THE PRE HACKING BOOK

NETWORKING

HOW THE COMPUTER WORKS

SACHIN

About The Author and The Book

My Name is Sachin and I'm from Rajasthan India
This book is written for People who have interest in Technology and want to become Ethical Hacker and Cybersecurity Researcher.
This book will help you clear all the basics of Networking.
In this book, I have explained all topics very easily and with the help of examples.

+----------+

Networking : How The Computer Works

BY SACHIN

+----------+

+----------+

Contents

+----------+

Introduction

Today The Internet is a part of our life, and we use it for different things like learning stuff, surfing the internet, etc.

But have you ever thought that when you search something on the internet, where that result comes from? The result comes from servers.

Server is a computer that contains OS (Operating System) and data storage.

We download a file from the internet. How does the file download on our device, why not on sachin's device?

1.1 Web vs Internet

Some mind thinks that Web and Internet are same, but that's not true,
Web is a part of the internet.

The Internet has different Protocols for different Services like HTTP for websites, SMTP for sending emails, FTP for transferring files etc.

Internet

The Internet is a system of computer networks that uses the TCP/IP model to communicate with networks and devices.

WEB

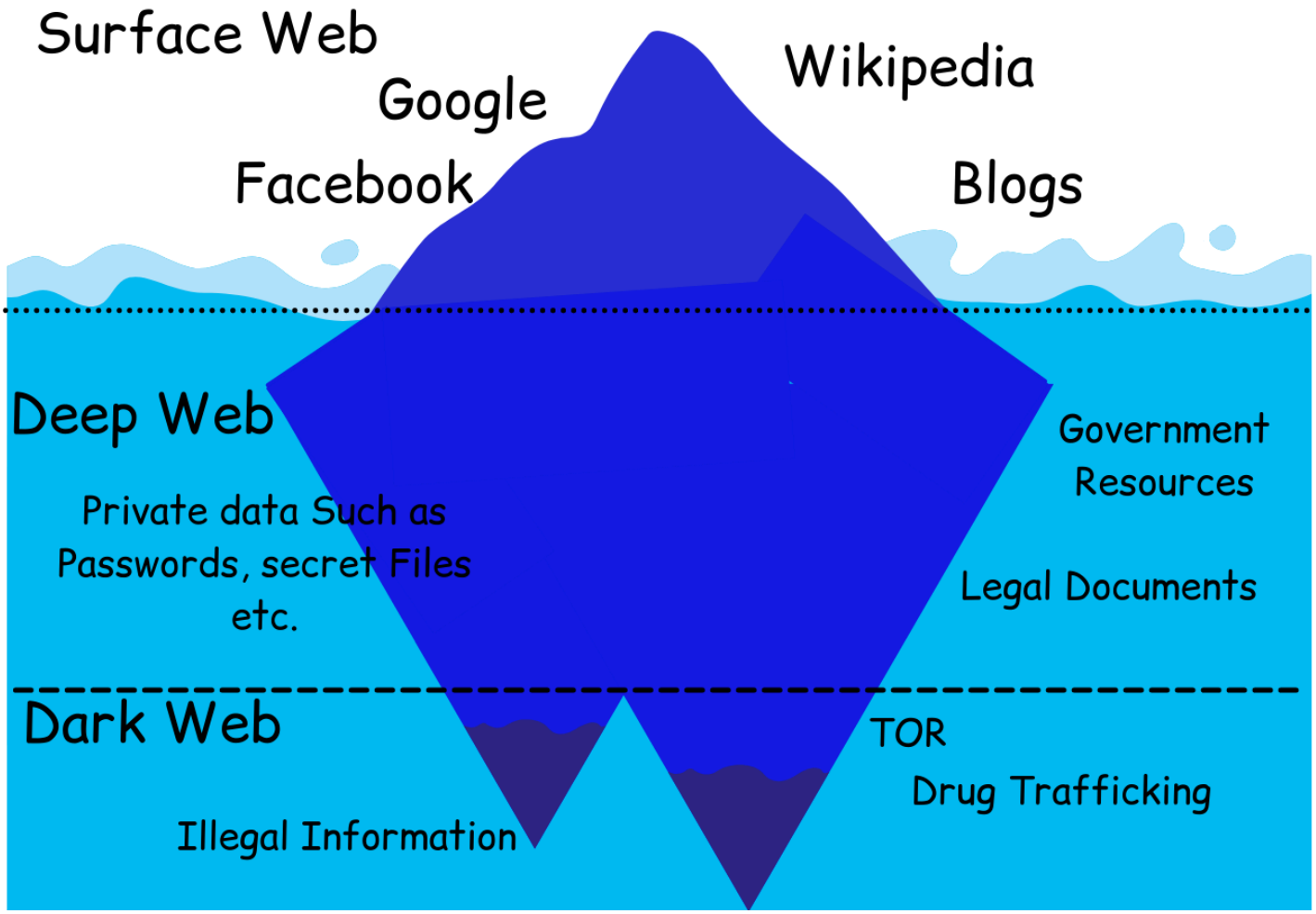
World Wide Web (WWW), also known as the WEB. On the web, resources are identified by URL (Uniform Resource Locators) such as www.example.com

WEB Page

Web page is a collection of contents provided by the websites. Collection of web pages makes websites.

1.2 Types Of WEB

1. Surface Web (4%)
2. Deep Web (90%)
3. Dark Web (6%)



1. Surface Web :-

When we search on the internet, the sites like shopping websites, banking websites, blogs websites, and etc, are on the surface web
These website is available for normal users

But These all website are only 4% of total websites

2. Deep Web :-

Deep web also called “Hidden Web” or “invisible Web” because it is not accessible for all users

Deep web’s data is not indexed on search engines like Google, Yahoo, Bing etc.

Deep web contains website’s secret files like government resources, legal documents, subscription information, scientific reports etc.

To see dark web data you must have that URL and credentials (Username Password)

3. Dark Web:-

Dark web contains illegal stuff like illegal pornography, terrorism, botnets, selling weapons and drugs, hiring hitmen, etc.

Normal users can't enter the dark web. To access it, we must have specific software and configuration to enter in the dark web like TOR browser.

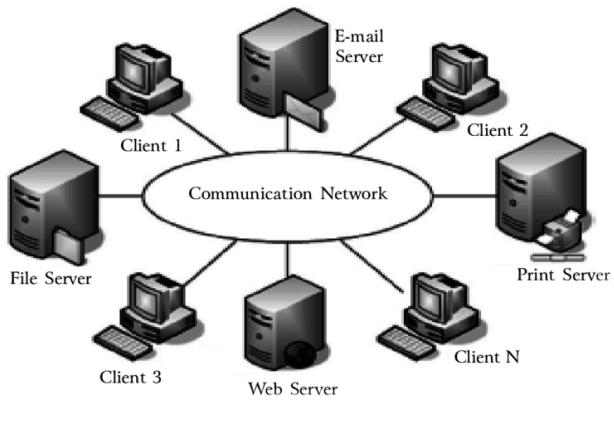
(*I recommend never use dark web)

1.3 Computer Networks

A group of computers that are connected to each other is called a computer network.

Or

Computer network is a group of two or more than two computers who are connected to each other.



Source: Saxena and Arora (2009)

Types

These are most common types of computer networks

- WLAN (Wireless Local Area Network)

  WLAN use Wireless Network Technology such as WiFi
  Same as LAN But these Networks don't require Physical Cables to connect with each other

- PAN (Personal Area Network)

  The smallest and most basic type of network, PAN is made up of a wireless modem, Basically Found in Buildings, small offices etc.

