

# Learning Report Networking



*L&T Technology Services*



GLOBAL  
ENGINEERING  
ACADEMY

Genesis



**Document History**

Sl.No.	Release Date	Prepared. By	Reviewed By	To be approved By	Remarks/Revision Details
1		Name/PS No	Name/PS No	Module Owner Name	Comments
2	26/03/21	99003788			
3					

## Contents

### NETWORKING CONCEPTS:

<b>NETWORKING AND TYPES OF NETWORK:</b> .....	<b>4</b>
<b>NETWORK TOPOLOGY:</b> .....	<b>9</b>
<b>WIRELESS AND WIRED NETWORKS:</b> .....	<b>14</b>
<b>QUEUEING AND SCHEDULING</b> .....	<b>16</b>

### NETWORK SECURITY:

<b>OVERFLOWS (STACK AND HEAP)</b> .....	<b>19</b>
<b>CRYPTOGRAPHY AND ENCRPTION</b> .....	<b>19</b>
<b>SSH , TLS , MTLS</b> .....	<b>22</b>

### NETWORK COMPONENTS:

<b>ROUTER:</b> .....	<b>26</b>
<b>HUB:</b> .....	<b>27</b>
<b>SWITCH:</b> .....	<b>29</b>
<b>BRIDGE:</b> .....	<b>30</b>
<b>GATEWAY:</b> .....	<b>31</b>
<b>ACCESS POINT:</b> .....	<b>32</b>

### OSI MODEL:

<b>PHYSICAL LAYER:</b> .....	<b>34</b>
<b>DATA LINK LAYER:</b> .....	<b>35</b>
<b>NETWORK LAYER:</b> .....	<b>35</b>
<b>TRANSPORT LAYER:</b> .....	<b>36</b>
<b>SESSION LAYER:</b> .....	<b>38</b>
<b>PRESENTATION LAYER:</b> .....	<b>38</b>
<b>APPLICATION LAYER:</b> .....	<b>39</b>

### OSI MODEL:

<b>TCP/IP &amp; UDP/IP PROTOCOLS:</b> .....	<b>40</b>
<b>L2 &amp; L3 PROTOCOLS:</b> .....	<b>43</b>
<b>WLAN PROTOCOL:</b> .....	<b>45</b>
<b>BGP PROTOCOL:</b> .....	<b>47</b>

## IP ADDRESSING:

<b>IPV4 &amp; IPV6:</b> .....	<b>47</b>
<b>IPV4 SUBNETTING:</b> .....	<b>51</b>

## NETWORK TOOLS:

<b>PACKET TRACER:</b> .....	<b>53</b>
<b>WIRESHARK:</b> .....	<b>55</b>
<b>END TO END DATA FLOW:</b> .....	<b>56</b>
<b>REFERENCE:</b> .....	<b>57</b>

## **NETWORKING**

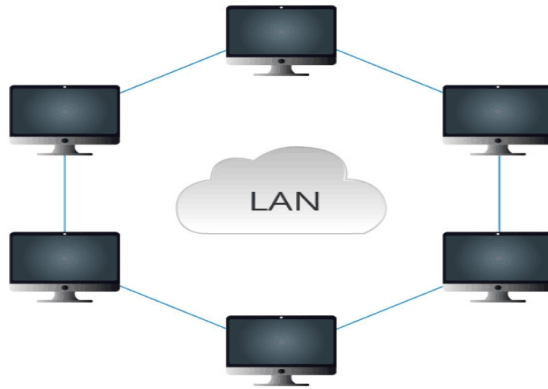
A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes. The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of network topologies.

### **Types of Networks**

A computer network can be categorized by their size. A computer network is mainly of four types:

#### **➤ LAN (Local Area Network):**

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- In LAN, connecting is done with the help of twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate.
- LAN provides higher security.



➤ **PAN (Personal Area Network):**

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

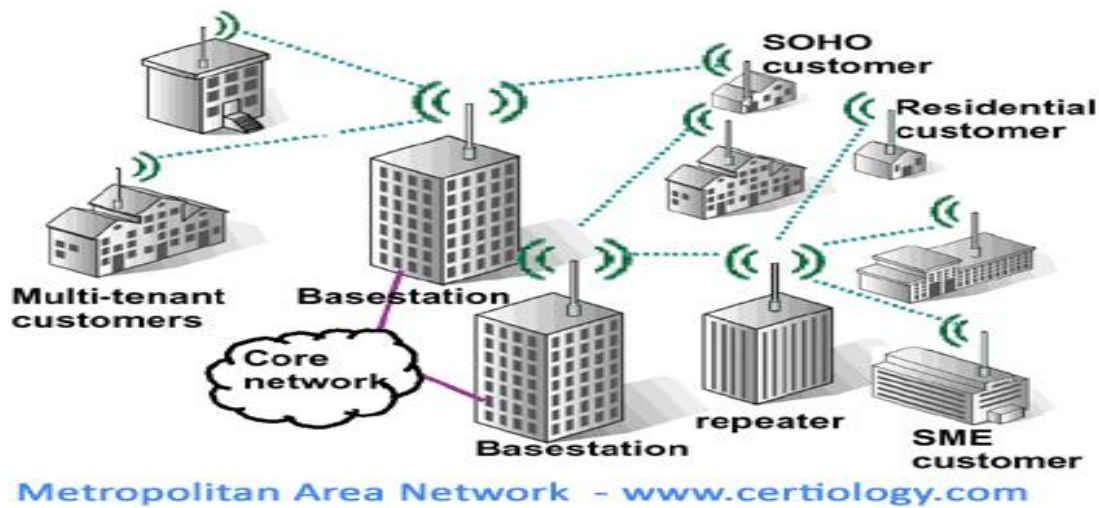


There are two types of Personal Area Network:

- **Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as Wi-Fi, Bluetooth.
- **Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

Examples of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. For example, a mobile network moves with a person.
  - **Offline Network:** An offline network can be created inside the home, so it is also known as a home network.
  - **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN.
- **MAN (Metropolitan Area Network):**
- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
  - Government agencies use MAN to connect to the citizens and private industries.
  - In MAN, various LANs are connected to each other through a telephone exchange line.
  - The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
  - It has a higher range than Local Area Network (LAN).



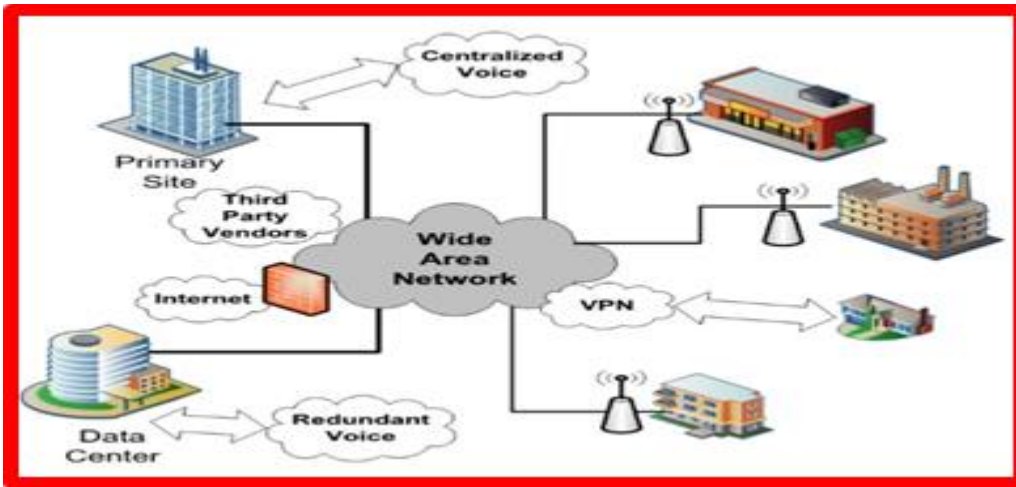
### Uses of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

### ➤ WAN (Wide Area Network):

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.





### Examples of Wide Area Network:

- Mobile Broadband
- Last mile
- Private network

### Advantages of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN..
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.



- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

## Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

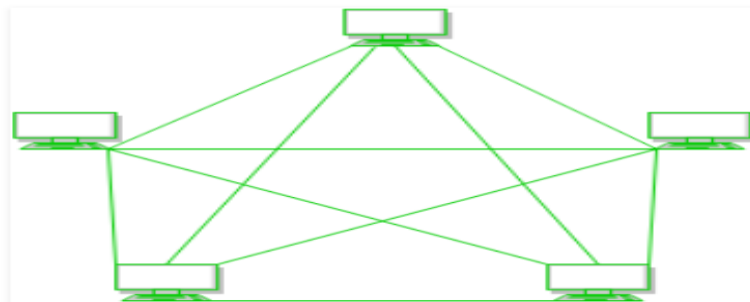
- **Security issue:** As all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used.
- **High Setup cost:** An installation cost of the WAN network is high
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

**Topology:** Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

## Types of Topology:

There are five types of topology in computer networks:

- **Mesh Topology:** In mesh topology, every device is connected to another device via particular channel.



Every device is connected with another via dedicated channels. These channels are known as links.

- If suppose, N number of devices are connected with each other in mesh topology, then total number of ports that is required by each device is N-1. In the figure, there are 5 devices connected to each other, hence total number of ports required is 4.
- If suppose, N number of devices are connected with each other in mesh topology, then total number of dedicated links required to connect them is  ${}^NC_2$  i.e.  $N(N-1)/2$ . In the Figure 1, there are 5 devices connected to each other, hence total number of links required is  $5*4/2 = 10$ .

