**NETWORKING**

A computer network is a group of [computers](https://en.wikipedia.org/wiki/Computer) that use a set of common [communication protocols](https://en.wikipedia.org/wiki/Communication_protocol) over [digital](https://en.wikipedia.org/wiki/Digital_signal) interconnections for the purpose of sharing resources located on or provided by the [network nodes](https://en.wikipedia.org/wiki/Node_(networking)).  The interconnections between nodes are formed from a broad spectrum of [telecommunication network](https://en.wikipedia.org/wiki/Telecommunication_network) technologies, based on physically wired, optical, and wireless radio-frequency methods that may be arranged in a variety of [network topologies](https://en.wikipedia.org/wiki/Network_topology).

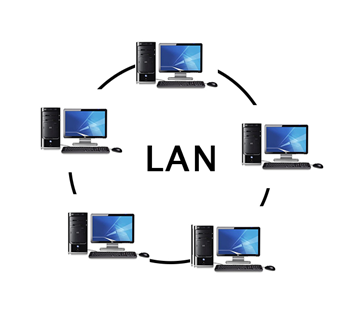
**Types of Networks**

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

* LAN (Local Area Network)
* PAN (Personal Area Network)
* MAN (Metropolitan Area Network)
* WAN (Wide Area Network)

## **LAN (Local Area Network):**

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as 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 in Local Area Network.
* Local Area Network 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.
* **Thomas Zimmerman** was the first research scientist to bring the idea of the 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:**

1. Wired Personal Area Network

2. Wireless Personal Area Network

**Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as Wi-Fi, Bluetooth. It is a low range network.

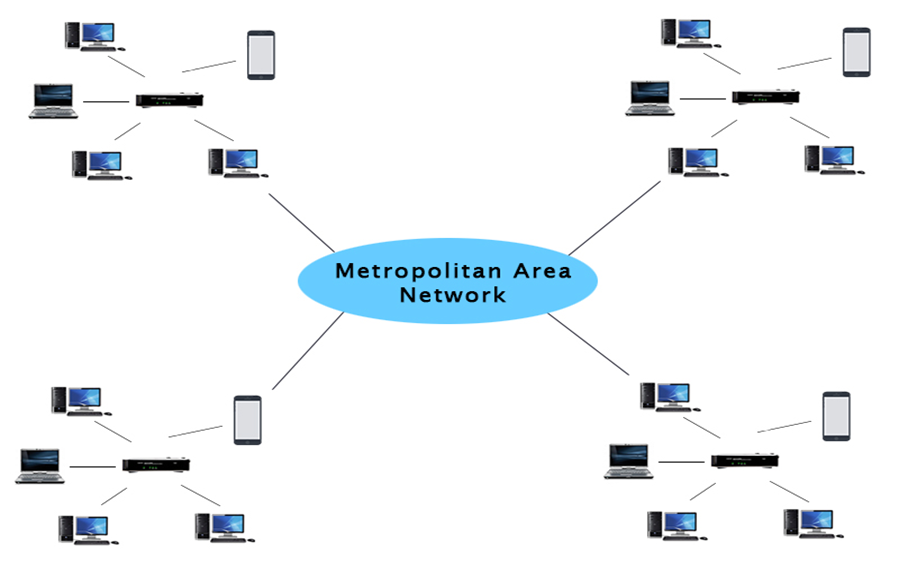
**Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

### 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. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
* **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
* **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).

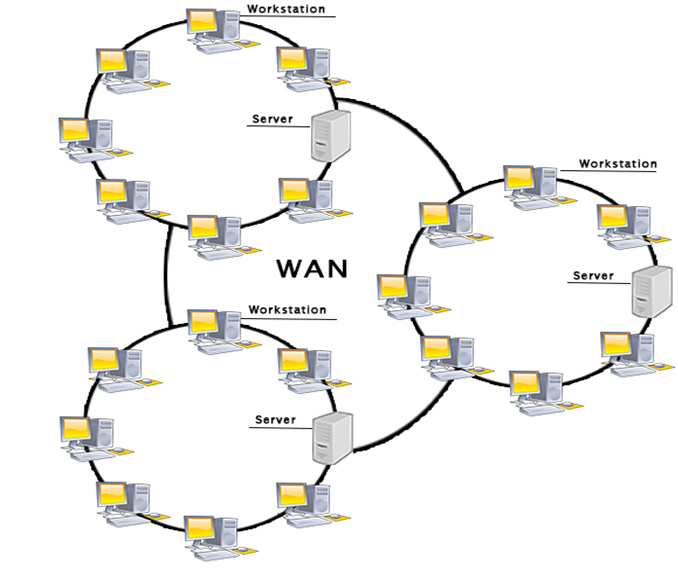


### Uses of Metropolitan Area Network:

* 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 quite bigger network than the LAN.
* 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:** A 4G network is widely used across a region or country.
* **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
* **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