- LAN (Local Area Network)

  LAN is one of most common, simple, and original area network,
  LANs connect groups of computers and low-voltage devices together across short distances

- MAN (Metropolitan Area Network)

  MAN used in Entire Geographical Area (City, Town)
  maintenance is handled by a company or a single person

- WAN (Wide Area Network)

  WAN allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate. Slightly more complex than LAN

- VPN (Virtual Private Network)

  VPN is encrypted connection from a device to network, it's used to access private resources for user

Features of Computer Network

- Resource sharing
- Communication Speed
- Backup
- Reliability
- Scalability
- Software and Hardware Sharing
- Security

Packets

Let's suppose we are downloading a file from the internet, that file is divided into pieces called packets, and when all packets arrive, they combine and create a full working file.
(*data transfer in packets)

Torrent

Torrent is not illegal itself, downloading copyright material using it is illegal. Torrent downloads multiple packets from multiple seeders, combines all the packets and creates a full working file. Also you become a seeder[sender] while downloading the file.

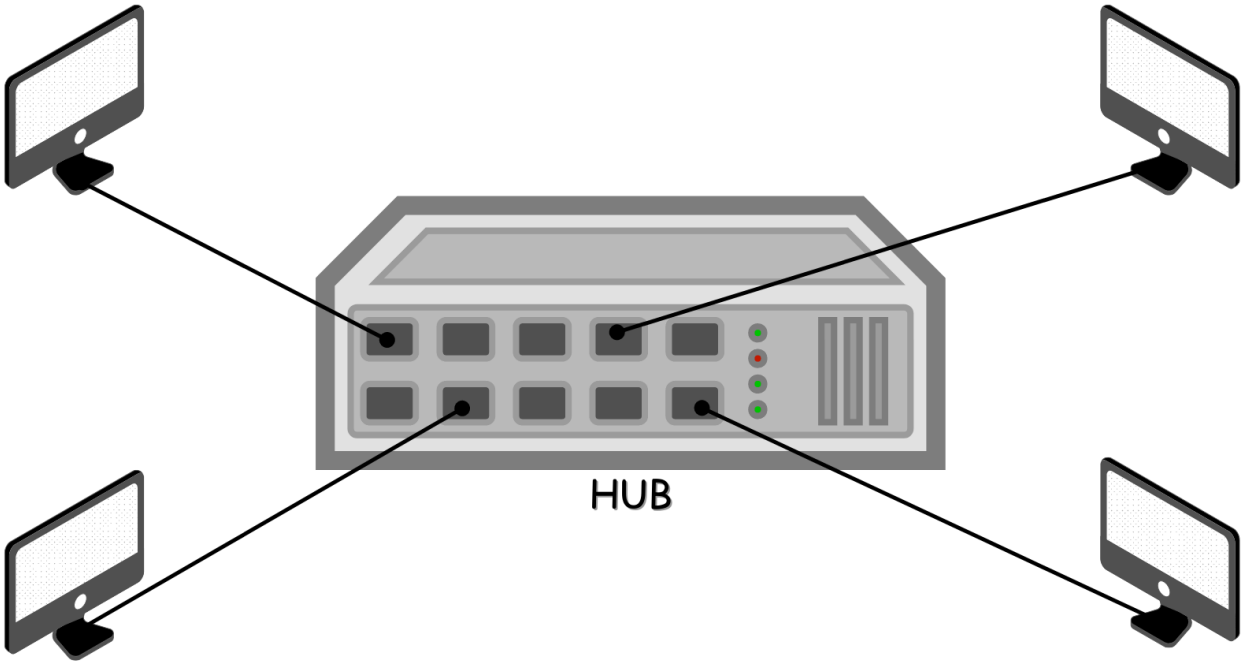
1.4 Network Devices

Hub

Hub is a less expensive and less complicated network device that is used to connect multiple computers in a network.

All the information sent to the hub is automatically sent to every connected device (Example: social Groups)

Hub uses LAN Network
Hub uses in Broadcast (One-to-All)

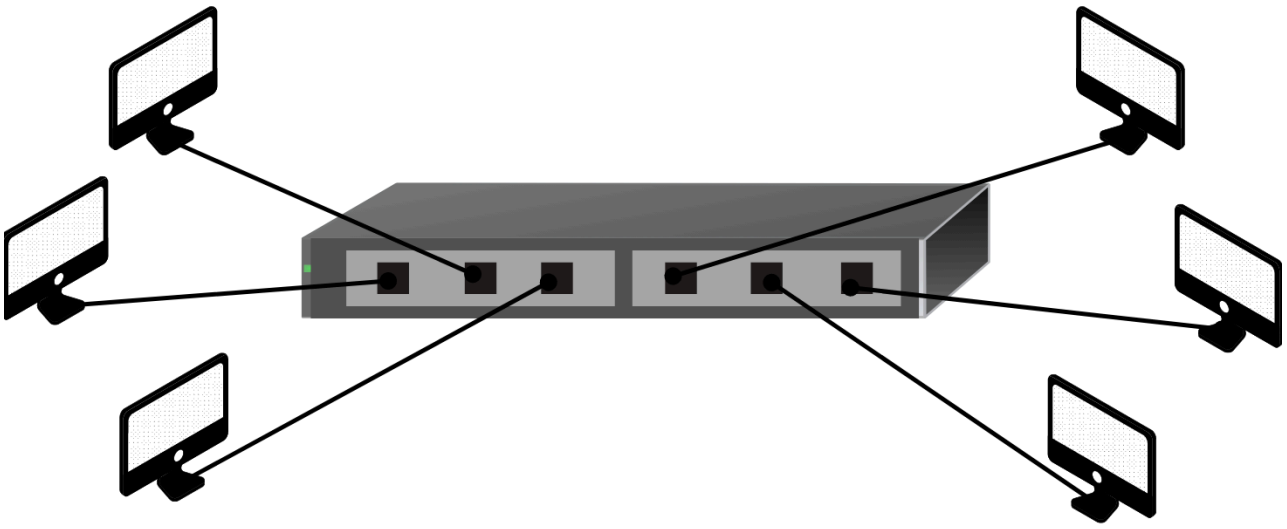


Switch

Switch is a network device that is mainly used to send private data without losing it.

With the help of a MAC address, the switch can know which device is connected to which port,
So it delivers messages or data to a particular machine.

Switch is more intelligent, and more secure than hub
Switch used to Unicast (One-to-One Transfer) the message.

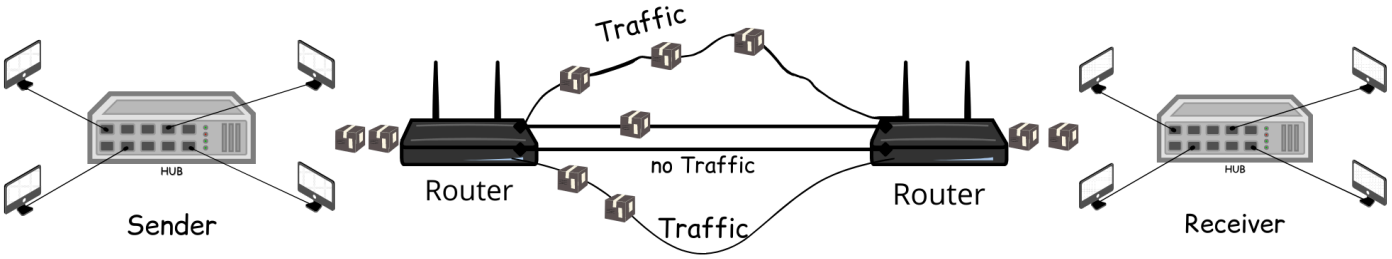


Router

Router is a network device that is used to receive incoming data and forward it to the destination path with the lowest traffic route.

The router is used in both LAN & WAN networks.

Router provides both wired and wireless facility, with a very high transmission rate.



Repeater

Repeater is a network device that is used to boost weak signals.

