GYANMANDIR

www.akdnetwork.com

INTERNET

The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection. The short form of internet is the 'net'.

LAN

A network that connects computers and devices within a building or small group of buildings is known as a local area network (LAN). A LAN may link the computers within a home, office, or campus, for example, allowing the individual users to share resources.

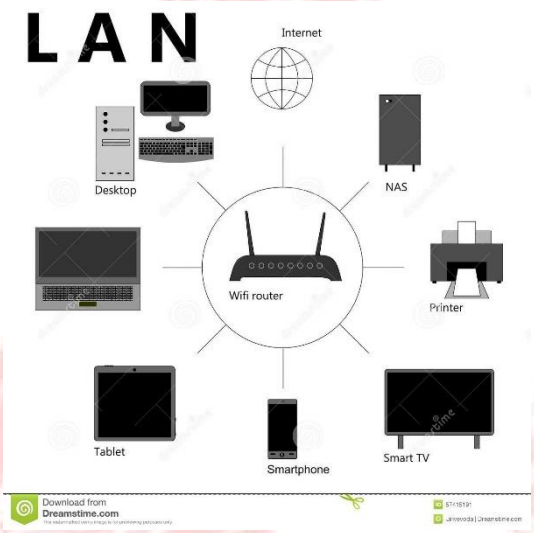


Fig:- Local Area Network

BROADBAND

Broadband refers to various high-capacity transmission technologies that transmit data, voice, and video across long distances and at high speeds. Common mediums of transmission include coaxial cables, fiber optic cables, and radio waves.

Broadband is always connected and removes the need for dial-up. Its importance is far-reaching; it allows for high-quality and quick access to information, teleconferencing, data transmission, and more in various capacities, including healthcare, education, and technological development.

WI-FI

Wireless connectivity, often known as Wi-Fi, is the technology that allows a PC, laptop, mobile phone, or tablet device to connect at high speed to the internet without the need for a physical wired connection. Wi-Fi (pronounced “Why-Fy”) is a term that was coined by a branding company in 1999 as a name which would be easily recalled, due to its similarity to the then well-known term “hi-fi”.

MOBILE DATA

Mobile data allows your phone to access the Internet even when you're not on Wi-Fi. Mobile data gives you an Internet connection anywhere as long as you're connected to a cellular network. The speed is lesser than Wi-Fi and Broadband connection.

IP (INTERNET PROTOCOL)

IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.An IP address allows information to be sent and received by the correct parties, which means they can also be used to track down a user's physical location.

ROUTER

A router is a computer whose software and hardware are designed to move data between computer networks. Routers make sure traffic between computers goes where it needs to go. They do this by choosing the shortest path between the computers using a complicated system of rules called routing protocols.

Fig :- Wireless Router

SWITCH

A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended. Each networked device connected to a switch can be identified by its network address, allowing the switch to direct the flow of traffic maximizing the security and efficiency of the network.

Fig :- Network Switch

CAT 5

Alternatively known as an Ethernet cable or LAN cable, a Cat 5 or category 5 is a network cable that consists of four twisted pairs of copper wire terminated by an RJ-45 connector. The picture shows an example of a Cat 5 cable. Cat 5 cable is used in home and business networks, providing data transmission speeds of up to 100 Mbps. The maximum recommended length of a Cat 5 cable is 100 meters. Exceeding this length without the aid of a bridge or other network device could cause network issues, including data packet loss and data transmission speed degradation.

Fig :- CAT 5 Cable

RJ45

The eight-pin **RJ45** connector is a standardised interface which often connects a computer to a local area network (LAN). This type of connector was originally developed for telephone communications but is now used in a range of applications. The abbreviation, RJ45, stands for Registered Jack-45. Registered jack specifications are related to the wiring patterns of the jacks, rather than their physical characteristics. The term RJ45 has also come to refer to a range of connectors for Ethernet jacks. An 8 Position/8 Contact connector, called an 8P8C, is a modular connector for telecommunication cables. It is also informally referred to as an RJ45.

Fig:- RJ45 Connector

OPTICAL FIBER

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.

Fig:- Optical Fiber

BANDWIDTH

The maximum amount of data transmitted over an internet connection in a given amount of time. Bandwidth is often mistaken for internet speed when it's actually the volume of information that can be sent over a connection in a measured amount of time – calculated in megabits per second (Mbps).