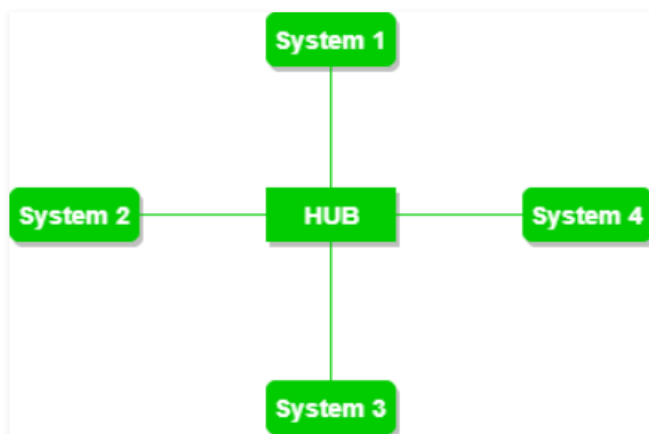
**Advantages of this topology:**

- It is robust.
- Fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

**Problems with this topology:**

- Installation and configuration is difficult.
- Cost of cables are high as bulk wiring is required, hence suitable for less number of devices.
- Cost of maintenance is high.

- **Star Topology:** In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node.



A star topology having four systems connected to single point of connection i.e. hub.

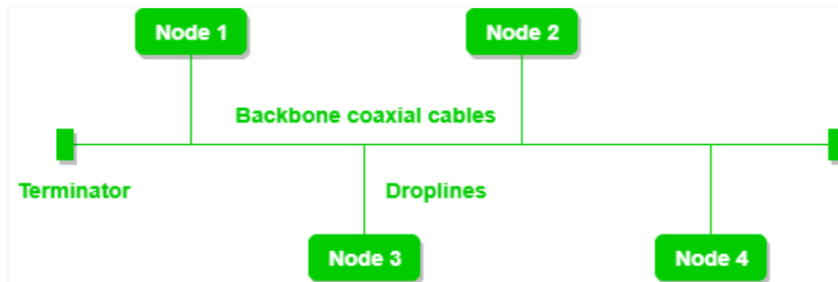
**Advantages of this topology:**

- If N devices are connected to each other in star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub.

**Problems with this topology:**

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- Cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

- **Bus Topology:** Bus topology is a network type in which every computer and network device is connected to single cable. It transmits the data from one end to another in single direction. No bi-directional feature is in bus topology.

**Advantages of this topology:**

- If N devices are connected to each other in bus topology, then the number of cables required to connect them is 1 which is known as backbone cable and N drop lines are required.
- Cost of the cable is less as compared to other topology, but it is used to build small networks.

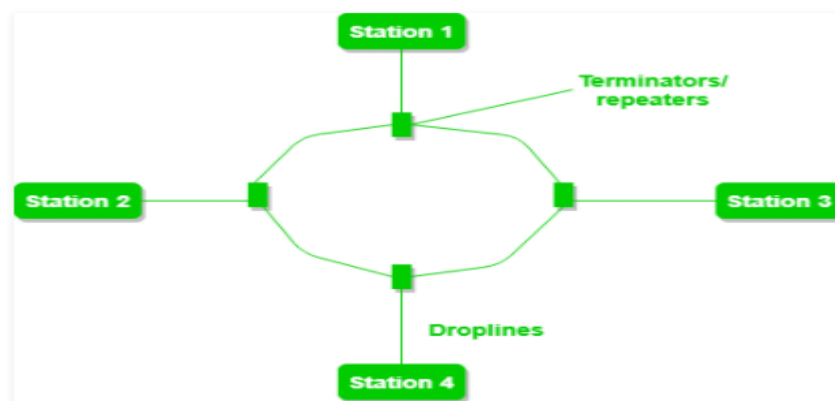
**Problems with this topology:**

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD etc.

- **Ring Topology:** In this topology, it forms a ring connecting devices with its exactly two neighboring devices.

Many repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.



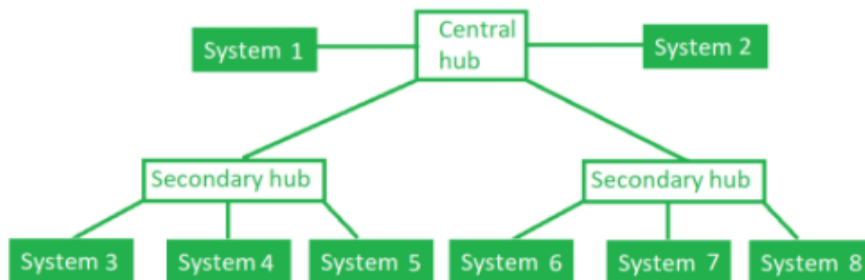
The following operations takes place in ring topology are:

- One station is known as **monitor** station which takes all the responsibility to perform the operations.
- To transmit the data, station must hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.
- There are two types of token release techniques: **Early token release** releases the token just after the transmitting the data and **Delay token release** releases the token after the acknowledgement is received from the receiver.

#### **Advantages of this topology:**

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- **Problems with this topology:** Troubleshooting is difficult in this topology.
- Addition of stations in between or removal of stations can disturb the whole topology.

- **Tree Topology:** This topology is the variation of Star topology. This topology has hierarchical flow of data.



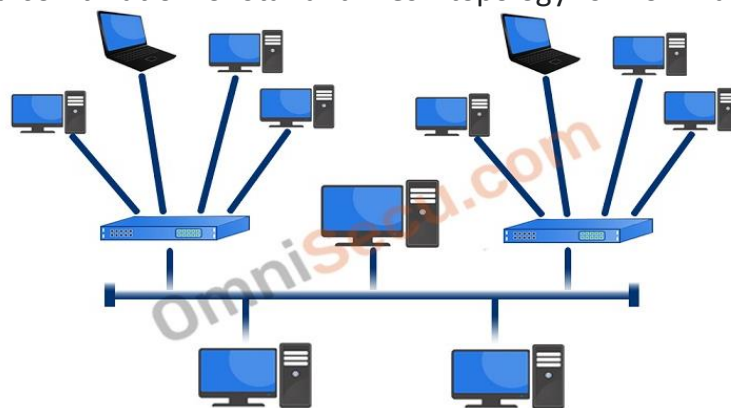
In this the various secondary hubs are connected to the central hub which contains the repeater. In this data flow from top to bottom i.e. from the central hub to secondary and then to the devices or from bottom to top.

#### **Advantages of this topology:**

- It allows more devices to be attached to a single central hub thus it increases the distance that is travel by the signal to come to the devices.
- It allows the network to get isolate and also prioritize from different computers.

#### **Problems with this topology:**

- If the central hub gets fails the entire system fails.
- The cost is high because of cabling.
- **Hybrid Topology:** A combination of two or more topology is known as hybrid topology. For example, a combination of star and mesh topology is known as hybrid topology.



#### **Advantages of Hybrid Topology:**

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

### Disadvantages of Hybrid topology:

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

## Wired & wireless networks

“**Wired**” as the name suggests refers to any physical medium connected through wires and cables. The wires/cables can be copper wire, twisted pair or even fiber optic. Wired connectivity is responsible for providing high security with high Bandwidth provisioned for each user.

In fact, Wired connectivity is considered highly reliable and incurs very low delay.

**Wireless**” as the term refers, uses air as a medium to send electromagnetic waves or infrared waves. Wireless devices have antennas for communication. Wireless connectivity provides a major benefit of user mobility and ease of deployment.

**Wired types:****➤ Twisted Pair**

- It consists of a pair of copper wires twisted around each other; the wires are around 1 to 2 mm thick and they are twisted to reduce the interference from the surrounding wires
- Twisted pairs consist of four wires or two pairs. In computer networks, eight wires or four pairs are utilized. This is also known as the Ethernet cable or RJ-45 cable.
- The pairs of wires are bundled together and covered by a protective shield.
- Transmission rate of 10-100 Mbps
- Maximum cable segment of 100 meter.

**➤ Coaxial Cable**

- Transmission rate of about 10 Mbps
- Maximum cable length of 185 meters for Thin-net, 500 meters for Thick-net
- ·Good resistance to electrical interference
- Less expensive than fiber-optics but more expensive than twisted pair.
- Flexible and easy to work with (Thin-net)
- Wire type is 20 AWG for Thin-net (R-58) and 12 AWG for Thick-net.