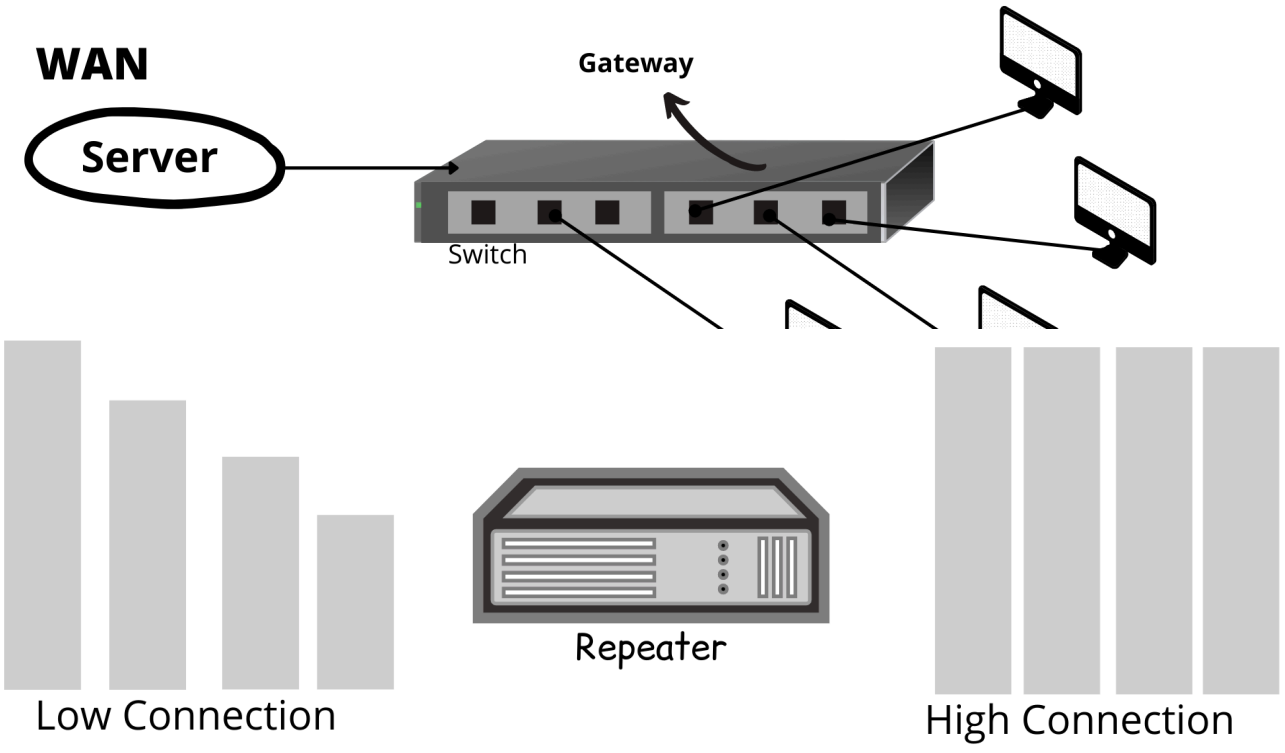
The signal travels in the network, the intensity of the signal becomes low after traveling some distance, to regenerate the weak signal we use repeater.

For example, in the old days there was cable TVs, which had a signal from far away, due to the signal coming from far away in the TV, the signal in our TV was very bad, to fix it between the original place and our TV A black box was kept, which helped signal good, That was called repeater.
Repeater used in both LAN & WAN

Gateway

Gateway is a network device that is used to connect different types of network and also the same types of network. Gateway operates all 7 Layer of OSI Model

It send or receive data with The help of internet even it is a LAN network

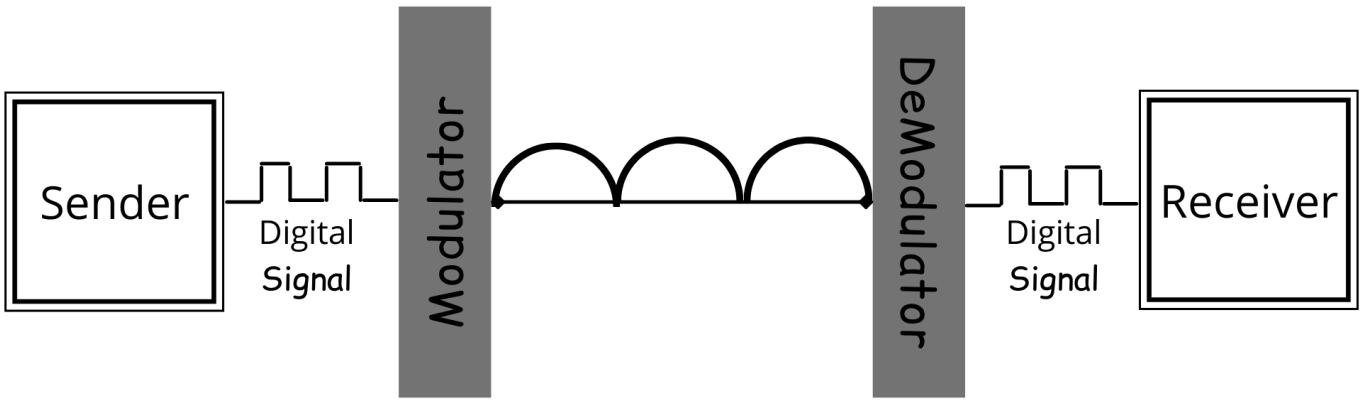


Modem

Modem stands for Modulator & Demodulator.

Modem is a network device that is placed between the computer and telephone line.

Modem is used to connect the computer with the internet (wired)



It has two part modulator (Convert digital signal to analog signal) and Demodulator (Convert analog signal to digital signal)

Bridge

Bridge is a network device that is used to separate LAN into a number of sections.

Bridge operates both physical layer and data link layer of OSI Model

It helps us to extend network coverage.

It broadcast the data to each node like hub or repeater

1.5 Network Protocols

The rule of transfer data from one device to Another device over the internet is called protocol.

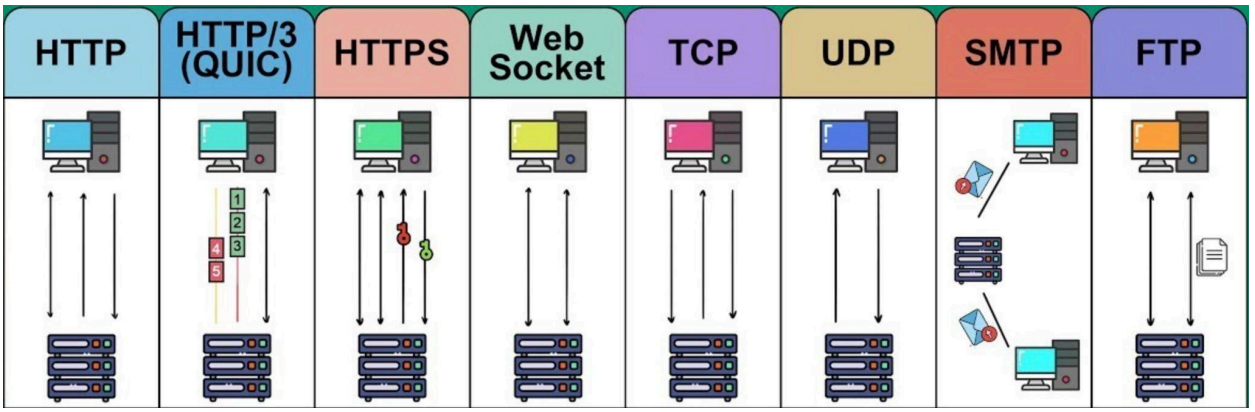
Or

Protocol is a set of rules that determines how the data is transmitted over the internet.

Protocol has 3 levels :

1. Hardware Level
2. Software Level
3. Application Level

Types Of Protocol



1. Standard Protocol :-

   Standard Protocols are published open standards that any organization or individual can use in their product.

   Ex. SMTP, FTP, DNS, DHCP, TelNet, TFTP

2. Proprietary Protocol :-

   Proprietary Protocols are developed by a single organization to use in their product.

