

# UNIT 1

## What are the Criteria of network?

- A network should meet a certain criterion

### Performance

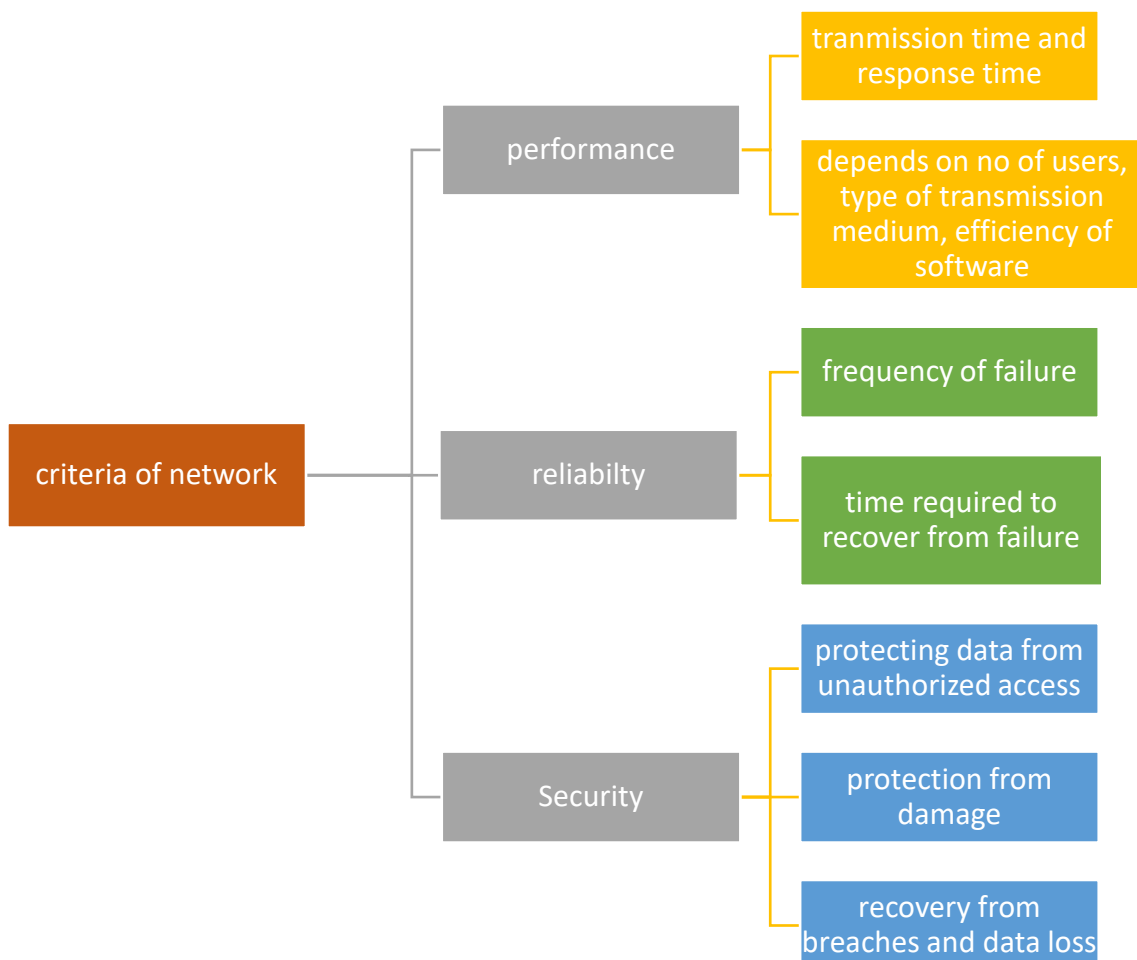
- It can be calculated in many ways like response time and transition time
- Transit time is the time required for data to be transfer from one node to another
- Response time is the time between inquiry and response
- Performance depends on many factors such as number of users, type of transmission medium, efficiency of software

### Reliability

- It how robust the Network is amid sudden major catastrophic events/ failures

### Security

- protecting data from unauthorized access, protecting data from damage and implementing policies and procedures for data recovery from breaches and data loss



## What are the types of connections in networking?

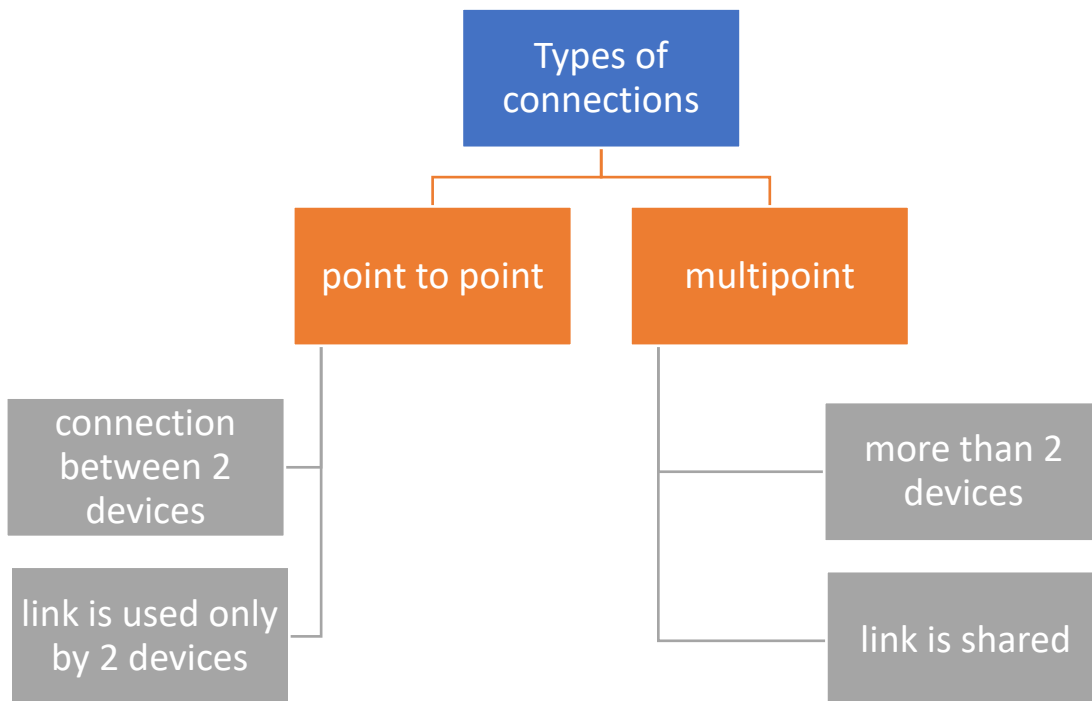
- A network is a connection of two or more devices
- 'link' is the pathway that transfers data from one device to another
- For communication these devices should be connected in some way

### Point to point

- Connection between two specific devices
- The entire link is used only by the two devices
- E.g., television and remote

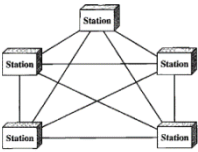
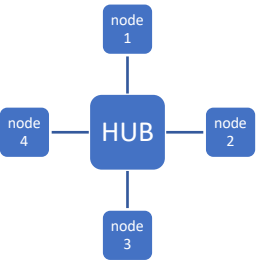
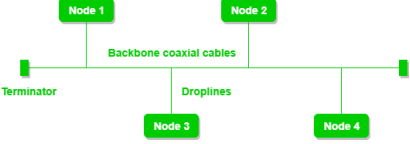
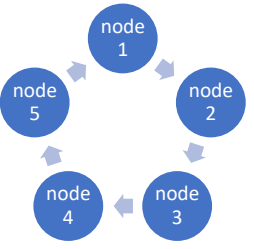
### Multipoint

- Here more than two devices share the network link
- The link is shared
- Several devices can share the link simultaneously
- E.g., WIFI connected with many devices



## What is topology?

- When 2 or more devices connect together it forms a topology
- Topology refers to the structure in which the network is formed
- There are 4 types of topologies, mesh, bus, ring and star

<u>Mesh</u>	<u>Star</u>	<u>Bus</u>	<u>Ring</u>
			
All devices are connected with each other	All devices are connected with a centred device called as hub	All the devices are connected with a single cable	All the devices are connected forming a ring
Direct communication between the devices	Indirect communication between the devices	Direct communication between devices	Data flows in one direction
Even if one device crashes the others can still communicate	If the hub crashes the whole network is disturbed and all devices are disconnected	If the hub crashes the whole network is disturbed and all devices are disconnected	If one device crashes, all the whole network will be disturbed as data will not flow

Types of Networks?

- Computer network are categorized by their size
- Lan, wan, pan, man

### LAN(local area network)

- Connection of devices in a small area e.g., building or office
- Ranges up to 2km
- Transmission speed is high
- Easy maintenance and low cost

### PAN(personal area network)

- Connection of devices in a personal space, e.g., home
- Ranges up from 10 meters to 30 meters
- E.g., network connection between mobile laptop and play stations
- There are two types of PAN networks
- Wireless and Wired
- Wireless PAN uses wireless technologies like WIFI and Bluetooth
- Wired Pan uses USB

### MAN(Metropolitan area network)

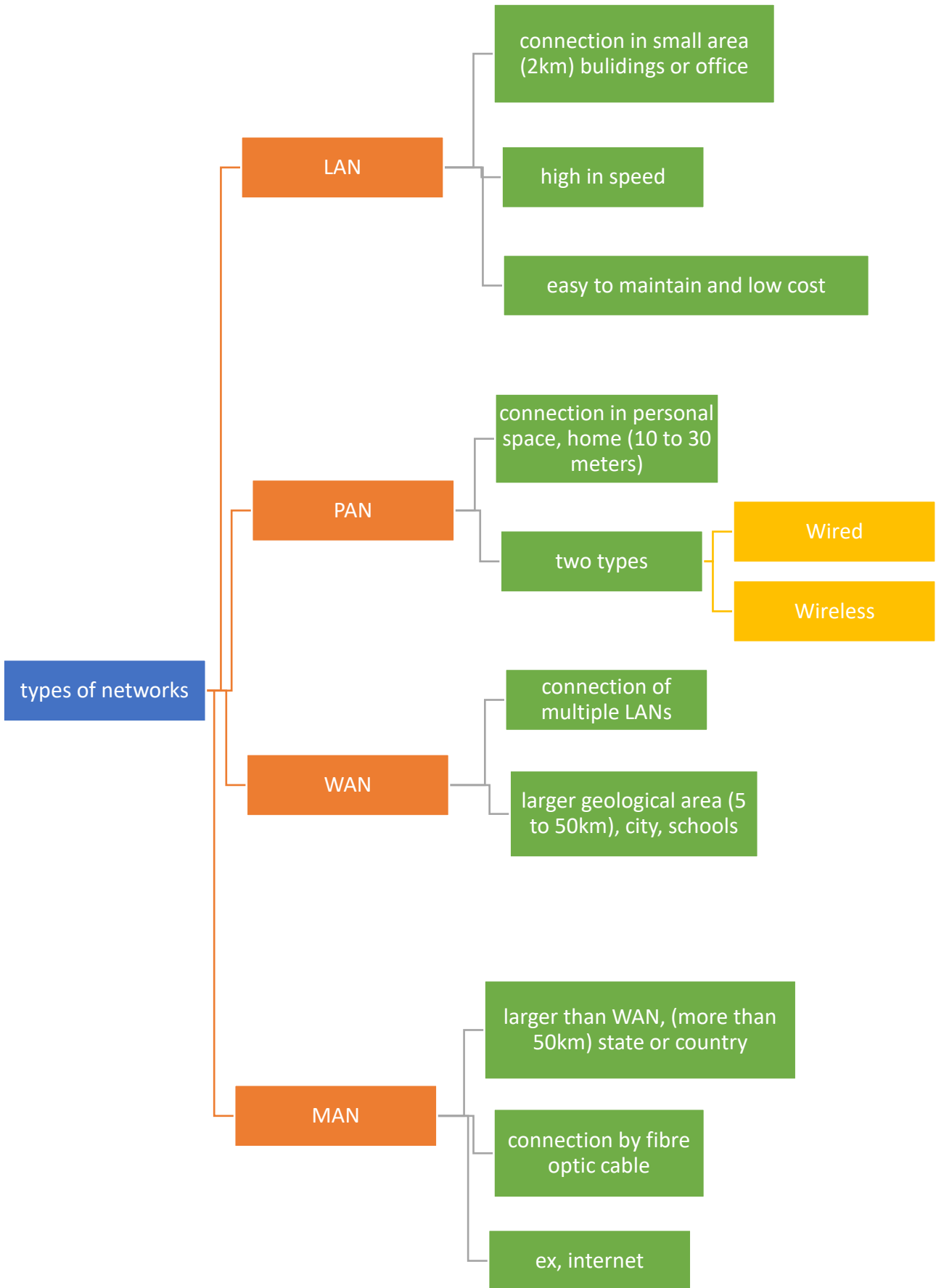
- Man is collection of multiple LAN networks
- It covers larger geographical area network
- Ranges from 5 to 50 km
- Higher range than Lan
- Government city WIFI, school WIFI networks

### WAN(Wide area network)

- WAN extends over a larger geological area e.g., states or country
- Bigger than LAN and Man
- Ranges over 50km
- Connected through telephone wire, fibre optic cable
- Internet is biggest WAN network in the world