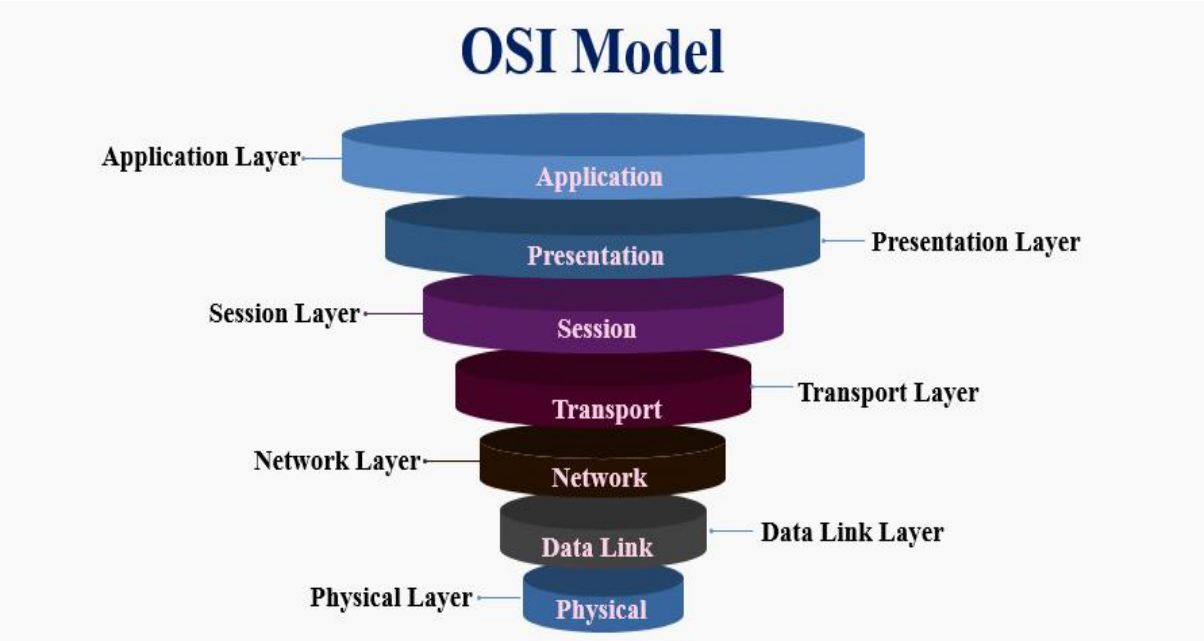
BANDWIDTH VS SPEED

Internet speed is the measure of how fast information is transferred, while bandwidth refers to the capacity of an individual internet connection. So if your internet connection has a bandwidth of 5 Mbps, your speed would only be that fast if it's operating at full capacity.

WWW (World Wide Web)

World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

Layers of OSI Model



Discussed below is each stage of the Open Systems Interconnection Model in detail. Please go through these carefully to understand the structure and the functioning of the model in a systematic manner:

1. Physical Layer

- It is the bottom-most or the first layer of the OSI Model
- It comprises the raw data which is further transmitted to the higher layers of the structure
- Preparing the physical devices in the network and accepting the received data for transmission
- The termination of connection between two nodes of a network also takes place at this stage
- This layer converts the digital bits into electrical, radio, or optical signals

2. Data Link Layer

- Access to get the data is achieved at this layer
- It breaks the input data into frames which makes analysing the data easier
- Ensures that the data received is free of any errors
- It controls the flow of data in the stipulated time duration and along with a set speed of transmission
- The data is sent to the next layer in the form of packets which are then reviewed for further processing

3. Network Layer

- It acts as a network controller
- Transferring of variable data from one node to another, connected in a network, takes place at this layer

- Each node has a specific address and the network layer ensures that the data is sent to its destination address
- The data is sent in the form of fragments which are then connected to each other once the processing is done

4. Transport Layer

- The delivery of data packets is managed by the transport layer
- It manages the flow of data, segmentation and desegmentation and error control
- There are five classes of the transport protocol, starting from 0 and continuing till 4 (TP0 to TP4)
- Fragmentation and reassembly of data packets occur that this stage

5. Session Layer

- The connection between the computers connected in a network is managed at this layer
- Establishment, management and termination between the remote and local application takes place here
- Authentication and authorisation happen at this layer
- This layer can also terminate or end any session or transmission which is complete

6. Presentation Layer

- The data is converted into the syntax or semantics which an application understands
- Before passing on the data any further, the data is formatted at this stage
- Functions including compression, encryption, compatible character code set, etc. are also done at this layer of the model
- It serves as a data translator for the network

7. Application Layer

- The interaction with the user or the user application takes place at this stage
- When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit

On the whole, the entire process of transfer of raw data into processed data and finally to the user or the application can be done through this OSI model. It can detect eros, transmit the data and format it during the course of the above-mentioned seven layers.