**➤ Fiber Optic**

- Transmission rate of 100 Mbps
- Cable length of 2 kilometers or more
- Not affected by electrical interference
- Supports voice, video, and data
- Provides the most secure media
- Most expensive cable
- Not very flexible; difficult to work with

**WIRELESS NETWORK**



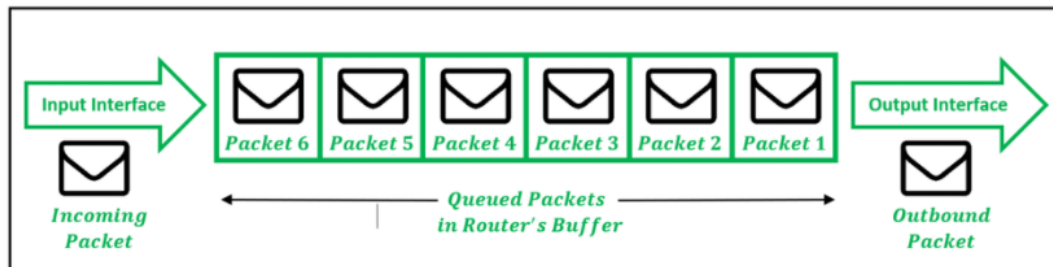
Name	Distance	Speed
LAN	1 KM	10 Mbps
WAN	--	10 Mbps– 20 Mbps
MAN	100 Kms	100 Mbps
Wi-Fi	1.6 Kms	30 Mbps -140 Mbps
Wi-max	50 Kms	25 Mbps

STANDARD	BANDWIDTH	RANGE
802.11	1–2 Mbps	100 meters (300 feet)
802.11a	54 Mbps	50 meters (150 feet)
802.11b	11 Mbps	100 meters (300 feet)
802.11g	54 Mbps	100 meters (300 feet)
HomeRF	10 Mbps	50 meters (150 feet)
HIPERLAN/1	Theoretically 20 Mbps	-
HIPERLAN/2	54 Mbps	150 meters (450 feet)

## Queuing:

Routers are essential networking devices that direct the flow of data over a network. Routers have one or more **input** and **output interfaces** which receive and transmit packets respectively. Since the router's memory is

finite, a router can run out of space to accommodate freshly arriving packets. This occurs if the rate of arrival of the packets is greater than the rate at which packets exit from the router's memory. In such a situation, new packets are ignored *or* older packets are dropped. As part of the resource allocation mechanisms, routers must implement some queuing discipline that governs how packets are buffered or dropped when required.



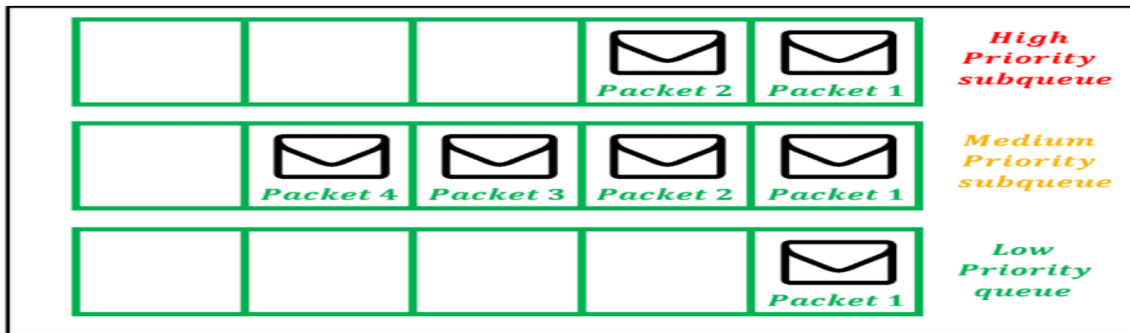
To manage the allocation of router memory to the packets in such situations of congestion, different disciplines might be followed by the routers to determine which packets to keep and which packets to drop. Accordingly, we have the following important queuing disciplines in routers:

### **First-In, First-Out Queuing (FIFO):**

The default queuing scheme followed by most routers is FIFO. This generally requires little no configuration to be done on the server. All packets in FIFO are serviced in the same order as they arrive in the router.

### **Priority Queuing (PQ):**

In Priority Queuing, instead of using a single queue, the router bifurcates the memory into multiple queues, based on some measure of priority. After this, each queue is handled in a FIFO manner while cycling through the queues one by one.

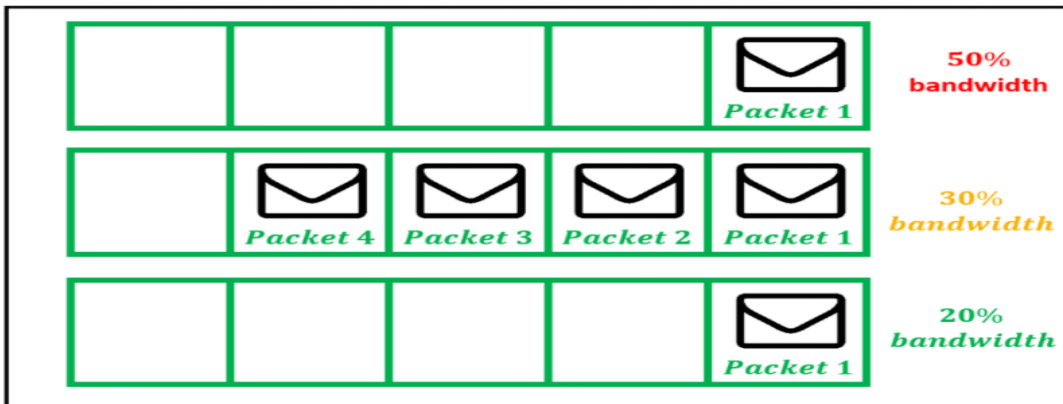


### Weighted Fair Queuing (WFQ):

Weighted Fair Queuing (WFQ) dynamically creates queues based on traffic flows and assigns bandwidth to these flows based on priority. The sub-queues are assigned bandwidths dynamically

**Traffic flows** are distinguished and identified based on various header fields in the packets, such as:

- Source and Destination IP address
- Source and Destination TCP (or UDP) port
- IP Protocol number
- Type of Service value (IP Precedence or DSCP)



### Network scheduling

The network scheduler logic decides which network packet to forward next. The network scheduler is associated with a queuing system, storing the network packets temporarily

until they are transmitted. Systems may have a single or multiple queues in which case each may hold the packets of one flow, classification, or priority.

## **OVERFLOWS**

Overflows can be caused deliberately by hackers and then exploited to run malicious code.

There are two types of overflows: **stack** and **heap**. The stack and the heap are two areas of the memory structure that are allocated when a program is run. Function calls are stored in the stack, and dynamically allocated variables are stored in the heap. A particular amount of memory is allocated to the buffer. Static variable storage (variables defined within a function) is referred to as stack, because they are stored on the stack in memory. Heap data is the memory that is dynamically allocated at runtime, such as by C's malloc () function.

## **CRYPTOGRAPHY**

The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Cryptographic systems are characterized along three independent dimensions:

- The type of operations used for transforming plaintext to ciphertext.
- The number of keys used.
- The way in which the plaintext is processed.

Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.

4. **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Three types of cryptographic techniques used in general :

**1) Symmetric-key Cryptography:** Both the sender and receiver share a single key to encrypt plaintext and to decrypt the message.

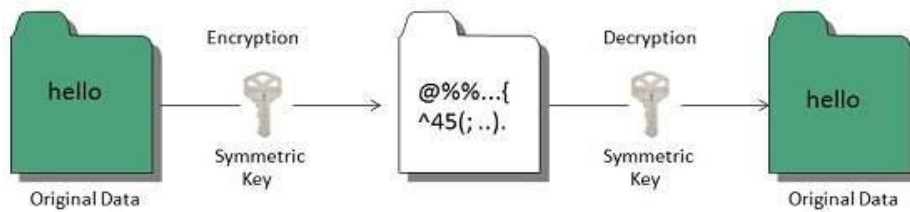
**2) Public-Key Cryptography:** In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

**3) Hash Functions:** No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered.

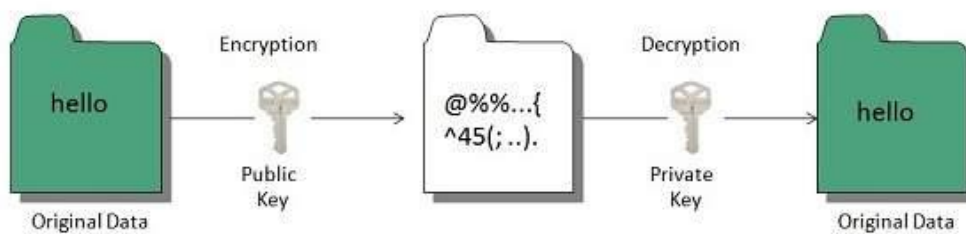
**ENCRYPTION** :Encryption in cryptography is a process by which a plain text or a piece of information is converted into cipher text or a text which can only be decoded by the receiver for whom the information was intended. The algorithm that is used for the process of encryption is known as cipher. It helps in protecting consumer information, emails and other sensitive data from unauthorized access to it as well as secures communication networks. Types of Encryption

There are two types of encryptions schemes as listed below:

- **Symmetric key encryption** algorithm uses same cryptographic keys for both encryption and decryption of cipher text.



- **Public key encryption** algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



## Types of Encryption

- **Data Encryption Standard (DES)**

Data Encryption Standard is considered a low-level encryption standard. Due to advances in technology and decreases in the cost of hardware, DES is essentially obsolete for protecting sensitive data.

- **Triple DES**

Triple DES runs DES encryption three times.

- **RSA**

RSA takes its name from the familial initials of three computer scientists. It uses a strong and popular algorithm for encryption.

- **Twofish**

Twofish is considered one of the fastest encryption algorithms and is free for anyone to use. It's used in hardware and software.

**Why is encryption important? Here are three reasons:**

- Internet privacy concerns are real Encryption helps protect your online privacy by turning personal information into “for your eyes only” messages intended only for the parties that need them — and no one else.
- Hacking is big business Cybercrime is a global business, often run by multinational outfits.
- Regulations demand it the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers to implement security features that help protect patients’ sensitive health information online.
  - Encryption helps businesses stay compliant with regulatory requirements and standards. It also helps protect the valuable data of their customers.

