What is some network Utilities/ commands?  
Ans:-

1:-If\_config -> Network Configuration Information

2:- Hostname - > find the name of the Host

3:- NetState -> tells us about the all open and close ports   
 determine all the network connections   
 routing table’s information and interface statistics

4:- NSLOOKUP -> Stands for the name server lookup. It trouble shoots DNS servers. It finds the all the   
 ip addresses for given domain name.

5:- traceroute - >

6:- ping -> the ping command is a network utility used to check the reachability of a host on an Internet   
 Protocol (IP) network and measure the round-trip time for messages sent from the originating   
 host to a destination computer. It works by sending Internet Control Message Protocol (ICMP)  
 Echo Request packets to the target host and waiting for ICMP Echo Reply packets in response.

7: - dig - > Stands for the Domain Information Greeper... It queries DNS related information to obtain all types of the record information.

# Q: - What is Subnet Addressing?

Each 32 bit address is divided into 2 parts, like 123.1.1.8/24

1:- A network Prefix (/24 denotes that 24 bits is used as Network Prefix so 123.1.1 show network information)

2:- A host Suffix (remaining 8 bits show information about the host in tha network)

This is called subnet addressing and also called ***classless addressing***

a.b.c.d/n --> is called the **CIDR** notation (**Classless Inter Domain Routing**)

# Q: - Then? What is class full addressing?

Ans:- Introduced in 1981, with classful routing, IP v4 addresses were divided into 5 classes(A to E).

Classes A-C: unicast addresses

Class D: multicast addresses

Class E: reserved for future use

Class A:-

In a class A address, the first bit of the first octet is always ‘0’. Thus, class A addresses range from 0.0.0.0 to 127.255.255.255(as 01111111 in binary converts to 127 in decimal). The first 8 bits or the first octet denote the network portion and the rest 24 bits or the 3 octets belong to the host portion. Its Subnet mask is 255.0.0.0.

**Example:** 10.1.1.1

**Exception –**

- 127.X.X.X is reserved for loopback

- 0.X.X.X is reserved for default network.

Class B:-

In a class B address, the first octet would always start with ’10’. Thus, class B addresses range from 128.0.0.0 to 191.255.255.255. The first 16 bits or the first two octets denote the network portion and the remaining 16 bits or two octets belong to the host portion. Its Subnet mask is 255.255.0.0 .

**Example:** 172.16.1.1

Class C:-

In a class C address, the first octet would always start with ‘110’. Thus, class C addresses range from 192.0.0.0 to 223.255.255.255. The first 24 bits or the first three octets denote the network portion and the rest 8 bits or the remaining one octet belong to the host portion. Its Subnet mask is 255.255.255.0.

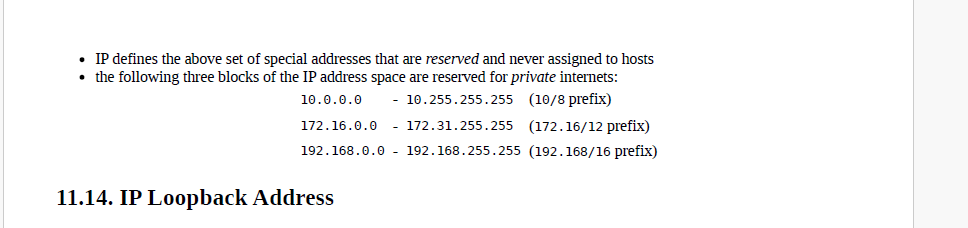
**Example:** 192.168.1.1

**Class D :**   
Class D is used for multicast addressing and in a class D address the first octet would always start with ‘1110’. Thus, class D addresses range from 224.0.0.0 to 239.255.255.255. Its Subnet mask is not defined.

**Example:** 239.2.2.2

Class D addresses are used by routing protocols like OSPF, RIP, etc.

**Class E :**   
Class E addresses are reserved for research purposes and future use. The first octet in a class E address starts with ‘1111’. Thus, class E addresses range from 240.0.0.0 to 255.255.255.255. Its Subnet mask is not defined.



# Routing Algorithms

**Link State Routing Algorithms:-**

The Link State Routing Algorithm is an interior protocol used by every router to share information or knowledge about the rest of the routers on the network. The link state routing algorithm is distributed by which every router computes its routing table.

## 1:- Shortest Path First (SPF):

SPF is used in link-state routing protocols such as OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System). It calculates the shortest path from a source node to all other nodes in the network based on the link costs or metrics.