Structure and Types of IP Address

An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different

routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

IP address structure:

IP addresses are displayed as a set of four digits- the default address maybe 192.158.1.38. Each number on the set may range from 0 to 255. Therefore, the total IP address range ranges from 0.0.0.0 to 255.255.255.255.

```
IP address is basically divided into two parts: X1. X2. X3. X4

1. [X1. X2. X3] is the Network ID

2. [X4] is the Host ID
```

1. **Network ID–**
   It is the part of the left-hand IP address that identifies the specific network where the device is located. In the normal home network, where the device has an IP address 192.168.1.32, the 192.168.1 part of the address will be the network ID. It is customary to fill in the last part that is not zero, so we can say that the device's network ID is 192.168.1.0.
2. **Hosting ID–**
   The host ID is part of the IP address that was not taken by the network ID. Identifies a specific device (in the TCP / IP world, we call devices "host") in that network. Continuing with our example of the IP address 192.168.1.32, the host ID will be 32- the unique host ID on the 192.168.1.0 network.

IP Address Types:

There are 4 types of IP Addresses- Public, Private, Fixed, and Dynamic. Among them, public and private addresses are derived from their local network location, which should be used within the network while public IP is used offline.

1. **Public IP address–**
   A public IP address is an Internet Protocol address, encrypted by various servers/devices. That's when you connect these devices with your internet connection. This is the same IP address we show on our homepage. So why the second page? Well, not all people speak the IP language. We want to make it as easy as possible for everyone to get the information they need. Some even call this their external IP address. A public Internet Protocol address is an Internet Protocol address accessed over the Internet. Like the postal address used to deliver mail to your home, the public Internet Protocol address is a different international Internet Protocol address assigned to a computer device. The web server, email server, and any server device that has direct access to the Internet are those who will enter the public Internet Protocol address. Internet Address Protocol is unique worldwide and is only supplied with a unique device.
2. **Private IP address–**
   Everything that connects to your Internet network has a private IP address. This includes computers, smartphones, and tablets but also any

Bluetooth-enabled devices such as speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is likely to increase. Your router needs a way to identify these things separately, and most things need a way to get to know each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that separates the network.

3. **Static IP Address–**
   A static IP address is an invalid IP address. Conversely, a dynamic IP address will be provided by the Dynamic Host Configuration Protocol (DHCP) server, which can change. The Static IP address does not change but can be changed as part of normal network management. Static IP addresses are incompatible, given once, remain the same over the years. This type of IP also helps you get more information about the device.
4. **Dynamic IP address–**
   It means constant change. A dynamic IP address changes from time to time and is not always the same. If you have a live cable or DSL service, you may have a strong IP address. Internet Service Providers provide customers with dynamic IP addresses because they are too expensive. Instead of one permanent IP address, your IP address is taken out of the address pool and assigned to you. After a few days, weeks, or sometimes even months, that number is returned to the lake and given a new number. Most ISPs will not provide a static IP address to customers who live there and when they do, they are usually more expensive. Dynamic IP addresses are annoying, but with the right software, you can navigate easily and for free.

Types of Website IP address:

Website IP address is of two types- Dedicated IP Address and Shared IP Address. Let us discuss the two.

1. **Dedicated IP address–**
   A dedicated IP address is one that is unique for each website. This address is not used by any other domain. A dedicated IP address is beneficial in many ways. It provides increased speed when the traffic load is high and brings in increased security. But dedicated IPs are costly as compared to shared IPs.
2. **Shared IP address–**
   A shared IP address is one that is not unique. It is shared between multiple domains. A shared IP address is enough for most users because common configurations don’t require a dedicated IP.

IP Address Classification Based on Operational Characteristics:

According to operational characteristics, IP address is classified as follows:

1. **Broadcast addressing–**
   The term ‘Broadcast’ means to transmit audio or video over a network. A broadcast packet is sent to all users of a local network at once. They do not have to be explicitly named as recipients. The users of a network can open the data packets and then interpret the information, carry out the instructions or discard it. This service is available in IPv4. The IP address commonly used for broadcasting is 255.255.255.255
2. **Unicast addressing–**
   This address identifies a unique node on the network. Unicast is nothing but one-to-one data transmission from one point in the network to another. It is the most common form of IP addressing. This method can be used for both sending and receiving data. It is available in IPv4 and IPv6.
3. **Multicast IP addresses–**
   These IP addresses mainly help to establish one-to-many communication. Multicast IP routing protocols are used to distribute data to multiple recipients. The class D addresses (224.0.0.0 to 239.255.255.255) define the multicast group.
4. **Anycast addressing–**
   In anycast addressing the data, a packet is not transmitted to all the receivers on the network. When a data packet is allocated to an anycast address, it is delivered to the closest interface that has this anycast address

Class A Network

This IP address class is used when there are a large number of hosts. In a Class A type of network, the first 8 bits (also called the first octet) identify the network, and the remaining have 24 bits for the host into that network.

