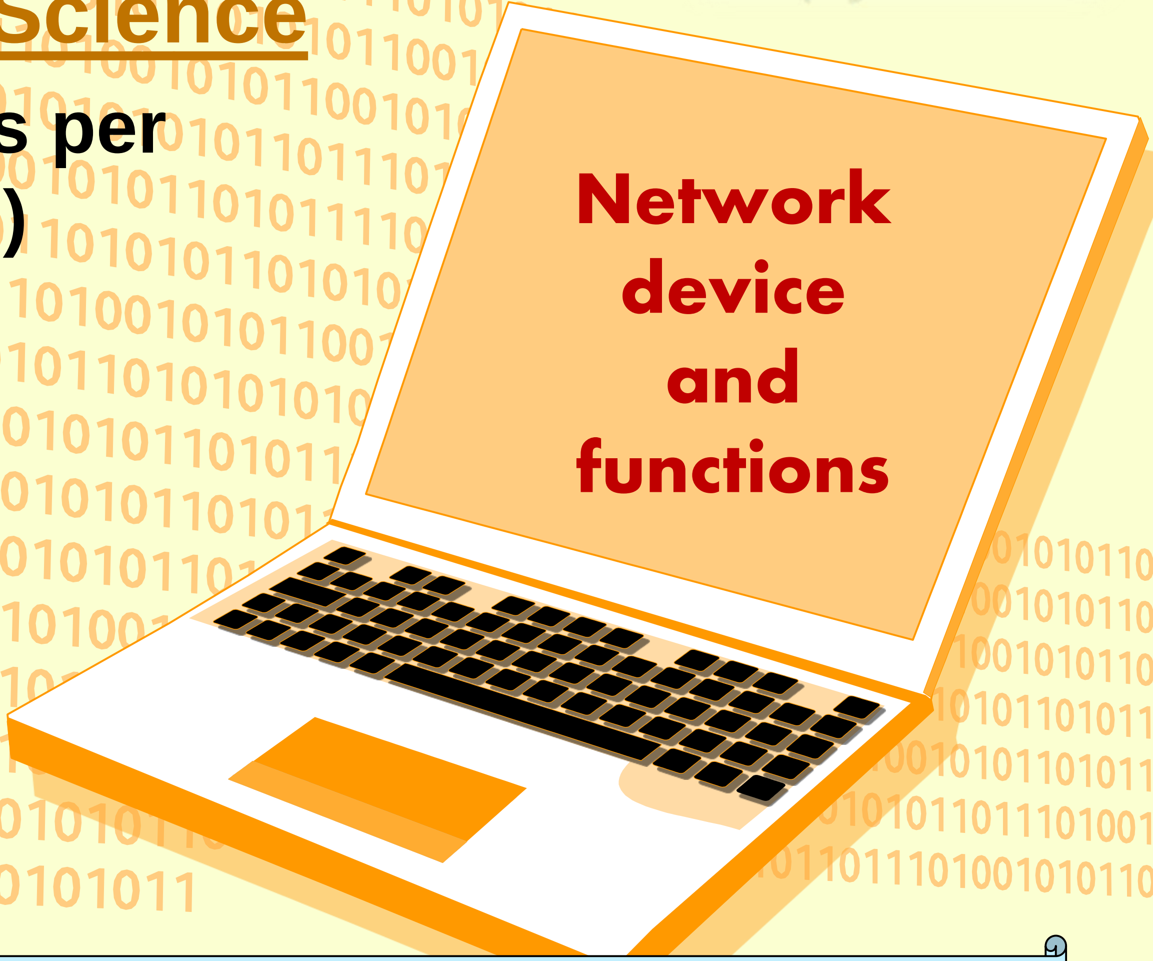
Chapter 10 :

Computer Science

Class XII (As per CBSE Board)



Network device and functions

New Syllabus 2019-20

Visit : python.mykvs.in for regular updates

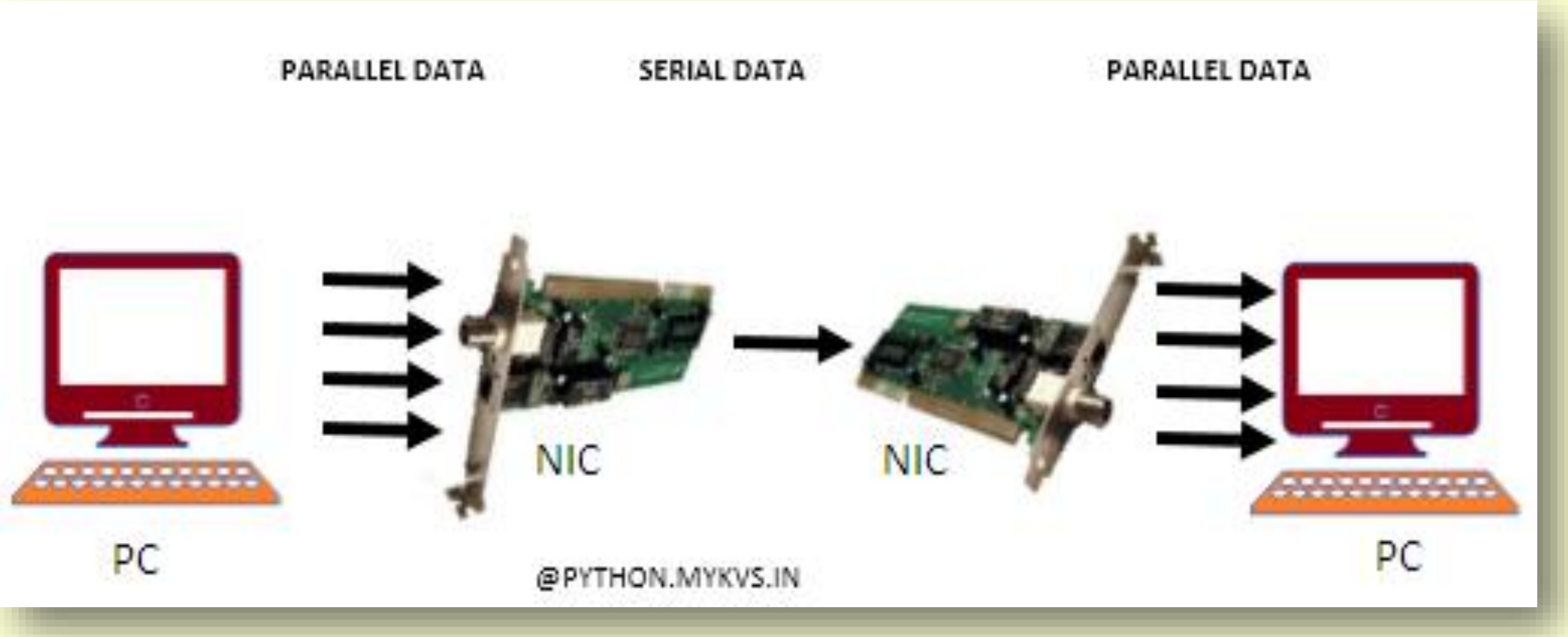
Network devices

Computer hardware devices which are used to connect computers, printers, or any other electronic device to a computer network are called network devices. These devices transfer data in a fast, secure and correct way with some specific functionality over same or different networks.

Some devices are installed on the device, like Internal modem, NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc.

Network devices

NIC – This is at top among other networking devices and mostly used networking device. This is also known as network adapter card, Ethernet Card and LAN card. It allows our PC to communicate with other PCs. A PC uses parallel data transmission to transmit data between its internal parts where as the media that connects this PC with other device/PCs uses serial data transmission. A NIC converts parallel data stream into serial data stream and vice versa.



Network devices

NIC –

Usually all modern PCs have inbuilt NICs in motherboard. NICs are also available separately in adapter format which can be plugged into the available slots of motherboard. For laptop or other small size devices they available in PCMCIA (Personal Computer Memory Card International Association) card format which can be inserted in PCMCIA slots.

