Computer Networks (Part-2)
Based on CBSE Syllabus
Class XII

By-
Neha Tyagi
PGT CS
KV No. 5 Jaipur II Shift
Website: www.pythontrends.wordpress.com
Email: python.kvs@gmail.com

In previous part, we learnt following points… .

- Network
- Benefits of Network
- Terminology of Network
- Structure of Network
- Types of network
- LAN, MAN, WAN, PAN
- Internet
- Intranet
- Node
- Server
- NIU
- Interspace
- Channel
- Transmission Media
- Twisted Pair
- Co-axial Cable
- Fiber Optical Cable
- Wireless Media
- Microwaves
- Infrared Waves
- Satellite Link
- Client Server Architecture
- Cloud Computing
- IoT
- Network Devices
- HUB, Switch,
- Repeater, Router
- Gateway
- WAP
- Setting Computer Network
- Technique for solving questions

In Part – 2 , we will discuss following points……

1. Topology
2. Network stack
3. Modulation
4. Collision
5. Error Checking And correcting codes
6. MAC
7. Routing
8. Domain name Systems
9. URL Structure
10. Basic Networking tools
11. Protocols

12.HTTP

13.E-mail

14.HTTPS

15.Network applications

16.FTP

17.Telnet

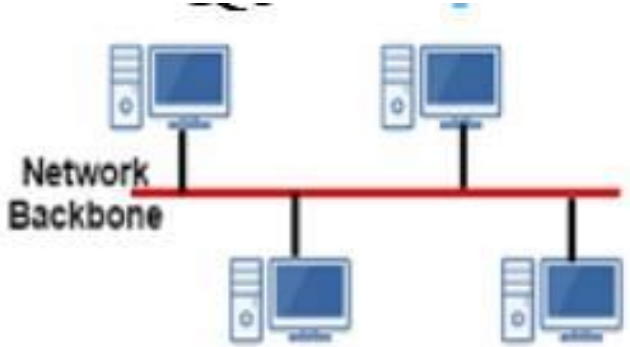
18.SMTP

19.VoIP

20.POP

Topology

Topology is the manner of connecting computers in a network, as shown in given diagrams. Topology is of following types-

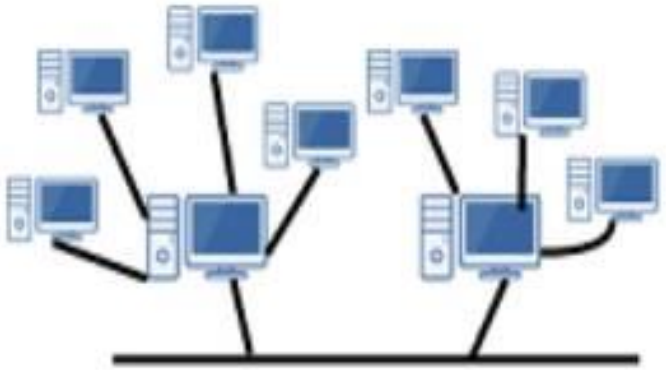


Bus

Star

Ring

Mesh

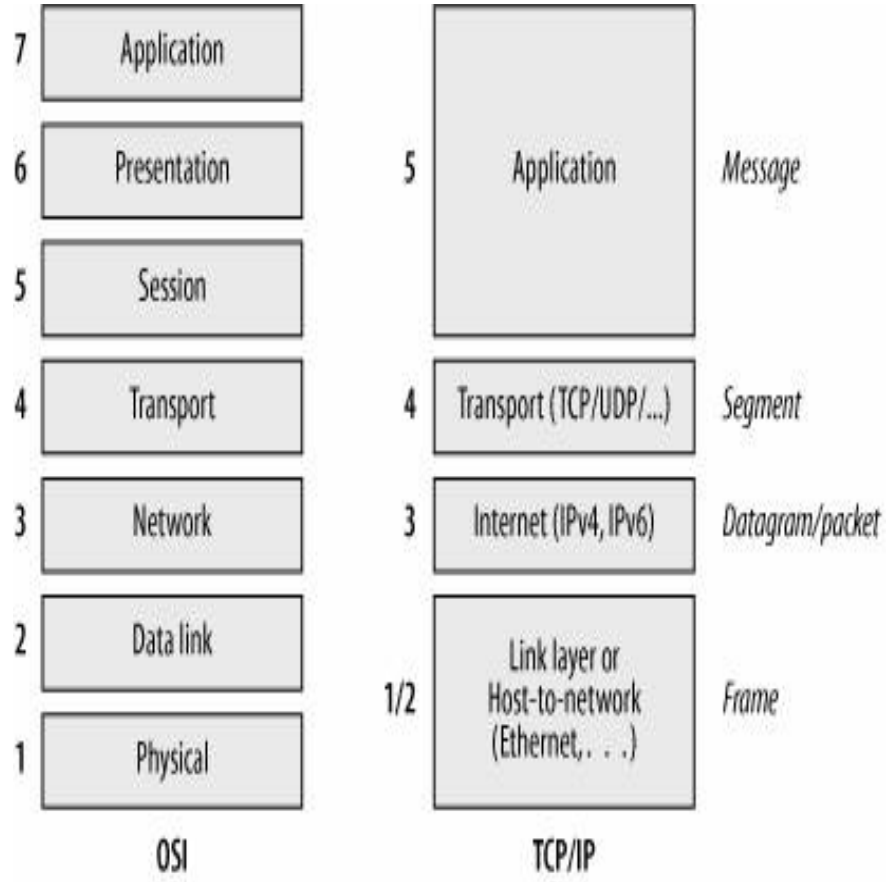


Tree

Point-to-Point

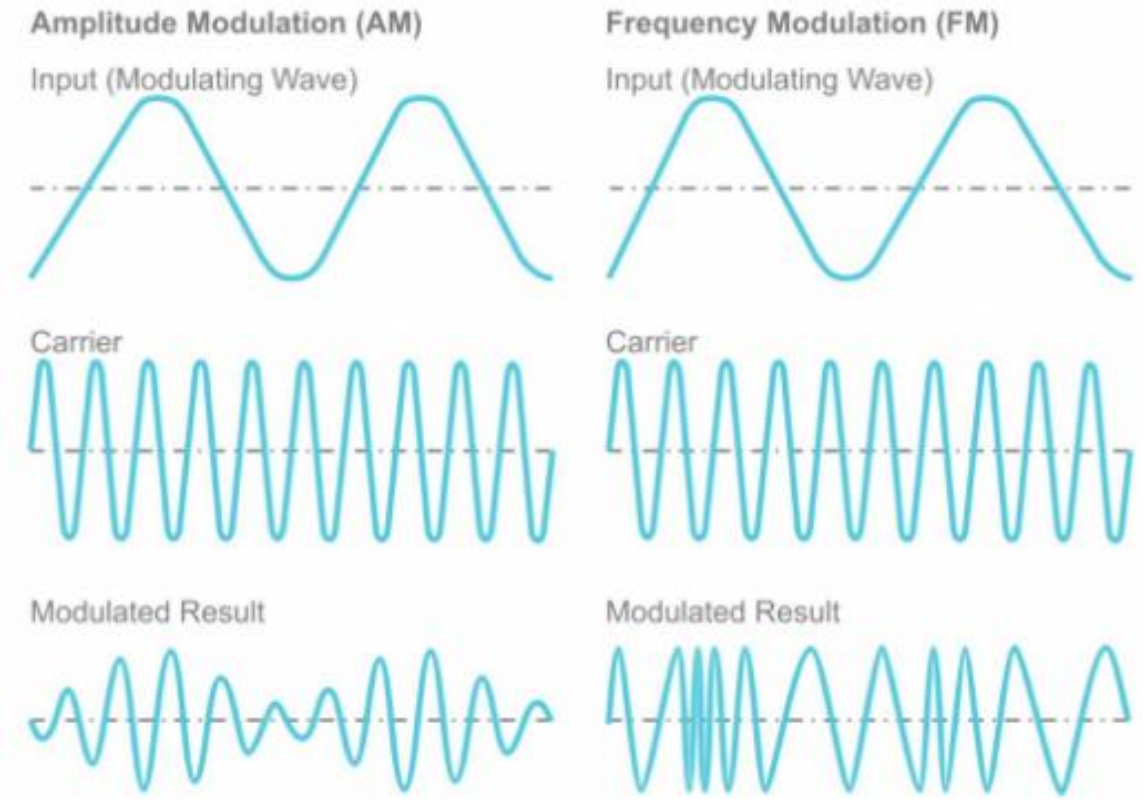
Network Stack

- Protocol stack or Network stack is a implementation of a computer networking protocol suite.
- Suite is a medium of transmission protocols and stack is a software to implement these suites.
- In a suite, individual protocols are designed to achieve one common goal.
- It ease the process of modularization, design and evaluation.
- While implementing, protocol stack is generally divided in to three main parts- Media, Transport and Application.
- In a special operating system or platform, there are two well designed software interface exists- one in between a media layer and transport layer and one in between transport layer and application layer.