## SSH PROTOCOL

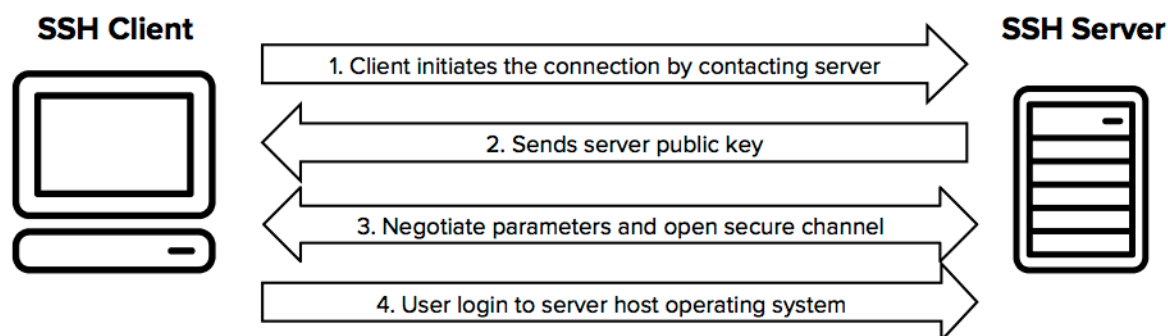
SSH (also known as the Secure Shell or **Secure Socket Shell**) can be defined as a **cryptographic network protocol**. SSH aims to give the users (mostly the system administrators) a secure means to reach a computer within a network.

Although SSH is often used for applications like remote login, remote command line and remote command execution, almost all network services can be secured with the use of SSH.

Secure Socket Shell employs the **public-key cryptography** methods in order to carry out **authentication** processes for the remote computer.

SSH offers two main functions:

- Logging on to remote systems and running terminal sessions, remote commands and such on these remote systems.
- Transferring files between remote systems on the same network.



It always comes in key pair:



- **Public key** – Everyone can see it, no need to protect it. (for encryption function)
- **Private key** – Stays in computer, must be protected. (for decryption function)

Key pairs can be of the following types:

- **User Key** – If public key and private key remain with the user.
- **Host Key** – If public key and private key are on a remote system.
- **Session key** – Used when large amount of data is to be transmitted.

### How SSH Works?

It uses asymmetric cipher for performing encryption and decryption. There are many encryption methods: rsa, dsa, ed25519 etc.

General procedure is: -

- Public keys from the local computers (system) are passed to the server which is to be accessed.
- Server then identifies if the public key is registered. If so, the server then creates a new secret key and encrypts it with the public key which was send to it via local computer.
- This encrypted code is sent to the local computer. This data is unlocked by the private key of the system and is send to the server.
- Server after receiving this data verifies the local computer.
- SSH creates a route and all the encrypted data are transferred through it with no security issues.

SSH is key based authentication that is not prone to brute-force attack. It is more convenient and secure than login ids and passwords (which can be stolen in middle). There is no exposure of valid credentials, if a server has been compromised.

### Generating an SSH key pair:

- Open your command prompt
- type: ssh-keygen
- Press enter
- It will ask you for a location. Press Enter for default location.
- If it's already there, press 'y' to overwrite.
- You may enter passphrase as you like, press enter.
- **Generating SSH keys on Windows, Linux and Mac:**
- OMAC OsX and Linux: terminal (build in)

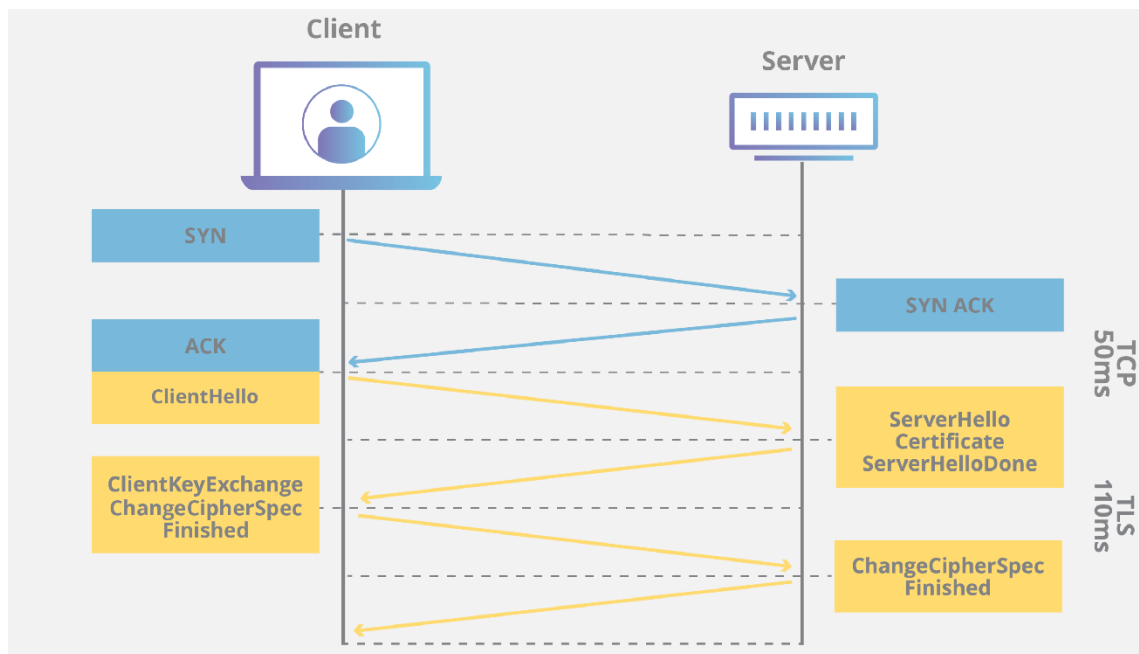
- OWindows:- PuTTY

## **TLS PROTOCOL**

TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP

There are several benefits of TLS:

- **Encryption:** TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:** TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:** TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:** Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:** Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.



### **MTLS:**

Server-to-server connections rely on MTLS for mutual authentication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other. In Skype for Business Server deployments, certificates issued by the enterprise CA that are during their validity period and not revoked by the issuing CA are automatically considered valid by all internal clients and servers because all members of an Active Directory domain trust the Enterprise CA in that domain. In federated scenarios, the issuing CA must be trusted by both federated partners. Each partner can use a different CA, if desired, so long as that CA is also trusted by the other partner. This trust is most easily accomplished by the Edge Servers having the partner's root CA certificate in their trusted root CAs, or by use of a third-party CA that is trusted by both parties.

## Network Devices:

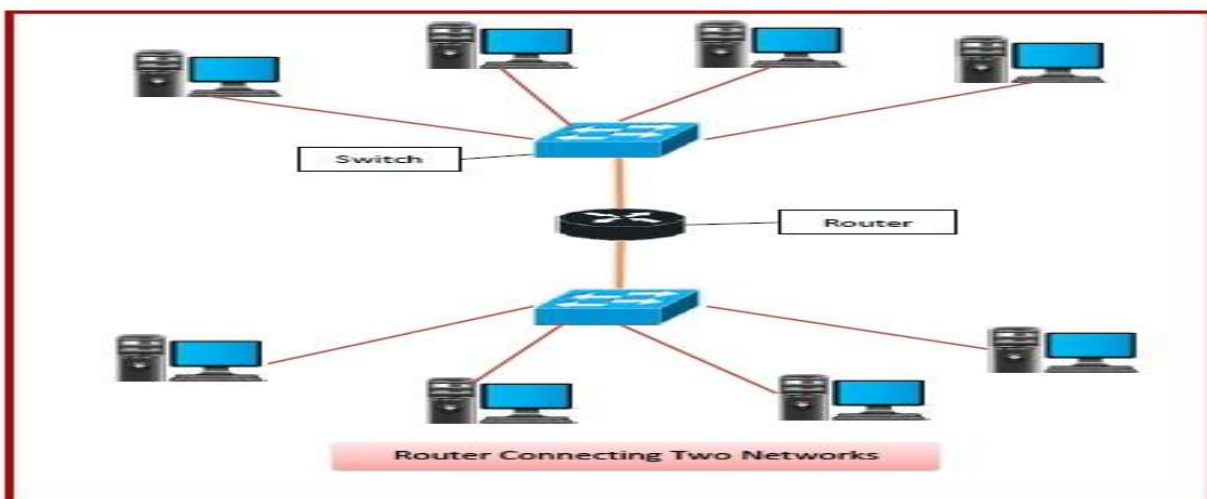
Network devices, or networking hardware, are physical devices that are required for communication and interaction between hardware on a computer network.

### Types of network devices –

#### ➤ ROUTER:

A **router**<sup>[a]</sup> is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.<sup>[2]</sup>

A router is connected to two or more data lines from different IP networks.<sup>[b]</sup> When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.



## Routing Table -

The functioning of a router depends largely upon the routing table stored in it. The routing table stores the available routes for all destinations. The router consults the routing table to determine the optimal route through which the data packets can be sent.