LAN	MAN	WAN
-----	-----	-----

Local area network	Metropolitan area network	Wide area network
Small area e.g., buildings, office	Larger area such as city	Larger area like states or country
High in speed	Medium in speed	Low in speed
Easy design and maintenance	Difficult and complex design and hard to maintain	Also, Difficult and complex design and hard to maintain
Private ownership	Can be private and public	Might not be owned by one organization
2km	5-50km	More than 50km



## What is NIC?

- NIC stands for network interface card which is a network adapter which is used to connect the computer in a network
- It is installed in a computer
- NIC has a unique id on a chip and has a connector to connect cable
- This cable is connected to the router or modem
- Also called as ethernet card, connection card and LAN adapter

## What is modem?

- Modem is modulator and demodulator
- Network between computer and telephone line
- Has two parts
  - i. Modulator (analogue to digital)
  - ii. Demodulator (digital to analogue)
- Types of modem connections
  - iii. Dial up (telephone line)
  - iv. DSL (phone wire by high speed)
  - v. Cable (cable tv line)

## What is a HUB?

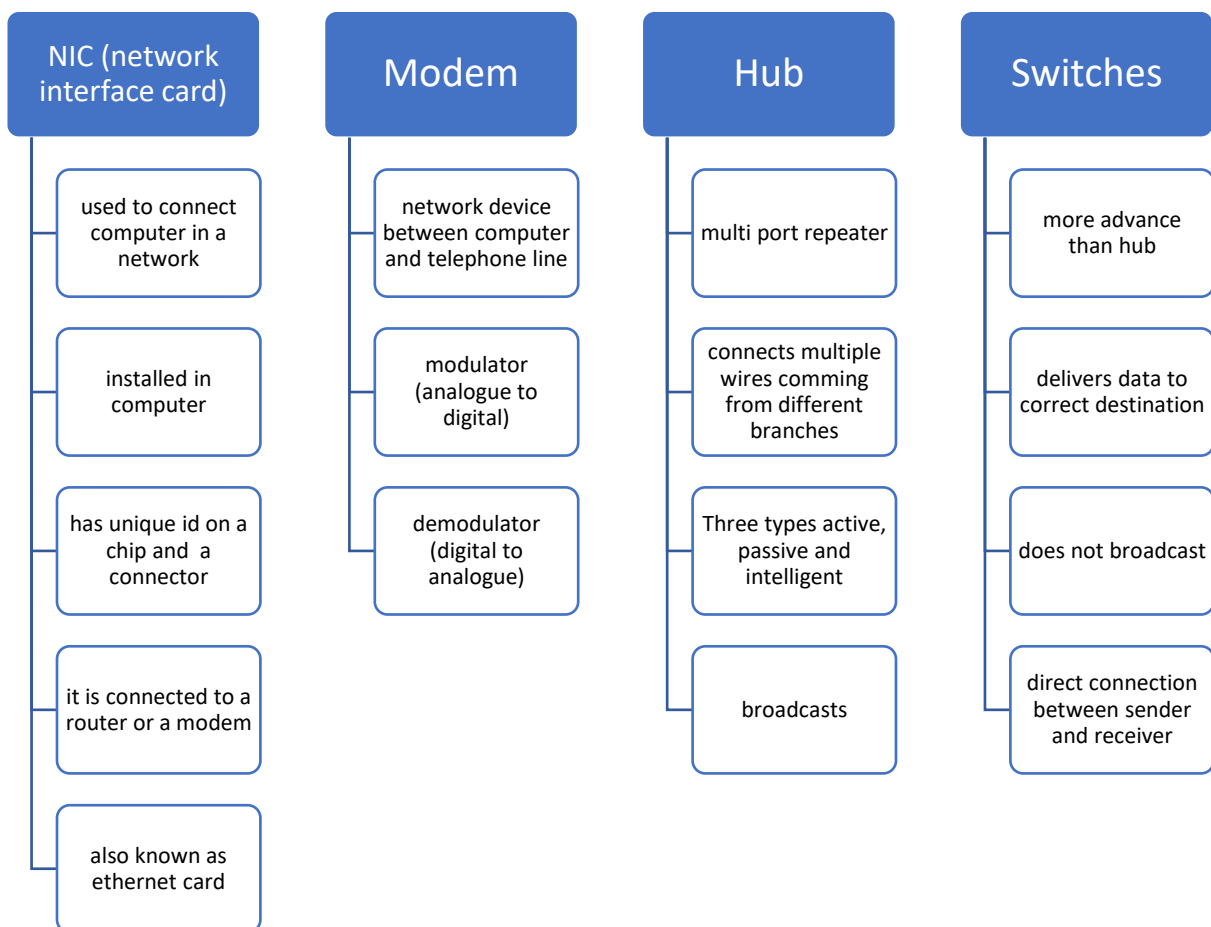
- Multi-port repeater
- Connects multiple wires coming from different branches
- Like star topology
- Cannot filter data so packets are sent
- three types of hubs
  - vi. Active (amplifies the signal)
  - vii. Passive (simply connects signals of network)
  - viii. Intelligent (network management)

## What are switches?

- Switches are hardware devices that connect multiple devices
- Has more advanced features than HUB
- Switches deliver data to the correct destination based on the physical address
- It does not broadcast the message to the entire system like hub
- It provides direct connection between sender and receiver
- There are two types of switches (L1 and L2)



<b>Switch</b>	<b>HUB</b>
Connects multiple devices on a computer network	Used to transmit a signal to each port to respond from which the signal was received
Works at both physical and data link layer	Operates only at physical layer
Full duplex	Half duplex
Unicast multicast and broadcast transmission	Broadcast transmission
Expensive as compared to HUB	Less expensive as compared to Switch
Easy to hack	Hacking is complex
24 to 48 ports	4-12 ports

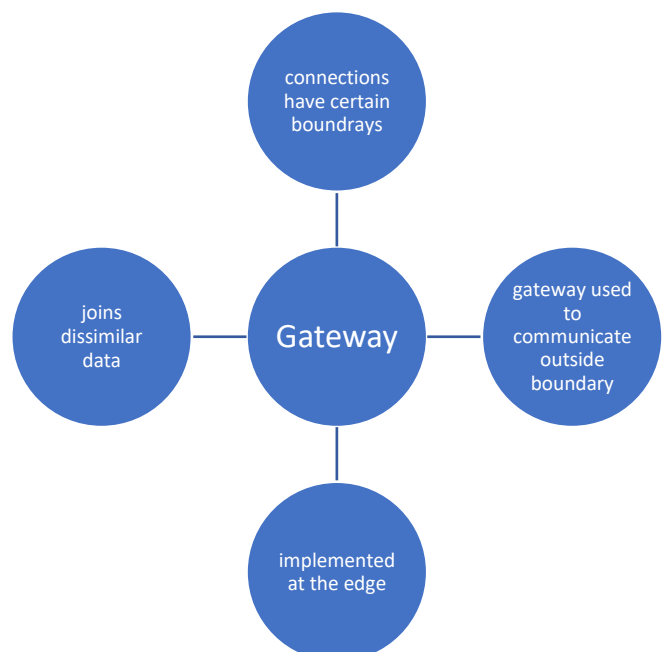
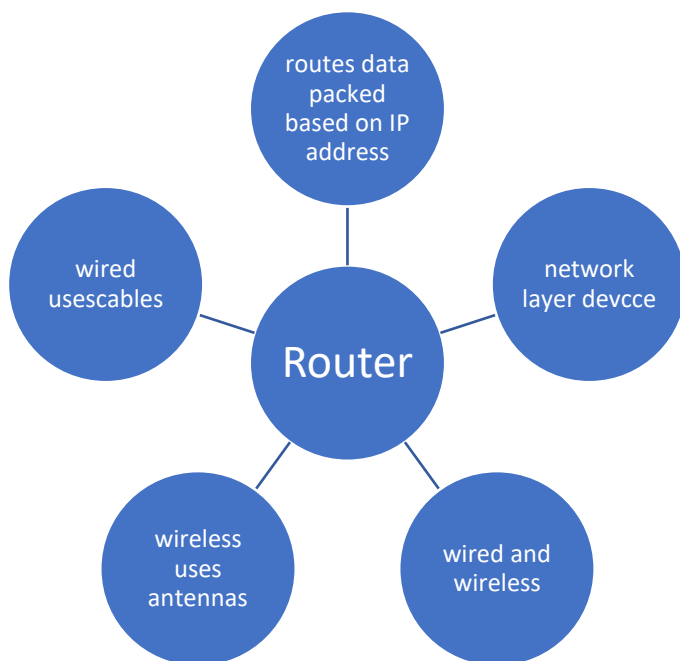


## Router

- Devices that route data packets based on the IP address
- Network layer device
- Connects LANs and WANs
- Two types wired and wireless
- Wireless (broadcast using antennas)
- Wired uses cable to connect to network devices

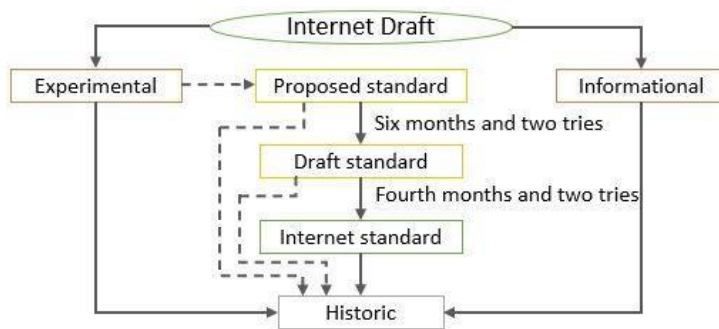
## Gateway

- All connections have certain boundary that limits the connection
- Due to this if it needs to communicate outside this boundary, it needs a gateway
- Gateway is implemented at the edge of the network
- When one network wants to communicate with another the data is passed through the gateway which is routed to the destination through most efficient path
- It joins two or more dissimilar networks



## Maturity levels of RFC

- Proposed standard (stable and understood specification with wide community interest, it is tested and implemented in various programs)
- Draft standard (next stage to proposed stage is draft stage after two successful implementations)
- Internet standard (we reach this stage after demonstrating these successful implementation)
- Historic (these are specifications which are suspended or has not met the required specification to be an internet standard)
- Experimental (describes work related experimental situation)
- Informational (contains general and historical and tutorial information)



## What is internet administration

- Internet administration is a group that coordinates and guides the internet with its growth and development
- It makes sure that the protocols are followed by the devices and the network
- Organizations
  - ISCO – internet society
  - IETF – internet engineering task force
  - IRTF – internet research task force
  - IAB – internet architecture board

## What is Protocol layering

- Protocol is a set of instructions or rules that outline a language that a device should use
- When it comes to networking there are a lot of protocols
- When a communication is simple, we can only use one protocol
- But when the communication is complex, we need to divide the task into layers so we need to implement protocols at every layer
- This is called as protocol layering

## OSI Model

### 7 Layers of OSI model

- Physical layer
- Data link layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

### Physical layer

- Transfers bits from one node to another node
- Lowest layer in OSI model
- It connects, maintains and deactivates the physical connection
- Some functions of Physical layer
  - Line Configuration : It defines how the devices can be connected
  - Data transmission : Defines if the transmission is simplex, half duplex or Full Duplex
  - Topology : defines how the arrangement of devices is
  - Signals : defines the type of transmission signal

## Data link Layer

- Data link layer converts bits into frames and passes it to the network layer
- It adds header and tailer to the frames
- Header contains the source address and hardware destination
- The frames are transmitted to the destination written in the header
- Data link layer controls the flow, so that no data is corrupted
- Data link layer controls the error by placing some values in the trailer before sending it to the physical layer, if error occurs the receiver sends acknowledgement message

## Network Layer

- It is the third layer in the OSI model
- It manages device addressing and tracks location of devices in the network
- it determines the best possible path to transfer data from source to the destination
- Network layer provides logical connection between networks
- Network layer determines the best optional path out of multiple paths in the network connection between the source and destination
- Network layer converts the frames into packets

## Transportation layer

- It is the 4<sup>th</sup> layer in the OSI model
- It ensures that the messages are transmitted in the order in which they are sent and there is no duplication of data
- It converts packets into segments
- It establish and maintains connection
- Each segments travels usings multiple different routes and they arrive in different order
- The TCP reorders this segments in proper order as each segment has a sequence number

## Session layer

- It is the 5<sup>th</sup> layer in OSI model
- Used to establish, synchronize and interact between the connections
- Session layer adds some checkpoints between the transmission so, if any error occurs during transmission the transmission occurs again from the checkpoint