### 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. The internet provides a leased line through which we can connect with another branch.
* **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. The web application like Facebook, WhatsApp, Skype allows you to communicate with friends.
* **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:** A WAN network has more security issues as compared to LAN and MAN network 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. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
* **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
* **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

# **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:**

### 1.    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 meters

### 2.    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.

### 3.    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

·

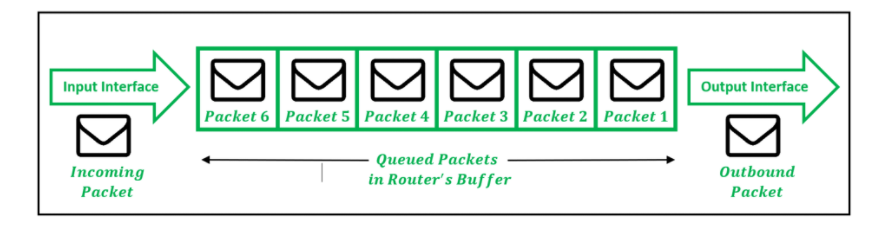
**WIRELESS NETWORK**

|  |  |  |
| --- | --- | --- |
| **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.



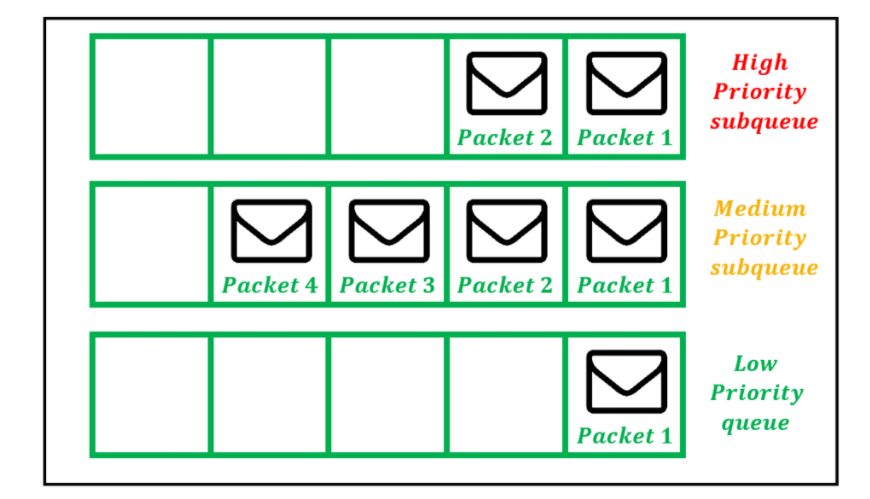
To manage the allocation of router memory to the packets in such situations of congestion, different disciplines might be followed by the routers to determine which packets to keep and which packets to drop. Accordingly, we have the following important queuing disciplines in routers:

#### **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. On reaching saturation within the memory, new packets attempting to enter the router are dropped (*tail drop*). Such a scheme, however, is not apt for real-time applications, especially during congestion. A real-time application such as VoIP, which continually sends packets, may be starved during times of congestion and have all its packets dropped.

#### **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. The queues are marked as **High**, **Medium**, or **Low**based on priority. Packets from the High queue are always processed before packets from the Medium queue. Likewise, packets from the Medium queue are always processed before packets in the Normal queue, etc. As long as some packets exist in the High priority queue, no other queue’s packets are processed. Thus, high priority packets cut to the front of the line and get serviced first. Once a higher priority queue is emptied, *only then* is a lower priority queue serviced.

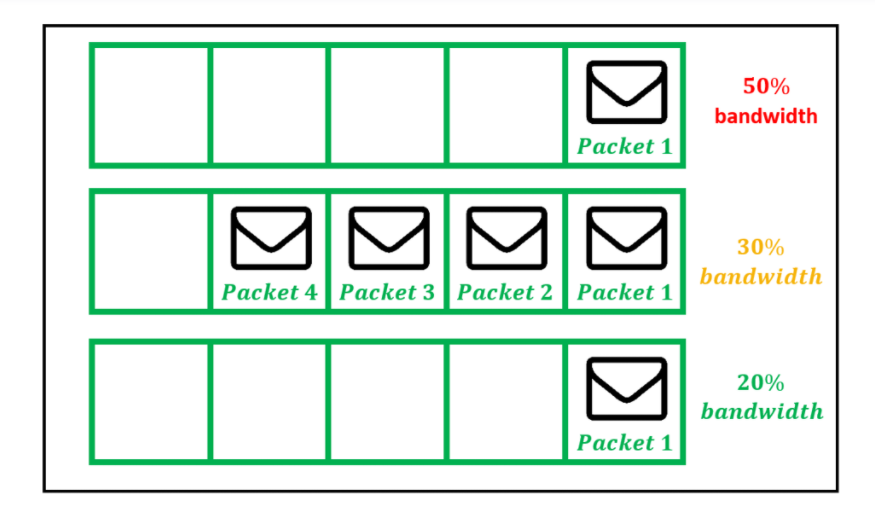


#### **Weighted Fair Queuing (WFQ):**

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. Suppose 3 queues exist which have bandwidth percentages of 20%, 30%, and 50% when they are all active. Then, if the 20% queue is idle, the freed-up bandwidth is allocated among the remaining queues, while preserving the original bandwidth ratios. Thus, the 30% queue is now allotted (75/2) % and the 50% queue is now allotted (125/2) % bandwidth.