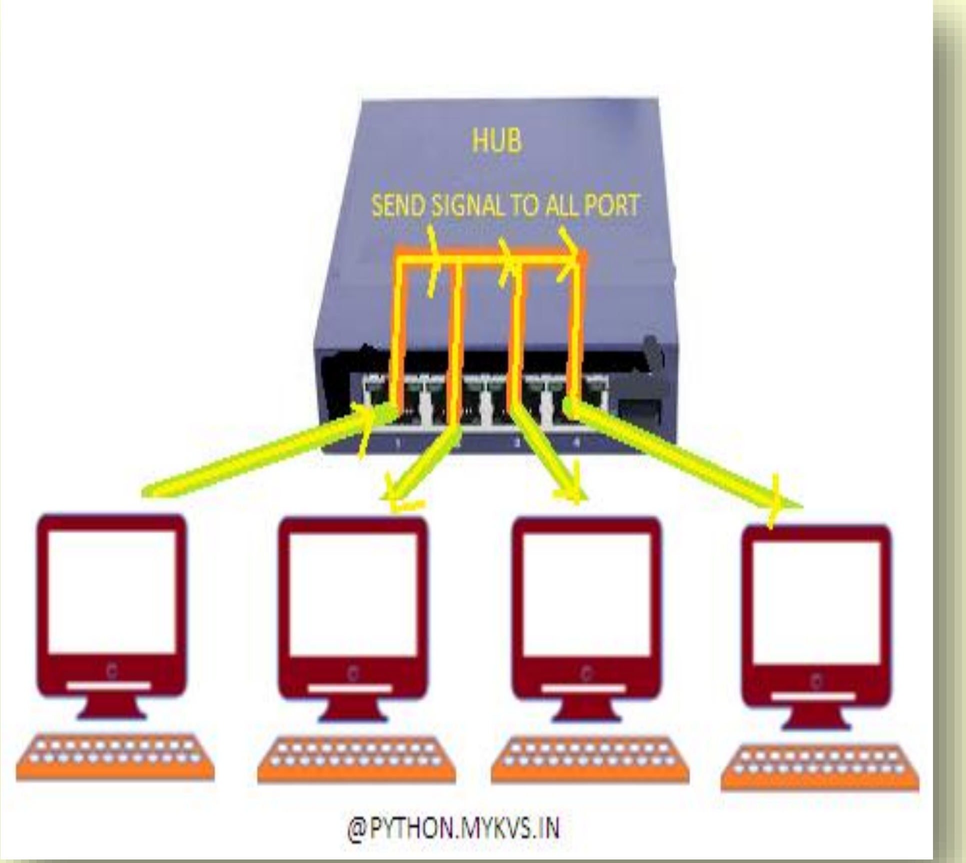
Types of NICs

- **Media Specific :- Different types of NICs are available for establishing connection with different types of media. For e.g. we cannot connect wireless media with wired NIC card or vice versa. similarly we can't connect coaxial cable with Ethernet LAN card. So we have to use specific NIC, which is best suited for particular media .**
- **Network Design Specific :- FDDI, Token Ring or Ethernet have their own distinctive type of NICs card. NIC can't be used interchangeably.**

Network devices

HUB – HUB is used to connect multiple computers in a single LAN network of one workgroup. Generally HUBs are available with 4,8,12,24,48 ports.

When a hub receives signal on its port, it repeats the signal and forwards that signal from all ports except the port on which the signal arrived. In below diagram leftmost node try to send signal to rightmost node ,but signals are distributed to all ports(nodes).



There are two types of HUB

Passive HUB:- It only forwards the signal on all ports without amplifying the signal.

Active HUB:- it forwards the signal with improvement in the quality of data signal by amplifying it. That why such hubs need additional power supply.

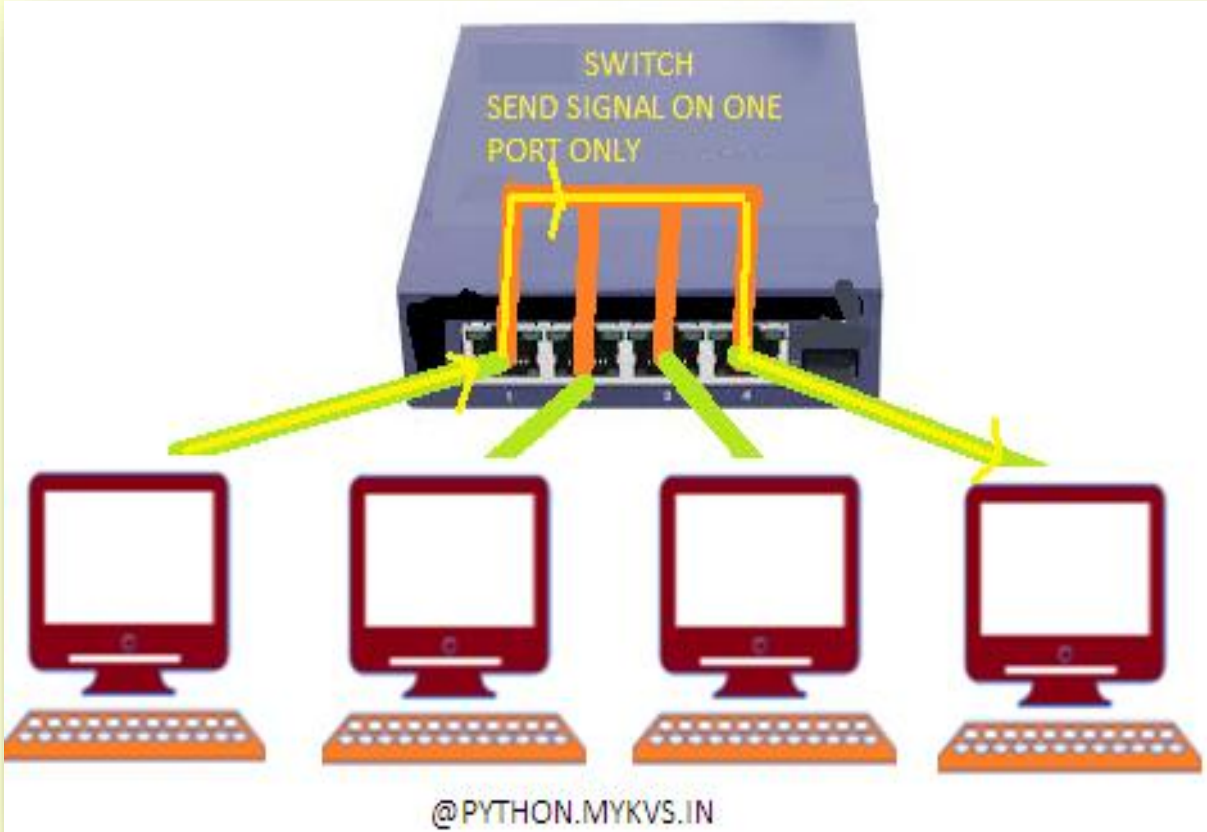
Based on port type, there are two types of HUB:-

Ethernet HUB :- All ports have RJ-45 connectors.

Combo HUB :- Several different types of connectors such RJ-45, BNC, and AUI available as ports in such HUB.