## Presentation Layer

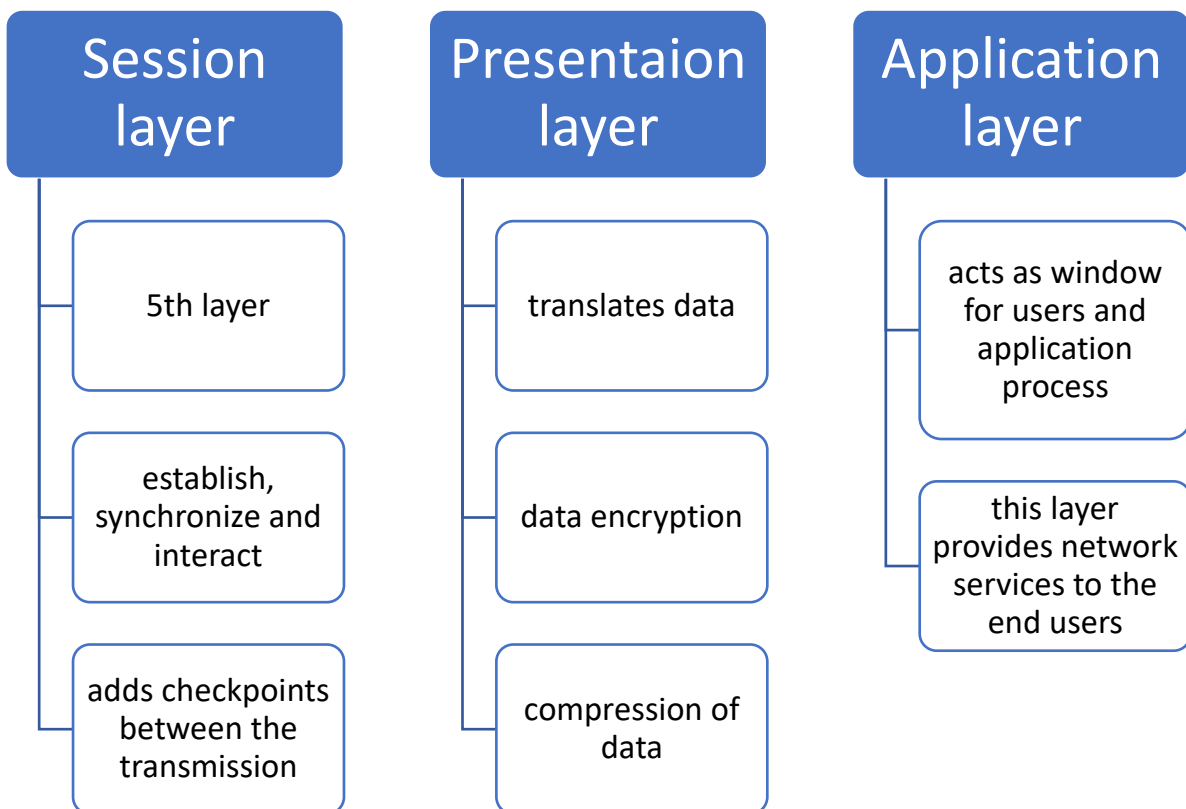
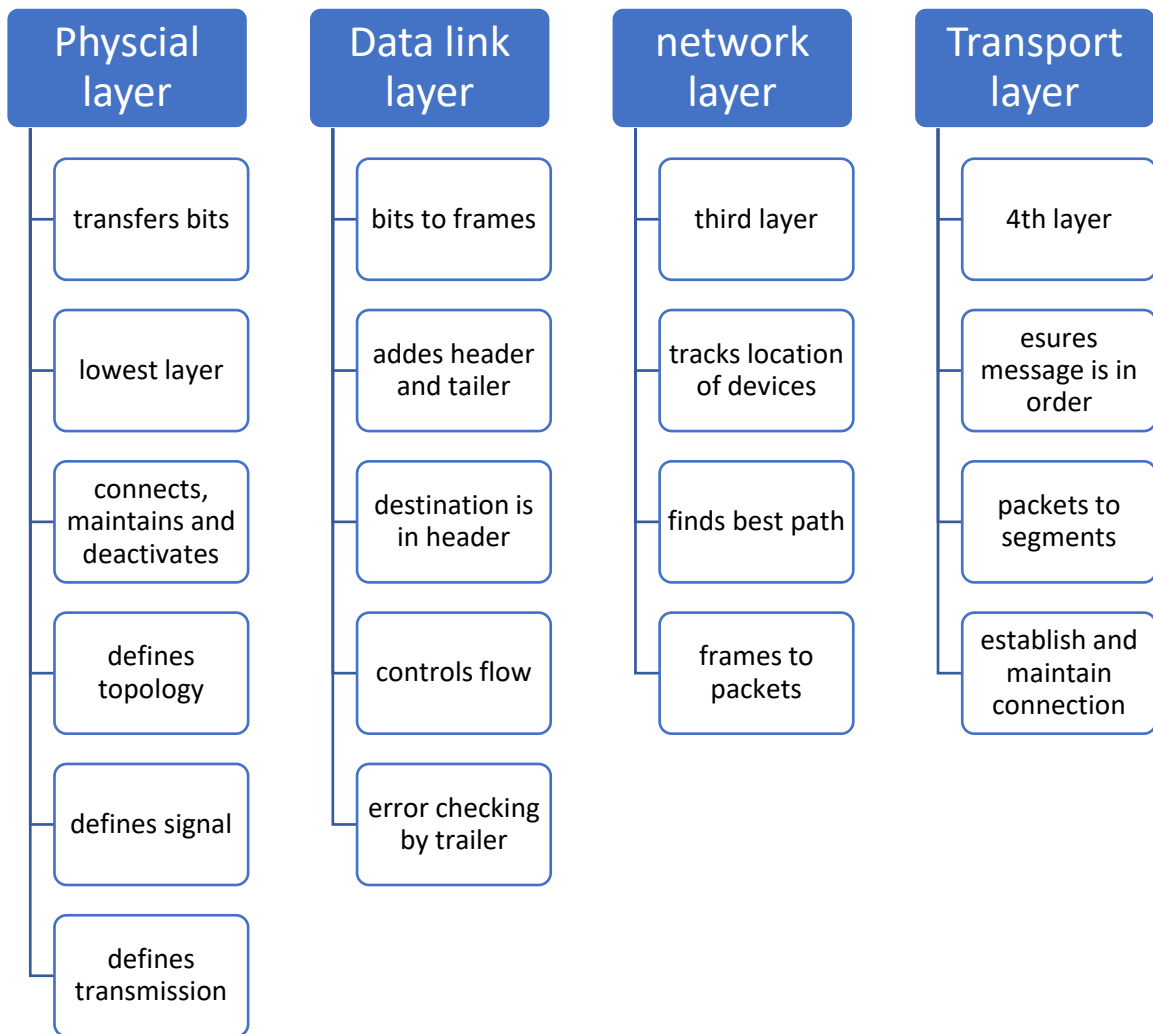
- It acts as the data translator for the network
- Different devices uses different encoding methods the presentation layer handles interoperability between the different encoding methods
- Presentation layer provides data encryption
- It also provides compression of data, which results in sending less number of bits

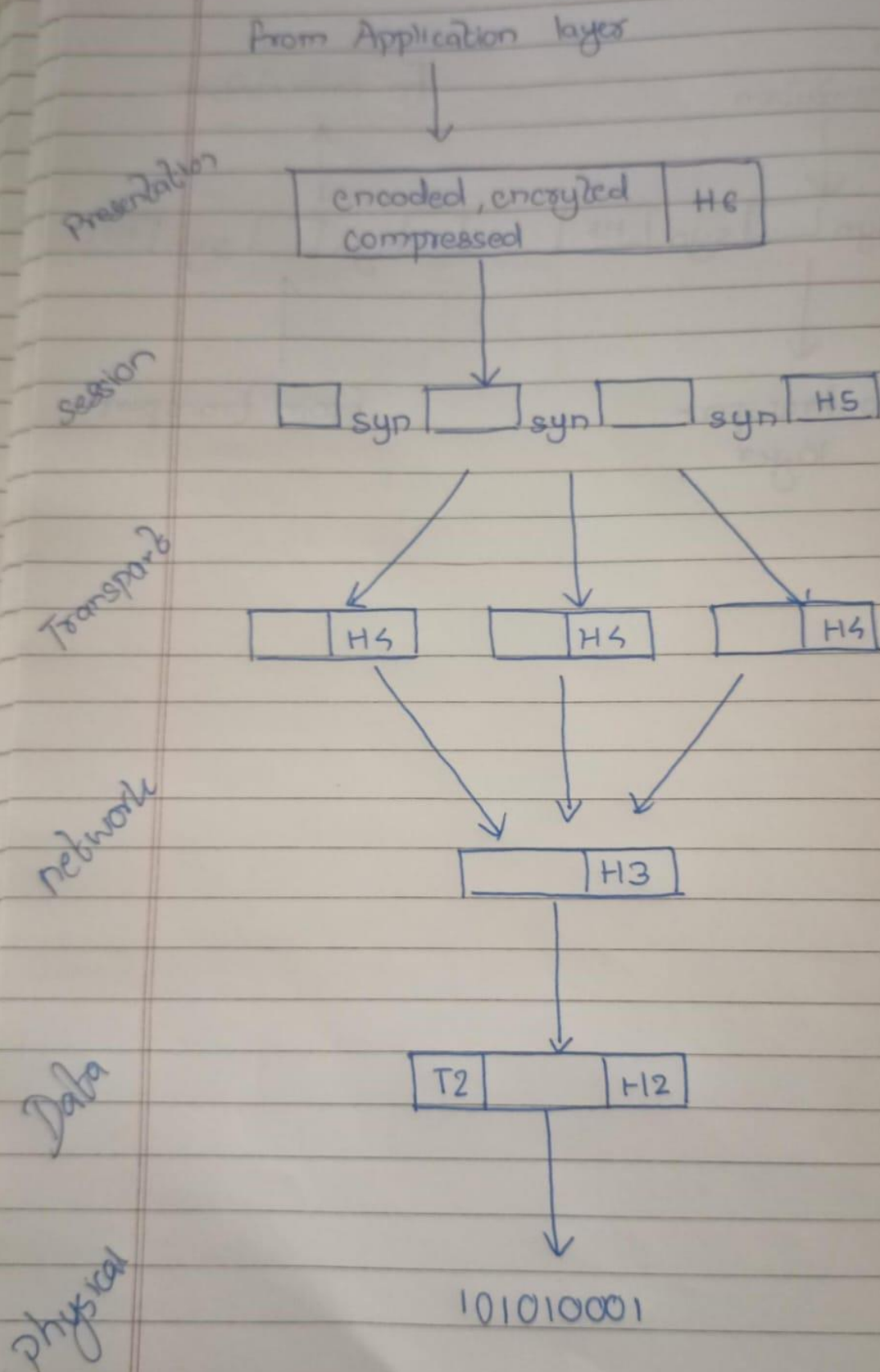
## Application layer

- Application layer serves as window for users and application process
- This layer provides network services to the end-user



OSI Model Diagram







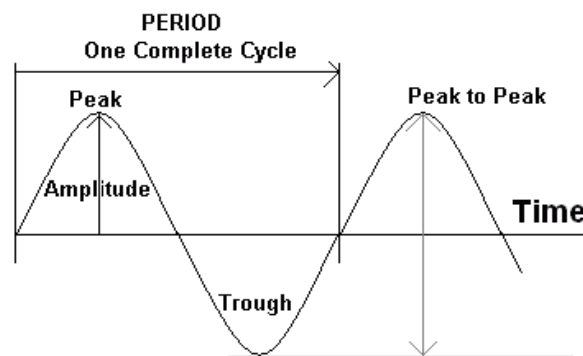
# UNIT 2

## Analog And Digital

Analog data refers to data that changes continuously over time for example Analog watch, on other hand Digital data refers to non-continuous change in data.