**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)



Thus, packets are separated into distinct queues based on the traffic flow that corresponds to them. Once identified, packets belonging to the same traffic flow are inserted into a queue, created specifically for such traffic. By default, a maximum of 256 queues can be established within the router, however, this number may be cranked up to 4096 queues. Unlike PQ schemes, the WFQ-queues are allotted differing bandwidths based on their queue priorities. Packets with a higher priority are scheduled before lower-priority packets arriving at the same time.

## **Network scheduling**

A **network scheduler**, also called **packet scheduler**, **queueing discipline**, **qdisc** or **queueing algorithm**, is an [arbiter](https://en.wikipedia.org/wiki/Arbiter_(electronics)) on a [node](https://en.wikipedia.org/wiki/Node_(networking)) in [packet switching](https://en.wikipedia.org/wiki/Packet_switching) communication network. It manages the sequence of [network packets](https://en.wikipedia.org/wiki/Network_packet) in the transmit and receive [queues](https://en.wikipedia.org/wiki/Queue_(abstract_data_type)) of the [network interface controller](https://en.wikipedia.org/wiki/Network_interface_controller). There are several network schedulers available for the different [operating systems](https://en.wikipedia.org/wiki/Operating_system), that implement many of the existing network [scheduling algorithms](https://en.wikipedia.org/wiki/Scheduling_algorithm).

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](https://en.wikipedia.org/wiki/Traffic_flow_(computer_networking)), 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 actually stored on the stack in memory. Heap data is the memory that is dynamically allocated at runtime, such as by C's malloc () function. This data is not actually stored on the stack, but somewhere amidst a giant "heap" of temporary, disposable memory used specifically for this purpose. Actually, exploiting a heap buffer overflow is a lot more involved, because there are no convenient frame pointers (as are on the stack) to overwrite.

Attackers can use buffer overflows in the heap to overwrite a password, a filename, or other data. If the filename is overwritten, a different file will be opened. If this is an executable file, code will be run that was not intended to be run. On UNIX systems, the substituted program code is usually the command interpreter, which allows the attacker to execute commands with the privileges of the process's owner, which (if the setup id bit is set and the program has ownership of the root) could result in the attacker having Superuser privileges. On Windows systems, the overflow code could be sent using an HTTP requests to download malicious code of the attacker's choice. In either case, under the right circumstances, the result could be devastating.

**CRYPTOGRAPHY**

Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security. It is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. 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. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (i.e., that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.

* The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
* The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

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. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.  
  
**2) Public-Key Cryptography:** This is the most revolutionary concept in the last 300-400 years. 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. Hash functions are also used by many operating systems to encrypt passwords.

# **ENCRYPTION**

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate ciphertext that can only be read if decrypted. They can help to protect data we send, receive, and store, using a device, that can include text messages stored on your smartphone, running logs saved on your fitness watch, and banking information sent through your online account. Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information.

Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format — called “cipher text.” This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet.

When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption.

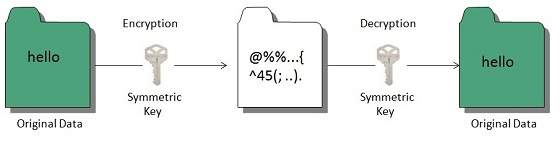
To unlock the message, both the sender and the recipient have to use a “secret” encryption key — a collection of algorithms that scramble and unscramble data back to a readable format.

### Types of Encryption

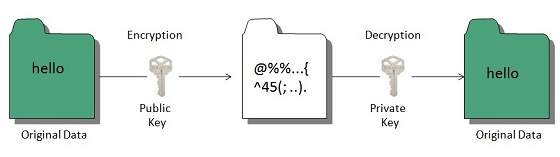
There are two types of encryptions schemes as listed below:

* Symmetric Key encryption
* Public Key encryption

**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. The U.S. government established the standard in 1977. 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. Here’s how it works: It encrypts, decrypts, and encrypts data — thus, “triple.” It strengthens the original DES standard, which became regarded as too weak a type of encryption for sensitive data.
* RSA
* RSA takes its name from the familial initials of three computer scientists. It uses a strong and popular algorithm for encryption. RSA is popular due to its key length and therefore widely used for secure data transmission.
* 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.

You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.