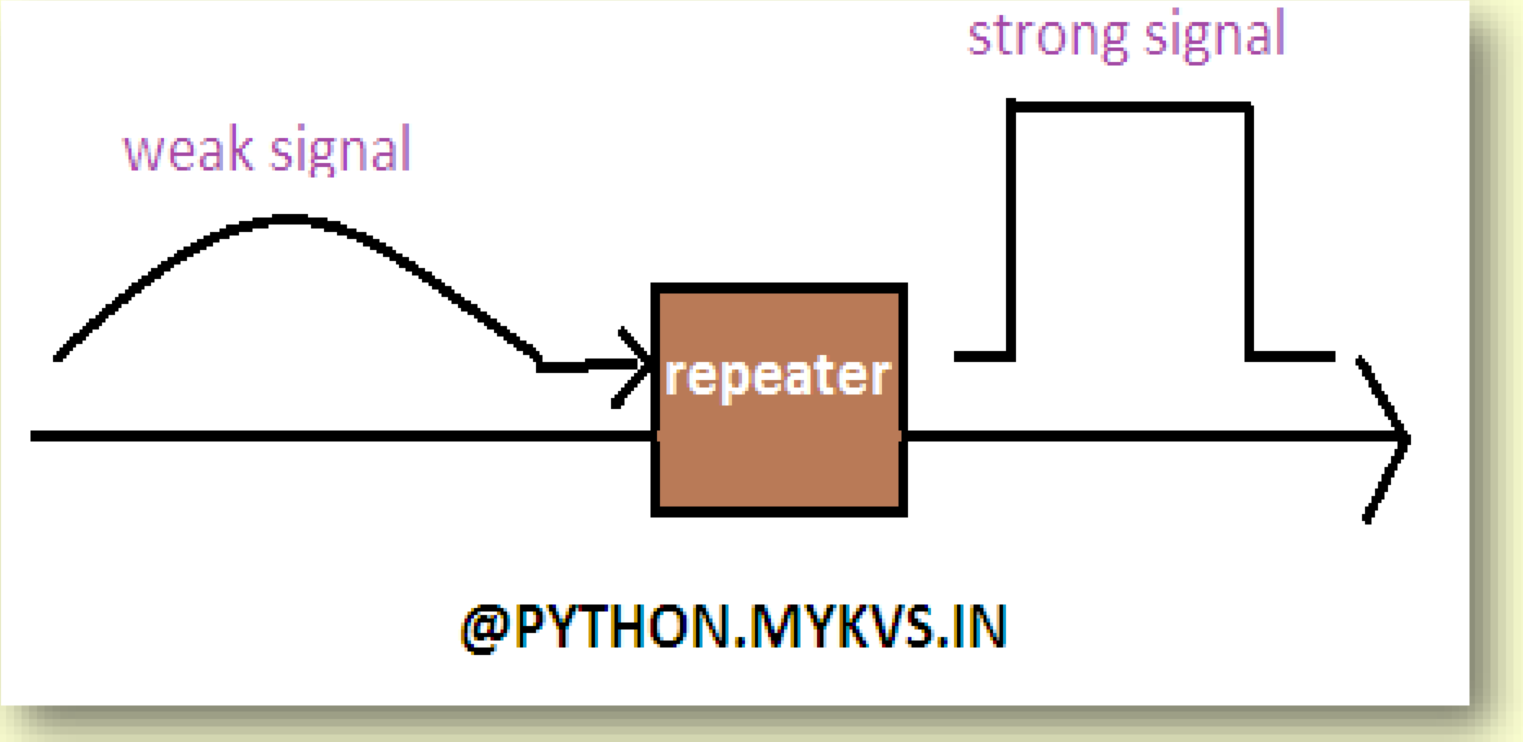
Network devices

SWITCH –Switch is also used to connect multiple computers together in a LAN workgroup,just like hub. Switches are available with 4,8,12,24,48,64 ports. Switch makes their switching decisions by using application specific integrated circuits (ASICs).Due to switching decision capability, switch sends signal to recipient only and that's why switches are called as intelligent hub. In below diagram leftmost node sending signal to rightmost node.



Network devices

Repeater – In a network signal travels a long distance in transmission media. Due to resistance of media signal becomes weak. Repeater is a networking device which regenerates the signal and forwards these signal with more power.



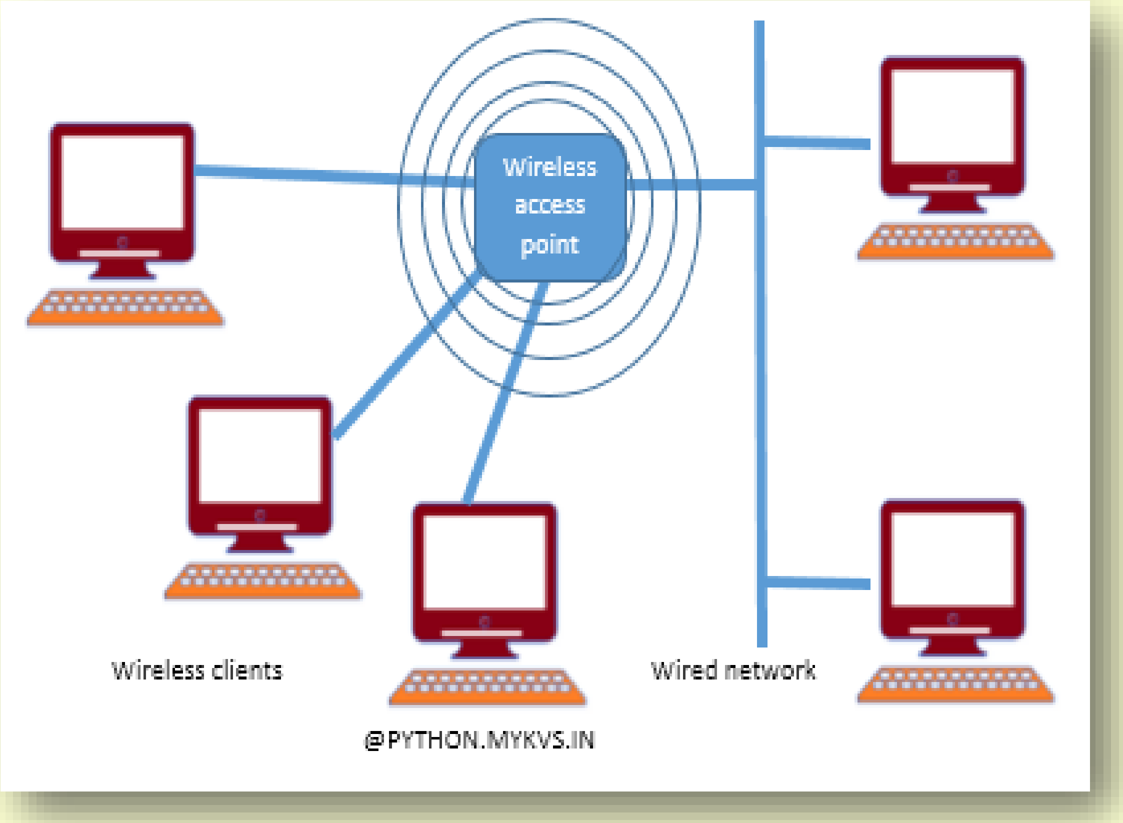
Network devices

Router – Routers operate in the physical, data link and network layers. Router is a networking device which chooses the best optimal path from available pats to send the signals. It interconnects different networks. The simplest function of a router is to received packets from one connected network and pass them to second connected network.

Gateway – A networking device capable to convert protocols so that two different network architecture based system can communicate with each other.It works as protocol convertor.