   Ex. Skype, Apple Talk

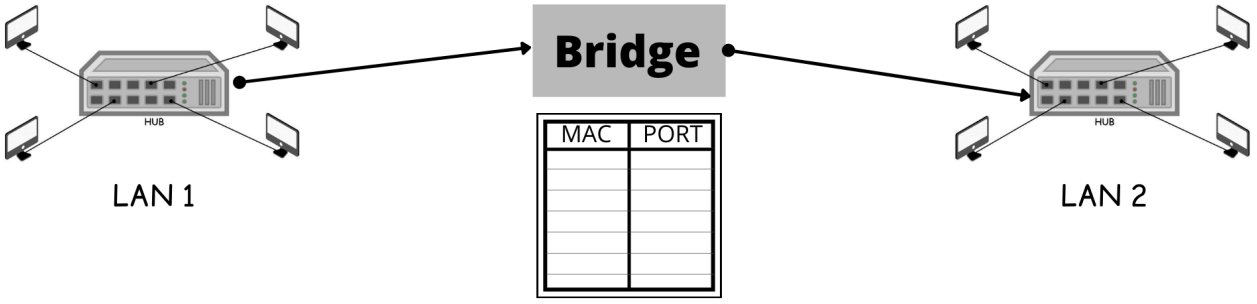
Here are Some Protocols

- HTTP (HyperText Transfer Protocol)

  Is a communication protocol that is used to transfer information on the internet and WWW (World Wide Web).

- FTP (File Transfer Protocol)

  Is the simple way to transfer files from one host to another over a TCP based network.



- TCP (Transmission Control Protocol)

  Is responsible for verifying the correct delivery of data from client to server.

- IP (Internet Protocol)

  Is used to move packets of data from node to node, by using four byte destination addresses (IP Number).

- VoIP (Voice Over Internet Protocol)

  Is used to enable voice communication over the internet. (Ex. Telephone Network)

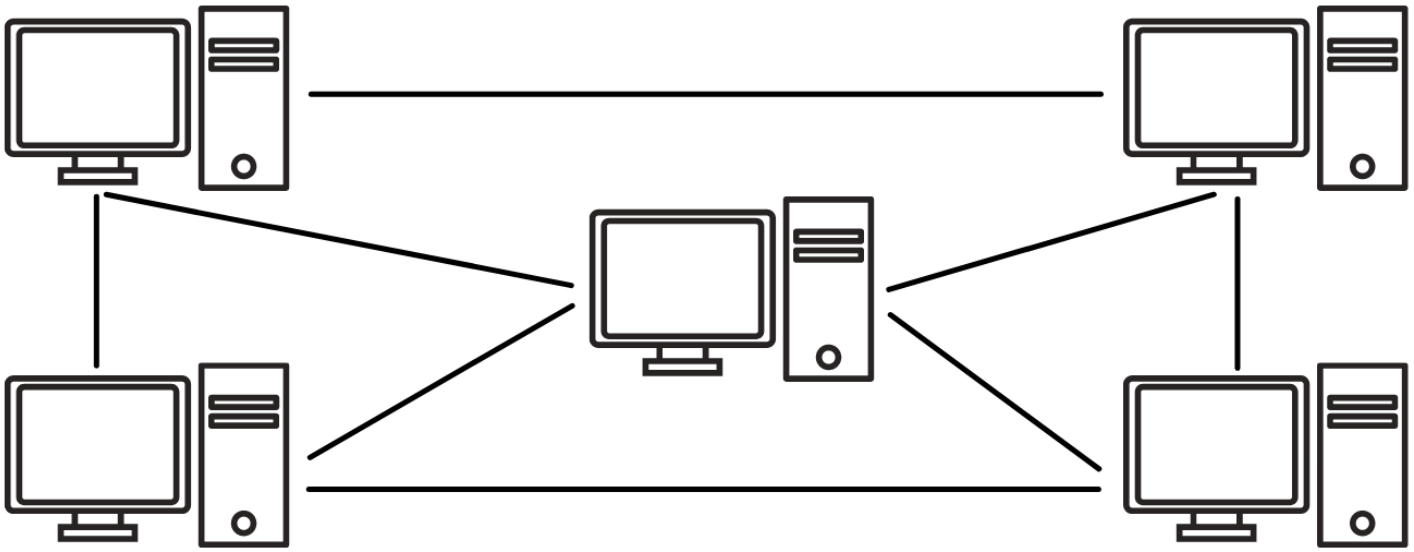
- SMTP (Simple Mail Transfer Protocol)

  Is used to send EMAIL (Electronic Mail) over the internet. (Ex. GMAIL, ProtonMail)

1.6 Peer-to-Peer Network

Peer-to-Peer (P2P) is a network, which helps to share resources from one device to another device using the internet.

P2P Network is not secure, because first you have to open one or more ports from your computer to receive data. The problem is that you can not control what type of data you receive.



OSI Model

Open systems interconnection model was developed by ISO (International Organization for Standardization).

OSI models define how data is transferred from one device to another device.

Two computers are connected via LAN cable and share data with each other.
But one computer is based on Microsoft Windows and the other one is based on Unix, then how these computers are going to communicate with each other.

The OSI model was designed to communicate with two different types of computers [Windows, Ubuntu(unix)] or networks with each other.

OSI Model has 7 layers

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

DATA	Layer
Data	Application Network Process to Application
Data	Presentation Data Representation & Encryptio
Data	Session Inter-Host Communication
Segments	Transport End-to-End Connections & Reliability
Packets	Network Path Determination & IP
Frames	Data Link MAC & LLC (Physical Addressing)
Bits	Physical Media,Signal,& Binary Transmission

1. Physical Layer

The first layer of OSI Model is a physical layer which contains information in the form of bits.
It is responsible for actual physical connection between two devices.

This layer will get the signal received and convert it into 0 and 1 and then send it to the data link layer.
Devices :- Cables, Hub, Modem, Repeater

2. Data Link Layer

The second layer of OSI model is a data link layer which picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to the upper layer.

It has 2 sub-layers

a. MAC (Media Access Control) :

controls the hardware responsible for interaction with the wired, optical or wireless transmission medium

b. LLC (Logical Link Control) :

Interface between the MAC sublayer and the network layer.

Data link layer adds MAC address (Physical Address) of sender and or receiver in the header of each frame, after creating frames.

The Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines
Devices : Switch & Bridge

3. Network Layer

The Third Layer of OSI model is the network layer who is responsible for packet transmission from one host to another host.
Also takes care of packet routing with selection of the shortest paths.

Provides connection oriented and connection less mechanism
On the internet addresses are known as IP (Internet Protocol).

Internet protocol is a network layer protocol which helps to communicate end to end devices over the internet. It comes in two versions.

IPv4 which has ruled the world for decades but now is running out of address space.
IPv6 is created to replace IPv4 and hopefully mitigates limitations of IPv4 too.

Network Layer, Data Link Layer and Physical Layer are also known as lower layers or hardware layers.

4. Transport Layer

The fourth layer of OSI model is the transport layer which helps to manage packet loss and is responsible for the end to end delivery of the complete message.

The Transport layer also provides the successful data transmission and re-transmits the data if an error is found.

Transport layer provides services to the application layer and takes services from the network layer.
Transform layer ensures that data must be received in the same sequence in which it was sent.

Transport layer is operated by the operating system. It is a part of the OS and communicates with the application layer by making system calls

*(*Data in the transport layer is called as **Segments**)*

Protocols :- TCP, UDP, RDP

5. Session Layer

The fifth layer of OSI model is the session layer responsible for token management and establishment of connection, maintenance of sessions, authentication and also ensures security.

It prevents two users to simultaneously attempt the same critical operation.

The session layer provides the mechanism for opening, closing and managing a session between end-user application processes,

If a connection is not used for a long period, the session-layer protocol may close it.

Protocol : SCP (Session Control Protocol)

6. Presentation Layer

The sixth layer of the OSI model is the presentation layer which is also called translation layer.

Presentation Layer ensures that the message is presented to the upper layer in a standardized format.

It is responsible for encryption and decryption of sensitive data before they are transmitted over common channels.

It is also responsible for data compression.

7. Application Layer

The seventh layer of OSI model is application layer which is implemented by the network applications also known as desktop layer

The application layer is used in both of the standard models of computer networking: the internet protocol (TCP/IP) and the OSI model

Ex. Browsers, Messenger etc.