A routing table typically contains the following entities –

- IP addresses and subnet mask of the nodes in the network
- IP addresses of the routers in the network
- Interface information among the network devices and channels

Routing tables are of two types –

- **Static Routing Table** – Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
- **Dynamic Routing Table** – Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

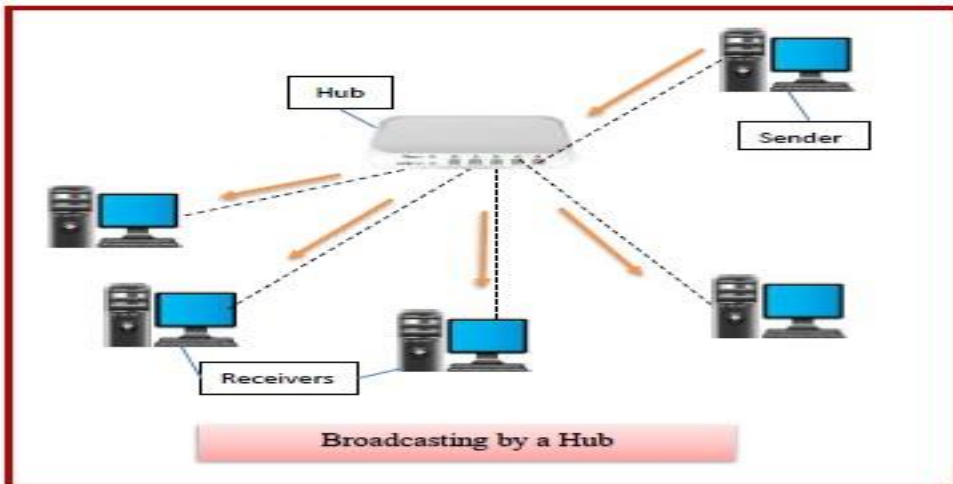
## Types of Routers –

- Wireless
- Broadband Routers
- Core
- Edge Routers
- Routers

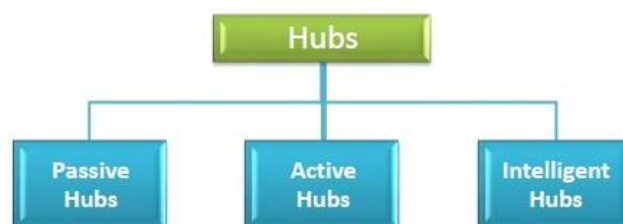
- **HUB**

Hubs are networking devices operating at a physical layer of the Open Systems Interconnection (OSI) model that are used to connect multiple devices in a network. They are generally used to connect computers in a LAN. A hub has numerous ports. A

computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination device or not.



### Types of Hubs:

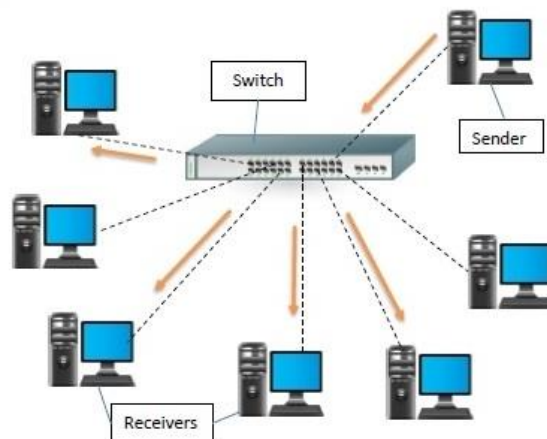


- **Passive Hubs** – Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.

- **Active Hubs** – Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting center. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.
- **Intelligent Hubs** – Intelligent hubs are active hubs that provide additional network management facilities. They can perform a variety of functions of more intelligent network devices like network management, switching, providing flexible data rates etc. These hubs have some kinds of management software that help to analyze the problem in the network and resolve them.

### ➤ SWITCH

A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network. A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s). It supports unicast, multicast as well as broadcast communications. A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance.



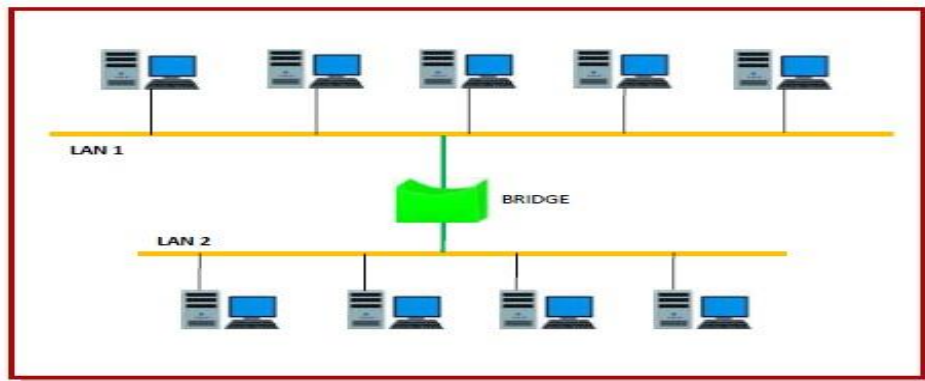


## Types of Switches :

- **Unmanaged Switch** – These are inexpensive switches commonly used in home networks and small businesses. They can be set up by simply plugging in to the network, after which they instantly start operating.
- **Managed Switch** – These are costly switches that are used in organizations with large and complex networks, since they can be customized to augment the functionalities of a standard switch.
- **LAN Switch** – Local Area Network (LAN) switches connects devices in the internal LAN of an organization. They are also referred as Ethernet switches or data switches. These switches are particularly helpful in reducing network congestion or bottlenecks.
- **PoE Switch** – Power over Ethernet (PoE) switches are used in PoE Gogabit Ethernets. PoE technology combine data and power transmission over the same cable so that devices connected to it can receive both electricity as well as data over the same line

### ➤ **BRIDGE:**

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. By looking at the MAC address of the devices connected to each segment, bridges can forward the data or block it from crossing. Bridges can also be used to connect two physical LANs into a larger logical LAN. Bridges work only at the Physical and Data Link layers of the OSI model. Bridges are used to divide larger networks into smaller sections by sitting between two physical network segments and managing the flow of data between the two.

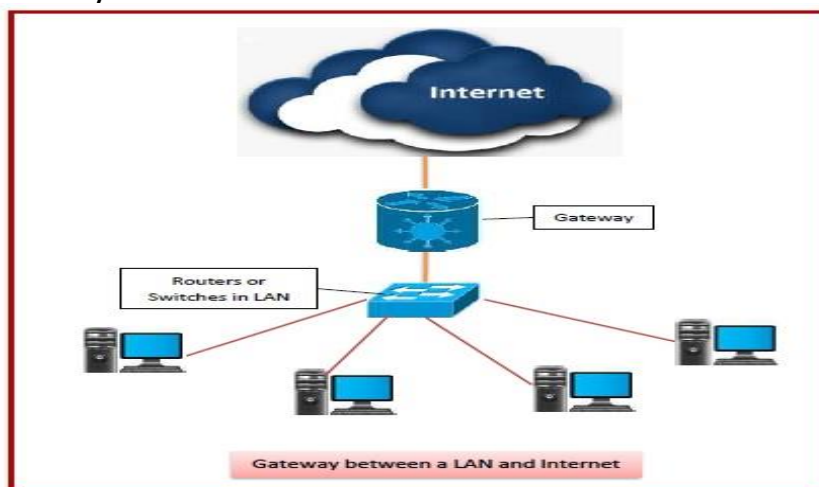


### Types of Bridges -

- Transparent Bridge
- Translational Bridge
- Source-route Bridge

### ➤ GATEWAY

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at network layer of the OSI model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.



## Types of Gateways -

On basis of direction of data flow, gateways are broadly divided into two categories –

- Unidirectional Gateways
- Bidirectional Gateways

On basis of functionalities, there can be a variety of gateways, the prominent among them are as follows –

- Network Gateway
  - Cloud Storage Gateway
  - Internet-To-Orbit Gateway (I2O)
  - IoT Gateway
  - VoIP Trunk Gateway
- 
- **ACCESS POINT**  
A wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in your network than to use wires and cables.

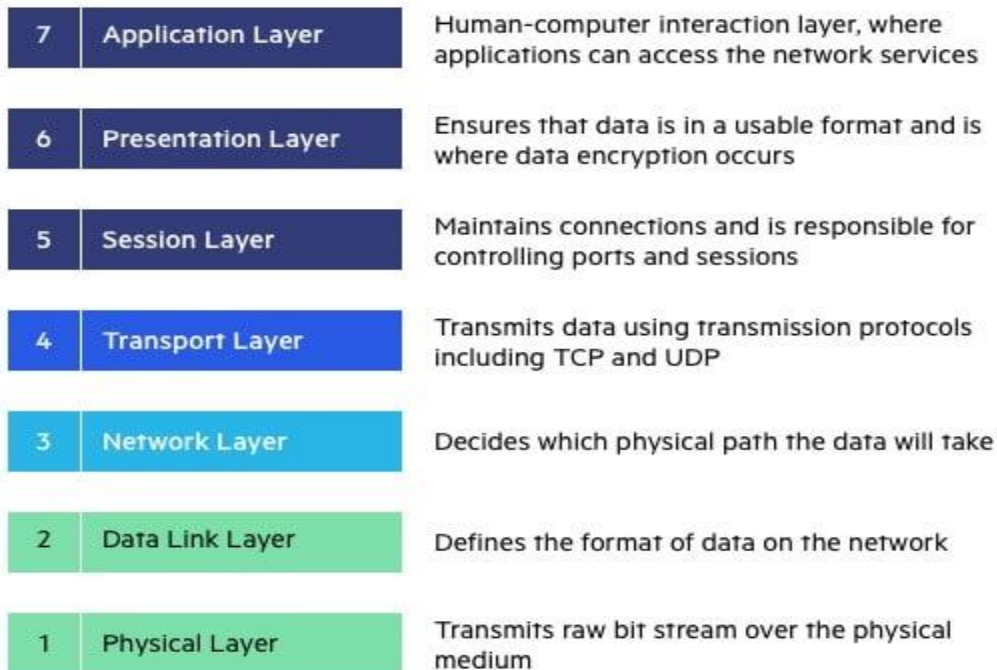
### Types of access points:

- Root access point
- Repeater access point
- Bridges

## **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. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



LAYER	NAME	DEVICES	PROTOCOLS
Layer 7	Application	-	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	-	MPEG, ASCH, SSL, TLS
Layer 5	Session	-	NetBIOS, SAP
Layer 4	Transport	-	TCP, UDP
Layer 3	Network	Routers	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	Switch and Bridge	RAPA, PPP, Frame Relay, ATM, Fiber Cable,

			etc.
Layer 1	Physical	Hub, repeater, modem and cables	RS232, 100BaseTX, ISDN, 11.