Modulation

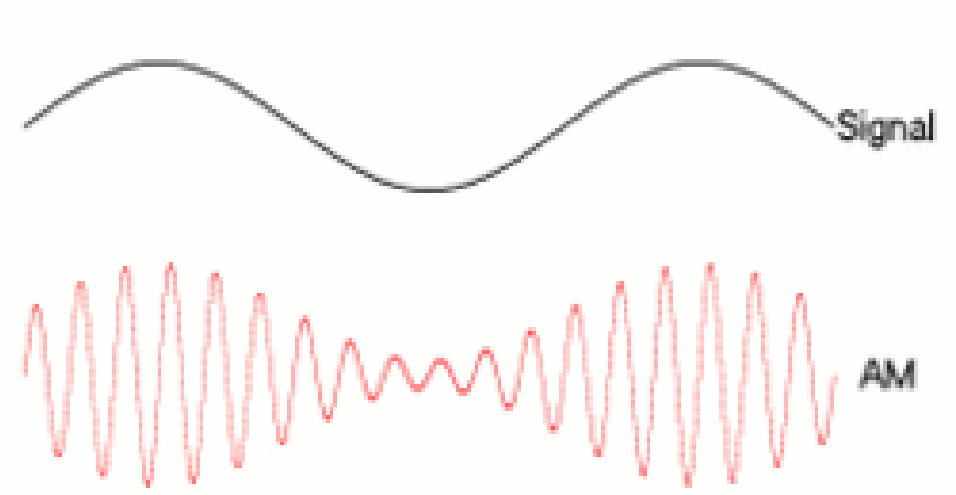
- Modulation is a technique of conversion of an electronic or optical carrier signal in to radio waves. There is a carrier signal in a stationary wave with certain height or dimensions or frequency. For optical signals, its dimensions, frequency, phase, polarization and spin like quantum level entities are to be separated to add in carrier. It is of three types-
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
  - Phase Modulation (PM)

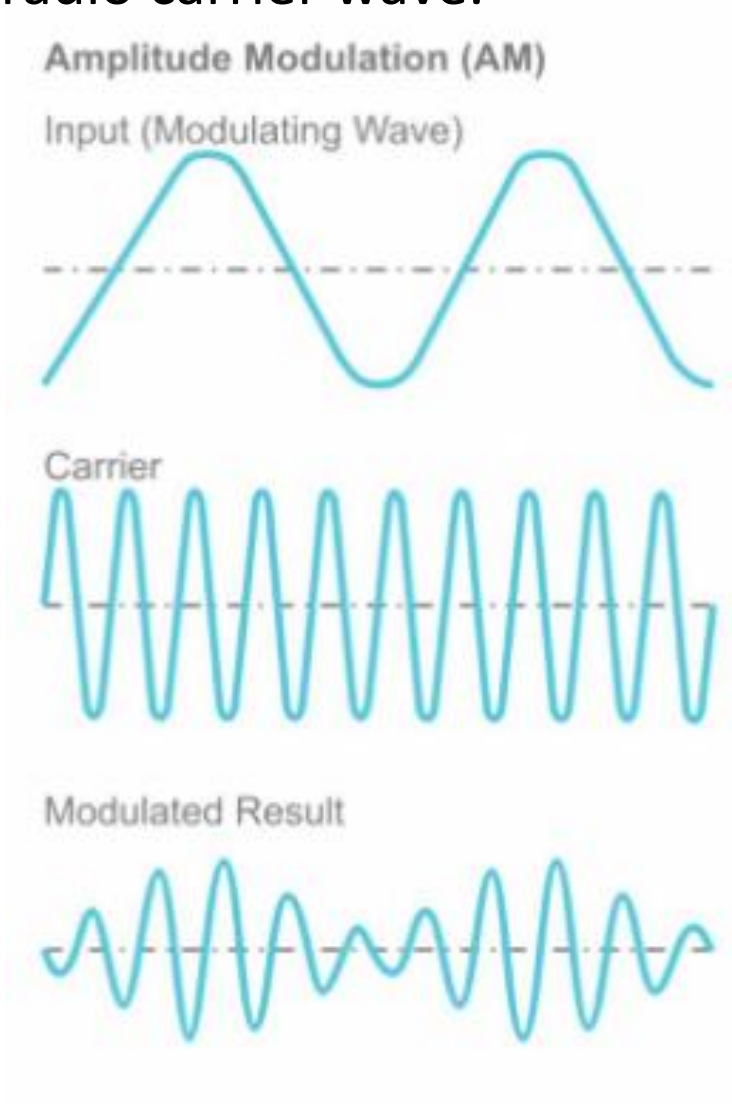


We will cover these points as per our syllabus only.

Amplitude Modulation (AM)

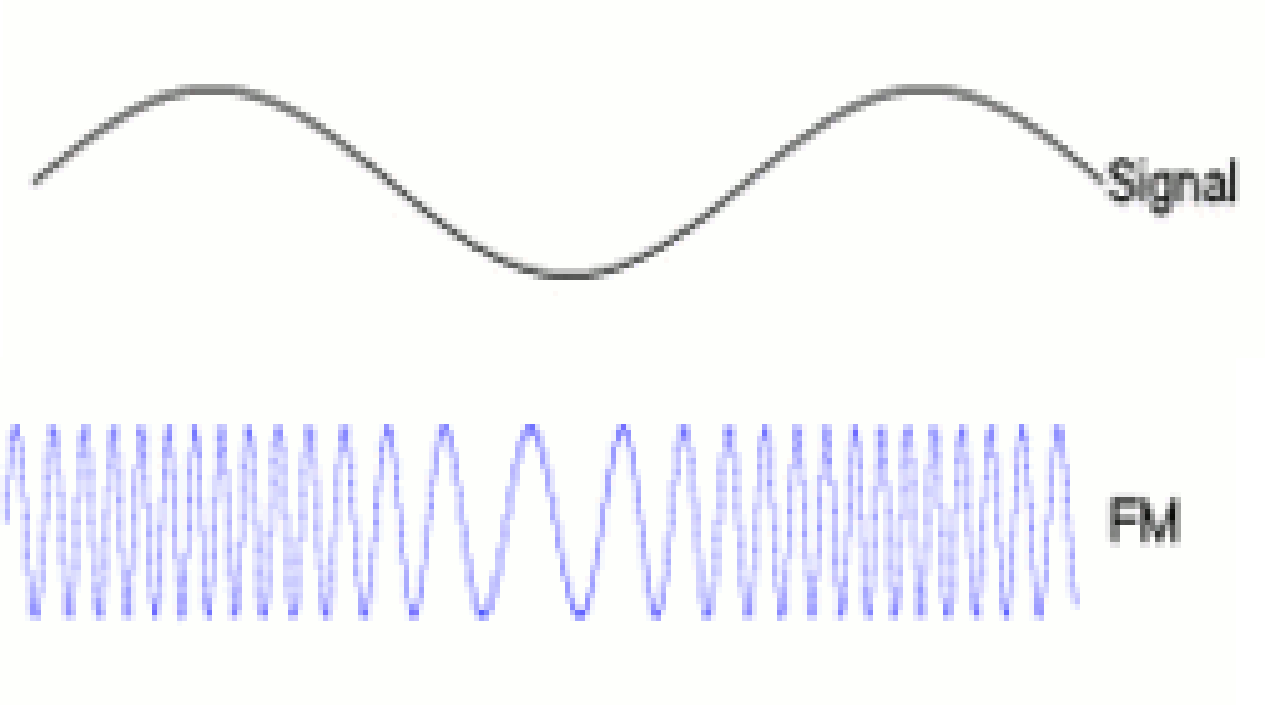
- The modulation of a wave by varying its amplitude, used especially as a means of broadcasting an audio signal by combining it with a radio carrier wave.