Most email clients come with the option for encryption in their Settings menu, and if you check your email with a web browser, take a moment to ensure that SSL encryption is available.

* Hacking is big business Cybercrime is a global business, often run by multinational outfits. Many of the large-scale data breaches that you may have heard about in the news demonstrate that cybercriminals are often out to steal personal information for financial gain.
* 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.

Institutions of higher learning must take similar steps under the Family Education Rights and Privacy Act (FERPA) to protect student records.

Retailers must contend with the Fair Credit Practices Act (FCPA) and similar laws that help protect consumers.

Encryption helps businesses stay compliant with regulatory requirements and standards. It also helps protect the valuable data of their customers.

**SSH PROTOCOL**

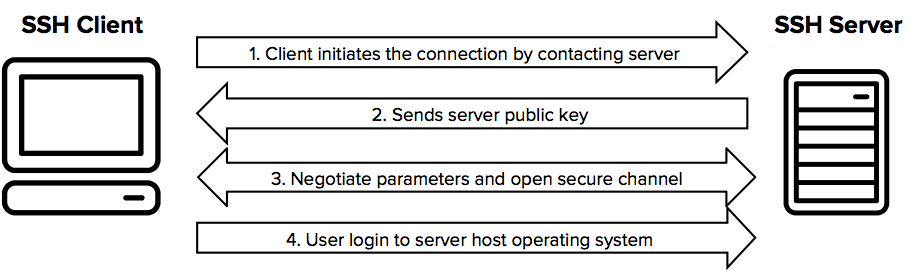
SSH (also known as the Secure Shell or **Secure Socket Shell**) can be defined as a **cryptographic network protocol**. SSH aims to give the users (mostly the system administrators) a secure means to reach a computer within a network.

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. You can opt for various **different ways to use SSH** -for instance you can first encrypt your network connection by using automatically generated key pairs (**public-private key pairs**), then you can go for password authentication for logging on. Or you can opt for using a **manually generated key pair** (public-private) for the **authentication process.** This way you can let the users and/or programs log in without hassling with a password.

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.
* Before SSH was developed and popularized, different methods were in use for each of these functions:
* Insecure emulation or login programs like rlogin, Telnet and remote shell (rsh) for remote log on and running remote terminal sessions.
* File transfer programs like rcp (remote copy) and File Transfer Protocol (FTP) for file transfer purposes in the 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](https://en.wikipedia.org/wiki/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](https://en.wikipedia.org/wiki/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](https://www.ietf.org/mail-archive/web/ietf-announce/current/msg17592.html) intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in [web application security](https://www.cloudflare.com/learning/security/what-is-web-application-security/).

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.

**Working of TLS:**

For a website or application to use TLS, it must have a TLS certificate installed on its [origin server](https://www.cloudflare.com/learning/cdn/glossary/origin-server/) (the certificate is also known as an "[SSL certificate](https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/)" because of the naming confusion described above). A TLS certificate is issued by a certificate authority to the person or business that owns a domain. The certificate contains important information about who owns the domain, along with the server's public key, both of which are important for validating the server's identity.

A TLS connection is initiated using a sequence known as the [TLS handshake](https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/). When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the *client* device) and the web server.

During the TLS handshake, the user's device and the web server:

Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use

Decide on which cipher suites (see below) they will use

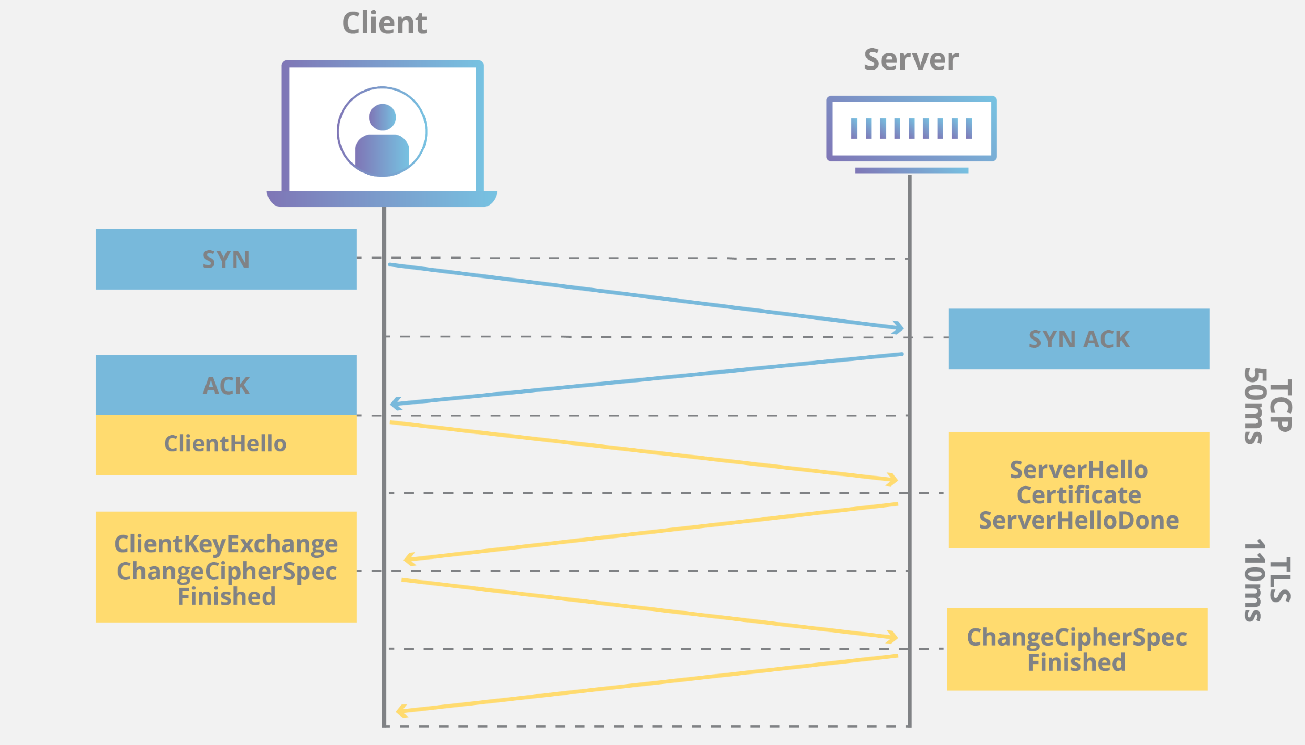
Authenticate the identity of the server using the server's TLS certificate