## Simple Analog signal

- Simple Analog signal is in the form of sin wave
- Analog signal is smooth and continuous
- Peak amplitude : absolute height intensity of the sine wave
- Period(T) : time required to complete one cycle
- Frequency(F) : number of cycles completed in one second
- Frequency is measured in Hz
- $F = 1/T$
- Wavelength : distance a signal travel in one period

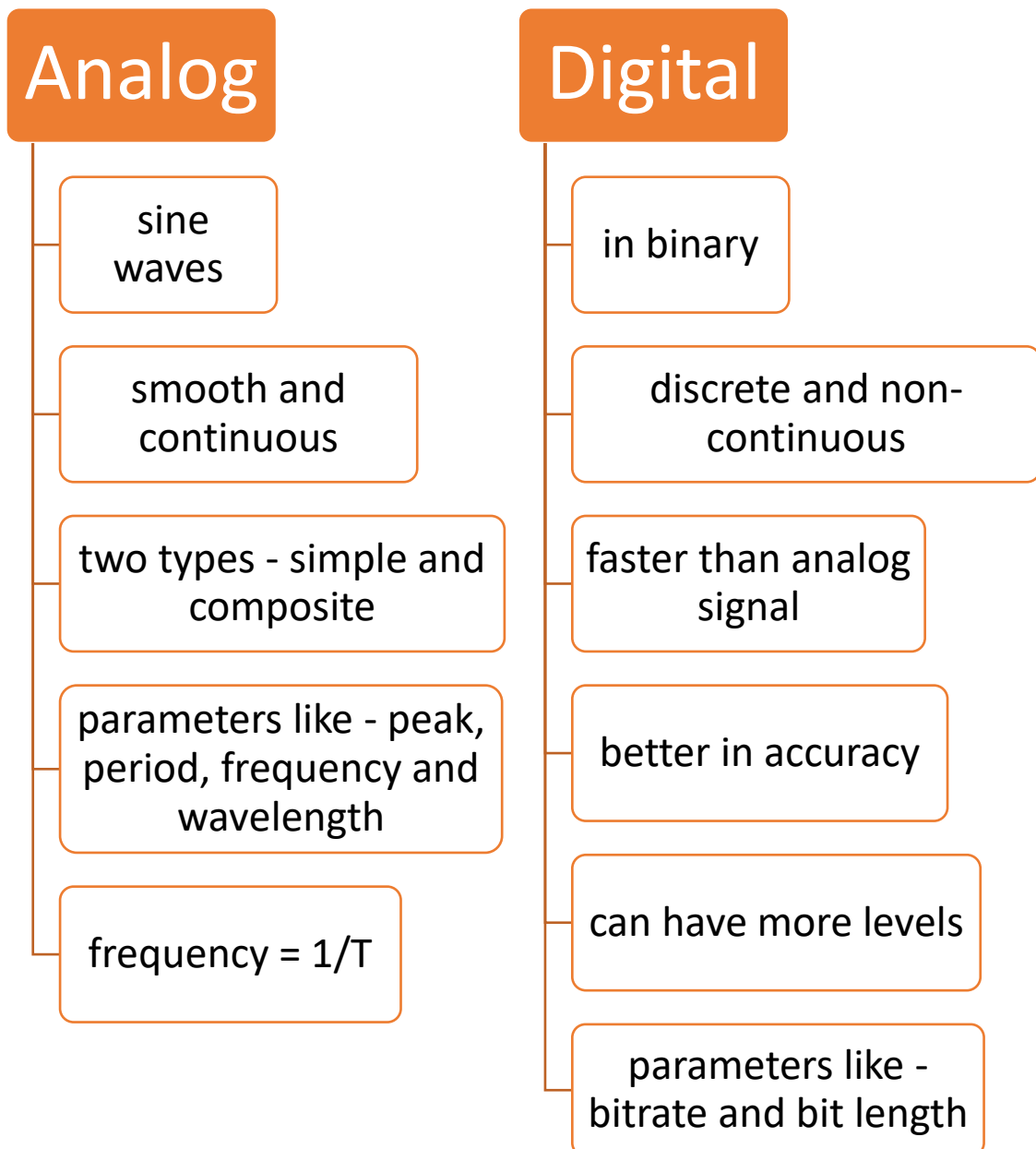


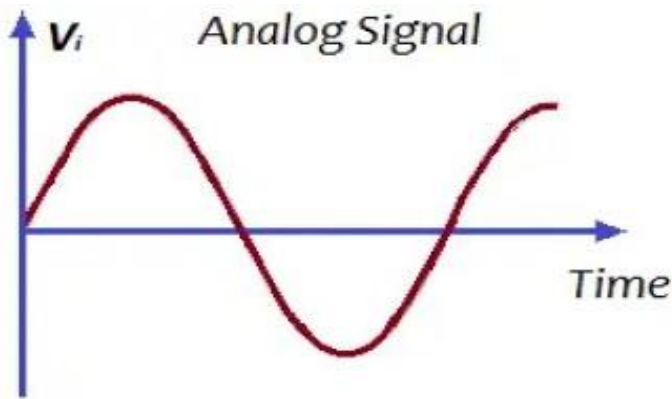
## Composite Analog Signal

- Composite signal is a combination of multiple simple analog signals of different frequencies and period
- Bandwidth : bandwidth is the range of frequencies in the composite signal, bandwidth is measured in Hz
- Let's say we have a composite signal with frequencies ranging from 2000 to 4000 then the bandwidth is  $4000 - 2000 = 2000\text{hz}$

## Digital Signal

- Digital signals are not continuous
- These signals are represented in binary numbers and consists of different voltage values
- Transmission of digital signal is better than Analog signal
- Better in accuracy than Analog signal
- Can have more than 2 levels
- Digital signals are non-periodic so frequency and period are not characteristics of digital signal
- bit rate : no of 1s in expressed in bits per second
- Bit length : distance bits occupies in the transmission medium

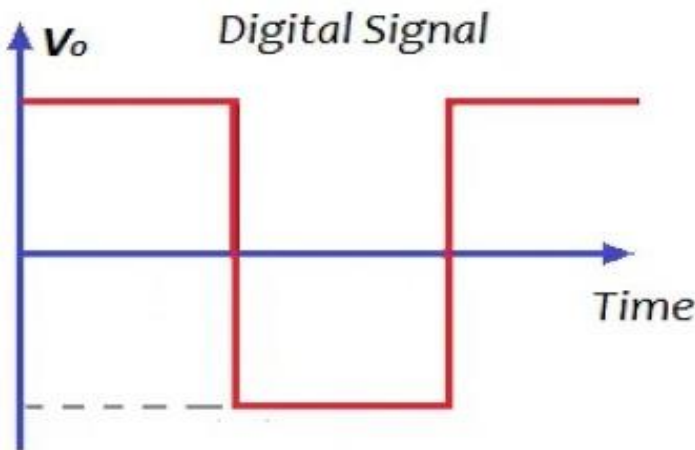




**period** : time required for one cycle to complete

**frequency** : number of cycles completed in 1 sec

**wavelength** : distance the signal travels in one period

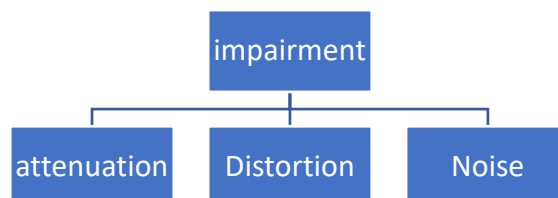


**bitrate** : no of 1s expressed in bits per second

**bitlength** : distance occupied in the transmission medium

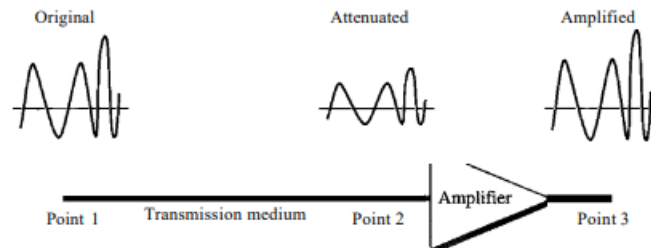
### Transmission impairment

- Some signals travelling through transmission medium may not be perfect
- Which means the signal sent and the signal received may not be same



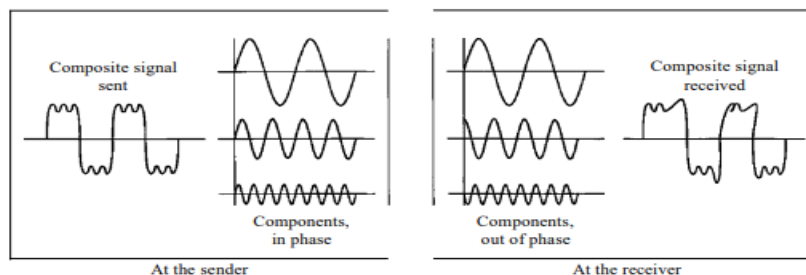
## Attenuation

- Attenuation means loss of energy
- When signal travels through some medium there is some loss of energy
- This is why wire that carries electric signal gets hot
- To recover this loss amplifiers are used



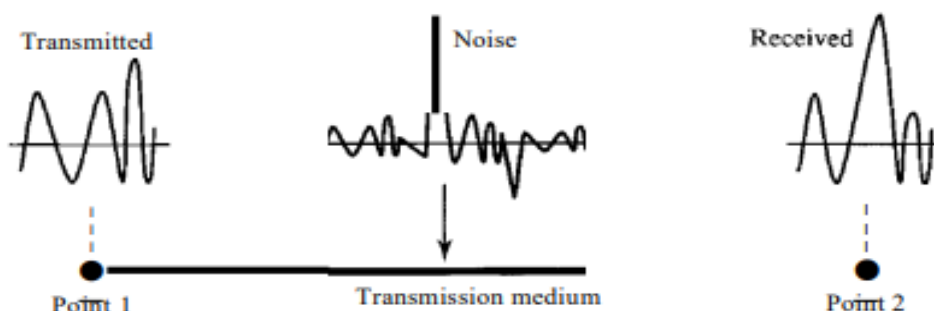
## Distortion

- Distortion means the signal changes its form and shape
- Each signal has its propagation speed through the medium and therefore its own delay arriving in the destination

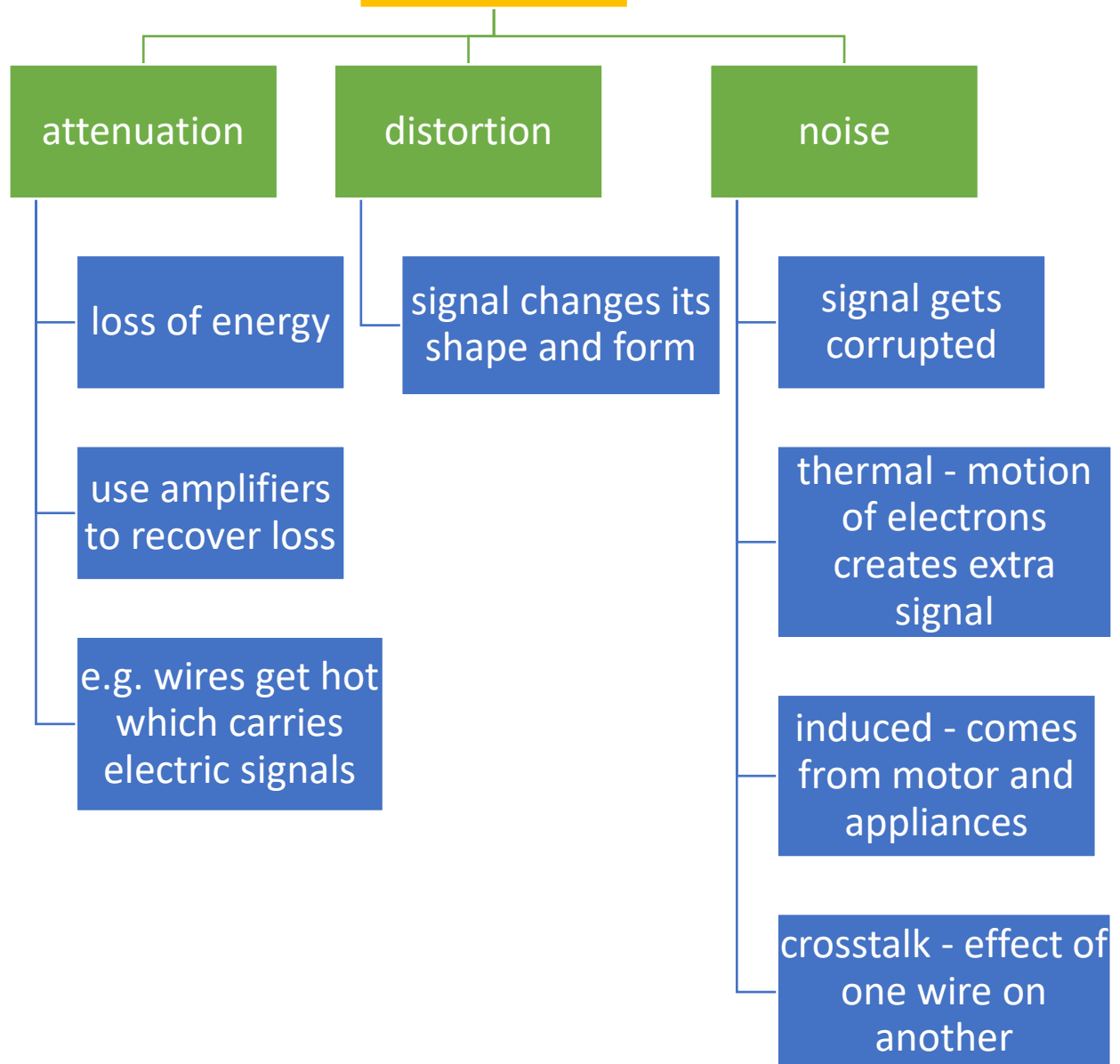


## Noise

- Several types of noise such as thermal noise, induced noise, crosstalk and impulse noise may corrupt the signal
- Thermal noise is motion of electrons which creates an extra signal which is not present in the signal that was sent
- Induced noise comes from motors and appliances
- Crosstalk is the effect of one wire on another