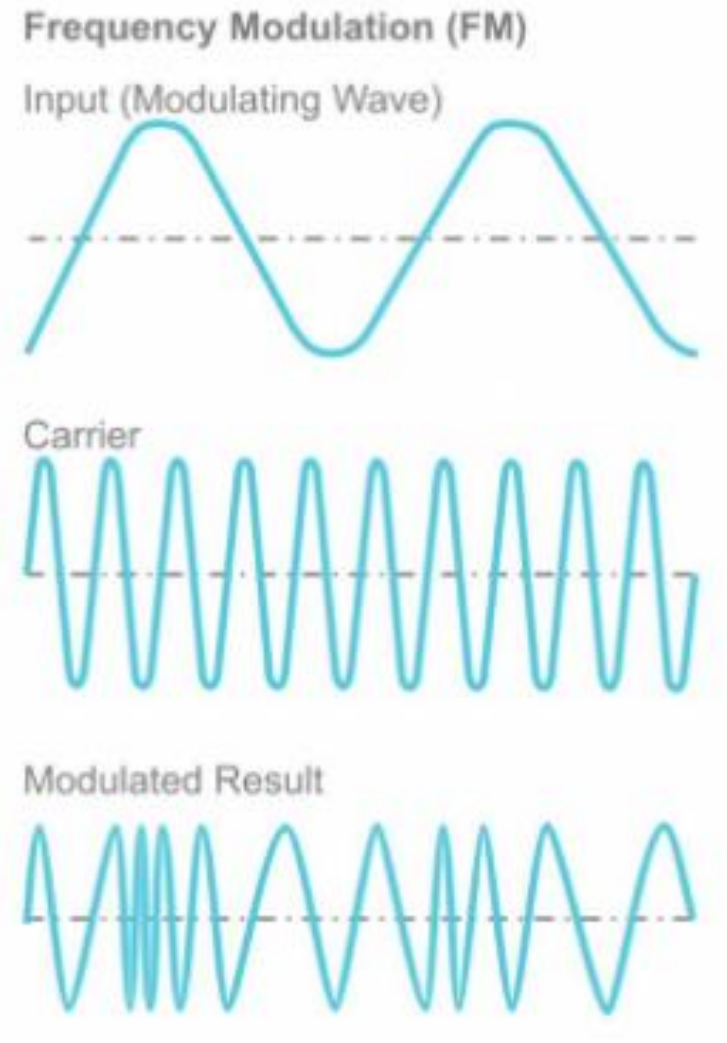




Frequency Modulation (FM)

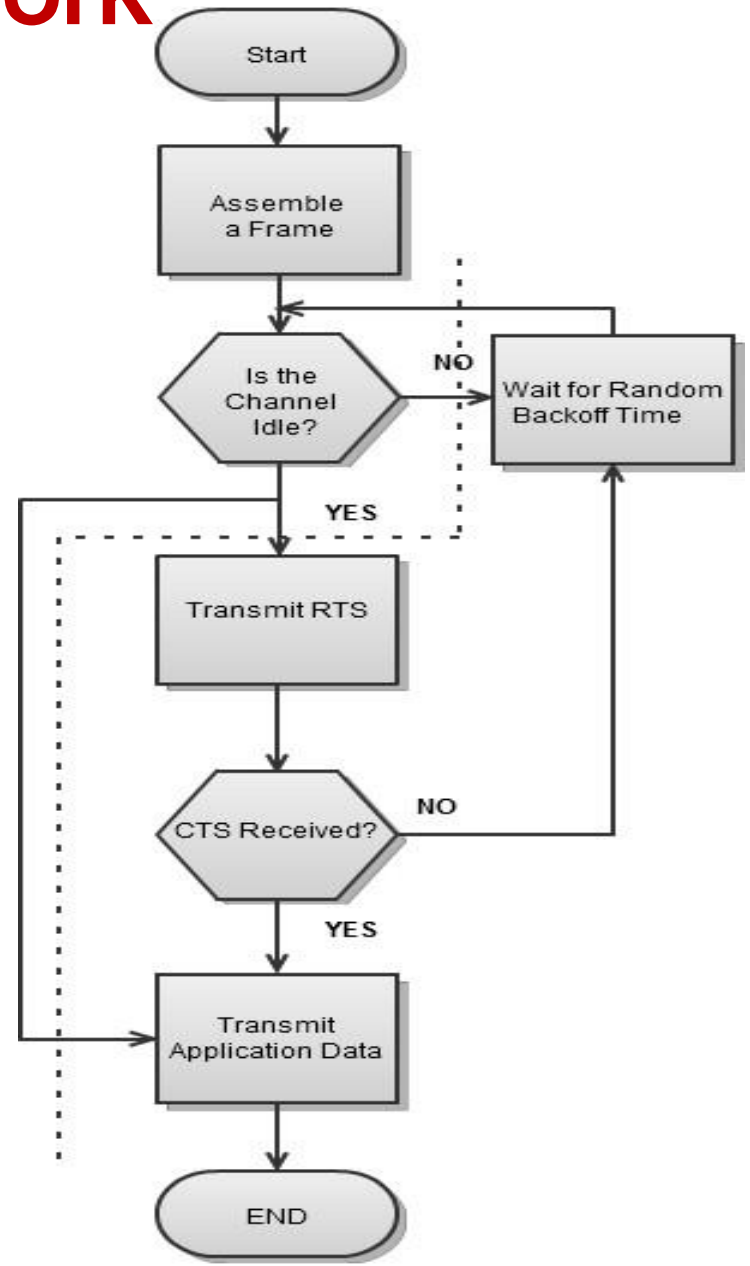
- **Frequency modulation** (FM) is the encoding of information in a carrier wave by varying the instantaneous **frequency** of the wave.





Collision in Wireless Network

- In a network, collision occurs when two or more devices tries to transmit data in a network at the same time. It is common in an Ethernet network.
- In an Ethernet network, if two computers sends data at the same time then collision occurs and transmission ends otherwise it transmits the data.
- To prevent this condition, we van implement **CSMA/CD** (Carrier Sense Multiple Access/Collision Detection) . In this, when a device wants to transmit data , it needs to first sense the carrier. It first check the signal of carrier line for any other transmission. If any transmission is already there it waits for its turn others starts transmitting the data.