## Physical layer

- The lowest layer of the OSI reference model is the physical layer.
- It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits**.
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

The functions of the physical layer are:

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e., the number of bits sent per second.
- **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e., bus, star or mesh topology.
- **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

## Data Link Layer

- The data link layer is responsible for the node-to-node delivery of the message.
- Main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

Data Link Layer is divided into two sub layers:

- **Link Control (LLC)** - This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.
- **Media Access Control (MAC)** - It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
- Framing which divides the data from Network layer into frames.
- Allows you to add header to the frame to define the physical address of the source and the destination machine
- Adds Logical addresses of the sender and receivers
- It is also responsible for the sourcing process to the destination process delivery of the entire message.
- It also offers a system for error control in which it detects retransmits damage or lost frames.
- Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.
- When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

## Network layer

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.

- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.
- The sender & receiver's IP address are placed in the header by the network layer. The functions of the Network layer are:
  - **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
  - **Logical Addressing:** In-order to identify each device on internet network uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.
  - **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

## Transport Layer

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.



- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
  
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

### Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

### **SESSION LAYER:**

This layer is responsible for establishment of connection, maintenance of sessions, authentication and it also ensures security.

The functions of the session layer are:

Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.

- **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

### **PRESENTATION LAYER:**

A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems. It acts as a data translator for a network.

This layer is a part of the operating system that converts the data from one presentation format to another format. The Presentation layer is also known as the syntax layer.

### Functions of Presentation Layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

### APPLICATION LAYER:

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

The functions of the Application Layers are:

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

## **TCP:**

Transmission Control Protocol is an internet protocol suite which breaks up the message into TCP Segments and reassembling them at the receiving side.

## **IP:**

An Internet Protocol address that is also known as an IP address is a numerical label. It is assigned to each device that is connected to a computer network which uses the IP for communication. Its routing function allows internetworking and essentially establishes the Internet. Combination of IP with a TCP allows developing a virtual connection between a destination and a source.

## **HTTP:**

The Hypertext Transfer Protocol is a foundation of the World Wide Web. It is used for transferring webpages and other such resources from the HTTP server or web server to the web client or the HTTP client. Whenever you use a web browser like Google Chrome or Firefox, you are using a web client. It helps HTTP to transfer web pages that you request from the remote servers.

## **SMTP:**

SMTP stands for Simple mail transfer protocol. This protocol supports the e-mail is known as a simple mail transfer protocol. This protocol helps you to send the data to another e-mail address.

## **SNMP:**

SNMP stands for Simple Network Management Protocol. It is a framework which is used for managing the devices on the internet by using the TCP/IP protocol.

## **DNS:**

DNS stands for Domain Name System. An IP address that is used to identify the connection of a host to the internet uniquely. However, users prefer to use names instead of addresses for that DNS.

## **TELNET:**

TELNET stands for Terminal Network. It establishes the connection between the local and remote computer. It established connection in such a manner that you can simulate your local system at the remote system.

## **FTP:**

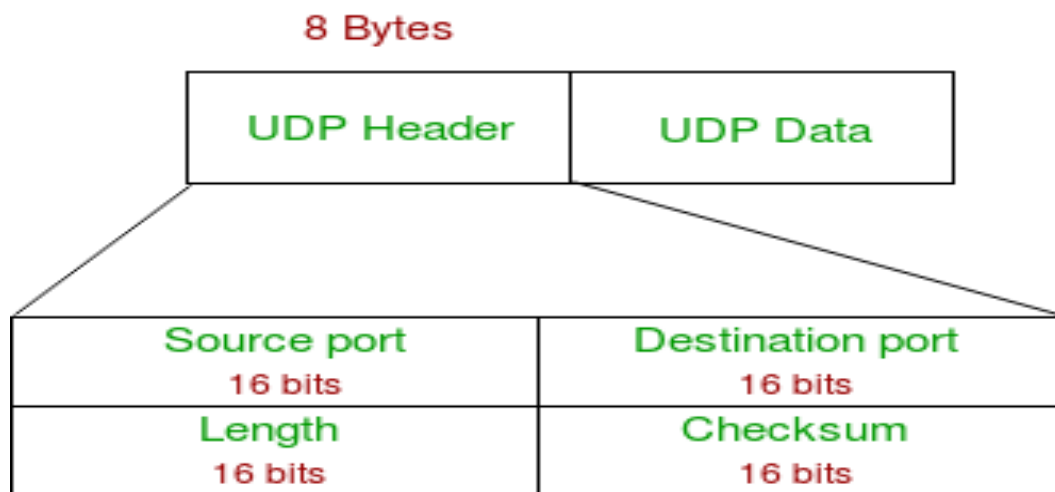
FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.

## **User Datagram Protocol (UDP)**

It is a Transport Layer protocol. The UDP protocol allows the computer applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network. The UDP is an alternative communication protocol to the TCP protocol (transmission control protocol). Like TCP, UDP provides a set of rules that governs how the data should be exchanged over the internet. The UDP works by encapsulating the data into the packet and providing its own header information to the packet. Then, this UDP packet is encapsulated to the IP packet and sent off to its destination.

## UDP Header

**UDP header** is 8-bytes fixed and simple **header**, while for TCP it may vary from 20 bytes to 60 bytes. First 8 Bytes contains all necessary **header** information and remaining part consist of data.



- **Source Port:** Source Port is 2 Byte long field used to identify port number of source.
- **Destination Port:** It is 2 Byte long field, used to identify the port of destined packet.
- **Length:** Length is the length of UDP including header and the data. It is 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

**Notes** – Unlike TCP, Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting.

## Applications of UDP:

- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- It is suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP (Routing Information Protocol).

- Normally used for real time applications which cannot tolerate uneven delays between sections of a received message.
- Following implementations uses UDP as a transport layer protocol:
  - NTP (Network Time Protocol)
  - DNS (Domain Name Service)
  - BOOTP, DHCP.
  - NNP (Network News Protocol)
  - Quote of the day protocol
  - TFTP, RTSP, RIP.
- Application layer can do some of the tasks through UDP-
  - Trace Route
  - Record Route
  - Time stamp
- UDP takes datagram from Network Layer, attach its header and send it to the user. So, it works fast.
- Actually, UDP is null protocol if you remove checksum field.
  - Reduce the requirement of computer resources.
  - When using the Multicast or Broadcast to transfer.
  - The transmission of Real-time packets, mainly in multimedia applications.

## **LAYER 2 PROTOCOLS:**

PROTOCOLS	FUNCTIONS
LLDP (Link layer discovery protocol)	LLDP is vendor neutral, and is commonly used as a component in network management and network monitoring applications.
CDP (Cisco Discovery Protocol)	CDP is a Cisco proprietary protocol that support the IEEE 802.1ab version of LLDP, and is primarily used to share information between directly connected Cisco devices.
IP route	This command contains information from the IP routing table that can be used to forward a packet

	through the best path towards its destination.
FDB (Forwarding database)	FDB stores MAC addresses of the discovered devices and their respective ports. This protocol is preferred for discovering switches.
ARP (Address Resolution Protocol)	ARP maps dynamic IP (Layer 3) with MAC addresses (Layer 2). ARP translates 32-bit addresses to 48-bit and vice versa, and is preferred by IPv4 devices.
Multi-link trunking Protocol (MLT)	MLT provides high-speed, fault tolerant connection between servers, switches and routers by grouping all ethernet links into a single logical ethernet link.
CAN (Controller area network)	CAN facilitates communication between the applications of microcontrollers and their devices without relying on a host computer.

## LAYER 3 PROTOCOLS:

### ➤ ARP:

- ARP stands for Address Resolution Protocol.
- It is used to associate an IP address with the MAC address.
- Each device on the network is recognized by the MAC address imprinted on the NIC. Therefore, we can say that devices need the MAC address for communication on a local area network.

### ➤ RARP:

- RARP stands for **Reverse Address Resolution Protocol**.



- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as **Reverse Address Resolution Protocol**.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

### ➤ ICMP:

- ICMP stands for Internet Control Message Protocol.
- The ICMP is a network layer protocol used by hosts and routers to send the notifications of IP datagram problems back to the sender.
- ICMP uses echo test/reply to check whether the destination is reachable and responding.
- ICMP handles both control and error messages, but its main function is to report the error but not to correct them.
- An IP datagram contains the addresses of both source and destination, but it does not know the address of the previous router through which it has been passed. Due to this reason, ICMP can only send the messages to the source, but not to the immediate routers.
- ICMP protocol communicates the error messages to the sender. ICMP messages cause the errors to be returned to the user processes.
- ICMP messages are transmitted within IP datagram.

### WLAN:

WLAN (Wireless local Area Network) are referred to as the LANs that uses high frequency radio waves instead of cables for connecting the devices. In simple terms, it

can be acknowledged as a set of laptops and other wireless devices communicating with each other via radio waves. Mostly WLANs are based upon the standard IEEE 802.11 or Wi-Fi.