# Transmission impairment



## Data rate

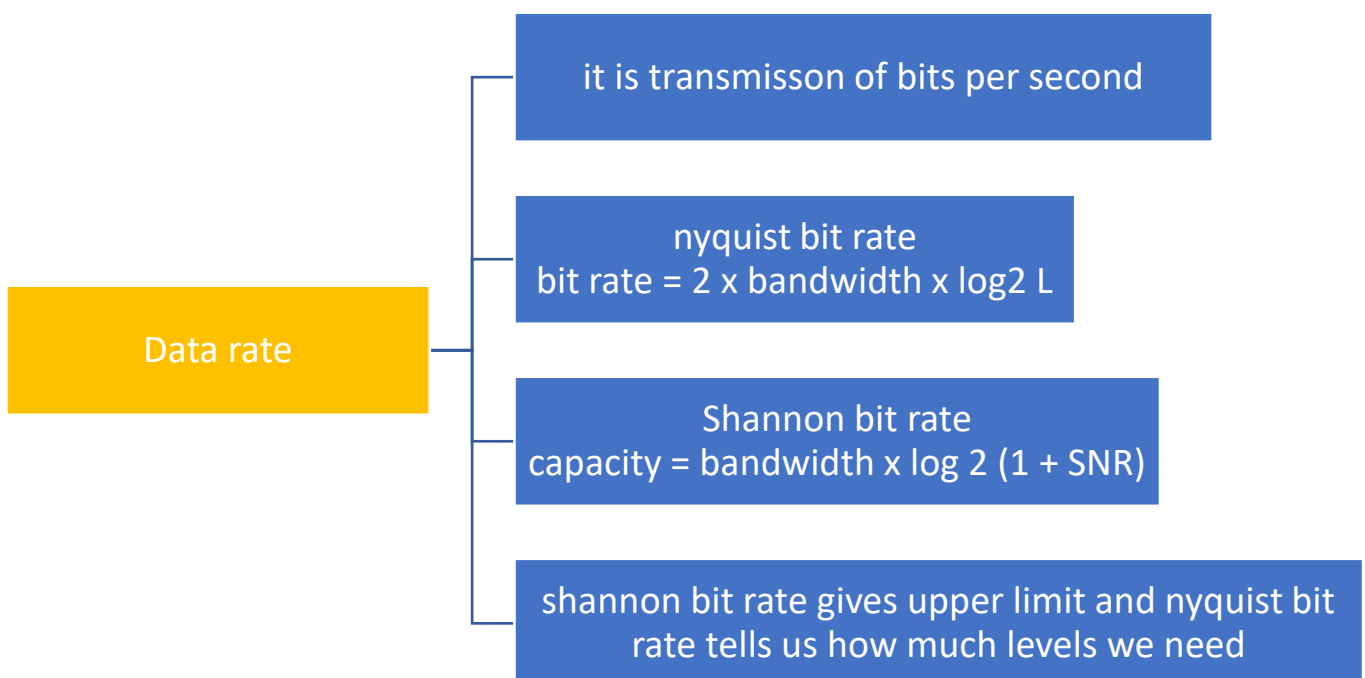
- Data rate is transmission of bits per second
- It depends on 3 factors
  - o Bandwidth available
  - o Level of signal
  - o Quality of channel (level of noise)
- Shannon bit rate gives the upper limit and Nyquist determines how many levels we need

## Nyquist Bit rate

- Used to calculate bit rate in noise less channel
- Bit rate =  $2 \times \text{bandwidth} \times \log_2 L$
- L is the level of signal
- We can have any bitrate just by increasing the levels
- But when levels of signals are increased there is burden on the receiver

## Shannon Bit rate

- In reality, the channel is always noisy
- Capacity =  $\text{bandwidth} \times \log_2 (1 + \text{SNR})$
- SNR is signal to noise ratio
- No matter how many levels we have we cannot achieve data rate higher than capacity



## Performance of network

### Bandwidth

- Bandwidth is a characteristic that can be used to measure the network performance
- Increase in bandwidth in hertz is increase in bandwidth in bits per second
- Bandwidth in Hertz : Range of frequencies a channel can pass
- Bandwidth Bit per seconds : Number of bits send to the channel

### Throughput

- Throughput is a measure of how fast we can send data through network

### Latency (delay)

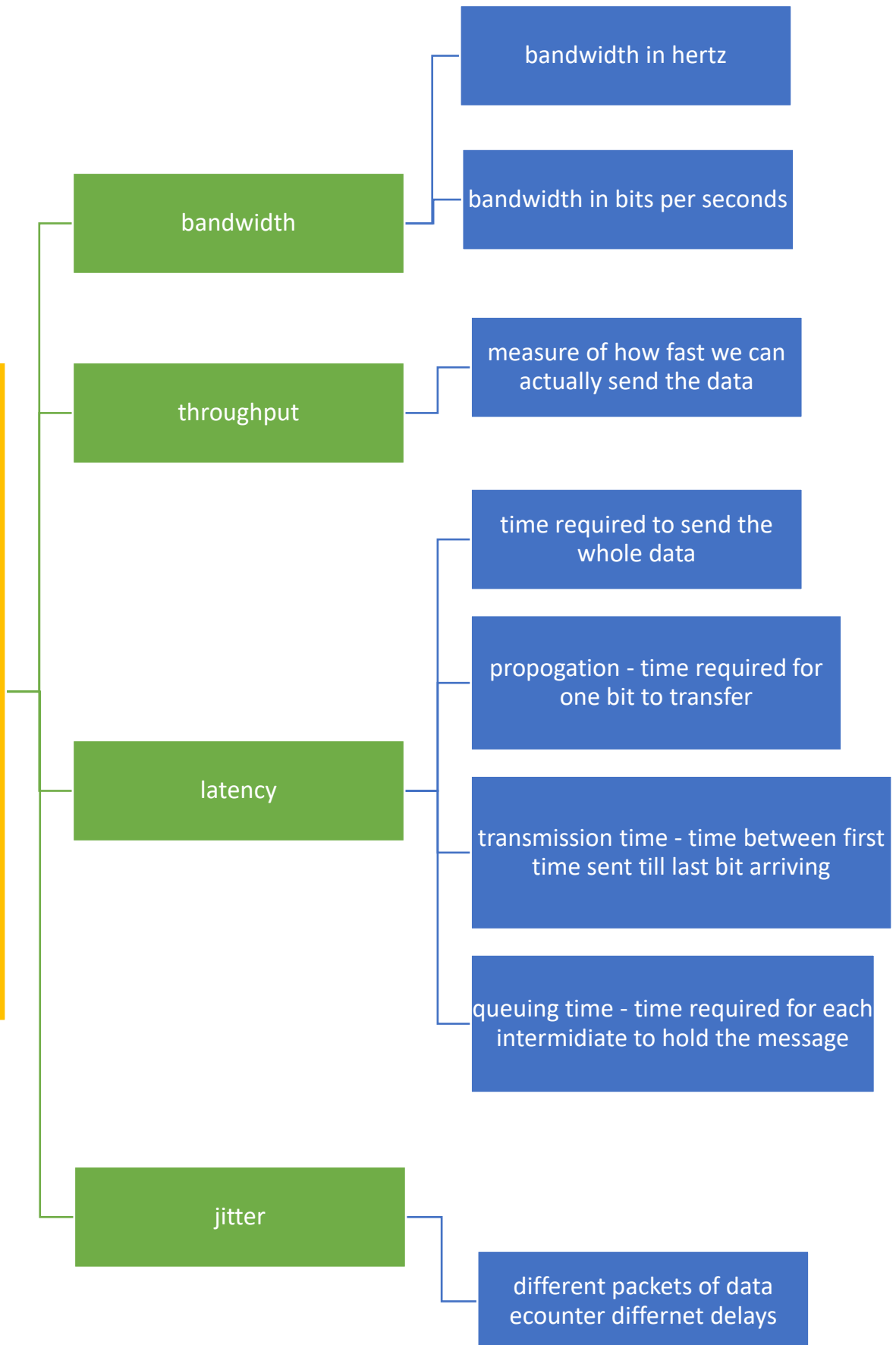
- How long it takes for the entire message to completely arrive to its destination from the time the first bit was sent
- Latency is made out of 4 terms
- Propagation time: time required for a bit to travel from source to destination
- Propagation time = distance/ propagation speed
- Transmission time : it is the time between the first bit leaving the sender till last bit reaching the receiver
- Transmission time = message size / bandwidth
- Queuing time : time needed for each intermediate to hold message before it can be processed
- Processing delay

### Jitter

- It is the problem if the different packets of data encounters different delays and the application using this data is time sensitive
- E.g., the delay of first packet is 10ms, second packet is 20ms and third packet is 45ms



# performance of network



## Data link layer error detection and error correction

### Types of errors

- When bits flow from one place to another they can change because of interference
- Single bit error : single bit error means that only one bit of data is changed from 0 to 1 or from 1 to 0
- Burst error: it means more than one bit are changed from 0 to 1 or from 1 to 0
- There are more chances of occurrences of burst error
- The changes depend on the data rate and duration of noise

### Detection versus Correction

- The correction of error is more difficulty than finding errors
- In error detection we only look if any error has occurred or not
- In error correction we need to know the exact number of bits that are changed or corrupted and their location in message
- Forward message correction: it is the process the receiver tries to guess the message by using redundant bits
- Correction by retransmission : if any error occurs the receiver asks the sender to send the message again

### Block Coding

- In block coding we divide the message into blocks each of  $k$  bits
- We add ' $r$ ' redundant bits to the end of each block
- This makes the length  $n = k + r$
- We can create a combination of  $2^k$  data words and  $2^n$  codewords

## Error detection

- The sender converts data words into codewords
- Each codeword sent to the receiver can change during the transmission
- If the received codeword is same as the valid codeword then the word is accepted
- If the codeword is not valid then it is discarded
- If the codeword gets corrupted during the transmission but still received the error remains undetected

<i>Datawords</i>	<i>Codewords</i>
00	000
01	011
10	101
11	110

### Example:

- 01 is converted into 011 and is sent
- The receiver gets 011 which is valid, 01 is extracted from it
- Let's say the receiver receives 111 which is not valid and is discarded
- If it receives 000 instead of 011 then the error remains undetected as 000 is valid

## Error Correction

- It is much more difficult than error detection
- The receiver needs to know that the received codeword is invalid and then it has to find(or guess) the original codeword
- We need more redundant bits for error correction

<i>Dataword</i>	<i>Codeword</i>
00	00000
01	01011
10	10101
11	11110

### Example:

- 01 data word is converted into 01011
- Let's say that it gets corrupted and turns into 01001
- The codeword 01001 is not in the table this means error has occurred
- Assuming that only one bit is changed
- We will check which codeword only differs from the 01001 by 1 bit
- 01011 is the only codeword which has only 1 bit different from the received one (01001)
- Hence, we can find out the corrupted codeword was 01011 and then data word 01 can be extracted from it

Error Detection	Error Correction																				
<table border="1" data-bbox="121 309 778 544"> <thead> <tr> <th><i>Datawords</i></th> <th><i>Codewords</i></th> </tr> </thead> <tbody> <tr> <td>00</td> <td>000</td> </tr> <tr> <td>01</td> <td>011</td> </tr> <tr> <td>10</td> <td>101</td> </tr> <tr> <td>11</td> <td>110</td> </tr> </tbody> </table>	<i>Datawords</i>	<i>Codewords</i>	00	000	01	011	10	101	11	110	<table border="1" data-bbox="823 309 1473 544"> <thead> <tr> <th><i>Dataword</i></th> <th><i>Codeword</i></th> </tr> </thead> <tbody> <tr> <td>00</td> <td>00000</td> </tr> <tr> <td>01</td> <td>01011</td> </tr> <tr> <td>10</td> <td>10101</td> </tr> <tr> <td>11</td> <td>11110</td> </tr> </tbody> </table>	<i>Dataword</i>	<i>Codeword</i>	00	00000	01	01011	10	10101	11	11110
<i>Datawords</i>	<i>Codewords</i>																				
00	000																				
01	011																				
10	101																				
11	110																				
<i>Dataword</i>	<i>Codeword</i>																				
00	00000																				
01	01011																				
10	10101																				
11	11110																				
less number of redundant bits	More number of redundant bits																				
Easy to detect error	Difficult to correct error																				
<p>10 is converted to 101 Receiver can extract 10 from 101</p>	<p>10 is converted to 10101 Receiver can extract 10 from 10101</p>																				
<p>Let's say the receiver receives 111 instead of 101 which is not in the table so it is not valid and is discarded</p>	<p>Let's say the receiver receives 10111 Assuming one bit is changed we can find out that 10101 is the closest</p>																				
<p>So, here we are able to detect error by looking at the table</p>	<p>So, we found out that 10101 was the corrupted code word</p>																				

# UNIT 3

## Basic Service Set (BSS)

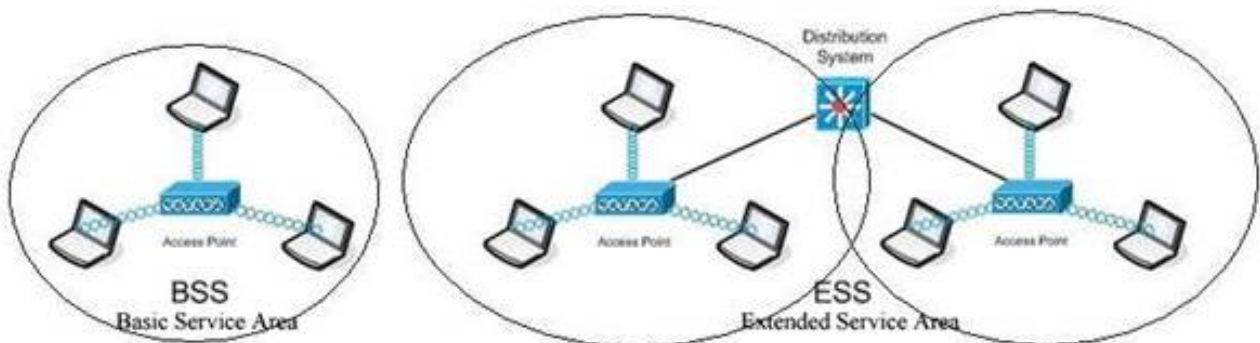
- Made out of stationary or mobile wireless stations and an optional station called as access point (AP)
- BSS without AP is called as Ad hoc network and it cannot send data to other BSS
- BSS with AP is called as infrastructure network