An example of a Class A address is 102.168.212.226. Here, “102” helps you identify the network and 168.212.226 identify the host.

Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for **loopback and diagnostic functions.**

Class B Network

In a B class IP address, the binary addresses start with 10. In this IP address, the class decimal number that can be between **128 to 191.** The number 127 is reserved for loopback, which is used for internal testing on the local machine. The first 16 bits (known as two octets) help you identify the network. The other remaining 16 bits indicate the host within the network.

An example of Class B IP address is 168.212.226.204, where *168 212* identifies the network and *226.204* helps you identify the Hut network host.

Class C Network

Class C is a type of IP address that is used for the small network. In this class, three octets are used to indent the network. This IP ranges between **192 to 223.**

In this type of network addressing method, the first two bits are set to be 1, and the third bit is set to 0, which makes the first 24 bits of the address them and the remaining bit as the host address. Mostly local area network used Class C IP address to connect with the network.

Example for a Class C IP address:

192.168.178.1

Class D Network

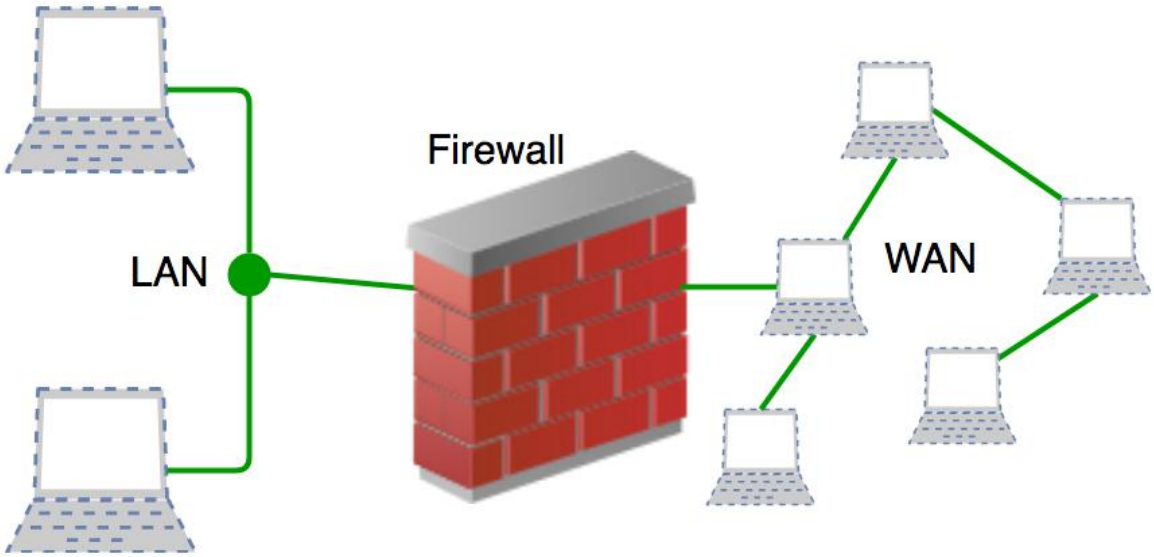
Class D addresses are only used for multicasting applications. Class D is never used for regular networking operations. This class addresses the first three bits set to “1” and their fourth bit set to use for “0”. Class D addresses are 32-bit network addresses. All the values within the range are used to identify multicast groups uniquely.

Therefore, there is no requirement to extract the host address from the IP address, so Class D does not have any subnet mask.

Introduction of Firewall in Computer Network

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an “unreachable error”
Drop : block the traffic with no reply
A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



History and Need for Firewall

Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers. ACLs are rules that determine whether network access should be granted or denied to specific IP address.
But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.

Connectivity to the Internet is no longer optional for organizations. However, accessing the Internet provides benefits to the organization; it also enables the outside world to interact with the internal network of the organization. This creates a threat to the organization. In order to secure the internal network from unauthorized traffic, we need a Firewall.

How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses type code instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).
Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to accept, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as drop (or reject) is always a good practice.

Types of Firewall

Firewalls are generally of two types: Host-based and Network-based.

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Why mask port numbers ?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies to the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are the same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.

- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.

- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.

- **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.

Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be dropped as only a fixed number of private IP addresses can be translated to public addresses.
3. Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

4. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

AKD
NETWORK