### **Types of WLAN Protocols:**

#### **➤ 802.11a Protocol:**

This protocol supports a transmission speed of 54Mbps and has a high frequency range of 5GHz, because of which signals face a lot of difficulty to pass through walls and other obstacles. This protocol makes use of OFDM (Orthogonal Frequency Division Multiplexing) which is a type of digital transmission and a method of encoding digital data on multiple carrier frequencies.

#### **➤ 802.11b Protocol:**

This protocol supports a transmission speed of 11Mbps and has a frequency range of 2.4GHz. It allows path sharing and is less vulnerable to obstruction. This protocol makes use of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) with Ethernet protocol. CSMA/CA in computer network, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be idle.

#### **➤ 802.11g Protocol:**

This protocol is a combination of 802.11a Protocol and 802.11b Protocol. Owing to its dual features, it is backward compatible with 802.11b devices. It provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.

#### **➤ 802.11n Protocol:**

This is an upgraded version of 802.11g Protocol and is also called Wireless N. It supports a transmission speed of 600Mbps and provides signal coverage. It makes use of MIMO (Multiple Input/Multiple Output) approach, having multiple antennas at both transmission as well as receiver end.

## **BGP:**

Border Gateway Protocol is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

### **Features of BGP:**

#### ➤ **Open Standard**

It is a standard protocol which can run on any window device.

#### ➤ **Exterior Gateway Protocol**

It is an exterior gateway protocol that is used to exchange the routing information between two or more autonomous system numbers.

#### ➤ **InterAS-domain Routing**

It is specially designed for inter-domain routing, where interAS-domain routing means exchanging the routing information between two or more autonomous number systems.

#### ➤ **Supports Internet**

It is the only protocol that operates on the internet backbone.

#### ➤ **Classless**

It is a classless protocol.

#### ➤ **Incremental and Trigger Updates**

Like IGP, BGP also supports incremental and trigger updates.

#### ➤ **Path Vector Protocol**

The BGP is a path vector protocol. Here, path vector is a method of sending the routes along with routing information.

#### ➤ **Configure Neighborhood relationship**

It sends updates to configure the neighborhood relationship manually.

#### ➤ **Application Layer Protocol**

It is an application layer protocol and uses TCP protocol for reliability.

#### ➤ **Metric**

It has lots of attributes like weight attribute, origin, etc. BGP supports a very rich number of attributes that can affect the path manipulation process.

### ➤ **Administrative Distance**

If the information is coming from the external autonomous system, then it uses 20 administrative distance. If the information is coming from the same autonomous system, then it uses 200 administrative distance.

### **Types of Packets:**

There are four different types of packets exist in BGP:

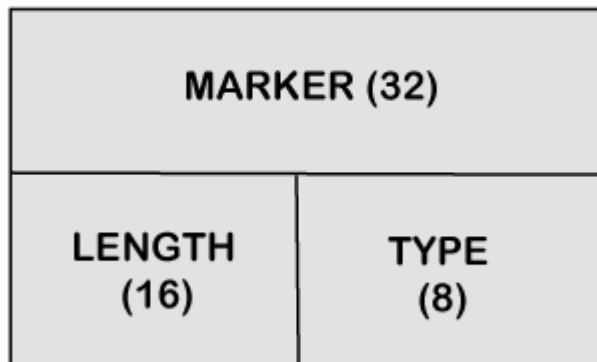
- **Open:** When the router wants to create a neighborhood relation with another router, it sends the Open packet.
- **Update:** The update packet can be used in either of the two cases:
  - It can be used to withdraw the destination, which has been advertised previously.
  - It can also be used to announce the route to the new destination.
- **Keep Alive:** The keep alive packet is exchanged regularly to tell other routers whether they are alive or not. For example, there are two routers, i.e., R1 and R2. The R1 sends the keep alive packet to R2 while R2 sends the keep alive packet to R1 so that R1 can get to know that R2 is alive, and R2 can get to know that R1 is alive.
- **Notification:** The notification packet is sent when the router detects the error condition or close the connection.

### **Packets Format:**

Now we will see the format in which the packet travels. The following are the fields in a BGP packet format:

- **Marker:** It is a 32-bit field which is used for the authentication purpose.
- **Length:** It is a 16-bit field that defines the total length of the message, including the header.
- **Type:** It is an 8-bit field that defines the type of the packet.

### BGP Packet Format



## IPv4

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address. It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.

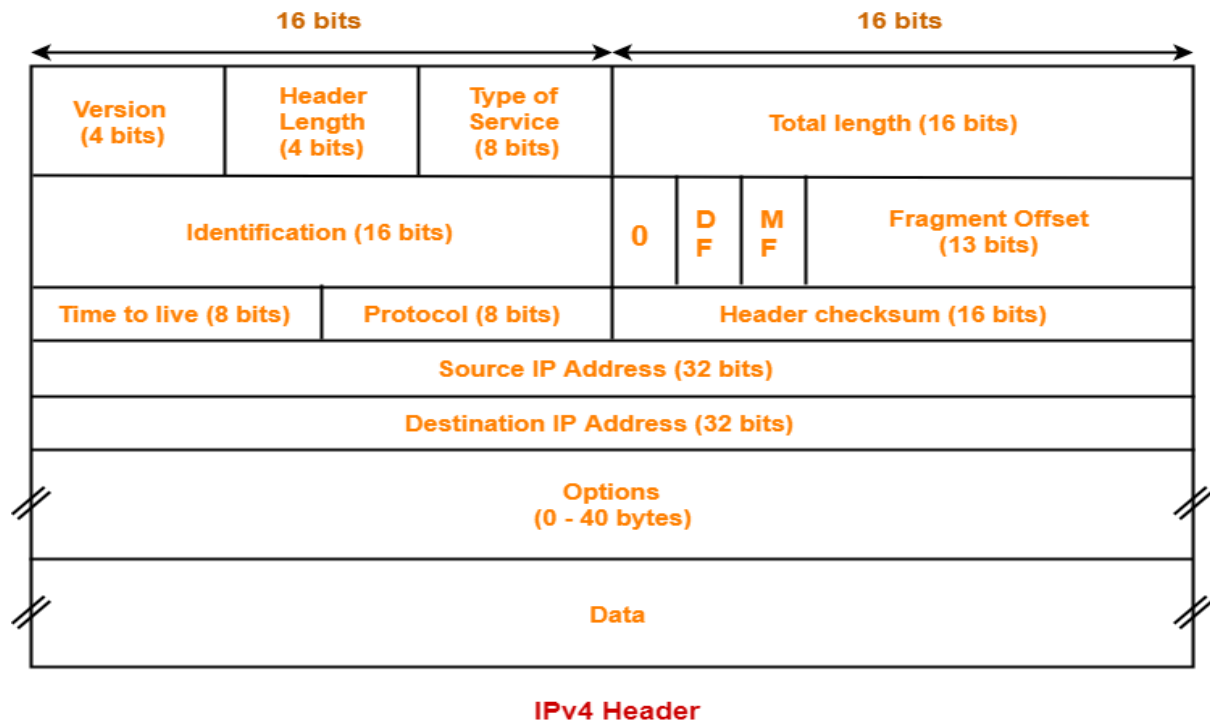
For example, **66.94.29.13**

The above example represents the IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255. This address can produce 4,294,967,296 possible unique addresses.

In today's computer network world, computers do not understand the IP addresses in the standard numeric format as the computers understand the numbers in binary form only. The binary number can be either 1 or 0. The IPv4 consists of four sets, and these sets represent the octet. The bits in each octet represent a number.

### Drawback of IPv4

Currently, the population of the world is 7.6 billion. Every user is having more than one device connected with the internet, and private companies also rely on the internet. As we know that IPv4 produces 4 billion addresses, which are not enough for each device connected to the internet on a planet.



## IPv6:

IPv6 is the next generation of IP addresses. The main difference between IPv4 and IPv6

IPv6 is the address size of IP addresses. The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4. It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

- **Dual stacking:** It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.

- **Tunnelling:** In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.
- **Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

## IPv4 Subnetting:

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 ( $2^1=2$ ) with ( $2^{23}-2$ ) 8388606 Hosts per Subnet.

Network ID	Subnet Mask	Host ID Range	No. of Hosts	Broadcast ID
110.0.0.0	/10	110.0.0.1 - 110.63.255.254	4,194,304	110.63.255.255
110.64.0.0	/10	110.64.0.1 - 110.127.255.254	4,194,304	110.127.255.255
110.128.0.0	/10	110.128.0.1 - 110.191.255.254	4,194,304	110.191.255.255
110.192.0.0	/10	110.192.0.1 - 110.255.255.254	4,194,304	110.255.255.255

**Creating 4 networks using 110.72.56.82 (Class A)**

### **Class B Subnets:**

By default, using Classful Networking, 14 bits are used as Network bits providing ( $2^{14}$ ) 16384 Networks and ( $2^{16}-2$ ) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits.