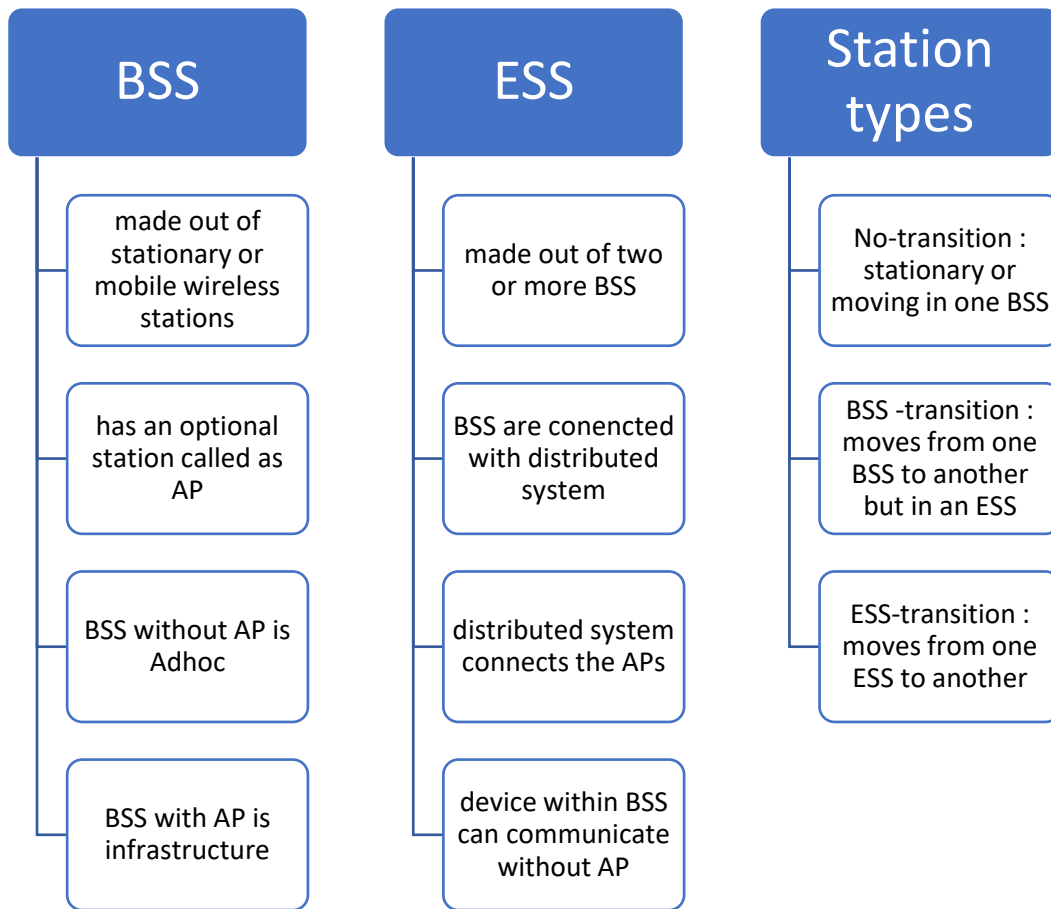
## Extended Service Set (ESS)

- Made out of two or more BSS with APs
- In this case BSS are connected through a distributed system which is wired
- This distributed system connects the APs in the BSS
- There are two stations in ESS, mobile and stationary
- Mobile stations are normal stations in BSS
- And stationary stations are APs in BSS which are wired LAN
- The stations within the BSS can communicate without APs
- The stations need AP to communicate from one BSS to another

## Station Types

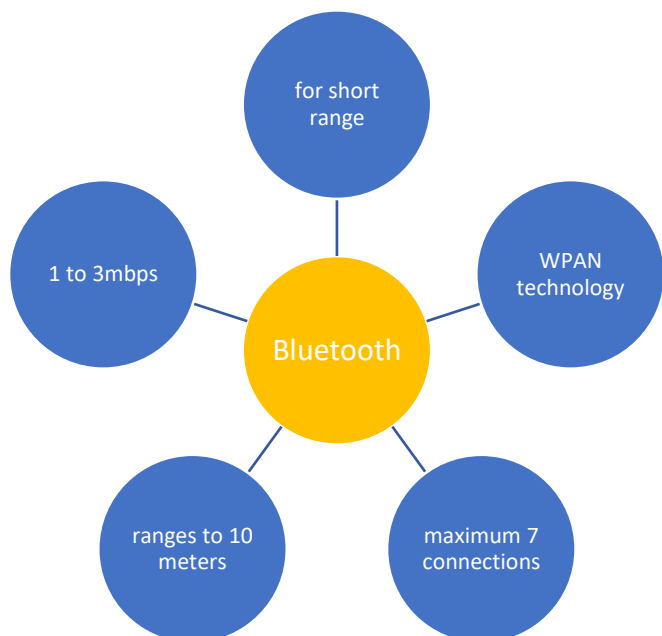
- no transition is either stationary or moving only in one BSS
- BSS transition can move from one BSS to another but is confined in one ESS
- ESS transition mobility can move from one ESS to another
- But as per IEEE 802.11 there is no guarantee that the communication will be continuous





## Bluetooth

- Bluetooth is for short range wireless communication
- It is a WPAN technology
- 2.4GHz to 2.485 GHz
- Maximum of 7 devices can be connected to Bluetooth
- Ranges up to 10 meters
- Provides data rate from 1 to 3 mbps based on version





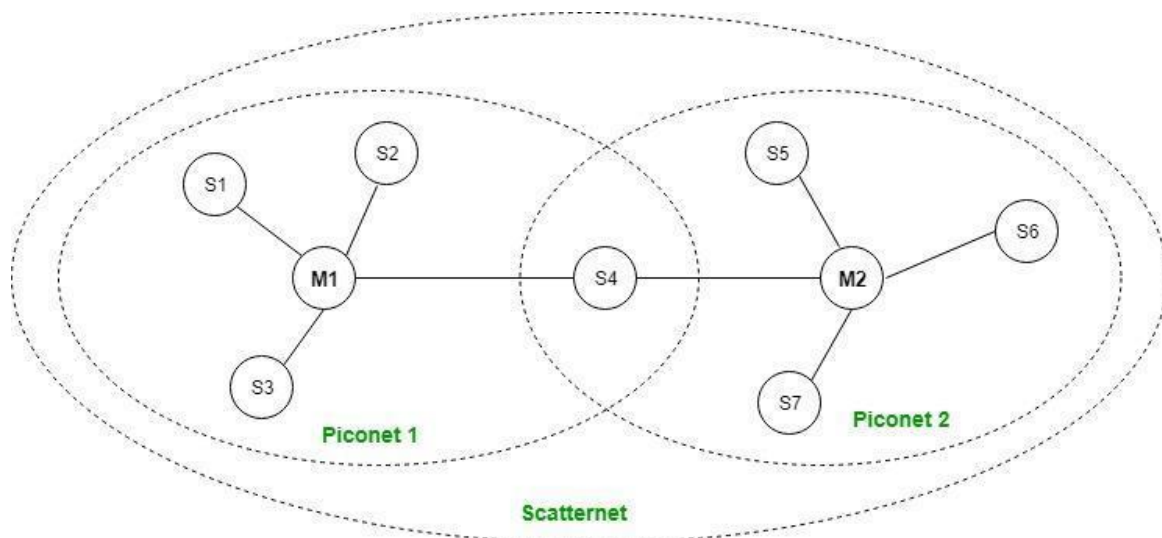
## Bluetooth Architecture (PICONET and SCATTERNET)

### Piconet

- Consist of one primary node called as master and seven secondary nodes called as slaves
- Total of 8 nodes which are in range of 10 meters
- Slave to slave communication is not possible
- Only slave and master can communicate

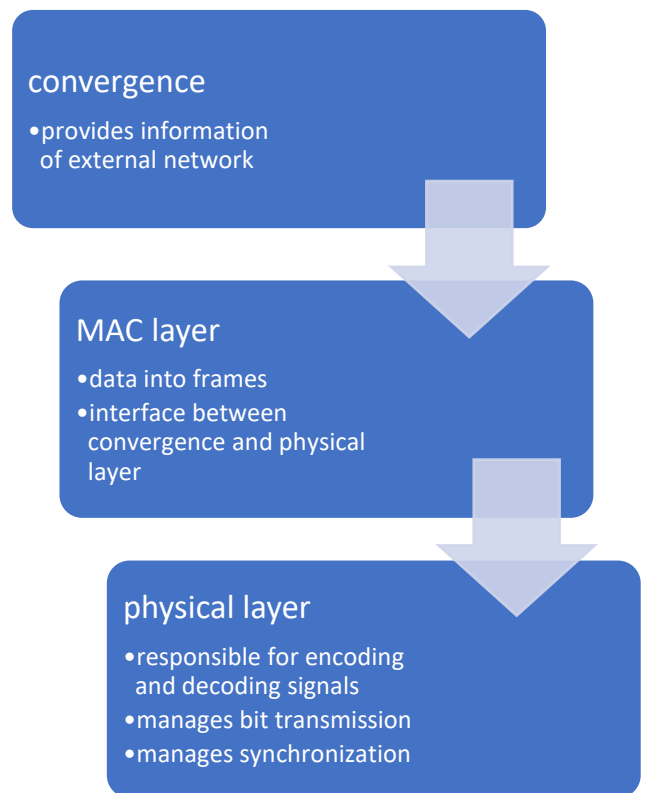
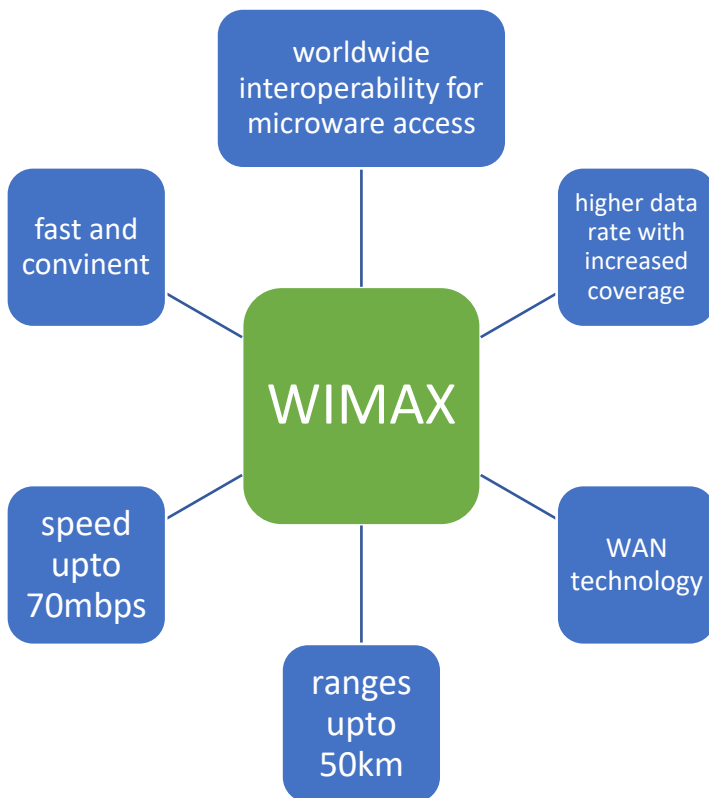
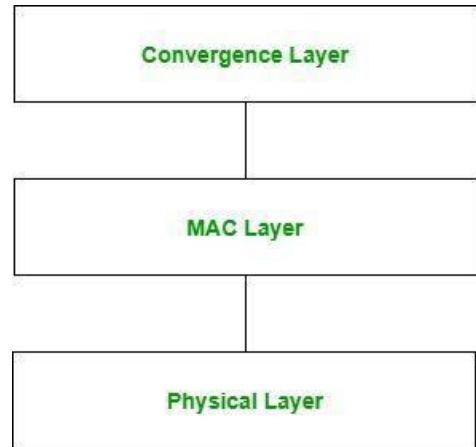
### Scatternet

- Formed with more than one piconet
- node can be slave for more than one master
- such a node can receive message from one master and send it to another master
- this node can also be called as bridge node



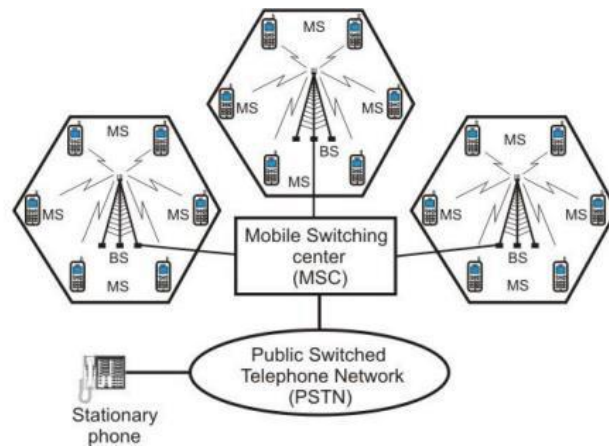
## WIMAX

- worldwide interoperability for microwave access
- based on IEEE 802.16
- provides higher data rate with increased coverage
- based on MAN technology
- ranges up to 50km
- speed up to 70mbps and can operate in non-line of sight
- it is fast convenient and cost efficient