## 2:-Distance Vector:

Distance Vector algorithms, such as Routing Information Protocol (RIP), use a decentralized approach where routers exchange information about the distance (metric) to reach various destinations. Each router maintains a routing table containing the distance and next-hop information for known destinations.

## 3; - Border Gateway Protocol (BGP):

BGP is an exterior gateway protocol used in large-scale networks to exchange routing information between autonomous systems (ASes). BGP employs the path vector algorithm, which considers various attributes (such as AS path length, preference, and policies) to determine the best path for routing between Ases

## 4:- Adaptive Routing:

Adaptive routing algorithms dynamically adjust routing decisions based on real-time network conditions. These algorithms monitor factors such as network congestion, link quality, and traffic load to determine the best path for forwarding packets.

## 5:- Static Routing:

Static routing involves manually configuring static routes in routers' routing tables. Administers explicitly define the paths that packets should follow to reach specific destinations. Static routing does not dynamically adjust routes based on network changes

# Forwarding and Routing

Forwarding (in data plane) and routing (in control plane).

## Forwarding:-

Refers to the router-local action of transferring a packet from an input link interface to the appropriate output link interface. Forwarding takes place at very short timescales (typically a few nanoseconds), and thus is typically implemented in hardware.

# Routing:-

Refers to the network-wide process that determines the end-to-end paths that packets take from source to destination. Routing takes place on much longer timescales (typically seconds), and as we will see is often implemented in software.

# Q:- What are special Ip addresses?

Special IP addresses are specific ranges or individual IP addresses reserved for special purposes in IPv4 networking. They are not used for regular public or private internet communication. Here are some common special IP addresses and their purposes:

### 1. **Private IP Addresses**

* **Definition**: These addresses are used within private networks and are not routable on the public internet.
* **Ranges**:
  + **Class A**: 10.0.0.0 to 10.255.255.255
  + **Class B**: 172.16.0.0 to 172.31.255.255
  + **Class C**: 192.168.0.0 to 192.168.255.255
* **Use**: Commonly used in home, office, and enterprise networks to assign IP addresses to devices without using public IP addresses.

### 2. **Loopback Addresses**

* **Definition**: Used by a host to send traffic to itself.
* **Range**: 127.0.0.0 to 127.255.255.255
* **Common Address**: 127.0.0.1
* **Use**: Network testing and debugging. For example, ping 127.0.0.1 tests if the TCP/IP stack is working on the local machine.

# Q:- What is DHCP:

Ans:- It stands for Dynamic Host Configration Protocol. Here are its functionalities which it perform for host.

1:- **Address Allocation is done through DHCP.**2:- Allows host to learn additional information like network prefix   
3:- The address of the its first hop router (often called the default gateway)  
4:- Host local DNS server.  
5:- DHCP uses client\_server protocol.  
6**:-Uses UDP and run in port 67.**  
7:- In a home network , the router usually act as the DHCP server.

Q:- Where ip addresses are managed?

Ans:- Ip addresses are managed by  **ICANN** which stands Internet Corporation for assigned Names and Numbers.

**Q;- What is the ICMP protocol?**

ICMP is the Internet Control Message Protocol. It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing if the data is reaching the preferred destination in time. It uses port 7 by default.  
  
Q:- Explain the port functionality ?

Ports are a transport layer (layer 4) concept. Only a transport protocol such as the [Transmission Control Protocol (TCP)](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) or [User Datagram Protocol (UDP)](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/) can indicate which port a packet should go to. TCP and UDP headers have a section for indicating port numbers. [Network layer](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) protocols — for instance, the [Internet Protocol (IP)](https://www.cloudflare.com/learning/network-layer/internet-protocol/) — are unaware of what port is in use in a given network connection. In a standard IP header, there is no place to indicate which port the data [packet](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) should go to. IP headers only indicate the destination IP address, not the port number at that IP address

**Q: - What is a port?**

Ans: - A port is a virtual point where network connection start and end. Ports are software-based and managed by a computer’s operating system. Each port is associated with a specific process or service . Ports allow computers to easily differentiate between different kinds of traffic : emails go to a different port than webpages, for instance even though both reach a computer over the same internet connection.

**Q: - What is a port number?**

Ports are standardized across all network-connected devices, with each port assigned a number. Most ports are reserved for certain [protocols](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) — for example, all [Hypertext Transfer Protocol (HTTP)](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) messages go to port 80. While [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) enable messages to go to and from specific devices, port numbers allow targeting of specific services or applications within those devices.

**Q: - What is the criticsms of NAT?**

Ans: - 1:- Port numbers should be used for addressing processes, not hosts   
 2:- Routers are supposed to do packet processing only upto the network layer.  
 3: - NAT violates end-to-end principles: hosts should be communicating directly.  
 4: - IPv6 should be used to solve problem of shortage of addresses.