Network devices

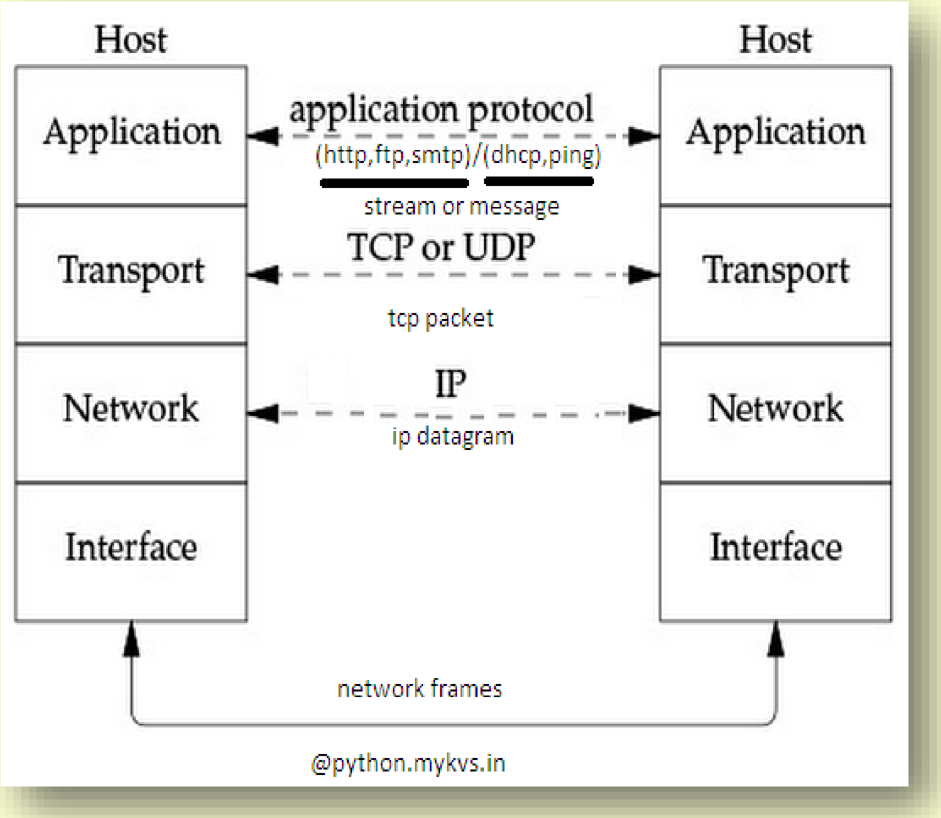
Access Point – Also known as wireless access point. An access point is a station which transmits and receives data (transceiver). It connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network.



Network devices

Network stack – It's a sub-system in a computer that deals with networking. In most computers it is TCP/IP stack but there are number of other protocols also. Computer programs only need to know about an IP address or hostname, a tcp or udp port number and the network stack takes care of forming this in standardized packets on the network to send the data towards remote system. The reverse action is done at the receiving end. This can be understood by given diagram.

Data delivered on host computer by any of application protocol e.g. http,ftp to transport layer where tcp Works,which makes packets of these data and deliver to network Layer ip protocol,which create Ip datagram,at interface these are Known as network frames.These packets move over the media and reverse action is performed at next computer.

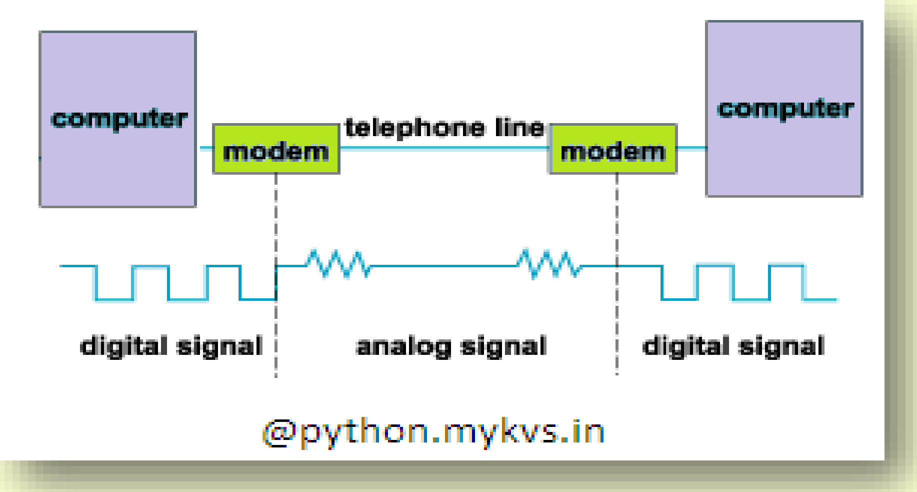


<----Network stack---->

Network devices

Modem – Modem is short for Modulator Demodulator. It’s an electronic device used to access the Internet that modulates carrier waves to encode information to be transmitted and also demodulates incoming carrier waves to decode the information they carry.

Modulation means digital to analog signal conversion and its vice versa is known as demodulation.



@python.mykvs.in

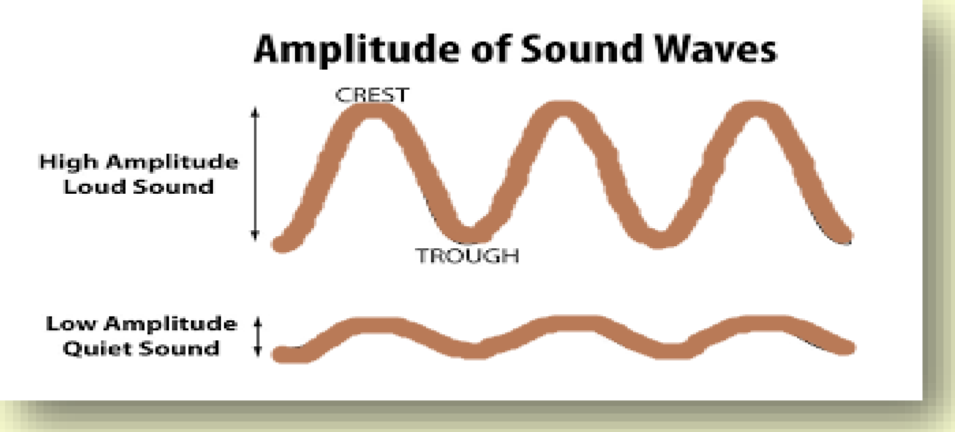
Computer Networking

Two common modulation techniques are

1. Amplitude modulation
2. Frequency modulation

1-Amplitude modulation

Amplitude-the maximum displacement or distance moved by a point on a vibrating body or wave measured from its equilibrium position. It is equal to one-half the length of the vibration path.



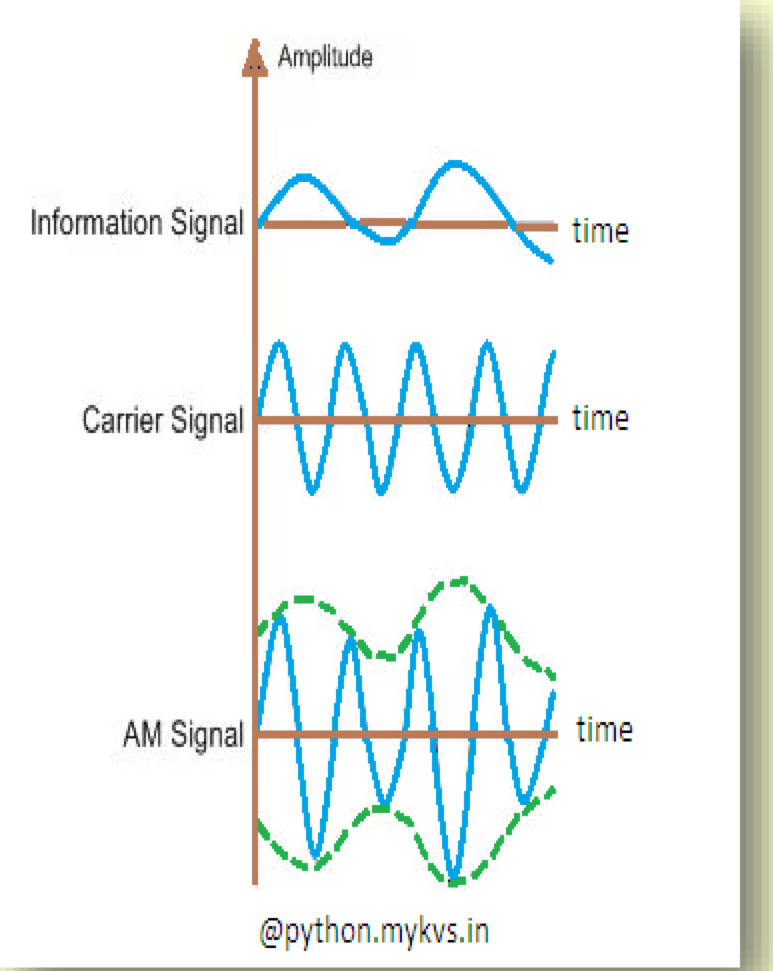
Computer Networking

1 - Amplitude modulation

Amplitude Modulation, in short AM, is a common method of broadcasting radio signals. Discovered in 1870s, that information in the form of audio can be broadcast over long distances through radio waves.