Network ID	Subnet Mask	Host ID Range	Number of Hosts	Broadcast ID
174.56.0.0	/18	174.56.0.1 - 174.56.63.254	16384	174.56.63.255
174.56.64.0	/18	174.56.64.1 - 174.56.127.254	16384	174.56.127.255
174.56.128.0	/18	174.56.128.1 - 174.56.191.254	16384	174.56.191.255
174.56.192.0	/18	174.56.192.1 - 174.56.255.254	16384	174.56.255.255

**Creating 4 networks using 174.56.65.98 (Class B)**

### **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.

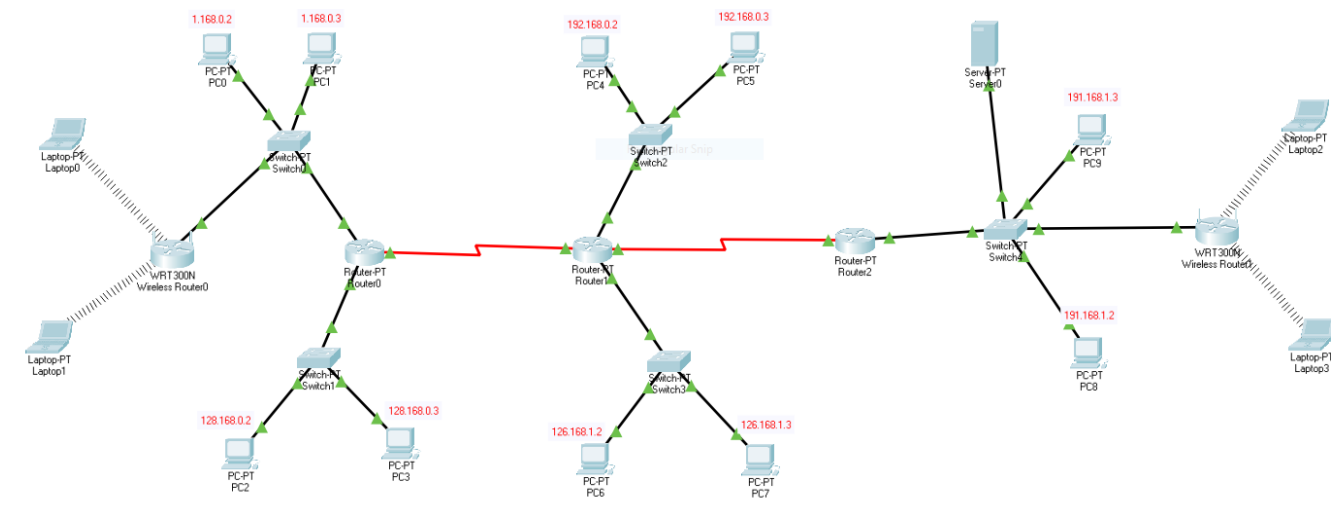
Network ID	Subnet Mask	Host ID Range	Number of Hosts	Broadcast ID
215.82.66.0	/26	215.82.66.1 - 215.82.66.62	64	215.82.66.63
215.82.66.64	/26	215.82.66.65 - 215.82.66.126	65	215.82.66.127
215.82.66.128	/26	215.82.66.129 - 215.82.66.190	64	215.82.66.191
215.82.66.192	/26	215.82.66.193 - 215.82.66.254	64	215.82.66.255









**Creating 4 networks using 215.82.66.75 (Class C)**



## Network Tools:

### ➤ Packet Tracer



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC3	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	PC4	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	PC5	ICMP		0.000	N	3	(edit)	(delete)

```
Packet Tracer PC Command Line 1.0
C:\>ping 128.168.0.2

Pinging 128.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 128.168.0.2: bytes=32 time<1ms TTL=127
Reply from 128.168.0.2: bytes=32 time<1ms TTL=127
Reply from 128.168.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 128.168.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 128.168.0.3

Pinging 128.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 128.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.2: bytes=32 time=3ms TTL=126
Reply from 192.168.0.2: bytes=32 time=7ms TTL=126
```

## ➤ WIRESHARK

### Ping amazon.com(Frame)

```

▼ Frame 223: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B9F63BCC-F615-4434-99C3-D77B30A96B9A}, id 0
  > Interface id: 0 (\Device\NPF_{B9F63BCC-F615-4434-99C3-D77B30A96B9A})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar 26, 2021 09:12:28.834570000 India Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1616730148.834570000 seconds
    [Time delta from previous captured frame: 0.040244000 seconds]
    [Time delta from previous displayed frame: 0.040244000 seconds]
    [Time since reference or first frame: 18.470075000 seconds]
    Frame Number: 223
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
  > Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:d6:50 (e4:54:e8:b1:d6:50)
  > Internet Protocol Version 4, Src: 176.32.103.205, Dst: 192.168.60.119
  > Internet Control Message Protocol

```

### Ping amazon.com(Ethernet)

```

  > Frame 223: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B9F63BCC-F615-4434-99C3-D77B30A96B9A}, id 0
  ▼ Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:d6:50 (e4:54:e8:b1:d6:50)
    > Destination: Dell_b1:d6:50 (e4:54:e8:b1:d6:50)
    > Source: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70)
      Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 176.32.103.205, Dst: 192.168.60.119
  > Internet Control Message Protocol

```

### Ping amazon.com(Ipv4)

```

  > Frame 223: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B9F63BCC-F615-4434-99C3-D77B30A96B9A}, id 0
  > Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:d6:50 (e4:54:e8:b1:d6:50)
  ▼ Internet Protocol Version 4, Src: 176.32.103.205, Dst: 192.168.60.119
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
      Total Length: 60
      Identification: 0xa0e5 (41189)
    > Flags: 0x00
      Fragment Offset: 0
      Time to Live: 235
      Protocol: ICMP (1)
      Header Checksum: 0x19ae [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 176.32.103.205
      Destination Address: 192.168.60.119
  > Internet Control Message Protocol

```

### Ping amazon.com(ICMP)

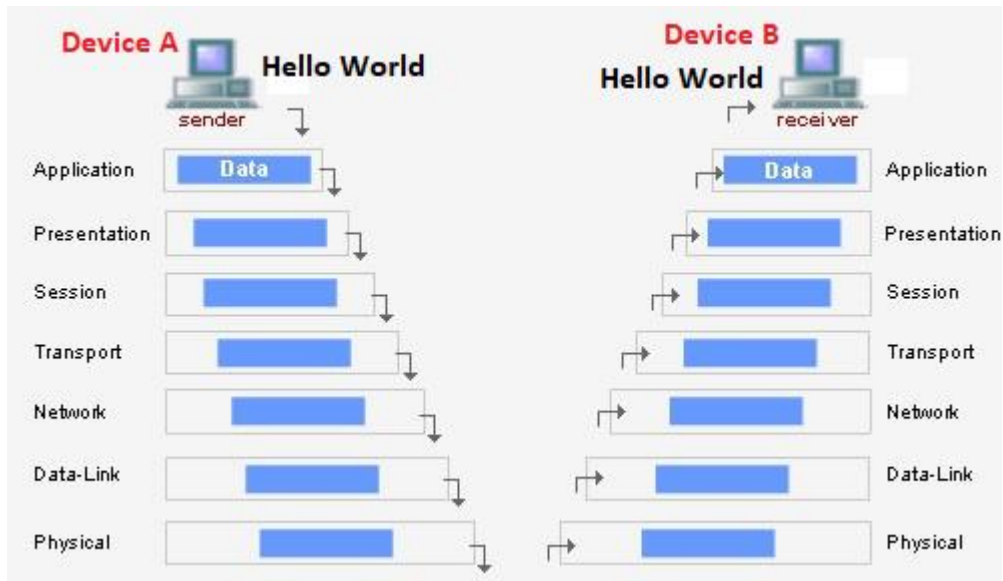
```

  > Frame 223: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B9F63BCC-F615-4434-99C3-D77B30A96B9A}, id 0
  > Ethernet II, Src: Cisco_0c:d2:70 (f4:0f:1b:0c:d2:70), Dst: Dell_b1:d6:50 (e4:54:e8:b1:d6:50)
  > Internet Protocol Version 4, Src: 176.32.103.205, Dst: 192.168.60.119
  ▼ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x52bb [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 672 (0x02a0)
    Sequence Number (LE): 40962 (0xa002)
    [Request frame: 213]
    [Response time: 227.606 ms]
  > Data (32 bytes)

```

## **End to end data flow:**

- A simple message, such as “**Hello World**”, needs to be sent by Device A to Device B. The Application layer (layer 7) places a header (encapsulation) field that contains information such as screen size and fonts, and passes the data to the Presentation layer (layer 6).
- The Presentation layer places layer 6 header information. For example, the text in the message might be converted to ASCII. The Presentation layer will then pass the new data to the Session layer (layer 5).
- The Session layer follows the same process by adding layer 5 header information, such as information that the Session layer will manage the data flow, and passes this data to the Transport layer (layer 4).
- The Transport layer places layer 4 information, such as an acknowledgment that the segment was received in the header, and passes it to the Network layer (layer 3).
- The Network layer places layer 3 header information, such as the source and destination address so the Network layer can determine the best delivery path for the packets, and passes this data to the Data Link layer (layer 2).
- The Data Link layer places layer 2 header and trailer information, such as a Frame Check Sequence (FCS) to ensure that the information is not corrupt, and passes this new data to the Physical layer (layer 1) for transmission across the media.
- The bit stream is then transmitted as ones and zeros on the Physical layer. It is at this point that the Physical layer ensures bit synchronization. Bit synchronization will ensure the end user data is assembled in the correct order it was sent.
- Steps 1 through 7 occur in reverse order on the destination device. Device B collects the raw bits from the physical wire and passes them up the Data Link layer. The Data Link layer removes the headers and trailers and passes the remaining information to the Network layer and so forth until data is received by the Application layer. Eventually, Device B will receive an email notification displaying a message to indicate that a new email message has been received.



## Reference:

- [Cryptography Introduction - GeeksforGeeks](#)
- [Data Encryption - Tutorialspoint](#)
- [Data Encryption - Tutorialspoint](#)
- [Network Devices \(Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter\) - GeeksforGeeks](#)
- [Layers of OSI Model - GeeksforGeeks](#)