**Q #16) What are IP classes and how can you identify the IP class of given an IP address?**

**Answer:** An IP address has 4 sets (octets) of numbers each with a value up to 255.

**For Example**, the range of the home or commercial connection started primarily between 190 x or 10 x. IP classes are differentiated based on the number of hosts it supports on a single network. If IP classes support more networks then very few IP addresses are available for each network.

There are three types of IP classes and are based on the first octet of IP addresses which are classified as Class A, B or C. If the first octet begins with 0 bit then it is of type Class A.

Class A type has a range up to 127.x.x.x (except 127.0.0.1). If it starts with bits 10 then it belongs to Class B. Class B having a range from 128.x to 191.x. IP class belongs to Class C if the octet starts with bits 110. Class C has a range from 192.x to 223.x.

**Q #17) What is meant by 127.0.0.1 and localhost?**

**Answer:** IP address 127.0.0.1, is reserved for loopback or localhost connections. These networks are usually reserved for the biggest customers or some of the original members of the Internet. To identify any connection issue, the initial step is to ping the server and check if it is responding.

If there is no response from the server then there are various causes like the network is down or the cable needs to be replaced or the network card is not in good condition. 127.0.0.1 is a loopback connection on the Network Interface Card (NIC) and if you are able to ping this server successfully, then it means that the hardware is in a good shape and condition.

127.0.0.1 and localhost are the same things in most of the computer network functioning.

**Q #18) What is NIC?**

**Answer:** NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.

Each NIC has a MAC address which helps in identifying the computer on a network.

**Q #19) What is Data Encapsulation?**

**Answer:** In a computer network, to enable data transmission from one computer to another, the network devices send messages in the form of packets. These packets are then added with the IP header by the OSI reference model layer.

The Data Link Layer encapsulates each packet in a frame that contains the hardware address of the source and the destination computer. If a destination computer is on the remote network then the frames are routed through a gateway or router to the destination computer.

**Q #20) What is the difference between the Internet, Intranet, and Extranet?**

**Answer:** The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

 **Internet**: Applications are accessed by anyone from any location using the web.

 **Intranet**: It allows limited access to users in the same organization.

 **Extranet**: External users are allowed or provided with access to use the network application of the organization.

**Q #21) What is a VPN?**

**Answer:** VPN is the Virtual Private Network and is built on the Internet as a private wide area network. Internet-based VPNs are less expensive and can be connected from anywhere in the world.

VPNs are used to connect offices remotely and are less expensive when compared to WAN connections. VPNs are used for secure transactions and confidential data can be transferred between multiple offices. VPN keeps company information secure against any potential intrusion.

**Given below are the 3 types of VPN’s:**

1. **Access VPN**: Access VPN’s provide connectivity to mobile users and telecommuters. It is an alternative option for dial-up connections or ISDN connections. It provides low-cost solutions and a wide range of connectivity.

2. **Intranet VPN**: They are useful for connecting remote offices using shared infrastructure with the same policy as a private network.

3. **Extranet VPN**: Using shared infrastructure over an intranet, suppliers, customers, and partners are connected using dedicated connections.



**Q #22) What are Ipconfig and Ifconfig?**

**Answer: Ipconfig** stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.

The command Ipconfig is useful for displaying all TCP/IP network summary information currently available on a network. It also helps to modify the DHCP protocol and DNS setting.

**Ifconfig** (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It is used to configure, control the TCP/IP network interface parameters from CLI i.e. Command Line Interface. It allows you to see the IP addresses of these network interfaces.

**Q #23) Explain DHCP briefly?**

**Answer:** DHCP stands for Dynamic Host Configuration Protocol and it automatically assigns IP addresses to the network devices. It completely removes the process of manual allocation of IP addresses and reduces the errors caused due to this.

This entire process is centralized so that the TCP/IP configuration can also be completed from a central location. DHCP has a “pool of IP addresses” from which it allocates the IP address to the network devices. DHCP cannot recognize if any device is configured manually and assigned with the same IP address from the DHCP pool.

In this situation, it throws the “IP address conflict” error.



DHCP environment requires DHCP servers to set-up the TCP/IP configuration. These servers then assign, release and renew the IP addresses as there might be a chance that network devices can leave the network and some of them can join back to the network.

**Q #24) What is SNMP?**

**Answer:** SNMP stands for Simple Network Management Protocol. It is a network protocol used for collecting organizing and exchanging information between network devices. SNMP is widely used in network management for configuring network devices like switches, hubs, routers, printers, servers.

**SNMP consists of the below components:**

 SNMP Manager

 Managed device

 SNMP Agent

 Management Information Base (MIB)

**The below diagram shows how these components are connected with each other in the SNMP architecture:**



SNMP is a part of the TCP/IP suite. There are 3 main versions of SNMP which include SNMPv1, SNMPv2, and SNMPv3.

**Q #25) What are the different types of a network? Explain each briefly.**

**Answer:** There are 4 major types of networks.

**Let’s take a look at each of them in detail.**

1. **Personal Area Network (PAN)**: It is the smallest and basic network type that is often used at home. It is a connection between the computer and another device such as phone, printer, modem tablets, etc

2. **Local Area Network (LAN)**: LAN is used in small offices and Internet cafes to connect a small group of computers to each other.

Usually, they are used to transfer a file or for playing the game in a network.

3. **Metropolitan Area Network (MAN):** It is a powerful network type than LAN. The area covered by MAN is a small town, city, etc. A huge server is used to cover such a large span of area for connection.

4. **Wide Area Network (WAN)**: It is more complex than LAN and covers a large span of the area typically a large physical distance. The Internet is the largest WAN which is spread across the world. WAN is not owned by any single organization but it has distributed ownership.

**There are some other types of the network as well:**

 Storage Area Network (SAN)

 System Area Network (SAN)

 Enterprise Private Network (EPN)

 Passive Optical Local Area Network (POLAN)