**Q:- Explain the packet, fragment, frame, datagram, and segment?**

Networks have made information transmission and sharing easier. The Internet enables us to share information within companies in local networks or worldwide. While sharing, data is represented by bytes.

The data bytes have a specific format in the OSI networking model since each layer has its specific unit. The data units also depend on the used protocols or connections.

1. PacketWhile communicating through networks it’s important to send and receive files and information. The basic unit of communication between a source and a destination in a network is a packet.

Data sent through the network is divided into packets, that are recombined by the destination devices. Dividing data into packets allows the network to manage different bandwidths, routes, and multiple connected devices that share data and receive packets independently from each other.It makes it easier to retransmit lost pieces of data or interrupted ones.

**Packets are data units within the network layer in**[**the OSI model**](https://www.baeldung.com/cs/osi-model)**.**

# 2. Fragment

In each network, there is a maximum size of the data to the transmitted called the MTU (Maximum Transmitted Unit). **Packets can often be larger than the maximum size, so each packet is also divided into smaller pieces of data called fragments. The network layer is responsible for fragmentation.**

# 3. Frame

Just like packets, frames are small parts of a message in the network. It helps to identify data and determine the way it should be decoded and interpreted. The main difference between a packet and a frame is the associate with the OSI layers.  
 **While a packet is the unit of data used in the network layer , a frame is the unit of data used in the OSI model’s data link layer.**A frame contain more information about the transmitted message than a packet.

# 4:- Datagram

**The datagram represents a data unit of transfer in networking.** Data transmitted in a network is divided into smaller parts called datagrams. In a datagram, we divide data frequently and transmitted from source to destination without a predefined route. We also can’t guarantee the order of delivery to the receiver end.

**While**[**TCP**](https://www.baeldung.com/cs/popular-network-protocols)**uses packets in connection-oriented protocols, datagrams are used in**[**UDP**](https://www.baeldung.com/cs/popular-network-protocols)**,** making them carry less information since they don’t need to have a response message from the destination. [The transport layer](https://www.baeldung.com/cs/osi-model) uses datagram as a unit of transfer data. A datagram comprises a header, IP addresses of destination and source, and the data.

**The problem with datagram is it can’t manage subsequent or prior data communication.**

# 5:- Segment

**A segment is a broken piece of a packet with a TCP header in each of them.** Alongside the source and destination ports, it contains the checksum field that ensures the conveyed data’s correctness through the network. **Segments increase the efficiency of network performance and improve security.**

**Q:- What is the difference between segmentation and fragmentation?**

1. **Fragmentation:**- Fragmentation typically occurs at the network layer (Layer 3 of the OSI model) in the networking protocol stack.  
   - Fragmentation is the process of breaking up a packet into smaller fragments to fit the Maximum Transmission Unit (MTU) size of the underlying network.  
   - Fragmentation is usually performed by routers when a packet is too large to be transmitted over a network with a smaller MTU size. Each fragment is treated as a separate packet and may take a different path to reach the destination.  
   - Fragments contain the necessary information to be reassembled at the destination. The original packet can be reconstructed by reassembling the fragments in the correct order.
2. **Segmentation:**- Segmentation typically occurs at the transport layer (Layer 4 of the OSI model) in the networking protocol stack.  
   - Segmentation is the process of dividing data from the application layer into smaller segments for transmission over the network.  
   - Segmentation is performed by the transport layer protocols such as TCP (Transmission Control Protocol) to break the data into segments that can be transmitted efficiently over the network.  
   - Segments are reassembled at the receiving end by the transport layer protocol to reconstruct the original data.  
   - Segmentation is mainly concerned with ensuring reliable data transfer, flow control, and error recovery.

Both Socket and Port are the terms used in [Transport Layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/). A port is a logical construct assigned to network processes so that they can be identified within the system. A socket is a combination of port and IP address. Port number can be represented  by a single number ( example: 1028) on the other hand socket address can be represented by (tcp, hostname ,1028). An incoming packet has a port number which is used to identify the process that needs to consume the packet. The lowest numbered 1024 port numbers are used for the most commonly used services. These ports are called the well-known ports. Higher-numbered ports are available for general use by applications and are known as ephemeral ports.

| **Socket** | **Port** |
| --- | --- |
| The word “Socket” is the combination of port and IP address. | The word “Port” is the number used by particular software. |
| It is used to identify both a machine and a service within the machine. | The same port number can be used in different computer running on same software. |