In AM, the amplitude of the carrier wave is modified in order to transmit the input signal.

The amplitude of the carrier wave varies proportionally according to the input signal, so when the input signal has a low amplitude, the amplitude of the carrier wave is decreased and vice-versa.

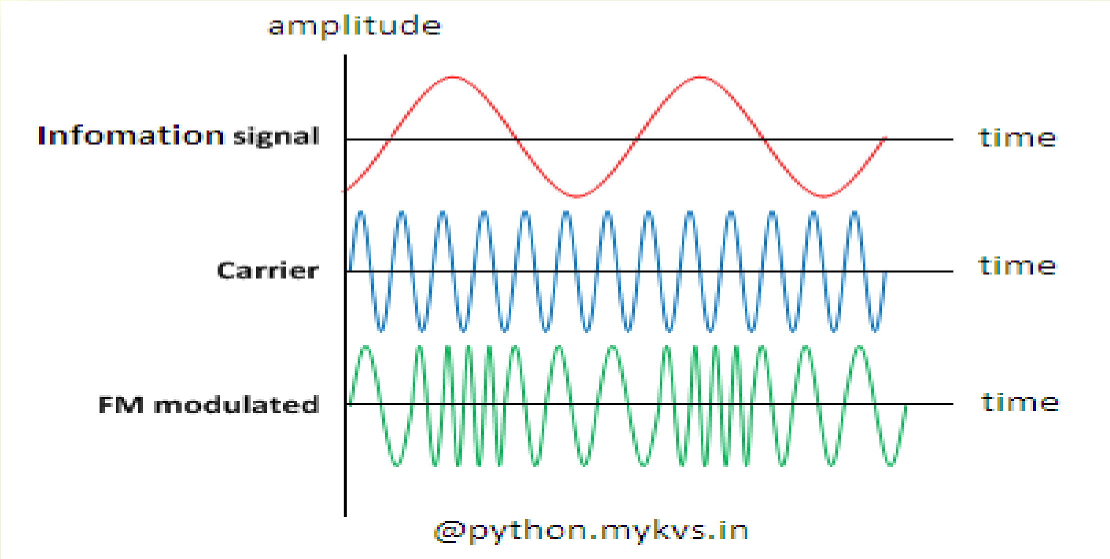


Computer Networking

2 - Frequency modulation

Frequency Modulation, in short FM.In FM, the instantaneous frequency of the carrier wave is altered according to the amplitude of the input signal.

Due to the much better transmission quality, most music radio stations prefer FM over AM to transmit information (mostly, songs) to their listeners.



Collision in wireless networks - Collisions occur on a network when two or more networked devices transmit data at the same time. The result is that the data collides, becomes corrupted, and needs to be re-sent.

Using CSMA/CD(Carrier Sense multiple access/Collision detection), if a collision is detected on the medium, end-devices would have to wait a random amount of time before they can start the retransmission process. For this reason, CSMA/CD works well for wired networks, however, in wireless networks, there is no way for the sender to detect collisions the same way CSMA/CD does.

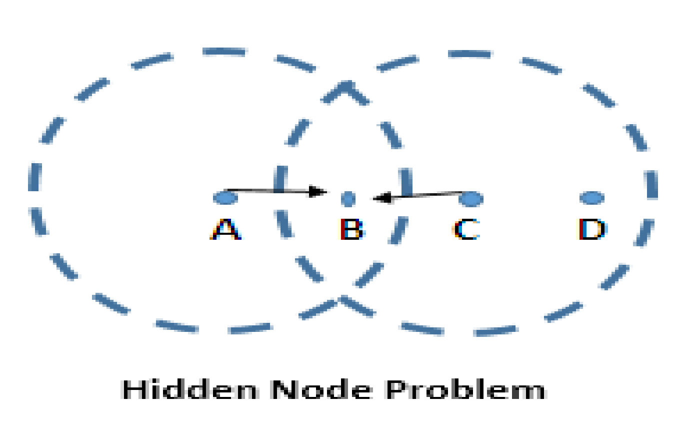
Therefore, CSMA/CA is used on wireless networks. CSMA/CA doesn’t detect collisions (unlike CSMA/CA) but rather avoids them through the use of a control message. Should the control message collide with another control message from another node, it means that the medium is not available for transmission and the back-off algorithm needs to be applied before attempting retransmission.

Computer Networking

Collision in wireless networks –

- **Hidden node problem**

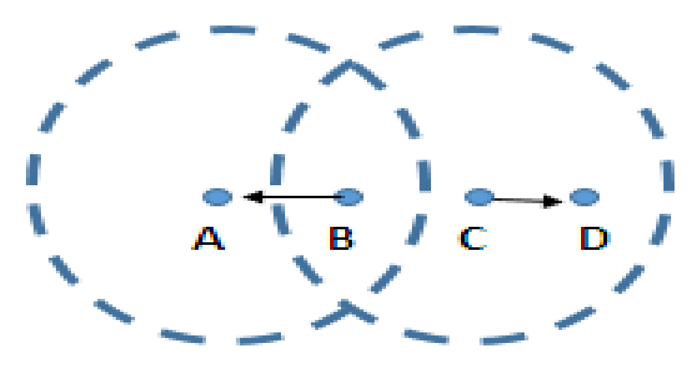
Node A and C send the signal to B at the same time and collision occurs at Node B this can't be detected so CSMA/CA scheme can be used here to avoid collision here.



Hidden Node Problem

- **Exposed Node problem**

Here if c want to transmit signal to b but knows that collision can occur so if needed can transmit the signal to d. such solution is possible with Multiple Access with Collision Avoidance (MACA) scheme.