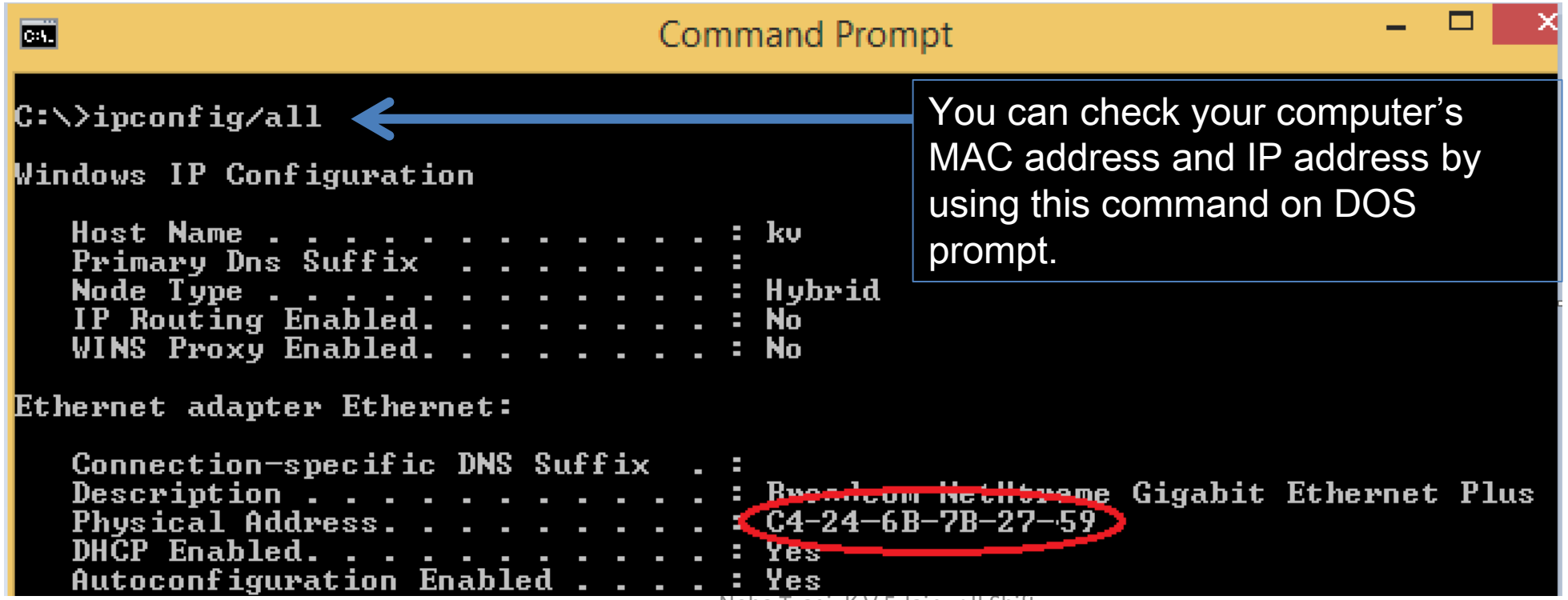


Error Checking and correction

- Error occurs when output does not match with input.
- During transmission, digital signals can be affected by noise and while traveling from one system to another, binary bit of data may get errors. i.e. change in 0 with 1 and vice versa can change whole data.
- Error detection is a technique which is used to observe change in noise or data during transmission.
- Error detection ensures the reliable delivery of data in a network.
- Error detection minimizes the probability of transmission of any incorrect frame .
- **Error Detecting Codes**: when a message transmits then due to noise or data the message got corrupted. To resolve this, some additional data is used to add in message which is known as error detecting codes . With the help of these codes, the errors that comes during transmission of message, are identified. Example is **Parity Check**.
- **Error-Correcting Codes:** when we pass come data to separate the original message from error-detecting codes, this data is called error-correcting code.

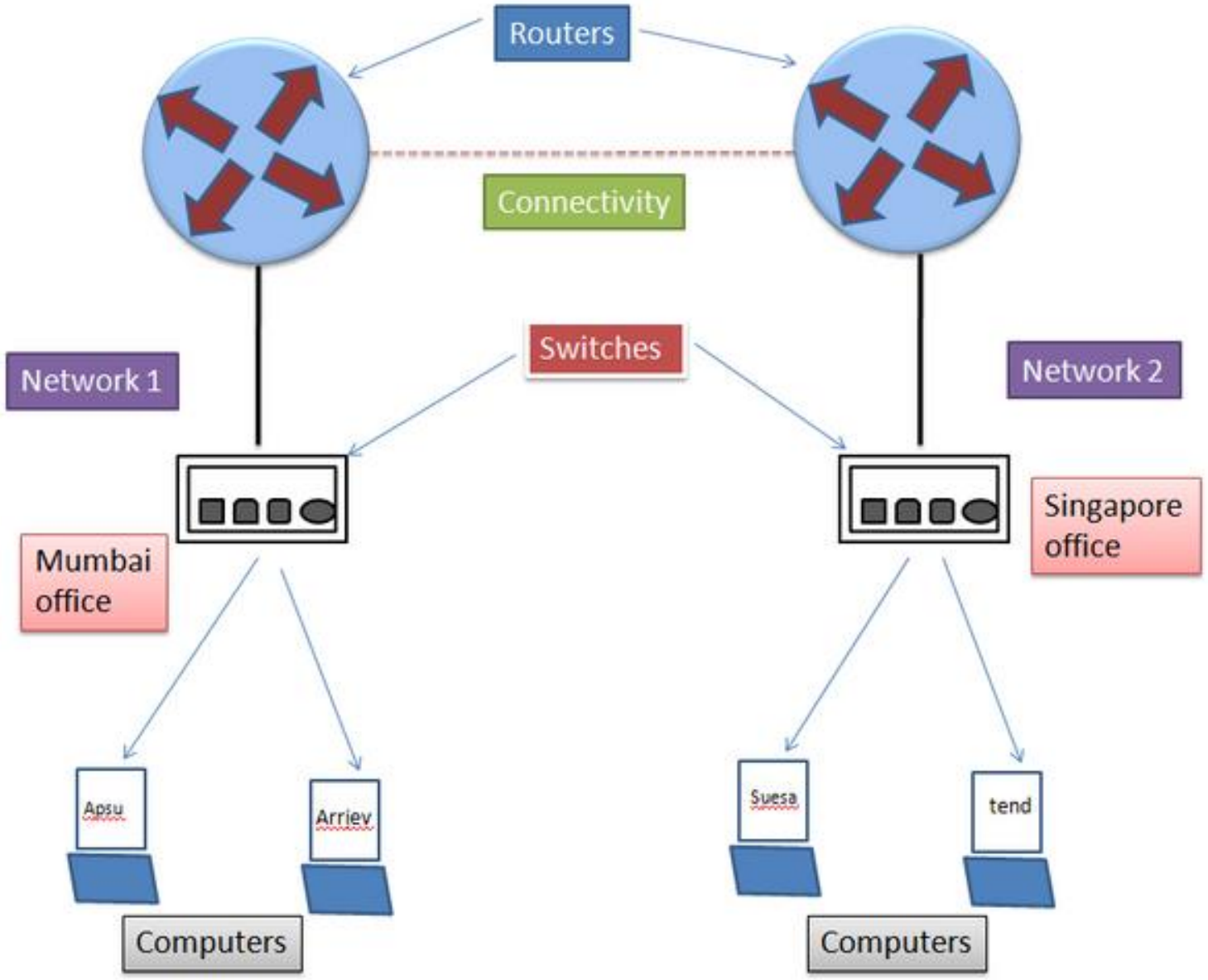
Media Access Control (MAC)

- A Media Access Control (MAC) address is a 48 bit address, used to establish communication between two hosts in an Ethernet network.
- It is a hardware address which gets fixed for individual network interface card (NIC) and can not be changed later.
- A MAC address should always be unique. It is also known as physical address.
- MAC address is a 6 digit hexadecimal number.



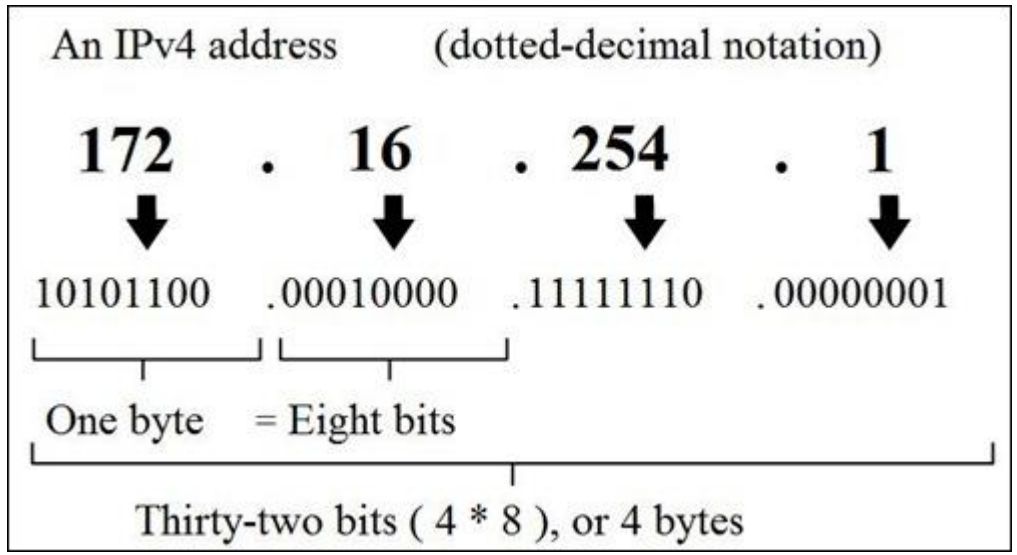
ROUTING

- Router is responsible for routing for traffic in a network.
- Routing is the process of moving data packets between different networks.
- Two different network can not communicate with each other. A medium is required to switch packets between them, router does this work.
- Router acts as an interface between two different networks. There is a routing table in a router.



