
Question 14 :- What is Piggybacking?

Piggybacking is used in bi-directional data transmission in the network layer (OSI model). The idea is to improve the efficiency. Piggyback acknowledgment (of the received data) is hooked on the data frame (to be sent) instead of sending a separate frame.



Question 15 :- What is the difference between a Domain and a Workgroup?

The main difference between a Domain and a Workgroup is where do the computer networks belong to. If it is a home network, then computers will be a part of a workgroup, and if it's a workplace network, then the computers will be a part of a domain.



In a workgroup, each computer manages its own security whereas in a domain, security is managed centrally

Below are some of the major differences between a Domain and a Workgroup:

Domain	**Workgroup**
The computers in a domain have a centralized database.	The computers in the workgroup have their own local database.

Computers can be on a different local network.	All computers must be on the same local area network.
One or more computers are servers for providing access, security permission to all other computers in a network.	All computers are peers and no computer has control over another computer.
A domain is used for transferring and sharing sensitive and important data.	It is used for sharing less secure data.
Domain has centralized authentication servers which set the rule of authentication.	Each computer has its own authentication rule for every user account.
If a user has an account in a domain then the user can log in to any computer in a domain.	Each computer has a set of user accounts. If the user has an account on that computer then only the user will be able to access the computer.
Changes made in one computer are automatically made to all other computers in a network.	Computer settings need to change manually for each computer.
It is used by large public and business networks.	A workgroup is better suited for fewer computers.
Thousands of computers can be connected.	Only 20 computers connected.

Question 16:- What are a MAC address and an IP address?

Ans. A **MAC** (Media Access Control) address is the unique 48-bit hardware address of a LAN card, usually stored in the ROM of the network adapter card.

The MAC address is a unique identifier that manufacturers assign to a network card or device. It is also known as a physical address represented by hexadecimal digits. Each MAC address is unique worldwide and, in theory, they are fixed for each device.

Each MAC address includes six pairs of numbers. The first three pairs help to identify the manufacturer and the next three to the specific model. It is important to bear in mind that a computer may have a variety of hardware to connect to networks; thus, it is common to have a MAC address for Ethernet, one for Wi-Fi, and another for Bluetooth

An Internet Protocol address (IP address) is a numerical unique address of a device in a network. IP is a datagram-oriented connectionless protocol, therefore each packet must contain a header with the source IP address, the destination IP address, and other data in order to be delivered successfully.

There are two types of IPs –

Private IP Address – A private IP address is a set of numbers that are assigned to each computer or system, connected to a private network. An example of a private IP address is your mobile phone or your home router which have a default local address.

Public IP Address – Public IP addresses are global addresses, visible to anyone browsing the Internet. A user just needs an internet connection to connect to such devices.

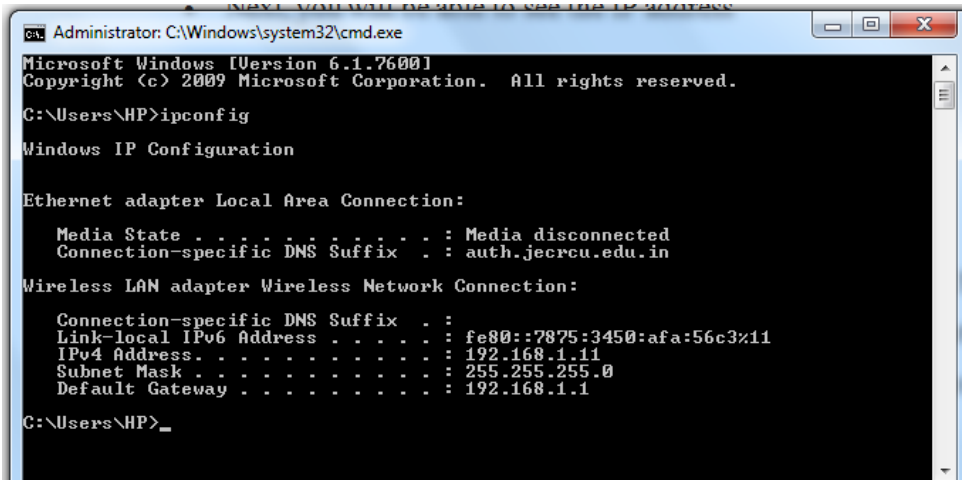
Question 17:- How to find the IP address of a website?

Ans. Finding the IP address of a website or a domain is not a tricky task and involves the below steps –

- Press the "Start" button on your computer
- Type in the program and file browser "cdm"
- Hit "Enter"
- The MS-DOS console will open, where you must type "nslookup facebook.com". Instead of "google.com", you must write the domain name of the page you want to consult
- Next, you will be able to see the IP address

Question 18 :- What is ipconfig and ifconfig?