Exposed Node problem

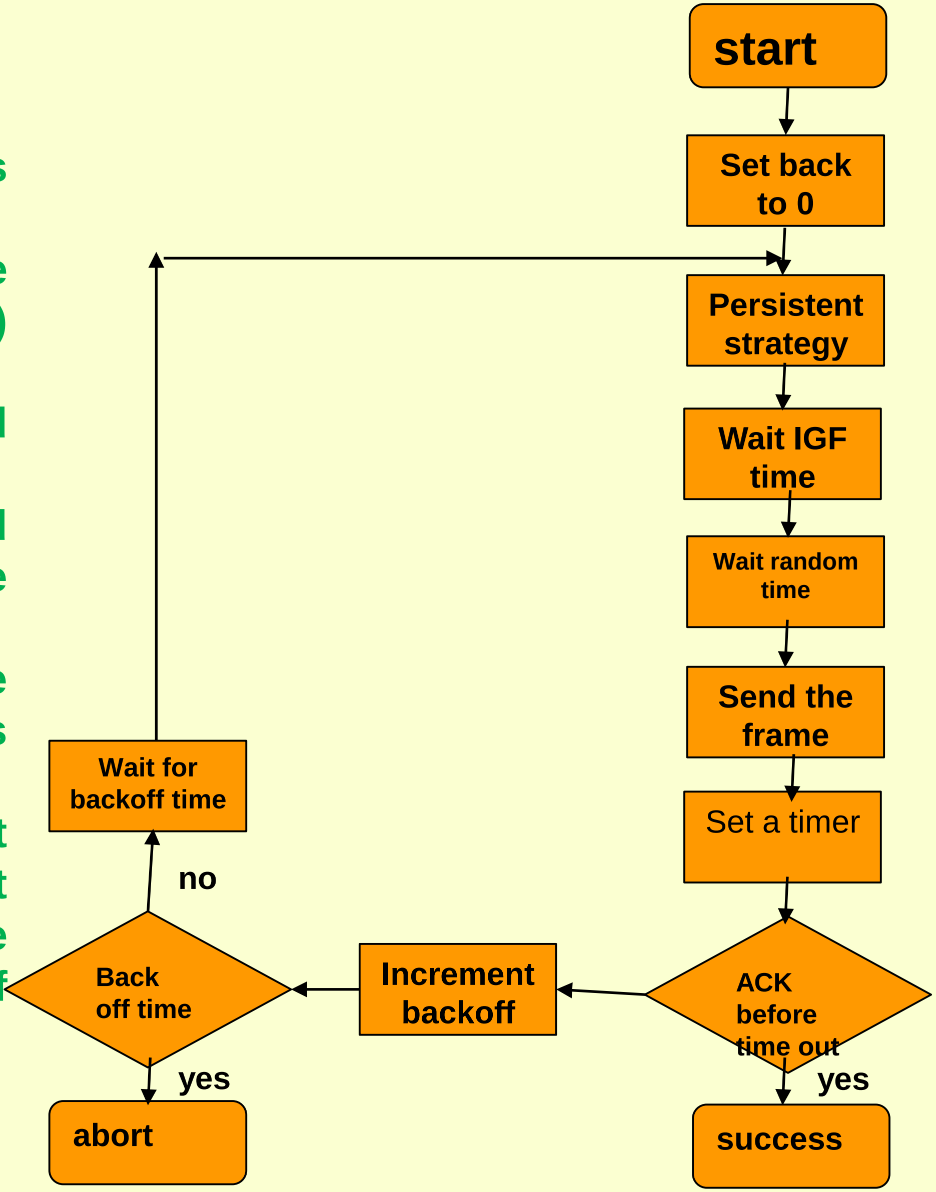
Sender transmits Request to Send (RTS) frame to receiver . The receiver then replies with clear to send (CTS) frame back to the sender as it is busy.if such CTS frame is not received then sender comes to know that receiver is free to send data.

Computer Networking

How CSMA/CA Works

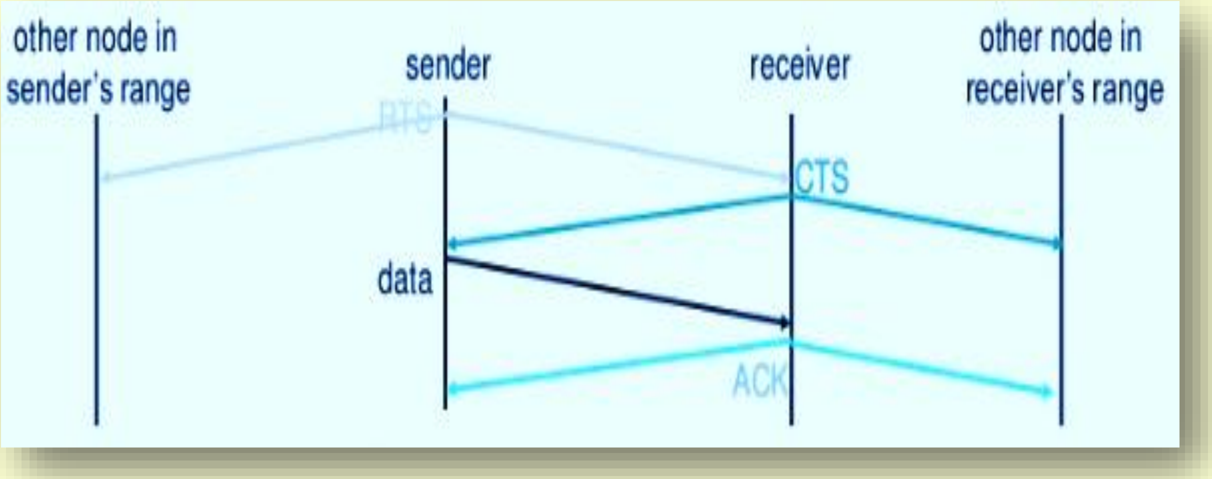
The station ready to transmit signal, senses the line by persistent strategies.

- As soon as it find the line to be idle, the station waits for an IFG (Interframe gap) amount of time.
- If then waits for some random time and sends the frame.
- After sending the frame, it sets a timer and waits for the acknowledgement from the receiver.
- If the acknowledgement is received before expiry of the timer, then the transmission is successful.
- But if the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameter, waits for the back off time and resenses the line.



Computer Networking

How MACA Works



- Sender sends a request to send (RTS) frame containing the length of transmission
- Receiver respond with clear to send (CTS) frame
- Sender sends data
- Receiver sends ACK,now another sender can send data
- When sender do not get a CTS back ,it is assumed that collision occurs

Computer Networking

Error checking –

Networks must be able to transfer data from one device to another with complete accuracy. Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

Parity Bit

A single bit is appended to each data chunk that makes the number of 1 bits even/odd.

Example: even parity
1000000(1)
1111101(0)
1001001(1)
Example: odd parity
1000000(0)
1111101(1)
1001001(0)

Computer Networking

Error checking –

Single dimension parity check

Suppose the sender wants to send the word ***word***. In ASCII the four characters are coded as

1110111 1101111 1110010 1100100

The following shows the actual bits sent in case **Even parity** is used:

1110111**0** 1101111**0** 1110010**0** 1100100**1**

Now suppose the word *word* in Example 1 is received by the receiver without being corrupted in transmission.

11101110 11011110 11100100 11001001

The receiver counts the 1s in each character and comes up with even numbers (6, 6, 4, 4). The data are **accepted**.

Computer Networking

Error checking –

Now suppose the word *word* in Example 1 is corrupted during transmission.

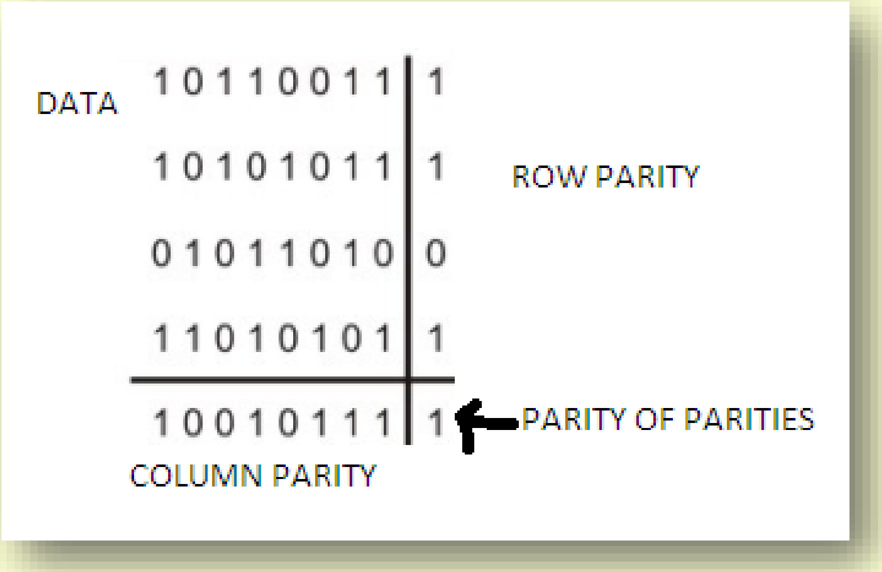
11111110 11011110 11101100 11001001

The receiver counts the 1s in each character and comes up with even and odd numbers (7, 6, 5, 4). The receiver knows that the data are **corrupted**, discards them, and asks for retransmission.