IP Addresses (V4 and V6)

- In a computer network, each computer has a unique address(IP address) which is used to get information about a computer on network. An IP address is an address of network layer.
- It may differ on computer restarting. It can be same at a time only.
- An IP address is a 4 digit hexadecimal number assigned to a node in a network. IP address settings of a node can be changed by user.



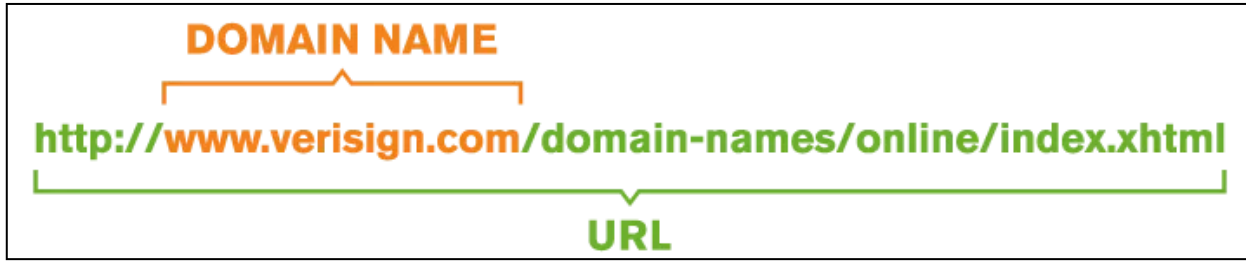
IPV4	IPV6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed

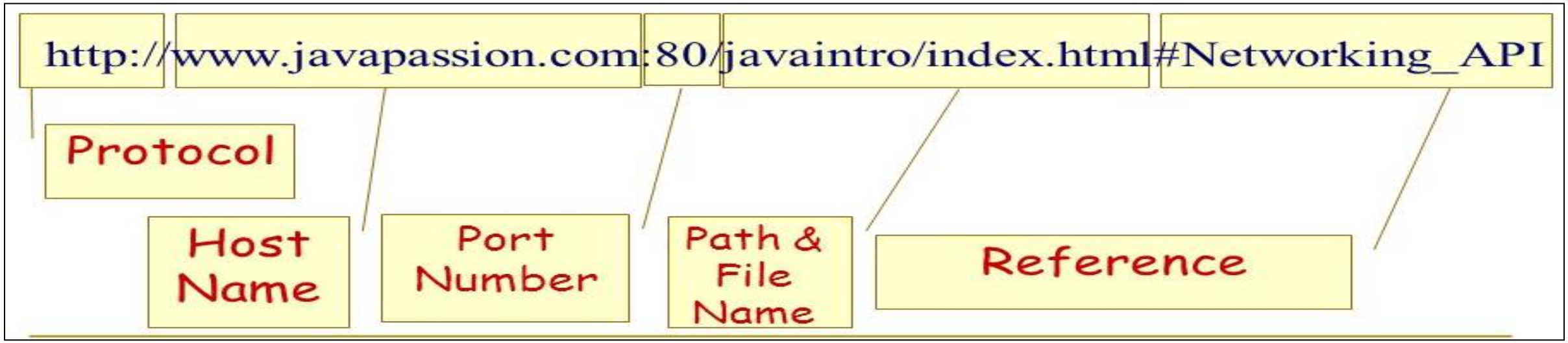
Domain Name System (DNS)

- Domain name system (DNS) is a hierarchical and decentralized naming system for computers, services or other resources connected to the internet. Domain Name system delegates the responsibility of assigning domain names and mapping those name to internet resources by designating authoritative name servers for each domain.
- Domain Name makes it easy to change names in IP addresses. Domain name is used to identify a web server in a URL i.e. a domain name is an address of a web server, for ex.- http://cbse.nic.in/index.html , index.html is a file here and this file is places at the server cbse.nic.in which is a domain name.
- A domain name has two parts-
  - Top-level domain name (.in is primary domain name in above example.)
  - Sub-domain name (.nic is sub domain name in above example and cbse is also sub domain name.)
- Example of domain names are- .com, .edu, .gov, .mil, .net, .org etc
- Domain name of some countries are- : .in, .au, .nz, .jp, .us etc

URL(Uniform Resource Locator) Structure

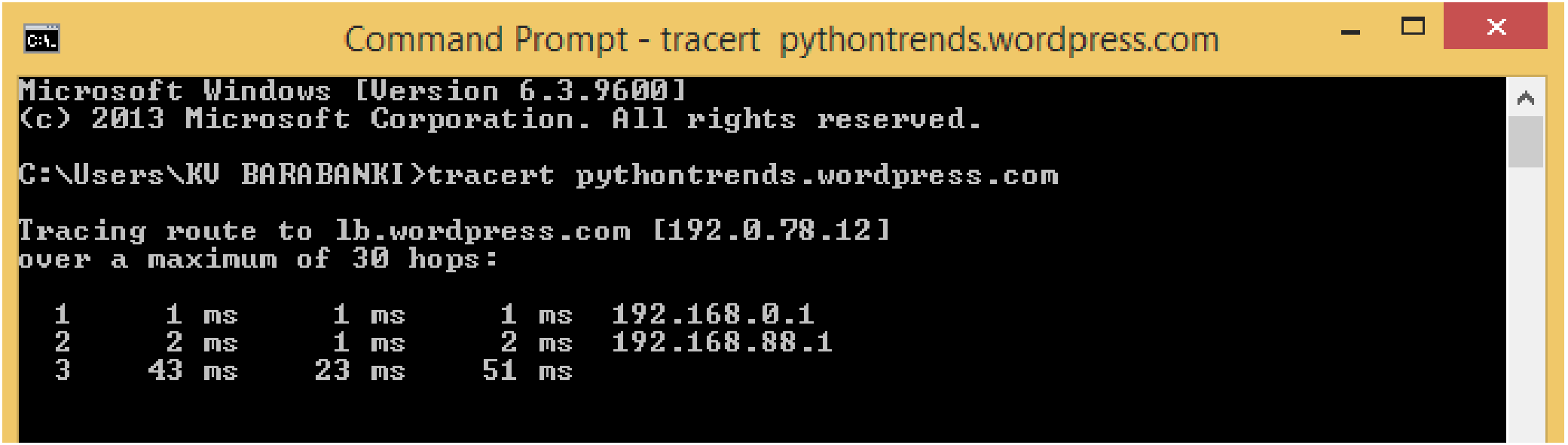
- URL is used to identify a website or webpage. HTTP locators are used to access distributed documents world wide.
- URL is used to specify any information on internet.
- URL structure has four factors-
  - Protocol → like http: , ftp:, https: etc.
  - Host computer → like cbse.nic.in
  - Port → it is optional. Like, a port has a number 8080 and it is placed between host and path.
  - Path → it is the name of that path or place where file is stored.



- 

Basic Networking tools

- Generally, network tools or commands are used for-
  - Netowrk configuration
  - Network Troubleshooting
  - To identify Network status
  - To identify a User
- We will discuss some tools and commands here-
- Traceroute – it is a network diagnostic tool. In different OS, different command name is there followed by domain name.



Basic Networking tools

- Ping – it is a network diagnostic tool carrying ip address or domain name . It tells that we are connected to server or not.

```
C:\Users\KV BARABANKI>ping facebook.com

Pinging facebook.com [157.240.198.35] with 32 bytes of data:
Reply from 157.240.198.35: bytes=32 time=33ms TTL=54
Reply from 157.240.198.35: bytes=32 time=20ms TTL=54
Reply from 157.240.198.35: bytes=32 time=40ms TTL=54
Reply from 157.240.198.35: bytes=32 time=37ms TTL=54

Ping statistics for 157.240.198.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 40ms, Average = 32ms
```