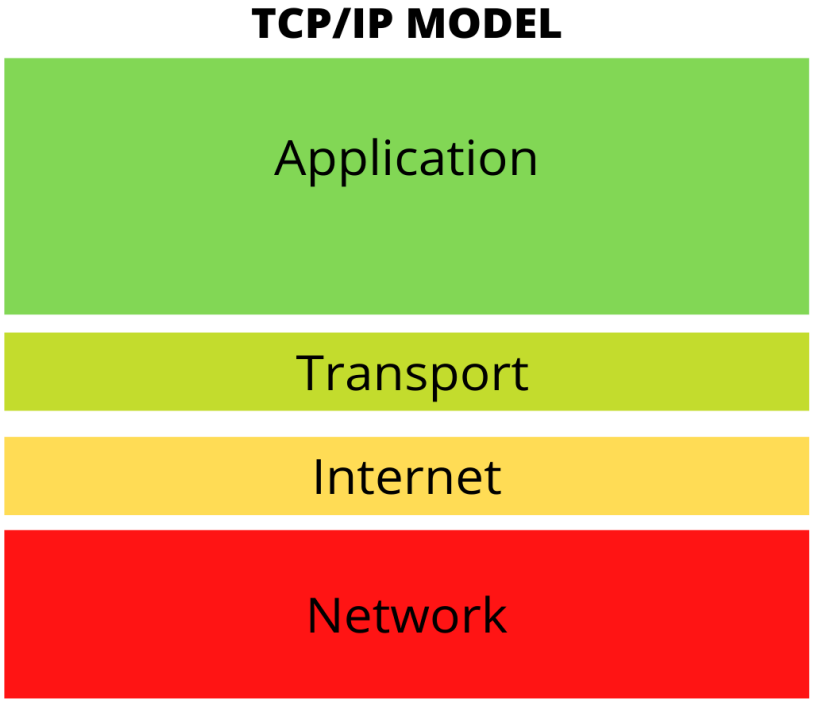
TCP/IP Model

Transmission control protocol/internet protocol was developed by ARPANET (Advanced Research Project Agency Network).

The TCP/IP model helps to connect the computer with the internet and transfer data between each other.

It helps you to create a virtual network when multiple computer networks are connected together.

It allows communication over large distances.



TCP/IP Model have 4 Layers

1. Network Layer
2. Internet Layer
3. Transport Layer (Host-to-Host Layer)
4. Application Layer

3.1 Network Layer

The network layer in TCP/IP is a combination of the first two, physical and data link layers of the OSI model.

It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

3.2 Internet Layer

The internet layer in TCP/IP works as network layer of OSI model

It defines the protocols which are responsible for transmission of data over the entire network

Main Protocols are

IP : Internet Protocol responsible for packets delivering from the source host to the destination host.

ICMP : Internet Control Message Protocol responsible for providing hosts with information about network problems.

ARP : Address Resolution Protocol who finds the hardware address of a host from a known IP address.

3.3 Transport layer (Host-to-Host Layer)

The transport layer in TCP/IP Model corresponds roughly to the fourth layer transport layer in the OSI model

It is responsible for end-to-end communication, error-free delivery of data with sequence

Two Main Protocols are

TCP (Transmission Control Protocol) : Provide reliable and error-free communication and send data in sequencing and segmentation (Connection-Oriented)

UDP (User Datagram Protocol) : Does not Provides reliable communication and does not send data in sequencing and segmentation (Connectionless)

3.4 Application Layer

The Application layer in TCP/IP is a combination of the last three, session, presentation and application layers of the OSI Model.

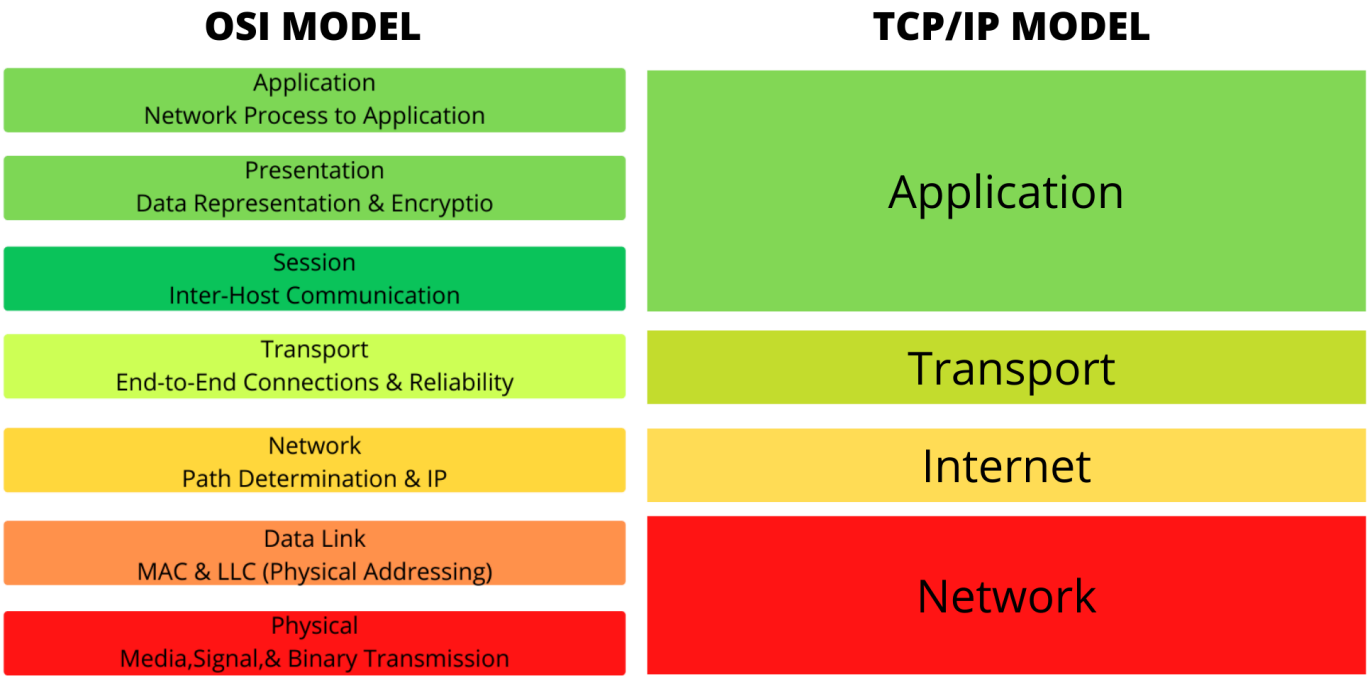
Application layer is responsible for node-to-node communication and helps you to identify communication partners, determine resource availability, and synchronize communication.

Main Protocols are

HTTP, HTTPS, FTP, Telnet, SSH, SMTP, DNS, NFS

OSI MODEL vs TCP/IP MODEL

OSI MODEL	TCP/IP MODEL
It has 7 Layers	It has 4 Layer
Less reliable	More reliable
Connection-oriented	Connection-oriented and connectionless
Follow vertical approach	Follow horizontal approach
It is defined after the advent of the internet.	It was defined before the advent of the internet.
Minimum header size 5 bytes	Minimum header size 20 bytes



MAC (Media Access Control) Address

MAC Address is the physical address which uniquely identifies each device. It is assigned to the NIC (Network Interface Card) of each device connected to the internet.

It is also called Physical Address and Hardware Address.

It is provided to NIC by the vendor at the time of manufacturing.