Generate session keys for encrypting messages between them after the handshake is complete

The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared [encryption keys](https://www.cloudflare.com/learning/ssl/what-is-a-cryptographic-key/), or [session keys](https://www.cloudflare.com/learning/ssl/what-is-a-session-key/), will be used for that particular session. TLS is able to set the matching session keys over an unencrypted channel thanks to a technology known as [public key cryptography](https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/).

The handshake also handles authentication, which usually consists of the server proving its identity to the client. This is done using public keys. Public keys are encryption keys that use one-way encryption, meaning that anyone with the public key can unscramble the data encrypted with the server's private key to ensure its authenticity, but only the original sender can encrypt data with the private key. The server's public key is part of its TLS certificate.

Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data. This is kind of like the tamper-proof foil found on a bottle of aspirin; the consumer knows no one has tampered with their medicine because the foil is intact when they purchase it.



**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.

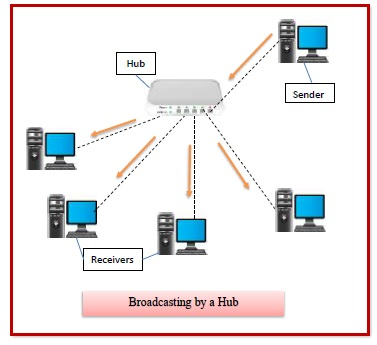
## **Types of network devices -**

* Hub
* Switch
* Router
* Bridge
* Gateway
* Modem
* Repeater
* Access Point

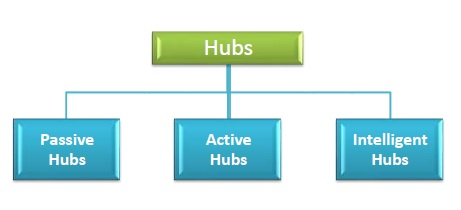
**HUB**

Hubs are networking devices operating at a physical layer of the [Open Systems Interconnection (OSI) model](https://www.netwrix.com/network_security_best_practices.html) 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. Also, they do not have the intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. Collision domain of all hosts connected through hub remains one. A hub can be used with both digital and analog data, provided its settings have been configured to prepare for the formatting of the incoming data. For example, if the incoming data is in digital format, the hub must pass it on as packets; however, if the incoming data is analog, then the hub passes it on in signal form. Transmission mode is half duplex. They generally have fewer ports of 4/12.



**Types of Hubs:**

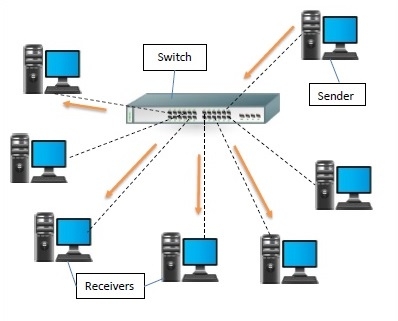


* **Passive Hubs** − Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN. The passive hubs are the connection point for wires that helps to make the physical network. It is capable of determining the bugs and faulty hardware. Simply, it accepts the packet over a port and circulates it to all ports. It includes connectors (10base-2 port and RJ-45) that can be applied as a standard in your network. This connector is connected to all [local area network (LAN)](https://www.javatpoint.com/wireless-lan-introduction) devices.
* **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 centre. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN. It is able to monitor the data sent to the connected devices. It plays an important role between the connected devices with the help of store technology, where it checks the data to be sent and decides which packet to send first.
* **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. It is beneficial to expend the business in networking; the management can assign users that help to work more quickly and share a common pool efficiently by using intelligent hubs. However, it offers better performance for the local area network. Furthermore, with any physical device, if any problem is detected, it is able to detect this problem easily.