Basic Networking tools

- Ipconfig – It is a network troubleshooting tool. With the help of this we get basic information about network like MAC address, ip address, subnetmask etc.

```
C:\Users\KV BARABANKI>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ece6:c2a5:f5a:d316%3
   IPv4 Address. . . . . . . . . . . : 192.168.0.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5ad5:6eff:fed1:7228%3
                                       192.168.0.1

Tunnel adapter isatap.{D41AA3EE-38F8-42CF-989D-7696FFB0216E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

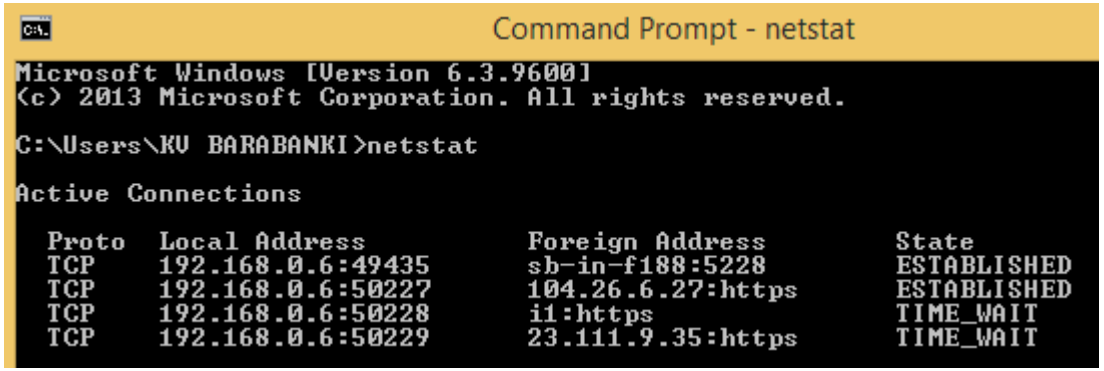
Basic Networking tools

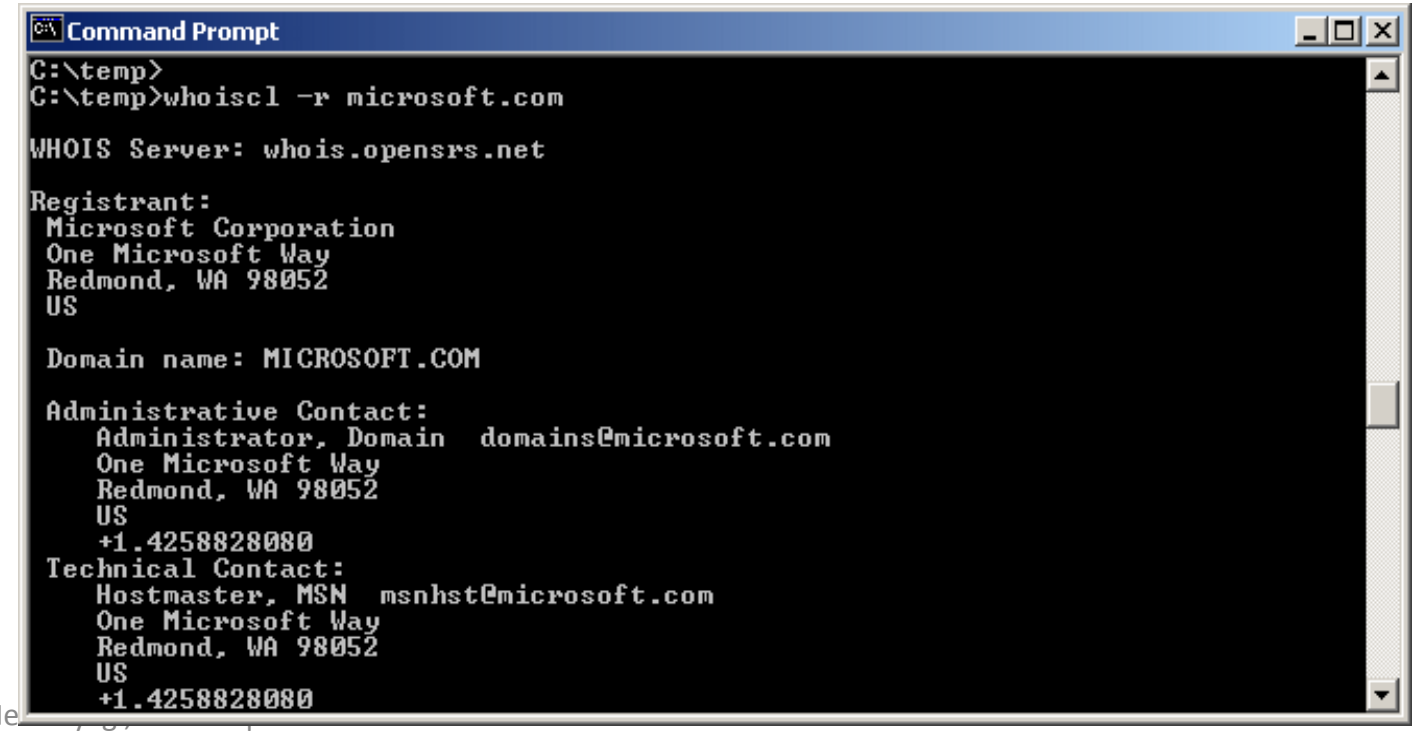
- nslookup – it means name server lookup and it is used to get information about internet server.