An acronym for Internet Protocol Configuration, Ipconfig is used on Microsoft Windows to view and configure the network interface. It displays all TCP/IP network summary information available on a network and helps to modify the DHCP protocol and DNS settings .



Ifconfig:- . It is an acronym for Interface Configuration and is used on Linux, Mac, and UNIX operating systems. ifconfig configures and controls the TCP/IP network interface parameters from Command Line Interface while allowing the user to check the IP addresses of these network interfaces

Question 19:- **If the bandwidth of the line is 1.5 Mbps, RTT is 45 msec and packet size is 1 KB, then find the link utilization in stop and wait.**

Stop and wait

Total Time-

Total time taken in sending one data packet

$$= (\text{Transmission delay} + \text{Propagation delay})_{packet} + (\text{Propagation delay})_{ACK}$$

$$= (\text{Transmission delay})_{packet} + 2 \times \text{Propagation delay}$$

Efficiency-

Efficiency of any flow control control protocol is given by-

$$\text{Efficiency } (\eta) = \frac{(\text{Transmission delay})_{packet}}{(\text{Transmission delay})_{packet} + 2 \times \text{Propagation delay}}$$

OR

$$\text{Efficiency } (\eta) = \frac{T_t}{T_t + 2T_p}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + 2\left(\frac{T_p}{T_t}\right)}$$

OR

$$\text{Efficiency } (\eta) = \frac{1}{1 + 2a}, \text{ where } a = \left(\frac{T_p}{T_t}\right)$$

Throughput-

- Number of bits that can be sent through the channel per second is called as its throughput.

$$\text{Throughput} = \text{Efficiency } (\eta) \times \text{Bandwidth}$$

Round Trip Time-

Round Trip Time = 2 x Propagation delay

Solution-

Given-

- Bandwidth = 1.5 Mbps
- RTT = 45 msec
- Packet size = 1 KB

Calculating Transmission Delay-

Transmission delay (T_t)

= Packet size / Bandwidth

= 1 KB / 1.5 Mbps

= (2^{10} x 8 bits) / (1.5 x 10^6 bits per sec)

= 5.461 msec

Calculating Propagation Delay-

Propagation delay (T_p)

= Round Trip Time / 2

= 45 msec / 2

= 22.5 msec

Calculating Value Of 'a'-

$a = T_p / T_t$

a = 22.5 msec / 5.461 msec

a = 4.12

Calculating Link Utilization-

Link Utilization or Efficiency (η)

= 1 / 1+2a

= 1 / (1 + 2 x 4.12)

= 1 / 9.24

= 0.108

= 10.8 %

Question 20 :- Station A uses 32 byte packets to transmit messages to station B using a sliding window protocol. The round trip delay between A and B is 80 msec and the bottleneck bandwidth on the path between A and B is 128 Kbps. What is the optimal window size that A should use?

Solution-

Given-

- Packet size = 32 bytes
- Round Trip Time = 80 msec
- Bandwidth = 128 Kbps

Calculating Transmission Delay-

Transmission delay (T_t)

= Packet size / Bandwidth

= 32 bytes / 128 Kbps

= (32 x 8 bits) / (128 x 10^3 bits per sec)

= 2 msec

Calculating Propagation Delay-

Propagation delay (T_p)

= Round Trip Time / 2

= 80 msec / 2

= 40 msec

Calculating Value of 'a'-

$a = T_p / T_t$

a = 40 msec / 2 msec

a = 20

Calculating Optimal Window Size-

Optimal window size

= 1 + 2a

=41

Question 20 . In Stop and wait protocol every 4th packet is lost and we need to send total 10 packets so how many transmission it took to send all the packets?
Explanation –
1 2 3 4 5 6 7 8 9 10 (Initially)

^

1 2 3 4 4 5 6 7 8 9 10 (Packet no. 4 retransmitted)

^

1 2 3 4 4 5 6 7 7 8 9 10 (Packet no. 10 retransmitted)

^

1 2 3 4 4 5 6 7 7 8 9 10 10 (Result)

So, we retransmitted packet noumber 4, 7, 10
Total count = 13

Example-21 . In GB3 if every 5th packet is lost & we need to send 10 packets so how many retransmissions are required ?

Explanation –
1 2 3 4 5 6 7 | 8 9 10

^ $ (packet no. 5 lost)

1 2 3 4 5 6 7 5 6 7 8 9 | 10

* ^ $

1 2 3 4 5 6 7 5 6 7 8 9 7 8 9 10

* ^ $

1 2 3 4 5 6 7 5 6 7 8 9 7 8 9 10 9 10 (count starts from * till ^)

(from ^ to $ retranmission is done)

Note – From the Last packet is window size to lost pocket we resend the entire window.
Total no. of transmissions = 18

Question 22 :- Station A needs to send a message consisting of 9 packets to station B using a sliding window (window size 3) and go back n error control strategy. All packets are ready and immediately available for transmission.

