Review of Networking Basics :-

A computer network is a group of two or more interconnected computer systems. You can establish a network connection using either cable or wireless media.

Every network involves hardware and software that connects computers and tools.

Here are essential computer network components:

Switches:-

Switches work as a controller which connects computers, printers, and other hardware devices to a network in a campus or a building.

It allows devices on your network to communicate with each other, as well as with other networks. It helps you to share resources and reduce the costing of any organization.

Routers:-
Routers help you to connect with multiple networks. It enables you to share a single internet connection with multiple devices and saves money. This networking component acts as a dispatcher, which allows you to analyze data sent across a network. It automatically selects the best route for data to travel and send it on its way.

Servers:-
Servers are computers that hold shared programs, files, and the network operating system. Servers allow access to network resources to all the users of the network.

Clients:-
Clients are computer devices which access and uses the network as well as shares network resources. They are also users of the network, as they can send and receive requests from the server.

Transmission Media:-
Transmission media is a carrier used to interconnect computers in a network, such as coaxial cable, twisted-pair wire, and optical fiber cable. It is also known as links, channels, or lines.

Access points:-
Access points allow devices to connect to the wireless network without cables. A wireless network allows you to bring new devices and provides flexible support to mobile users.

Shared Data:-
Shared data are data which is shared between the clients such as data files, printer access programs, and email.

Network Interface Card:-
Network Interface card sends, receives data, and controls data flow between the computer and the network.

Local Operating System:-
A local OS which helps personal computers to access files, print to a local printer and uses one or more disk and CD drives which are located on the computer.

Network Operating System:-
The network operating system is a program which runs on computers and servers. It allows the computers to communicate via network.

Protocol:-
A protocol is the set of defined rules that allows two entities to communicate across the network. Some standard protocols used for this purpose are IP, TCP, UDP, FTP, etc.

Hub:-
Hub is a device that splits network connection into multiple computers. It acts a distribution center so whenever a computer requests any information from a computer or from the network it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network.

LAN Cable:-
Local Area Network(LAN) cable is also called as Ethernet or data cable. It is used for connecting a device to the internet.

OSI:-
OSI stands for Open Systems Interconnection. It is a reference model which allows you to specify standards for communications.

—Unique Identifiers of Network
Below given are some unique network identifiers:

Hostname:-

Every device of the network is associated with a unique device, which is called hostname.

IP Address:-

IP (Internet Protocol) address is as a unique identifier for each device on the Internet. Length of the IP address is 32-bits. IPv6 address is 128 bits.

DNS Server:-

DNS stands for Domain Name System. It is a server which translates URL or web addresses into their corresponding IP addresses.

MAC Address:-

MAC (Media Access Control Address) is known as a physical address is a unique identifier of each host and is associated with the NIC (Network Interface Card). General length of MAC address is : 12-digit/ 6 bytes/ 48 bits

Port:-

Port is a logical channel which allows network users to send or receive data to an application. Every host can have multiple applications running. Each of these applications are identified using the port number on which they are running.

—Other Important Network Components

ARP:-
ARP stands for Address Resolution Protocol which helps network users to convert the IP address into its corresponding Physical Address.

RARP:-
Reverse Address Resolution Protocol gives an IP address of the device with given a physical address as input.

@Advantages of Computer Networking:-

Here are the fundamental benefits/pros of using Computer Networking:

Helps you to connect with multiple computers together to send and receive information when accessing the network.
Helps you to share printers, scanners, and email.
Helps you to share information at very fast speed
Electronic communication is more efficient and less expensive than without the network.

@Disadvantages of Computer Networking:-

Here are drawbacks/ cons of using computer networks:

Investment for hardware and software can be costly for initial set-up
If you don’t take proper security precautions like file encryption, firewalls then your data will be at risk.
Some components of the network design may not last for many years, and it will become useless or malfunction and need to be replaced.
Requires time for constant administration
Frequent server failure and issues of regular cable faults

Internet Protocol Version 4 (IPv4):-

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

#Subnetting :-

IPv4 allows for a variation of the network and host segments of an IP address, known as subnetting, can be used to physically and logically design a network. For example, an organization can have a single internet network address (NETID) that is known to users outside the organization, yet configure its internal network into different departmental subnets. Subnetwork addresses enhance local routing capabilities, while reducing the number of network addresses required.