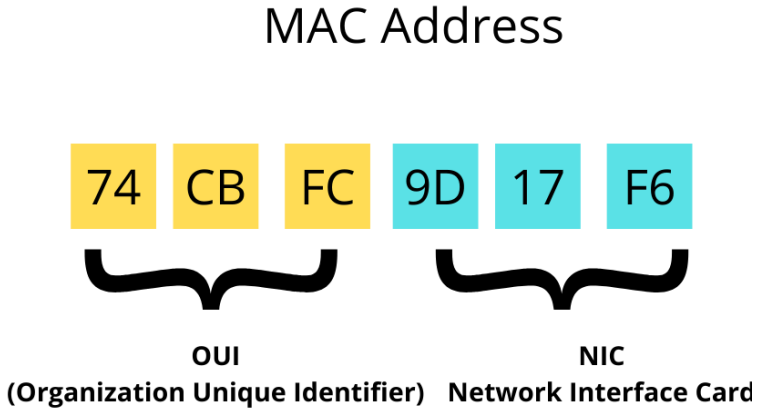
ARP protocol is used to associate a logical address with MAC address

MAC Address is represented in hexadecimal format 12-digit number and 48 bits long

74:CB:F3:9D:17:F6

First 24 Bits used for OUI (Organization Unique Identifier)

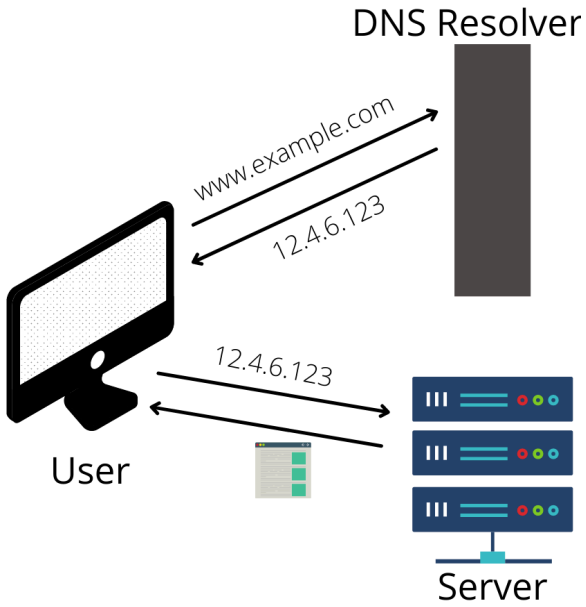
Second 24 Bits are for NIC (Network Interface Card)



DNS (Domain Name System)

DNS is a naming system which translates URLs (ex: www.google.com) into IP addresses

For example,
Just as a Hindi language person needs a translator to effectively talk with a person who speaks english. Similarly on the internet, browser understand the IP address and human understand URLs , here DNS act as translator
DNS translate URLs into IP addresses.



Internet Protocol (IP)

IP Address is a number that identifies devices on the internet. In real life, your home address is your identity, in the same way on the internet your IP address is your identity.

IP Address have 2 Versions : IPv4 and IPv6

6.1 IPv4 and IPv6

IPv4 (Internet Protocol version 4)

IPv4 is divided into 4 parts separated by .(dot) And Each part represents an eight-bit binary number from 0 to 255

0.0.0.0 - 255.255.255.255 (Ex. 192.168.0.1)

IPv4 Addresses length are 32-bit so maximum possible addresses are 2^{32} = 4,294,967,296 (About 4.3 billion)

IPv6 (Internet Protocol version 6)

IPv6 is divided into 6 parts separated by :(Colon) and there are eight numbers. There are letters in there because IPv6 addresses are written in hexadecimal (Base 16), which means 16 different symbols are required to uniquely represent. IPv6 used 0-9 + A-F.

2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b

IPv6 Addresses length are 128-bit so maximum possible addresses are 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 (About 340 undecillion)

Now the question is: When the IPv4 was there, what was the need of the IPv6?

Ans. Uses of the internet started growing, and the number of devices also started increasing day by day. IPv4 was able to deliver addresses to only about 4.3 billion devices. In 2015 there were 4.9 billion devices connected to the internet, IPv4 was not able to deliver addresses, so IPv6 was launched, its length was 128-bit and it was able to deliver addresses to 340 undecillion devices. It was more-than-enough. (IPv6 also provides more security than IPv4)

6.2 Private IP vs Public IP

Private IP

Private IP or Local IP is used to communicate in local networks(Printer, TV, Camera). Using local IP, data or information can be sent or received within the same network.

Suppose you have a router and the ISP gives the router a global IP when it is connected with The internet. When you are connecting your mobile to the router, The router assigns 192.168.0.1 IP to it, and when you connect your wifi camera to the router, it assigns 192.168.0.2 IP to it and so on.

(To find your device's local IP, use *ifconfig command)*

	Private address range	
Class	start address	finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Public IP

Public IP or Global IP are assigned by your ISP(Internet Service Provider). It is used to communicate over the internet,

There are 2 types of public ip :

1. Static IP
2. Dynamic IP

	Public address range	
Class	start address	finish address
A	0.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	254.255.255.255

6.3 Static IP vs Dynamic IP

Static IP

Static IP never changes, it remains constant and used mostly for web servers, geolocation, mail services, FTP services and other services that need a stable address for consistent access. It is costly

Dynamic IP

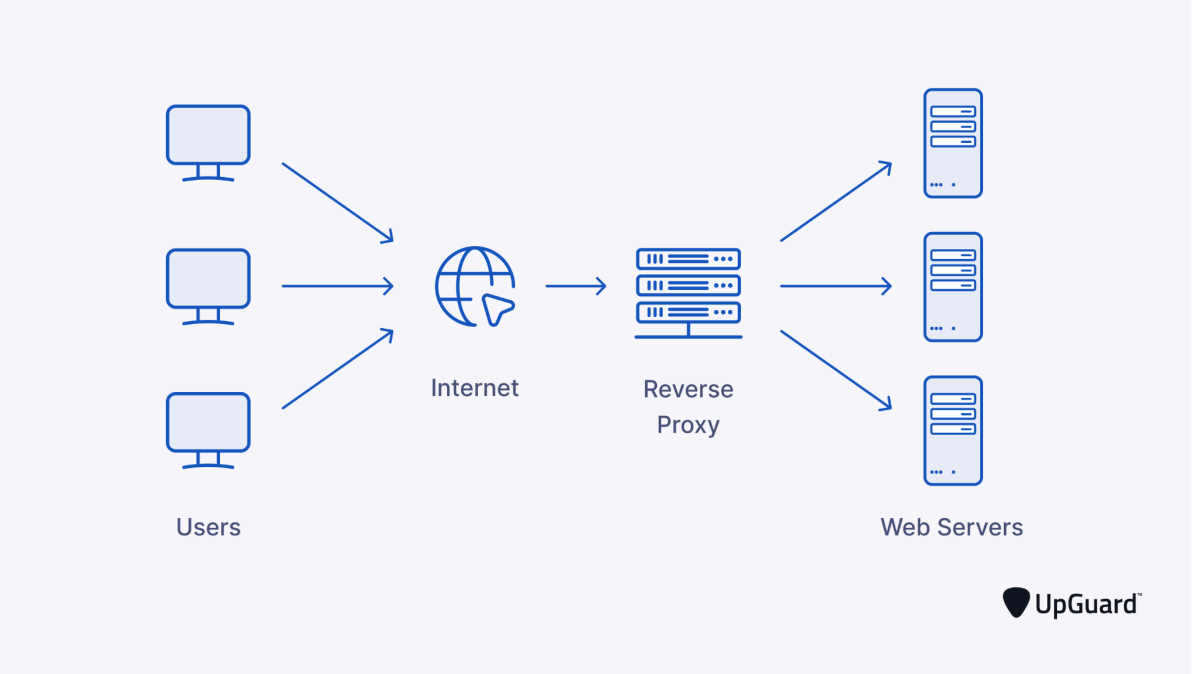
Dynamic IP Addresses are temporary provided by ISP using DHCP (Dynamic Host Configuration Protocol), Mostly used for our devices like mobile phone, It is less costly than Static IP

PROXY vs VPN (Virtual Private Network)

7.1 Proxy

Proxy is a server application which acts as a barrier between computer and the internet, and keeps your security.

Suppose, your IP address is 1.2.3.4 and you have a proxy. When you are surfing on the internet and requesting something [google.com], your IP address goes to the proxy server. The proxy server hides your original IP address, generates a new public IP address and sends it to the requested server [google.com]. The requested servers can not access your real IP. Thus, your privacy is maintained.



7.2 SOCKS Proxy

SOCKS stands for SOCKet Secure, which performs at the 5th layer of OSI Model (Session Layer).

SOCKS is an IP (Internet Protocol) that routes your traffic through a third-party server via TCP, assigning you a new IP address so web hosts can't determine your physical location.