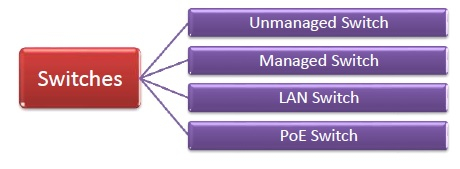
**SWITCH :**

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. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. Switch divides collision domain of hosts, but [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains same.

Using switches improves network efficiency over hubs or routers because of the virtual circuit capability. Switches also improve network security because the virtual circuits are more difficult to examine with network monitors. You can think of a switch as a device that has some of the best capabilities of routers and hubs combined. A switch can work at either the Data Link layer or the Network layer of the OSI model. A multilayer switch is one that can operate at both layers, which means that it can operate as both a switch and a router. A multilayer switch is a high-performance device that supports the same routing protocols as routers. Switches can be subject to distributed denial of service (DDoS) attacks; flood guards are used to prevent malicious traffic from bringing the switch to a halt. Switch port security is important so be sure to secure switches: Disable all unused ports and use DHCP snooping, ARP inspection and MAC address filtering.



**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. When more devices needs to be added, more switches are simply added by this plug and play method. They are referred to as u managed since they do not require to be configured or monitored.
* **Managed Switch** − These are costly switches that are used in organisations with large and complex networks, since they can be customized to augment the functionalities of a standard switch. The augmented features may be QoS (Quality of Service) like higher security levels, better precision control and complete network management. Despite their cost, they are preferred in growing organizations due to their scalability and flexibility. Simple Network Management Protocol (SNMP) is used for configuring managed switches.
* **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. They allocate bandwidth in a manner so that there is no overlapping of data packets in a network.
* **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. PoE switches offer greater flexibility and simplifies the cabling connections.

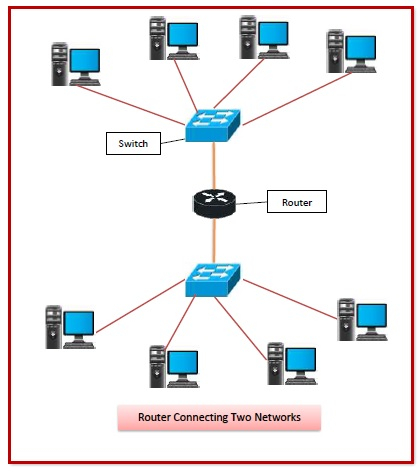
**ROUTER :**

Routers are networking devices operating at network layer of the OSI model. They are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Routers help transmit packets to their destinations by charting a path through the sea of interconnected networking devices using different network topologies. Routers are intelligent devices, and they store information about the networks they’re connected to. Most routers can be configured to operate as packet-filtering firewalls and use access control lists (ACLs). Routers, in conjunction with a channel service unit/data service unit (CSU/DSU), are also used to translate from LAN framing to WAN framing. This is needed because LANs and WANs use different network protocols. Such routers are known as border routers. They serve as the outside connection of a LAN to a WAN, and they operate at the border of your network.Routers usually communicate routing and other information using one of three standard protocols: Routing Information Protocol (RIP), Border Gateway Protocol (BGP) or Open Shortest Path First (OSPF).

Routers are your first line of defense, and they must be configured to pass only traffic that is authorized by network administrators. The routes themselves can be configured as static or dynamic. If they are static, they can only be configured manually and stay that way until changed. If they are dynamic, they learn of other routers around them and use information about those routers to build their routing tables.

Routers are general-purpose devices that interconnect two or more heterogeneous networks. They are usually dedicated to special-purpose computers, with separate input and output network interfaces for each connected network. Because routers and gateways are the backbone of large computer networks like the internet, they have special features that give them the flexibility and the ability to cope with varying network addressing schemes and frame sizes through segmentation of big packets into smaller sizes that fit the new network components. Each router interface has its own Address Resolution Protocol (ARP) module, its own LAN address (network card address) and its own Internet Protocol (IP) address. The router, with the help of a routing table, has knowledge of routes a packet could take from its source to its destination. The routing table, like in the bridge and switch, grows dynamically. Upon receipt of a packet, the router removes the packet headers and trailers and analyzes the IP header by determining the source and destination addresses and data type, and noting the arrival time. It also updates the router table with new addresses not already in the table. The IP header and arrival time information is entered in the routing table. Routers normally work at the Network layer of the OSI model.