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (21=2) with (223-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (214) 16384 Networks and (216-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address −

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

Multicasting:-

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network.

Multicasting works in similar to Broadcasting, but in Multicasting, the information is sent to the targeted or specific members of the network. This task can be accomplished by transmitting individual copies to each user or node present in the network, but sending individual copies to each user is inefficient and might increase the network latency. To overcome these shortcomings, multicasting allows a single transmission that can be split up among the multiple users, consequently, this reduces the bandwidth of the signal.

Applications :
Multicasting is used in many areas like:

- Internet protocol (IP)
- Streaming Media

It also supports video conferencing applications and webcasts.

IP Multicast :
Multicasting that takes place over the Internet is known as IP Multicasting. These multicast follow the internet protocol(IP) to transmit data. IP multicasting uses a mechanism known as 'Multicast trees' to transmit to information among the users of the network. Multicast trees; allows a single transmission to branch out to the desired receivers. The branches are created at the Internet routers, the branches are created such that the length of the transmission will be minimum.

IP multicasts also use two other essential protocols to function; Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM). IGMP allows the recipients to access the data or information. The network routers use PIM to create multicast trees.

Multicast Routing Protocols:-

IGMP :-

IGMP is acronym for Internet Group Management Protocol. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as IGMPv2 and MLDv2 is almost similar to IGMPv3. The communication protocol, IGMPv1 was developed in 1989 at Stanford University. IGMPv1 was updated to IGMPv2 in year 1997 and again updated to IGMPv3 in year 2002.

Applications:

Streaming – Multicast routing protocol are used for audio and video streaming over the network i.e., either one-to-many or many-to-many.
Gaming – Internet group management protocol is often used in simulation games which has multiple users over the network such as online games.
Web Conferencing tools – Video conferencing is a new method to meet people from your own convenience and IGMP connects to the users for conferencing and transfers the message/data packets efficiently.
Types: There are 3 versions of IGMP. These versions are backward compatible. Following are the versions of IGMP

PIM :-

Protocol Independent Multicast (PIM) is the name given to two independent multicastrouting protocols: Protocol Independent Multicast, Dense Mode (PIM-DM) and Protocol Independent Multicast, Sparse Mode (PIM-SM). Both protocols are unicast protocol-dependent, but the similarity ends here.

- PIM-DM

PIM-DM is used when there is a possibility that each router is involved in multicasting (dense mode). In this environment, the use of a protocol that broadcasts the packet is justified because almost all routers are involved in the process. PIM-DM is a source-based tree routing protocol that uses RPF and pruning and grafting strategies for multicasting. Its operation is like that of DVMRP.

- PIM-SM

PIM-SM is used when there is a slight possibility that each router is involved in multicasting (sparse mode). In this environment, the use of a protocol that broadcasts the packet is not justified; a protocol such as CBT that uses a group-shared tree is more appropriate. PIM-SM is used in a sparse multicast environment such as a WAN. PIM-SM is a group-shared tree routing protocol that has a rendezvous point (RP) as the source of the tree.

DVMRP :-

The DVMRP is used for multicasting over IP networks without routing protocols to support multicast. The DVMRP is based on the RIP protocol but more complicated than RIP. DVRMP maintains a link-state database to keep track of the return paths to the source of multicast packages.

The DVMRP operates as follows:

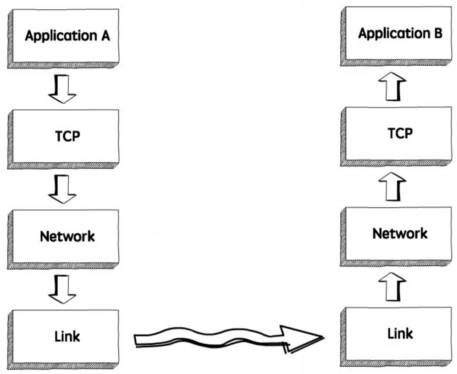
The first message for any source-group pair is forwarded to the entire multicast network, with respect to the time-to-live (TTL) of the packet.
TTL restricts the area to be flooded by the message.
All the leaf routers that do not have members on directly attached subnetworks send back prune messages to the upstream router.
The branch that transmitted a prune message is deleted from the delivery tree.
The delivery tree, which is spanning to all the members in the multicast group, is constructed.