SOCKS latest version is SOCKS5

SOCKS does not provide encryption so users are not safe from Public WiFi intercept attack.

7.3 VPN (Virtual Private Network)

VPN (Virtual Private Network) is a technology that is used to create a safe and encrypted connection.

VPN is commanly used to visit non trusted websites, unblock banned websites etc.

VPN is also used for privacy. For example, free wifi is available at railway stations, hotels, etc . They can know what you are visiting on the internet by intercepting your requests [http only]. To avoid this we should use VPN.

7.4 Difference

Proxy	VPN
No encryption	Use Encryption
Protocols : FTP HTTP SMTP	Protocols : PPTP L2TP
Works on Browsers	Works on Firewall
No tunnel creates between end user	creates a tunnel between end users.
Less security	High security

Carders use both SOCKS5 Proxy and VPN to be more anonymous.

Ports And Services

Port is a communication endpoint which identifies specific network services.
IP is like a building and port is like your room inside that.
Assume that ports are the multiple pipelines that flow the different types of data (Web Pages, Emails, Files, Connection) from one end to other.
Most common transport protocols that use port numbers are the TCP and the UDP.

Ports are 16-bit integer so maximum numbers are :
2^{16} = 65,536

Well known Ports	0 - 1023
Registered Ports	1024 - 49,151
Ephemeral Ports	49152 - 65,535

8.1 Common Ports

20 - FTP (Data Transfer)
21 - FTP (Command Control)

22 - SSH
23 - Telnet remote login service
25 - SMTP
53 - DNS Service
67, 68 DHCP (Dynamic Host Configuration Protocol)
80 HTTP (used in world wide web)
110 POP3 (Post Office Protocol)
119 NNTP (Network News Transfer Protocol)
123 NTP (Network Time Protocol)
143 IMAP (Internet Message Access Protocol)
161 SNMP (Simple Network Management Protocol)
194 IRC (Internet Relay Chat)
443 HTTPS (HTTP over TLS/SSL)

8.2 Port Scanning

Port scanning is a technique used to identify open ports and services available on a network host.
Port is a place in computer where information send and receive
Most common port scanning tools are nmap, naabu, angry ip scan etc.

Cryptography

The word cryptography comes from "crypt" which means “hidden” and "graphy" which means “writing”.
Cryptography is the techniques that is used to secure and protect data during communication
Encryption and decryption are the two essential functionalities of cryptography.

In simple words, we all know that all computers are connected to each other on the Internet, so when you send a message to your friend, the attacker can catch that message and see it.
If you want to send a secret message to someone, you have to encrypt the message with the help of a key and send that message.
That message still can be seen by the attacker but he cannot decrypt that message.
Only those who have the key to open that encrypted message can see and read the message

9.1 Features of Cryptography

1. Confidentiality

   The data will only be given to the person for whom it is created, no one else can see it.

2. Integrity

   Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3. Non-repudiation

   The owner of the information cannot deny his/her intention after sending information to the receiver.

4. Authentication

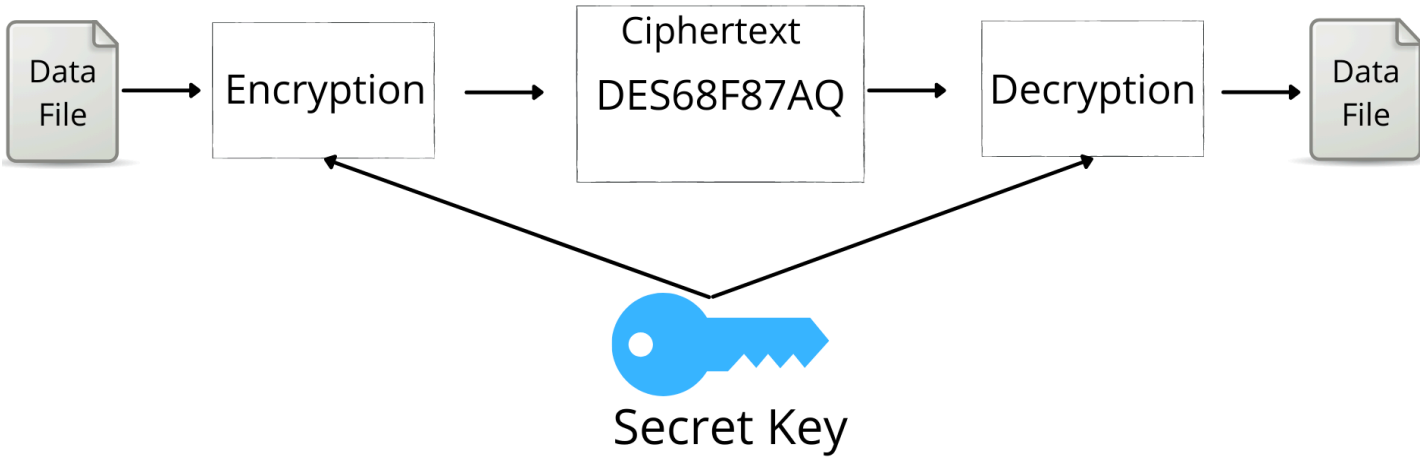
   The sender and receiver can confirm each other's identity and the destination of the information.

9.2 Types of Cryptography

1. Symmetric :

Symmetric method uses the same private key to encrypt and encrypt data that means, this private key is required for the sender to encrypt the data and for the receiver to decrypt the data.

It is old encryption and decryption technique

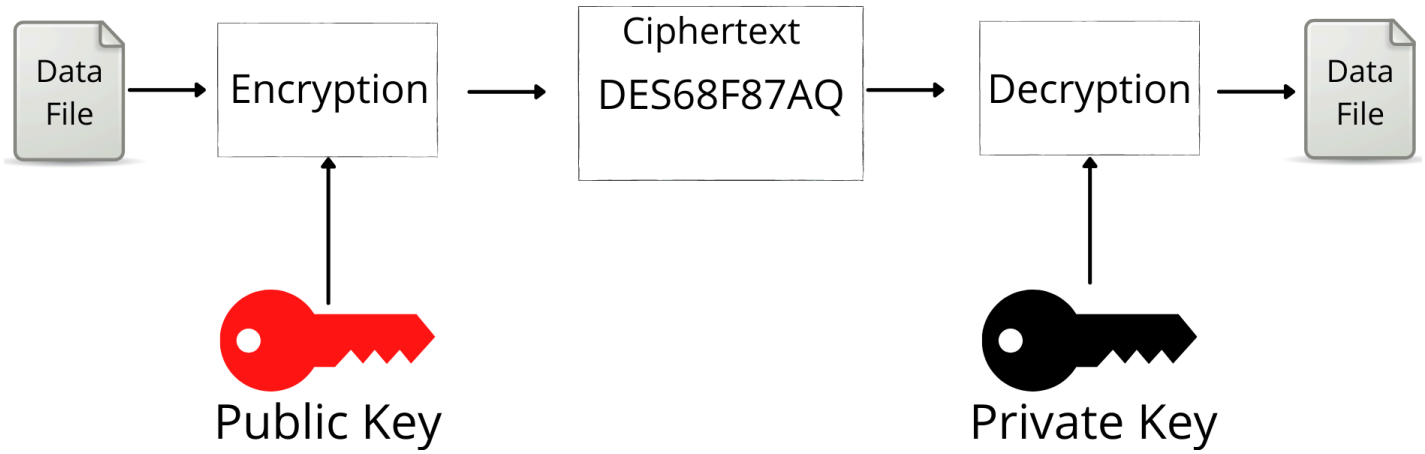


2. Asymmetric :

Asymmetric method uses two keys, one public key and one private key.

Public key is available to everyone and used to encrypt data,

Private key is the secret key and used to decrypt data



3. Hash Function :

Hashing is a one way function, It produces a fixed-length hash value from an input, but you cannot regenerate the original data from the hash. It does not use any type of key in its algorithms. Ex. MD5, SHA-256 (Most applications such as social media, bank accounts, etc. stored their user's password in MD5 hashes.)