## Cellular Telephony

- Instead of using one strong signal we use many small signals which are spread out
- This helps devices to connect over a big area
- The main purpose is to provide wireless communication between two mobile devices or one mobile and one stationary device
- MS : mobile stations used by the user to communicate
- CELL : each cellular service area is divided into small parts called as cell (5 to 20km)
- BASE STATION : each cell contains a antenna which is controlled by small office
- MSC (mobile switching office) : each base station is controlled by MSC



## Handoff

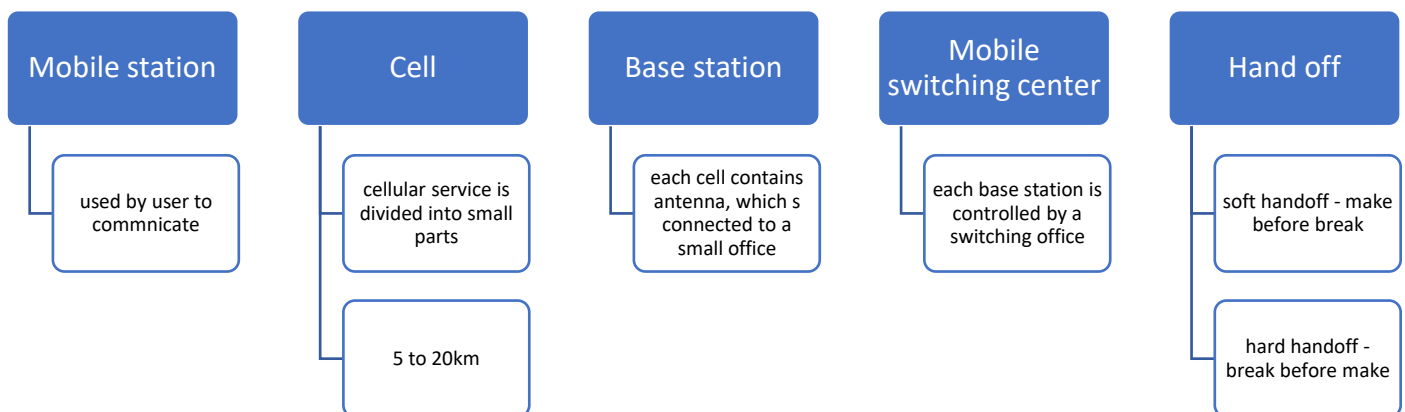
- mobile station is controlled by base station
- when the mobile station moves out of cell the base station notices the MS signal fading away and request the neighbour BS to report the strength of MS signal
- then the BS transfers the ownership to the cell which has strongest signal
- this whole process is called as handoff

## Hard handoff

- the connection breaks first then connection is established with new cell
- called as break before make
- transition is not smooth

## Soft handoff

- the MS continues with both cell A and cell B while moving from A to B
- as it moves further from A and close to B somewhere the connection is broken with A
- this is called as soft handoff
- also called as make before break



## Satellite Network

- satellite network is combination of nodes that provides communication from one point of earth to another
- a node can be satellite, earth station and end user
- transmission from earth to satellite is called as uplink
- transmission from satellite to earth is called as downlink
- uplink and downlink frequencies are different to avoid interference

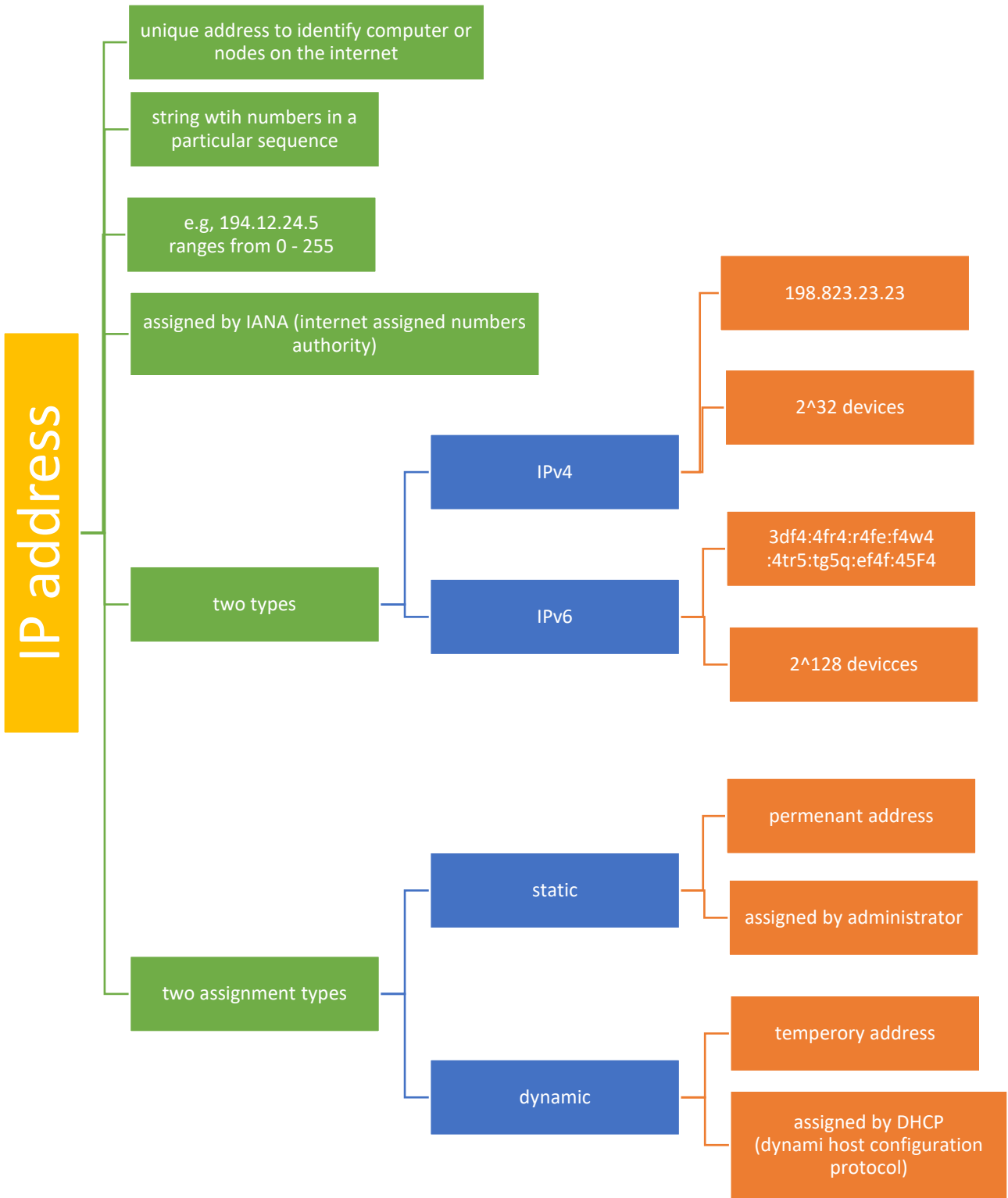
# UNIT 4

## IP address

- it is a unique address to identify a computer or a network in a network
- it is a string of numbers written in a certain format
- e.g., 192.124.32.4
- each number ranges from 0-255
- so IP address ranges from 0.0.0.0 to 255.255.255.255
- there are two types of IP addresses
- IPv4
  - 32-bit address, 4 numbers separated by dots (.)
  - Each number ranges from 0 to 255
  - Total of  $2^{32}$  devices can be connected
- IPv6
  - 128-bit address
  - 8 hexadecimal numbers separated with colons (:)
  - Total of  $2^{128}$  devices can be connected

## Types of IP address (assignment)

Static IP address	Dynamic IP address
It is a permanent address assigned to a device in a network	It is a temporary IP address that is assigned to a device or a node when it is connected to a network
Assigned by network administrator	Assigned by DHCP server
Less secure	More secure
Does not change again without human interface	Changes every time it is connected to a different network

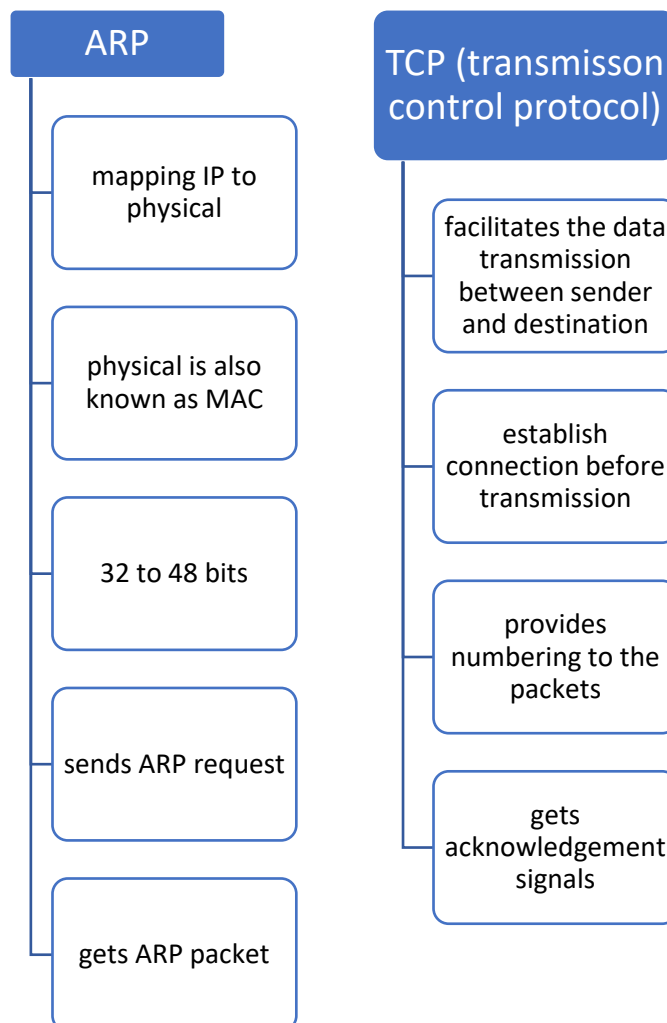


## ARP

- Arp stands for address resolution protocol it is used to map IP address to MAC address
- It translates 32-bit IP address to 48-bit MAC address
- example
  - If A wants to communicate with B
  - A knows the IP address of B, but does not know its MAC address
  - To find MAC address A send ARP request to B
  - B will reply with ARP reply listing its MAC address

## TCP

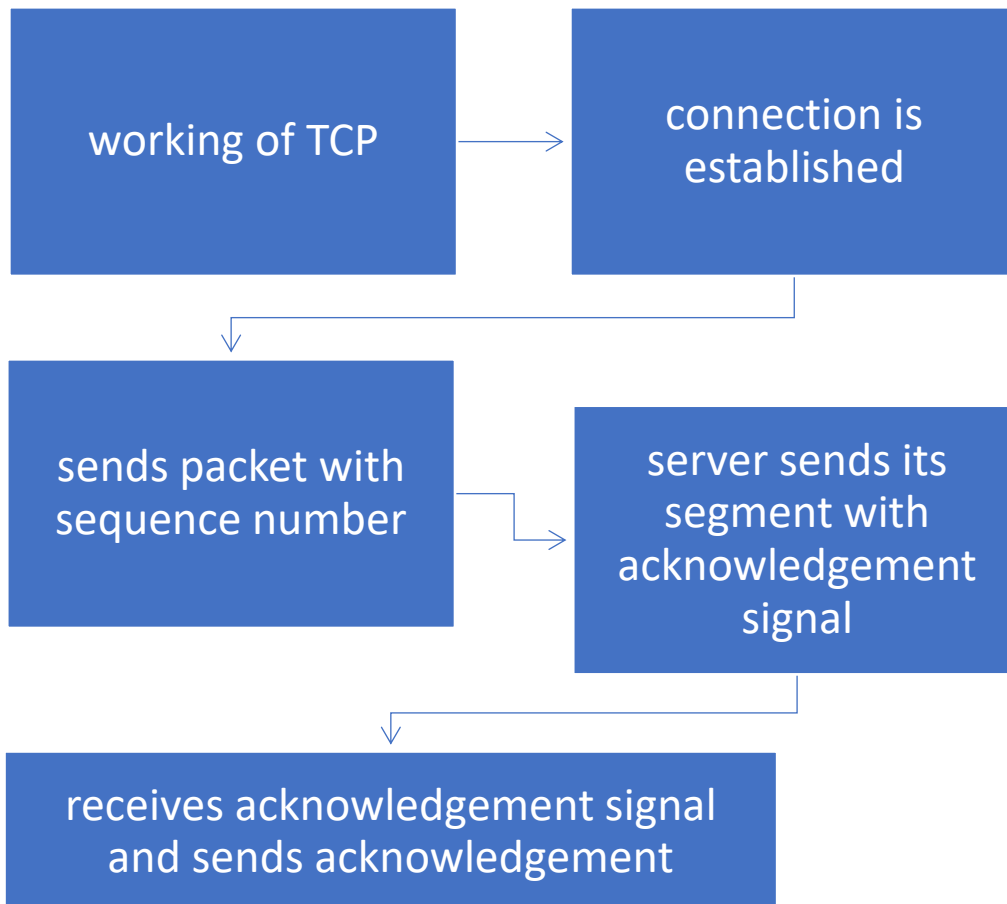
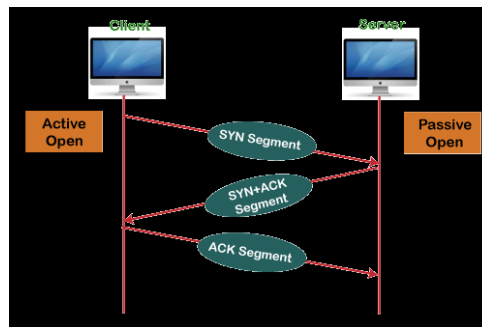
- TCP stands for transmission control protocol
- It is a transport layer protocol
- It is used to transmit data from sender to receiver
- It has an acknowledgement mechanism for error control
- It maintains the order of data