```
C:\Users\KV BARABANKI>nslookup pythontrends.wordpress.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    lb.wordpress.com
Addresses:  192.0.78.12
          192.0.78.13
Aliases:  pythontrends.wordpress.com
```

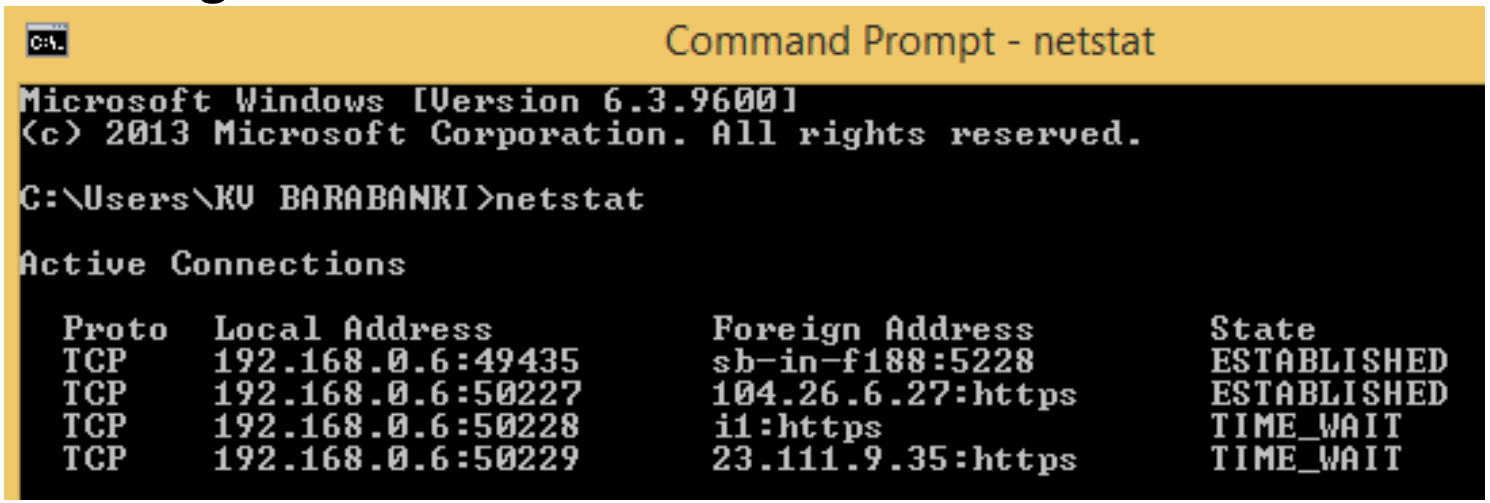
- whois – it is a query tool with which we can get information about registered user. It is an external command.



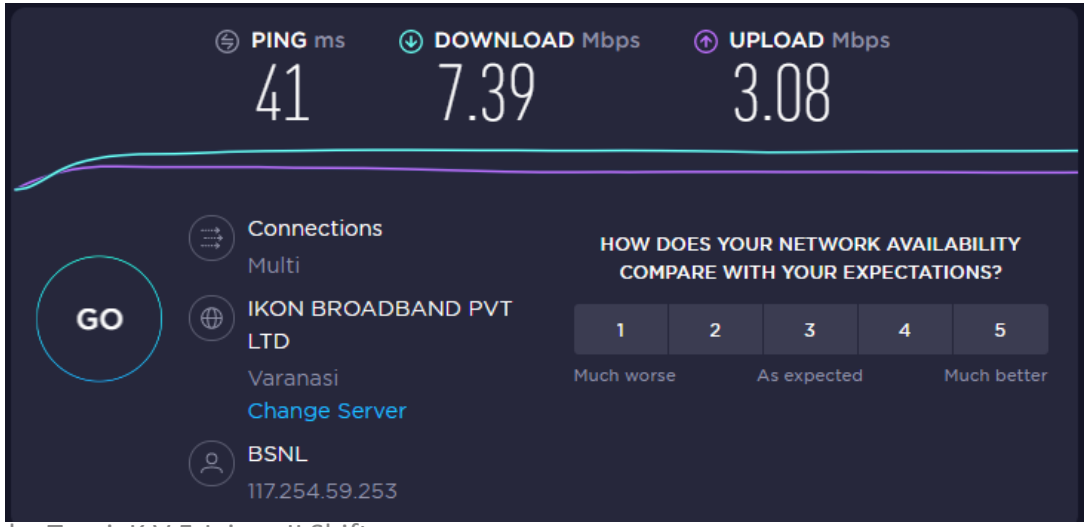


Basic Networking tools

- netstat – it is used to get information about network statistics.

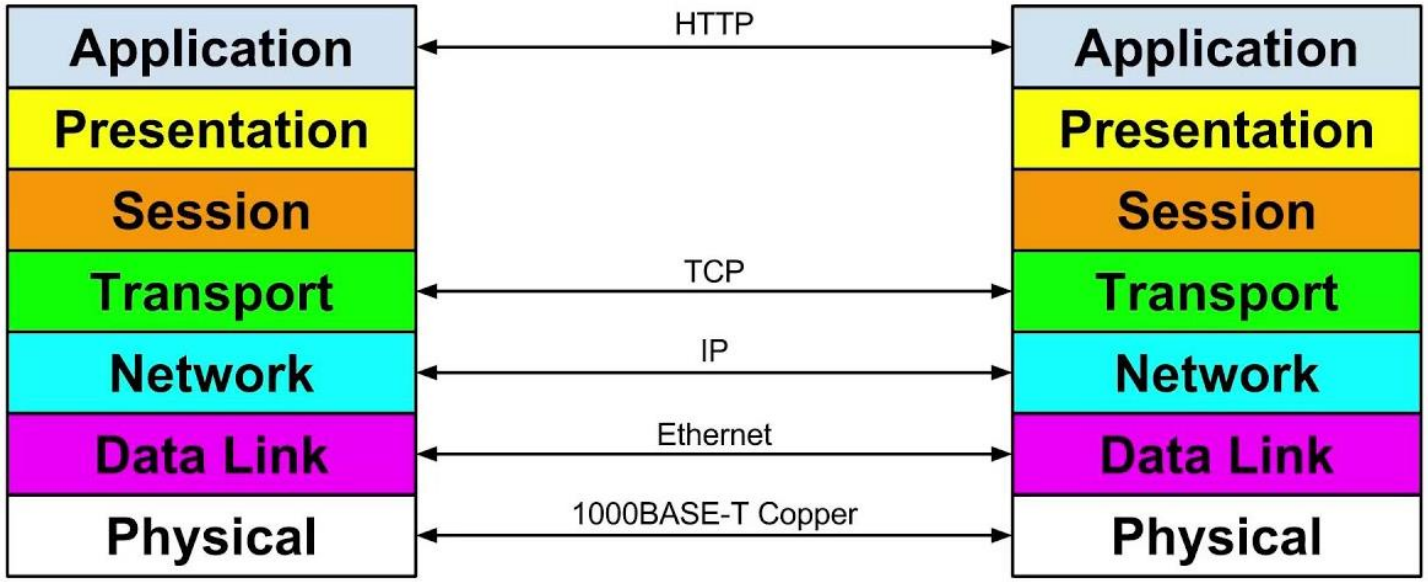


- Speedtest – We can use various web services to get information about network speed like ookla.



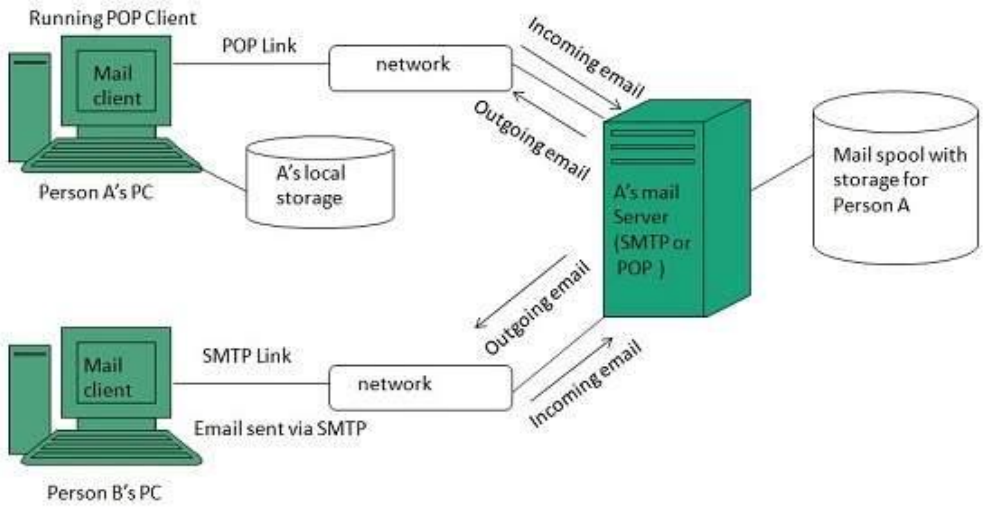
Protocols

- In a Network, there is a group of rules for transmission of data, developed by the organization AIEEE. These rules are termed as Protocols. i.e. Protocols are the set of rules to transmit the data over the network.
- As when we walk/drive on road, we need to follow traffic rules so that we can safely reach to our destination. Similarly, when the data flows in a network from sender to receiver, it needs to follow network rules. These rules are known as protocols.
- Some of the common protocol are-
  - TCP/IP
  - http:
  - https:
  - FTP
  - Telnet
  - POP
  - SMTP



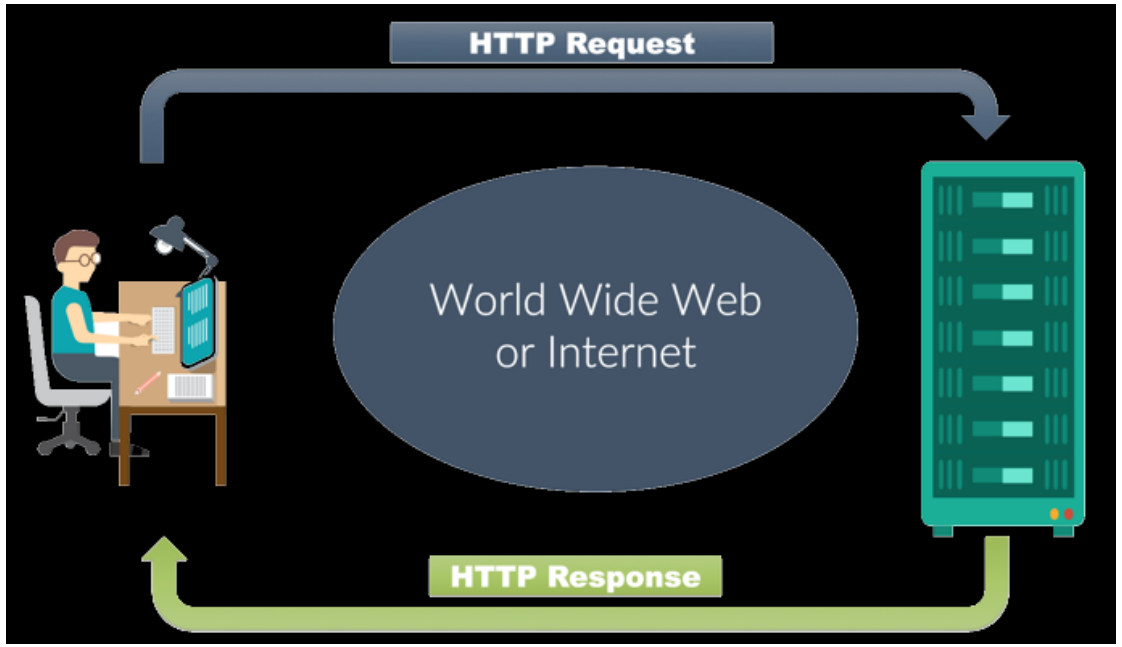
E-mail

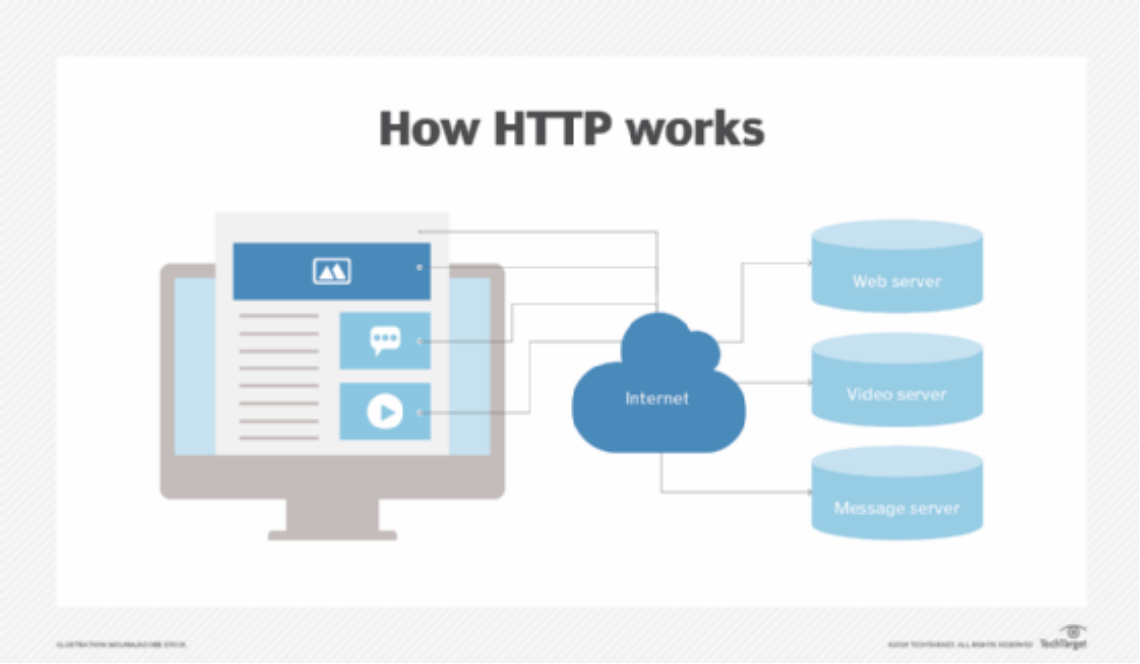
- Most common service of internet is e-mail used to send a message from sender to receiver.
- An email address is required for it like xyz@gmail.com where xyz is a unique ID of a user and gmail.com is its service provider for e-mail.
- A service provider has a mail server to keep all the mail safe. A user can access it's mail after login to his account. It is also based on client-server architecture. 2 protocols works together here- SMTP works during sending of email and POP works during receiving of email. Email sending has following phases- –
  - Composition → get ready the mail
  - Transfer → sending of mail from computer to server.