Advance Topics in TCP :-

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

#Flow Management:-

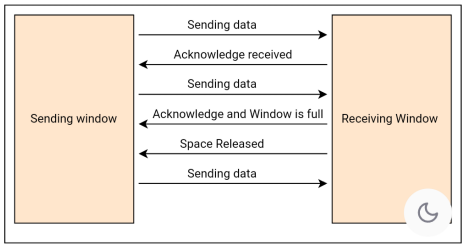
TCP Flow Control is a protocol designed to manage the data flow between the user and the server. It ensures that there is a specific bandwidth for sending and receiving data so the data can be processed without facing any major issues. In order to achieve this, the TCP protocol uses a mechanism called the sliding window protocol.



Sliding Window Protocol:-

In the **sliding window protocol** method, when we are establishing a connection between sender and receiver, there are two buffers created. Each of these two buffers are assigned to the sender, called the **sending window**, and to the receiver, called the **receiving window**.

When the sender sends data to the receiver, the receiving window sends back the remaining receiving buffer space. As a result, the sender cannot send more data than the available receiving buffer space. We'll understand the concept better once we take a look at the illustration below:



#Congestion Avoidance:-

TCP uses a congestion window and a congestion policy that avoid congestion. Previously, we assumed that only the receiver can dictate the sender's window size. We ignored another entity here, the network. If the network cannot deliver the data as fast as it is created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window.

Congestion policy in TCP –

1. Slow Start Phase: starts slowly increment is exponential to threshold
2. Congestion Avoidance Phase: After reaching the threshold increment is by 1
3. Congestion Detection Phase: Sender goes back to Slow start phase or Congestion avoidance phase.

- Slow Start Phase : exponential increment – In this phase after every RTT the congestion window size increments exponentially.

- Congestion Avoidance Phase : additive increment – This phase starts after the threshold value also denoted as ssthresh. The size of cwnd(congestion window) increases additive. After each RTT cwnd = cwnd + 1.
- Congestion Detection Phase : multiplicative decrement – If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment. Retransmission is needed to recover a missing packet that is assumed to have been dropped by a

router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

 # Protocol Spoofing:-

IP spoofing is a method in which TCP/IP or UDP/IP data packets are sent with a fake sender address. The attacker uses the address of an authorized, trustworthy system. In this way, it can inject its own packets into the foreign system that would otherwise be blocked by a filter system. In most cases, IP spoofing is used to perform DoS and DDoS attacks. Under certain circumstances, the attacker can also use the stolen IP to intercept or manipulate the data traffic between two or more computer systems. Such Man-in-the-Middle attacks that use the help of IP spoofing nowadays require (with few exceptions) that the attack be in the same subnet as the victim.

Ipv6 :-

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. IPv6 was designed by Internet Engineering Task Force (IETF) in December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

IPv4 vs IPv6

The common type of IP address (is known as IPv4, for “version 4”). Here’s an example of what an IP address might look like:
25.59.209.224
An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255. This group of separated numbers creates the addresses that let you and everyone around the globe to send and retrieve data over our Internet connections. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. To date, it is considered the primary Internet Protocol and carries 94% of Internet traffic. Initially, it was assumed it would never run out of addresses but the present situation paves a new way to IPv6, let’s see why? An IPv6 address consists of eight groups of four hexadecimal digits. Here’s an example IPv6 address:

3001:0da8:75a3:0000:0000:8a2e:0370:7334
This new IP address version is being deployed to fulfil the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation).

Types of IPv6 Address

Now that we know about what is IPv6 address let’s take a look at its different types.

- Unicast addresses It identifies a unique node on a network and usually refers to a single sender or a single receiver.
- Multicast addresses It represents a group of IP devices and can only be used as the destination of a datagram.
- Anycast addresses It is assigned to a set of interfaces that typically belong to different nodes.

Advantages of IPv6

- Reliability
- Faster Speeds: IPv6 supports multicast rather than broadcast in IPv4.This feature allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations all at once.
- Stronger Security: IPSecurity, which provides confidentiality, and data integrity, is embedded into IPv6.
- Routing efficiency
- Most importantly it’s the final solution for growing nodes in Global-network.

Disadvantages of IPv6

- Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
- Communication: IPv4 and IPv6 machines cannot communicate directly with each other. They need an intermediate technology to make that possible.