****

## **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.

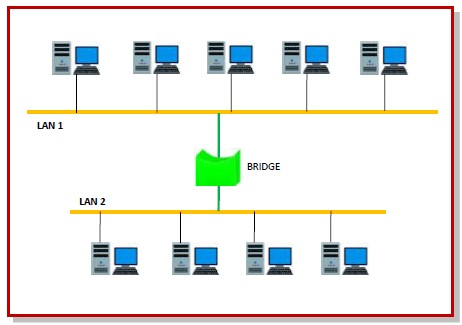
## **Types of Routers –**

* **Wireless Router** − They provide Wi-Fi connection Wi-Fi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
* **Broadband Routers** − They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
* **Core Routers** − They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
* **Edge Routers** − They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
* **Brouters** −Brouters are specialized routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

## **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.

Bridges are like hubs in many respects, including the fact that they connect LAN components with identical protocols. However, bridges filter incoming data packets, known as frames, for addresses before they are forwarded. As it filters the data packets, the bridge makes no modifications to the format or content of the incoming data. The bridge filters and forwards frames on the network with the help of a dynamic bridge table. The bridge table, which is initially empty, maintains the LAN addresses for each computer in the LAN and the addresses of each bridge interface that connects the LAN to other LANs. Bridges, like hubs, can be either simple or multiple port. Bridges have mostly fallen out of favor in recent years and have been replaced by switches, which offer more functionality. In fact, switches are sometimes referred to as “multiport bridges” because of how they operate.



**Types of Bridges -**

* + **Transparent Bridge**

As the name suggests, it is an invisible bridge in the computer network. The main function of this bridge is to block or forward the data depending on the MAC address. The other devices within the network are unaware of the existence of bridges. These types of bridges are most popular and operate in a transparent way to the entire networks which are connected to hosts.

This bridge saves the addresses of MAC within a table that is similar to a routing table. This estimates the information when a packet is routed to its position. So, it can also merge several bridges to check incoming traffic in a better way. These bridges are implemented mainly in Ethernet networks.

* + **Translational Bridge**

A translational bridge plays a key role in changing a networking system from one type to another. These bridges are used to connect two different networks like token ring & Ethernet. This bridge can add or remove the data based on the traveling direction, and forward the frames of the data link layer in between LANs which uses various types of network protocols. The different network connections are Ethernet to FDDI/token ring otherwise Ethernet on UTP (unshielded twisted pair) to coax & in between FOC and copper wiring.

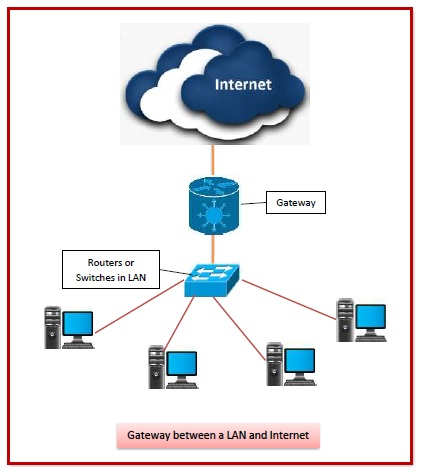
* + **Source-route Bridge**

Source-route Bridge is one type of technique used for Token Ring networks and it is designed by IBM. In this bridge, the total frame route is embedded in one frame. So that it allows the bridge to make precise decisions of how the frame is forwarding using the network. By using this method, two similar network segments are connected to the data link layer. It can be done in a distributed way wherever end-stations join within the bridging algorithm.

## **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.

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them. Gateways provide translation between networking technologies such as Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP). Because of this, gateways connect two or more autonomous networks, each with its own routing algorithms, protocols, topology, domain name service, and network administration procedures and policies. Gateways perform all of the functions of routers and more. In fact, a router with added translation functionality is a gateway. The function that does the translation between different network technologies is called a protocol converter.



## **Types of Gateways -**

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

* **Unidirectional Gateways** − They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.
* **Bidirectional Gateways** − They allow data to flow in both directions. They can be used as synchronization tools.

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

* **Network Gateway** − This is the most common type of gateway that provides as interface between two dissimilar networks operating with different protocols. Whenever the term gateway is mentioned without specifying the type, it indicates a network gateway.
* **Cloud Storage Gateway** − It is a network node or server that translates storage requests with different cloud storage service API calls, such as SOAP (Simple Object Access Protocol) or REST (REpresentational State Transfer).It facilitates integration of private cloud storage into applications without necessitating transfer of the applications into any public cloud, thus simplifying data communication.
* **Internet-To-Orbit Gateway (I2O)** − It connects devices on the Internet to satellites and spacecraft orbiting the earth. Two prominent I2O gateways are Project HERMES and Global Educational Network for Satellite Operations (GENSO).
* **IoT Gateway** − IoT gateways assimilates sensor data from IoT (Internet of Things) devices in the field and translates between sensor protocols before sending it to the cloud network. They connect IoT devices, cloud network and user applications.
* **VoiP Trunk Gateway** − It facilitates data transmission between plain old telephone service (POTS) devices like landline phones and fax machines, with VoIP (voice over Internet Protocol) network.