Computer Networking

Error checking –

Two dimensional parity checking - Performance can be improved by using two-dimensional parity check, which organizes the block of bits in the form of a table. Parity check bits are calculated for each row,which is equivalent to a simple parity check bit. Parity check bits are also calculated forall columns then both are sent along with the data.



```
DATA   1 0 1 1 0 0 1 1 | 1
       1 0 1 0 1 0 1 1 | 1
       0 1 0 1 1 0 1 0 | 0
       1 1 0 1 0 1 0 1 | 1
       ----------------+--
       1 0 0 1 0 1 1 1 | 1
```

Computer Networking

MAC Address–A MAC address is the unique identifier that is assigned by the manufacturer to a piece of network hardware (like a wireless card or an Ethernet card).

A MAC address is made up of six two-digit hexadecimal number , each separated by a colon.

$\underbrace{\text{00:1B:f4}}_{\text{Manufacturer id}}\text{:}\underbrace{\text{11:fA:B7}}_{\text{Card no}}$ is an example of a MAC address.

How do I find my device’s MAC address?

- Click Windows Start or press the Windows key.
- In the search box, type cmd.
- Press Enter
- A command window displays.
- Type ipconfig /all and Press Enter.
- A Physical Address displays for each adapter. The Physical Address is your device’s MAC address.

Steps for finding MAC address depends on the OS being used.

Computer Networking

IP Address – An IP address is a number which is used to identify any device on a network. This is an important concept as devices communicate with each other across the LAN and WAN based on IP addresses.

IP address is a logical address which is in the format of a.b.c.d i.e. using four octets.

An example of IP address is: 192.168.10.1

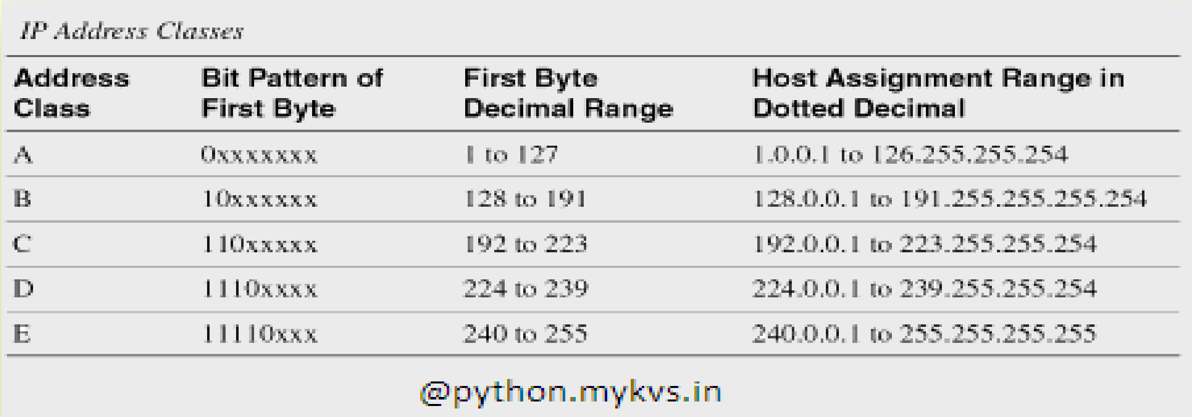
There are two types of version for IP addresses:

1. **IPv4 which is 32 bits**
2. **IPv6 which is 128 bits**

Computer Networking

IPv4 –IPv4 (Internet Protocol Version 4) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses. 32 binary bits are broken into four octets (1 octet = 8 bits)Dotted decimal format (for example, 172.16.81.100)

The public address space is divided into five classes:



IP Address Classes

Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

@python.mykvs.in

Class D addresses are used for multicast traffic. These addresses are not assignable. Class E addresses are reserved for experimental usage and are not assignable.

Computer Networking

IPv6 –A new Internet addressing system Internet Protocol version 6 (IPv6) is being deployed to fulfill the need for more Internet addresses.IPv6 is also called IPng (Internet Protocol next generation)IPv6 is the successor to Internet Protocol Version 4 (IPv4). IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts & total amount of data traffic transmitted.It is under development from 1990.

An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets,known as hextet). The groups are separated by colons (:). An example of an IPv6 address is: 2001:0db8:85f3:0000:0000:8f2e:0370:7334

The Benefits of IPv6

- **No more NAT (Network Address Translation)**
- **Simplified, more efficient routing**
- **Better multicast routing**
- **Auto-configuration**
- **No more private address collisions**
- **Simpler header format**
- **True quality of service (QoS), also called "flow labeling"**
- **Built-in authentication and privacy support**
- **Flexible options and extensions**
- **Easier administration (say good-bye to DHCP)**

Computer Networking

Routing –Routing is a process which is used to deliver the packet by choosing an optimal path from one network to another. Static routing is a process in which we have to manually add routes in routing table.

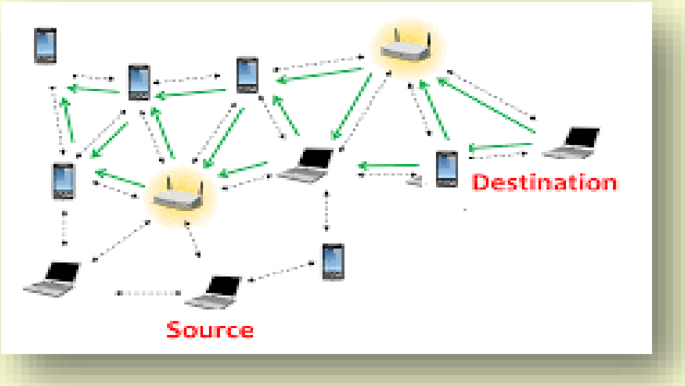
A **routing table** is a set of rules/viewed in table format is used to determine where data packets traveling on (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.

Routing table contains routing entries, that is list of destinations (often called: list of network prefixes or routes)

Where to route to 192.168.1.30?

From the routing table below

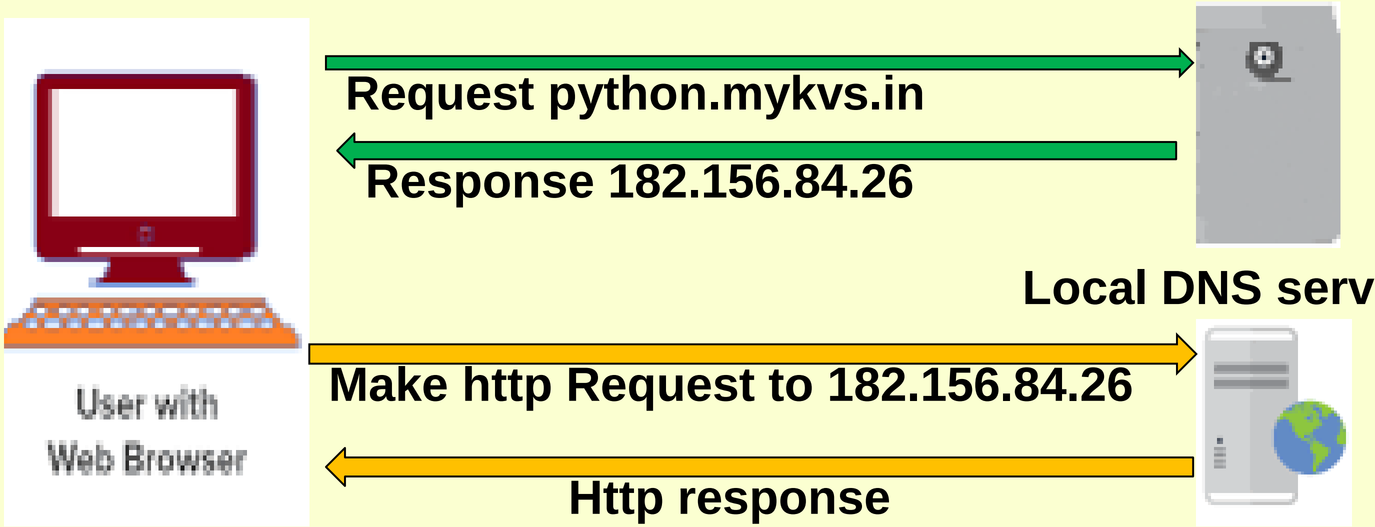
192.168.1.10/32	via 10.254.2.1	
192.168.1.30/24	via 10.254.3.1	✓
192.168.1.20/32	via 10.254.2.1	



Having the destination IP of packet, routers always choose best matching ROUTING ENTRY. That means LONGEST PREFIX MATCH. This means that in our case entry: 192.168.1.30/24 is more accurate that 192.168.1.10/32 in the search for 192.168.1.30.