  - Reporting → informing the sender about status of mail i.e. it is delivered or not.
  - Displaying → reading of mail by user.
  - Disposition → act is decided by user after reading mail.



HTTP

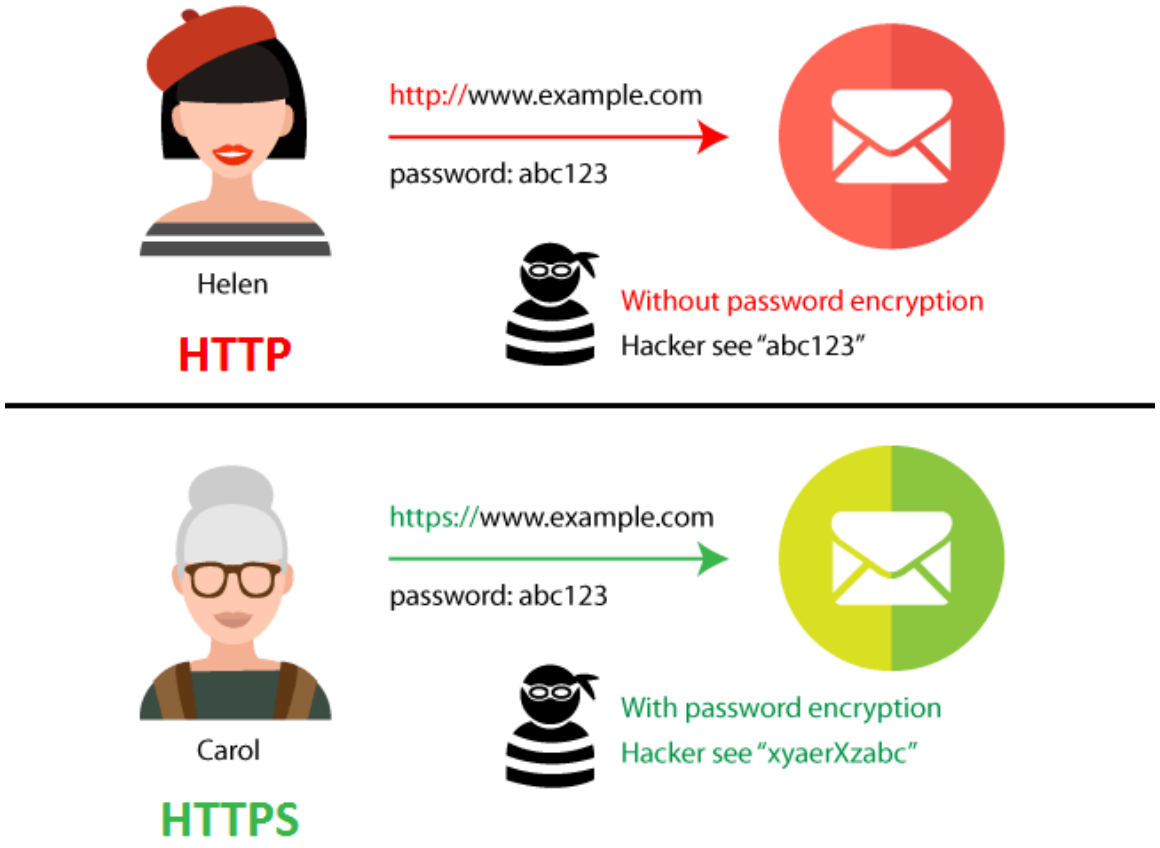
- Hyper Text Transfer Protocol is a protocol used to access data on internet or on world wide web.
- It is a mixture of FTP and SMTP protocol.
- It is based on client-server architecture.
- Here, client sends a request to server and server respond to this request. http send the code of a webpage for this.





HTTPS

- Hyper Text Transfer Protocol Secure is a safe protocol to send data on internet or on world wide web.
- It is a version of HTTP where ‘s’ stands for secure. Because of which the communication between web-browser and server remains encrypted.
- It is used at the places of high security like online banking or transaction etc.



Network Applications

- Remote Desktop→ accessing a computer from a far place (or different place known as remote computer).
- Remote Login →accessing a remote computer using user name and password.
- Telnet → also used for remote login where many users can connect to a server.
- FTP→ it is protocol to send a file from one computer to another in a network.
- SMTP→ it is a protocol used for e-mail . SMTP stands for Simple Mail Transfer Protocol.
- VoIP→ it means Voice over Internet Protocol , used to carry voice over internet.
- POP → it means Post Office Protocol used for distribution of mails from server.

Some Protocols

1. TCP/IP (Transmission Control Protocol/Internet Protocol) suite
2. ARP (Address Resolution Protocol)
3. DHCP (Dynamic Host Configuration Protocol)
4. DNS (Domain Name System)
5. FTP (File Transfer Protocol)
6. HTTP (Hyper Text Transfer Protocol)
7. HTTPS (Hypertext Transfer Protocol Secure)
8. ICMP (Internet Control Message Protocol)
9. IGMP (Internet Group Management Protocol)
10. IMAP4 (Internet Message Access Protocol version 4)
11. NTP (Network Time Protocol)
12. POP3 (Post Office Protocol version 3)

Thank you

Please follows us at-

www.pythontrends.wordpress.com