9.3 Encryption & Decryption

Encryption

Encryption is a process in which the original data is converted into ciphered data/unreadable data with the help of algorithms and keys.
Encryption is used to protect sensitive information, private data, passwords etc.

Decryption

Decryption is a process in which the ciphertext is converted into plain-text or original data with the help of algorithms and keys.

9.4 Types of Encryption & Decryption

Type of Encryption & Decryption is based on the ability to encrypt how much data they can handle at once.
There are many types of encryption & decryption, some of the major types are : DES, AES, RSA

DES (Data Encryption Standard)

DES encrypts 56-bits data at a time. It was not very safe and was easily hacked. But it laid the foundation for creating more secure encryption for the future. After this, the more secure version T-DES or 3DES was launched.

Triple DES or 3DES

3DES uses Symmetric key encryption and three separate 56-bit keys for triple protection. It is more secure but much slower than others.

AES (Advanced Encryption Standard)

AES is more secure encryption that uses Symmetric key Encryption.
AES is used by The Government and security organizations.
It is different from others because it encrypts fixed size's blocks data at a time and the block sizes determine name for each AES encryption
AES-128 encrypt a 128-bit size's blocks
AES-192 encrypt a 192-bit size blocks
AES-256 encrypt a 256-bit size blocks

RSA (Rivest–Shamir–Adleman)

RSA is another more secure encryption that uses Asymmetric key encryption. It uses a Public key to encrypt data and a Private key to decrypt data.
RSA Encryption works on 1024-bit and can extend up to 2048-bit key length.
The longer the length of the encryption key, the longer it will take to encrypt data.

9.5 Hash Functions & types

Hashing is a one way algorithm that is irreversible, There are many different types of hash functions such as RipeMD, Tiger, xxhash and more, but the most common type of hashing used for file integrity checks are :
MD5, SHA2

1. MD (Message Digest)

   MD Family includes the hash functions MD2, MD4, MD5 and MD6. It is a 128-bit hash function. MD5 hash function is widely used in the software world. MD5 hash encodes a string of information in a 128-bit fingerprint.

2. SHA (Secure Hash Algorithms)

SHA Family have 4 types of algorithms

SHA-0, SHA-1, SHA-2, SHA-3

1. SHA-0 :

SHA-0 is a 160-bit hash function, it had some weakness and it didn't become not very popular

2. SHA-1 :

SHA-1 is a 160-bit hash algorithm that was used widely in applications and SSL (Secure Socket Layer) Security. After encoded it converts into a 40 digit long number.

3. SHA-2 :

SHA-2 family have 4 variants :
SHA-224, SHA-256, SHA-384, and SHA-512
These all depend on the numbers of their encoded Hash value.
SHA-2 Hash is a very strong hash that has not been hacked yet.

SSL (Secure Socket Layer) & TLS (Transport Layer Security)

SSL operates as a presentation layer in OSI Model. SSL and its successor, TLS are protocols for establishing secure and encrypted connections between web-browsers and servers.

SSL creates secrets with the help of MD (Message digest) technique and provides basic security such as Authentication and confidentiality.
TLS creates secrets with the help of Pseudo-random functions and provides high security.

SSL and TLS both are provides secure communication and securely transmit private data or secret data such as user's passwords, credit card numbers etc from server to web-browsers

[*Attackers can not intercept https requests using wifi attack.]

10.1 SSL Usage

SSL and TLS both are used to secure web browsing via HTTPS protocol. HTTPS website provides : Authenticity, Integrity, Encryption.
Always remember that when you make bank transition, shopping, authenticating and entering personal credentials, always check that the site is running on HTTPS (Hypertext Transfer Protocol Secure).

10.2 Certificate & Their Types

SSL/TLS certificate, which authenticates a website, is a small data file that binds the entire website into cryptographic keys (one public key and one private key). The private key is kept safe and the public key distributed with an SSL certificate.
You must have seen that when we go to HTTPS websites, we get to see SSL/TLS certificates.

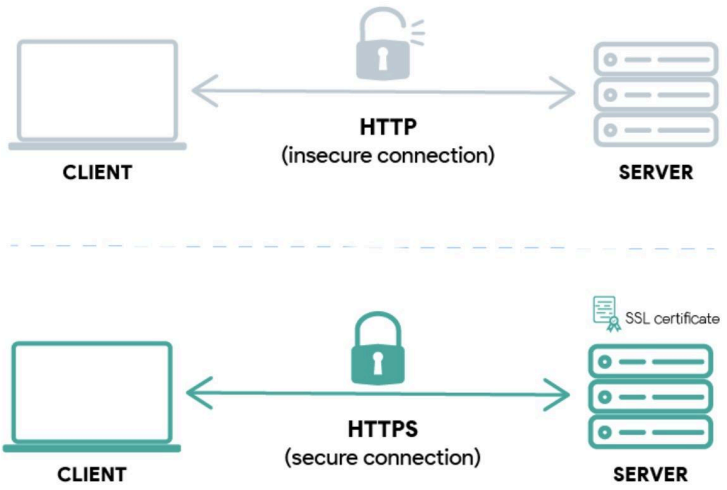
SSL/TLS certificates enable encryption of data that are sent to the server. Therefore attackers are not able to intercept requests to it. SSL changes the website protocol from HTTP to HTTPS.

SSL/TLS Certificate include :

- Domain name of website
- Sub-domains
- SSL/TLS version
- Issue date
- Expiration date
- Public key
- Certificate authority information
- Certificate signature algorithm

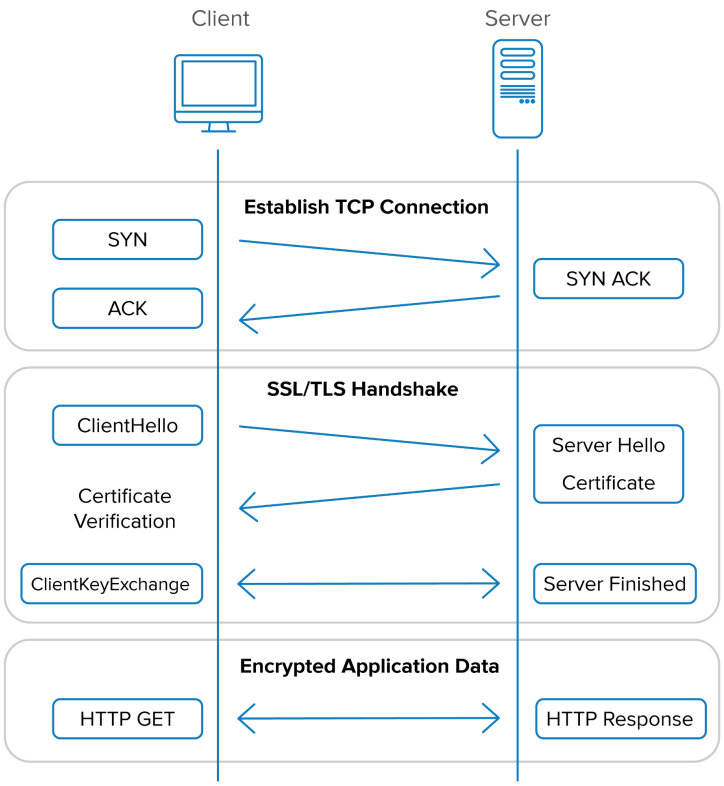
Types of SSL Certificate

1. Single-domain SSL certificates
2. Wildcard SSL certificates
3. Multi-Domain SSL certificates
4. Unified Communications SSL Certificate



10.3 How browsers validate certificates :

1. Browser connects to a website with SSL (HTTPS) and requests that the server identify itself.
2. Web-server sends a copy of the SSL certificate.
3. Browser checks the certificate and after successful validation it creates a session key with the help of a public key.
4. Server decrypts the session key with the help of its private key and sends a request to the browser for starting the encrypted session.
5. Encrypted session is started and server and browser now encrypt all transmitted data with the session key.



+----------+

Thank You very much for reading this book.
I hope you learned a lot

HACKERSTHAN

+----------+