**Access Point:**

A [wireless access point (WAP)](https://www.cisco.com/c/en/us/solutions/small-business/networking/wireless.html) 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:

In this configuration, an access point is connected directly to a wired LAN, providing a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their network connection.

### Repeater access point:

An access point or mesh extender can be configured as a standalone repeater to extend the range of your infrastructure or overcome an obstacle that blocks radio communication.

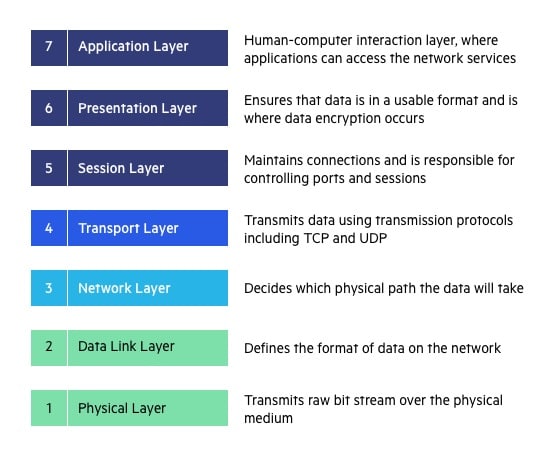
The repeater forwards traffic between wireless users and the wired network by sending data to either another repeater or an access point that is connected to the wired network. The data is sent through the route that provides the best performance for the client.

### Bridges:

Access points can be configured as root or non-root bridges to join multiple networks. An access point in this role will establish a wireless link with a non-root bridge. Traffic is then passed over the wireless link to the wired network.

# **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 internetwork 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. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
* **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. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
* **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](https://www.guru99.com/types-of-ip-addresses.html) 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.

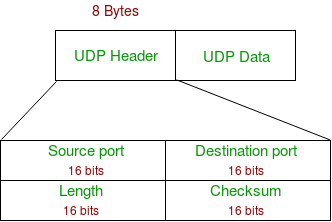
**User Datagram Protocol (UDP)**

It is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite. Unlike TCP, it is **unreliable and connectionless protocol.** So, there is no need to establish connection prior to data transfer.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency. Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also save bandwidth.   
User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

**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. UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or process.



* **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 can not 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. MAC address can be changed easily. For example, if the NIC on a particular machine fails, the MAC address changes but IP address does not change. ARP is used to find the MAC address of the node when an internet address is known.
* **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 back 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, as a result 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. Its 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 system.

* **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:**

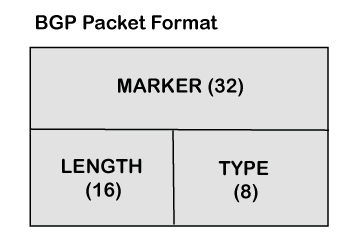
There are four different types of packets exist in BGP:

* **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.

****

**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.

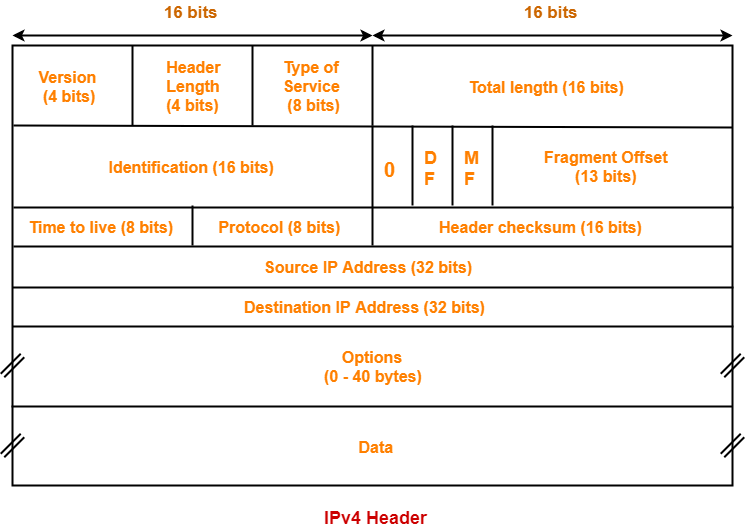
For example, **66.94.29.13**

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 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.

This hexadecimal address contains both numbers and alphabets. Due to the usage of both the numbers and alphabets, IPv6 is capable of producing over 340 undecillion (3.4\*1038) addresses.

IPv6 is a 128-bit hexadecimal address made up of 8 sets of 16 bits each, and these 8 sets are separated by a colon. In IPv6, each hexadecimal character represents 4 bits. So, we need to convert 4 bits to a hexadecimal number at a time