If every 5th packet that A transmits gets lost (but no ACKs from B ever get lost), then what is the number of packets that A will transmit for sending the message to B?

Solution-

Given-

- Total number of packets to be sent = 9
- Go back N is used where N = 3
- Every 5th packet gets lost

Step-01:

Since sender window size is 3, so sender sends 3 packets (1, 2, 3)-

Total packets sent till now from sender side = 3

Step-02:

After receiving the acknowledgement for packet-1, sender slides its window and sends packet-4.

Total packets sent till now from sender side = 4

Step-03:

After receiving the acknowledgement for packet-2, sender slides its window and sends packet-5.

Total packets sent till now from sender side = 5

Step-04:

After receiving the acknowledgement for packet-3, sender slides its window and sends packet-6.

Total packets sent till now from sender side = 6

Step-05:

After receiving the acknowledgement for packet-4, sender slides its window and sends packet-7.

Total packets sent till now from sender side = 7

Step-06:

- According to question, every 5th packet gets lost.
- So, packet-5 gets lost and when time out occurs, sender retransmits packet-5.
- In Go back N, all the following packets are also discarded by the receiver.
- So, packet-6 and packet-7 are discarded by the receiver and they are also retransmitted.
- Thus, the entire window is retransmitted.

So, we have-

Total packets sent till now from sender side = 10

Now, the next 5th packet that will be lost will be packet-7. (6, 7, 5, 6, 7)

Step-07:

After receiving the acknowledgement for packet-5, sender slides its window and sends packet-8.

Total packets sent till now from sender side = 11

Step-08:

After receiving the acknowledgement for packet-6, sender slides its window and sends packet-9.

Total packets sent till now from sender side = 12

Step-09:

- According to question, every 5th packet gets lost.
- So, packet-7 gets lost and when time out occurs, sender retransmits packet-7 and the following packets.
- Thus, the entire window is retransmitted.

So, we have-

Total packets sent till now from sender side = 15

Now, the next 5th packet that will be lost will be packet-9. (8, 9, 7, 8, 9)

Step-10:

After receiving the acknowledgement for packet-7, sender slides its window.

Total packets sent till now from sender side = 15

Step-11:

After receiving the acknowledgement for packet-8, sender slides its window.

Total packets sent till now from sender side = 15

Step-12:

- According to question, every 5th packet gets lost.
- So, packet-9 gets lost and when time out occurs, sender retransmits packet-9.

So, we have-

Total packets sent till now from sender side = 16

Finally, all the 9 packets got transmitted which took total 16 number of transmissions.

Question 23 . In SR $W_s = 5$ and we are sending 10 packets where every 5th packet is lost find number of retransmissions?
Explanation –
1 2 3 4 5 6 7 8 9 10

^

1 2 3 4 5 5 6 7 8 9 10

^

1 2 3 4 5 6 7 8 9 9 10

We see here there is no role of Window size in SR only the lost packet is resent.
Total transmissions = 12

Question 24:- If there is K bits sequence no. define require sender window size and receiver window size for S&W, GBN & SR?

Explanation –
Given, K bits, For S&W $W_s = 1$ and $W_r = 1$
For GBN, $W_s = 2^K-1$ and $W_r = 1$
For SR, $W_s = 2^{K-1}$ and $W_r = 2^{(K-1)}$

Question 25 :- Consider all links in the network use TDM with 24 slots and have a data rate of 1.536 Mbps. Assume that host A takes 500 msec to establish an end to end circuit with host B before begin to transmit the file. If the file is 512 kilobytes, then how much time will it take to send the file from host A to host B?

Solution-

Given-

- Total bandwidth = 1.536 Mbps
- Bandwidth is shared among 24 slots
- Connection set up time = 500 msec
- File size = 512 KB

Calculating Bandwidth Per User-

Total bandwidth = Number of users x Bandwidth per user

So, Bandwidth per user

= Total bandwidth / Number of users

= 1.536 Mbps / 24

= 0.064 Mbps

= 64 Kbps

Calculating Transmission Delay-

Transmission delay (T_t)

= File size / Bandwidth

= 512 KB / 64 Kbps

= (512 x 2^{10} x 8 bits) / (64 x 10^3 bits per sec)

= 65.536 sec

= 65536 msec

Calculating Time Required To Send File-

Time taken to send a file in circuit switched network

= Connection set up time + Transmission delay

= 500 msec + 65536 msec

= 66036 sec