Computer Networking

DNS –The Domain Name System, translates human readable domain names (for example, www.python.mykvs.in) to machine readable IP addresses (for example, 182.156.84.26). ... DNS servers translate requests for names into IP addresses.



Request python.mykvs.in

Response 182.156.84.26

Local DNS server

Make http Request to 182.156.84.26

Http response

A domain name is our website name. e.g. in python.mykvs.in , in is primary domain,mykvs is subdomain of in and python is subdomain of mykvs.

Generic domain name - .com,.edu,.gov,.mil,.net,.org etc

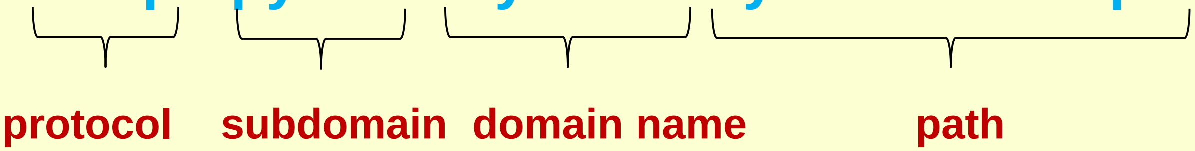
Country specific domain name - .in for india,.us for united states

Computer Networking

URL –Uniform Resource Locator is defined as the global address of documents and other resources on the World Wide Web. The URL is an address that sends users to a specific resource online, such as a webpage, video or other document or resource.

e.g.

http://python.mykvs.in/syllabus/cs12.pdf

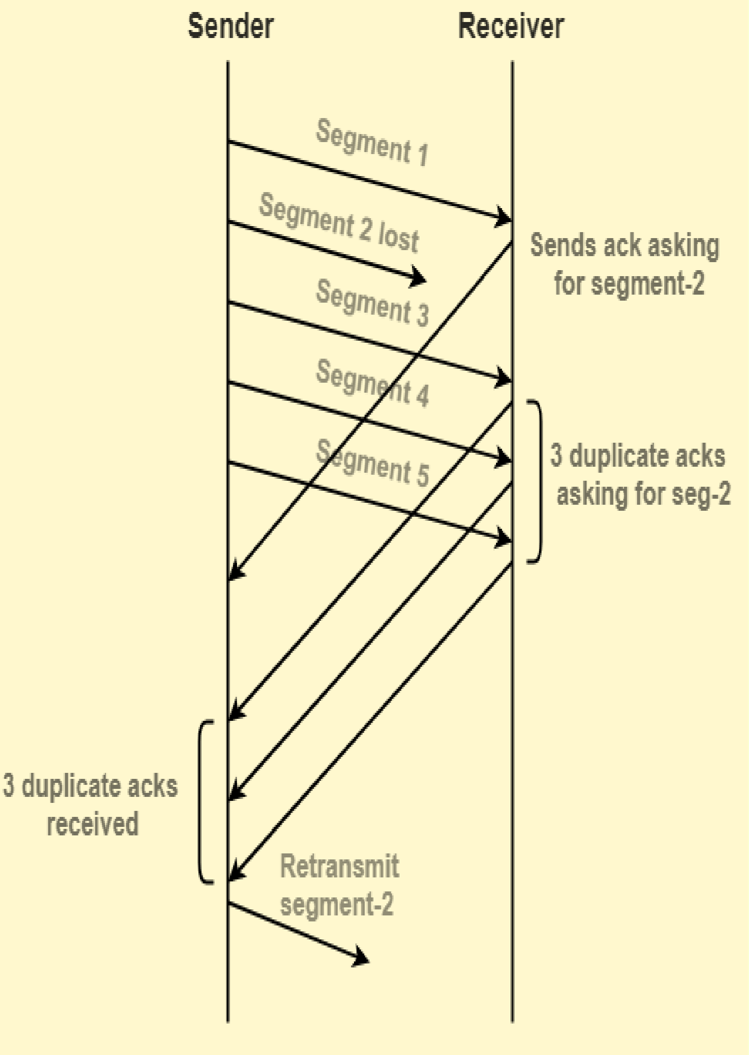


protocol subdomain domain name path

Computer Networking

TCP **–**The Transmission Control Protocol (TCP) is a connection-oriented reliable protocol. It provides a reliable transport service between end Systems (ES) using the network layer service provided by the IP protocol. TCP protocol exchange streams of data. Individual bytes of data are placed in memory buffers and transmitted by TCP in transport Protocol Data Units.

TCP Retransmission is a process of retransmitting a TCP segment. TCP Retransmission occurs when time out timer expires before receiving the acknowledgement or 3 duplicate acknowledgements are received from the receiver for the same segment.


Sender
Receiver
Segment 1
Segment 2 lost
Sends ack asking for segment-2
Segment 3
Segment 4
Segment 5
3 duplicate acks asking for seg-2
3 duplicate acks received
Retransmit segment-2

Retransmission after receiving 3 duplicate acks

Computer Networking

Rate modulation –Symbol rate /baud rate/modulation rate is the number of symbol / signaling changes during transmission per time unit .it is measured in baud(Bd)/symbol per second.

Rate modulation in congestion

Congestion occurs when the number of packets being transmitted through the network approaches the packet handling capacity of the network.

Whenever there is a timeout, TCP assumes congestion in the network and starts to reduce its sending rate.

If the sending rate is G at a wireless link with packet loss rate p, the throughput of this link is $S = G(1 - p)$. TCP should increase its sending rate G to get a large throughput if there is no congestion, rather than decreasing its rate

Computer Networking

Protocols –

1G – The analog 1G offered simple telephony service without data.

2G – Delivered digital signal and offered up to 250Kbps speed. Supports voice, text and data services.

3G – At least 200Kbps up to 3Mbps speed.

4G – 4G delivers up to 100Mbps for mobile access, and up to 1Gbps for wireless access. Most wireless carriers offering HSPA (High Speed Packet Access) at up to 6Mbps are claiming that they offer 4G network.

WiFi is a connection standard provided by a wireless network. A wireless network is in turn provided by any other any other device that connects into another Internet access, which is typically a physical line but can be 3G. That device then translates its own Internet connection into a WiFi network that other devices can share.

WiFi networks are small and typically only allow up to 30 devices to connect. They can be private, in which case we need to know a password to have access, or they can be an open, public "hotspot," allowing any device with WiFi capabilities to log in.

Computer Networking

What makes a protocol have higher bandwidth-

Each type of phone connection, 2G, 3G, and 4G have different frequency range that cell phones have to be designed to use to make and receive calls, and make a data connection. 2G has only 4 bands, typically 3G has 5 bands, and 4G has about 7 different bands.

In telecommunication, a band is a specific range of frequencies in the radio frequency (RF) spectrum, which is divided among ranges from very low frequencies (vlf) to extremely high frequencies (ehf). Each band has a defined upper and lower frequency limit. Because two transmitters sharing the same frequency band cause mutual interference, band usage is regulated. International use of the radio spectrum is regulated by the International Telecommunication Union (ITU). So protocols(2g,3g,4g..) higher bandwidth depends on the use of frequency band.