## Working of TCP

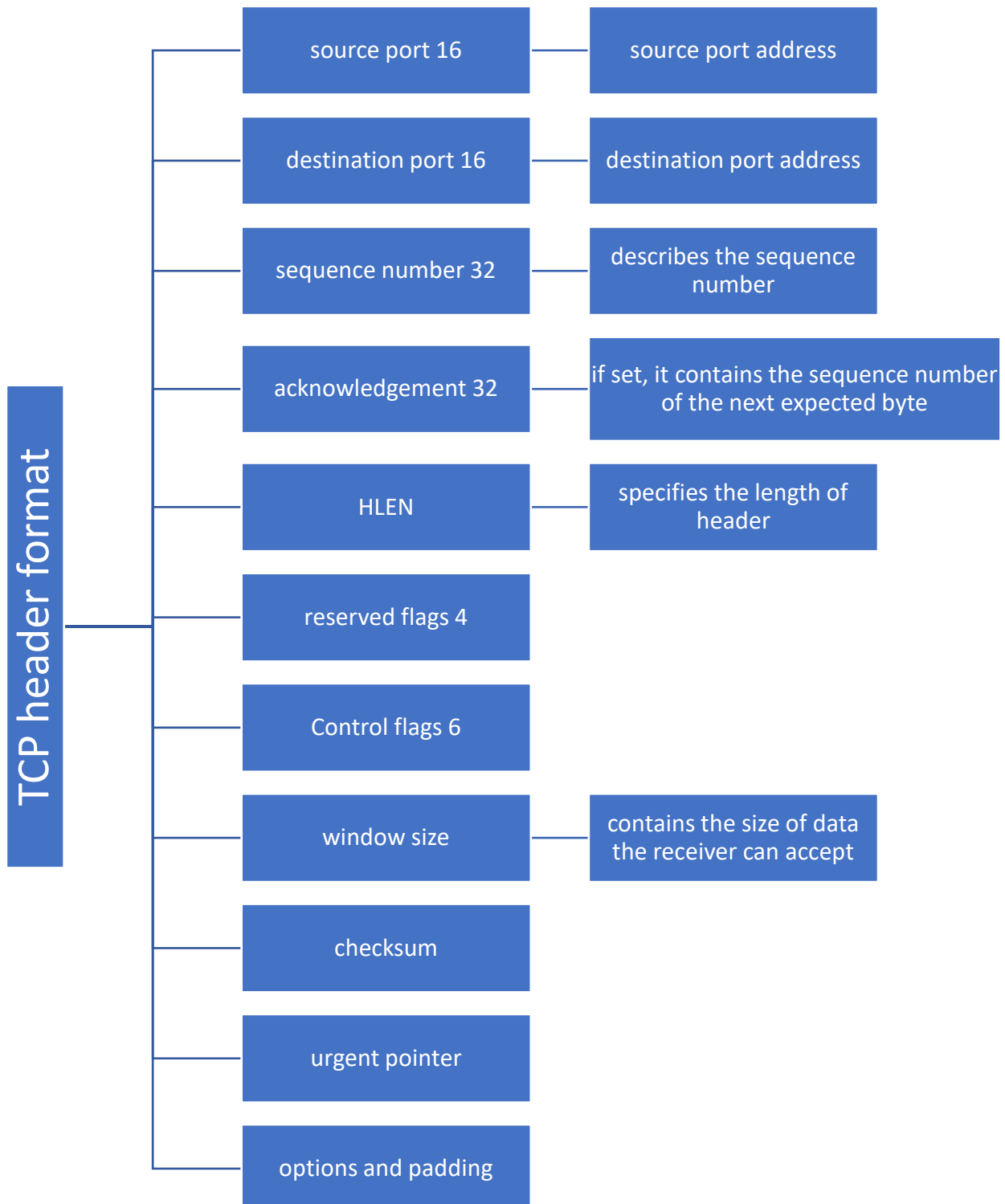
- TCP, the connection is established using 3-way handshake
- The client sends segment to the server
- The server sends its own segment with acknowledgement signal in return
- The client receives this acknowledgement signal then sends acknowledgement to the server
- This is how connection is established



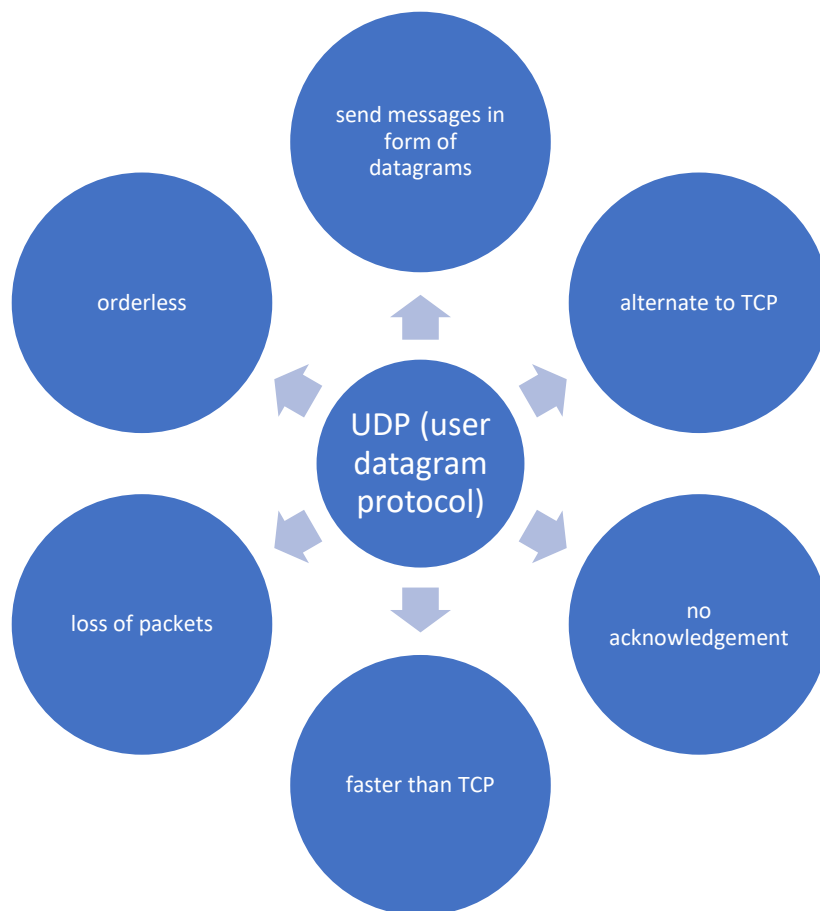
## TCP ports

- There are 65,535 ports
- 0-1023 : common ports
- 1024-49151 : registered ports

## TCP header format



TCP	UDP
Acknowledgement signal	No acknowledgement signal
Transmission control protocol	User datagram protocol
Slower than UDP	Faster as compared to TCP
Data packets are in order	Data arrives in order or receipt
Keeps track of data packets to ensure no data is lost	Does not keeps track, data loss might be unknown



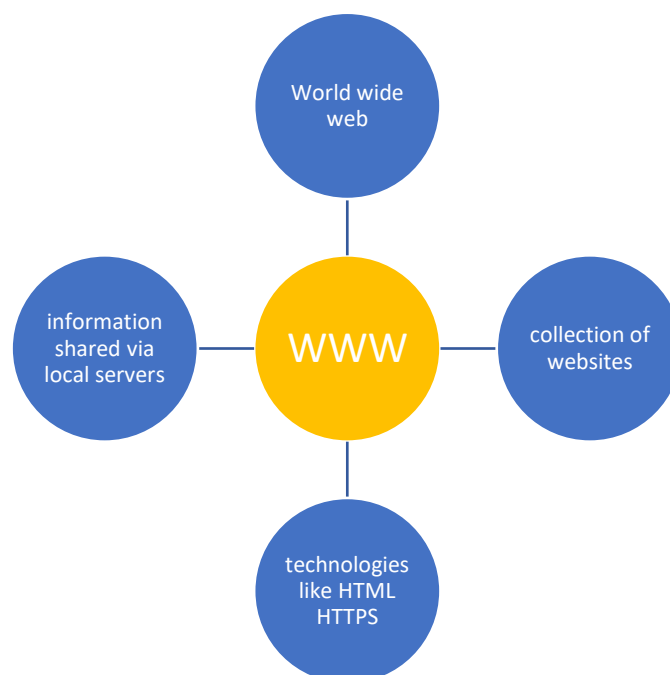
## UDP

- UDP stands for user datagram protocol
- It is a transport layer protocol
- It is used to transmit data from sender to receiver in the form of datagrams
- It is alternate to TCP
- It has not acknowledgement mechanism for error control
- Creates no virtual path to transfer data
- Delivery of data is not guaranteed
- Faster as compared to TCP

# UNIT 5

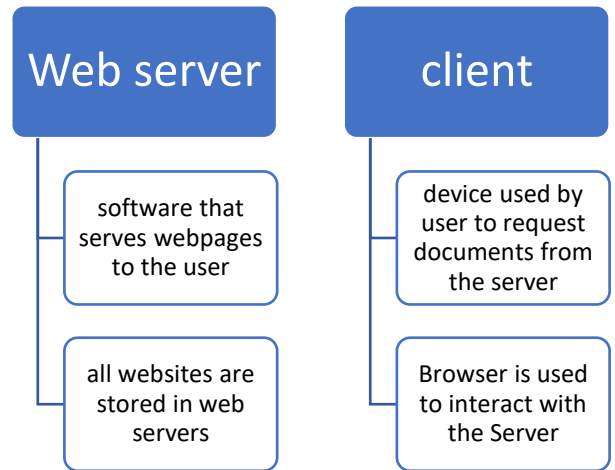
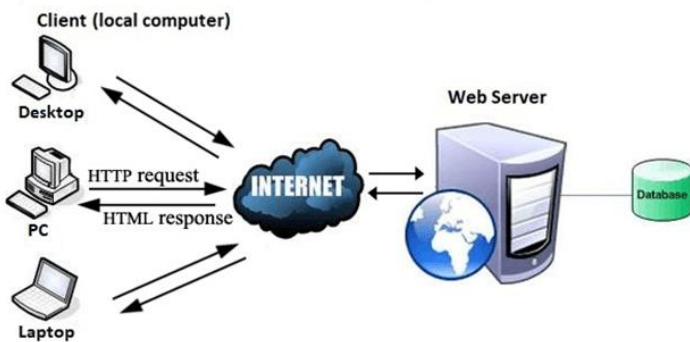
## WWW

- World wide web
- It is the collection of different websites
- These websites contain information shared via local servers
- It is based on technologies such as HTML, HTTP
- HTTP provides communication between server and browser



## Working of WWW

- Web works as per internet's basic client – server format
- Server transfers the web pages or information to the user's computer when requested by the user

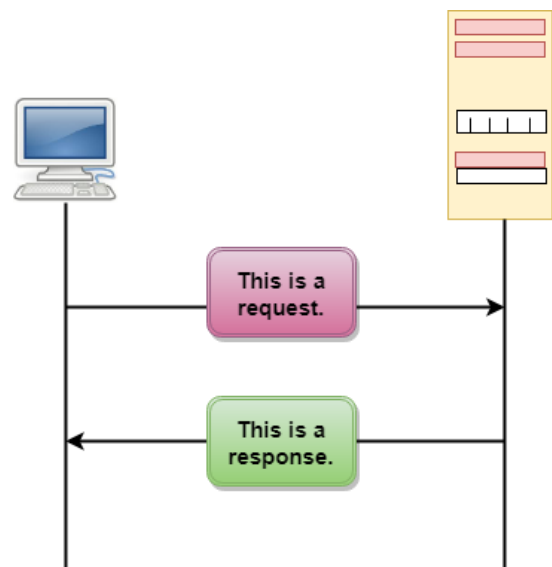


## HTTP

- Stands for hypertext transfer protocol
- Used to access data from the world wide web (WWW)
- It can be used to transfer data in the form of plain text, audio, video and may more

## HTTP transaction

- client initiates the transaction by sending request to the server
- the server replies by sending response message

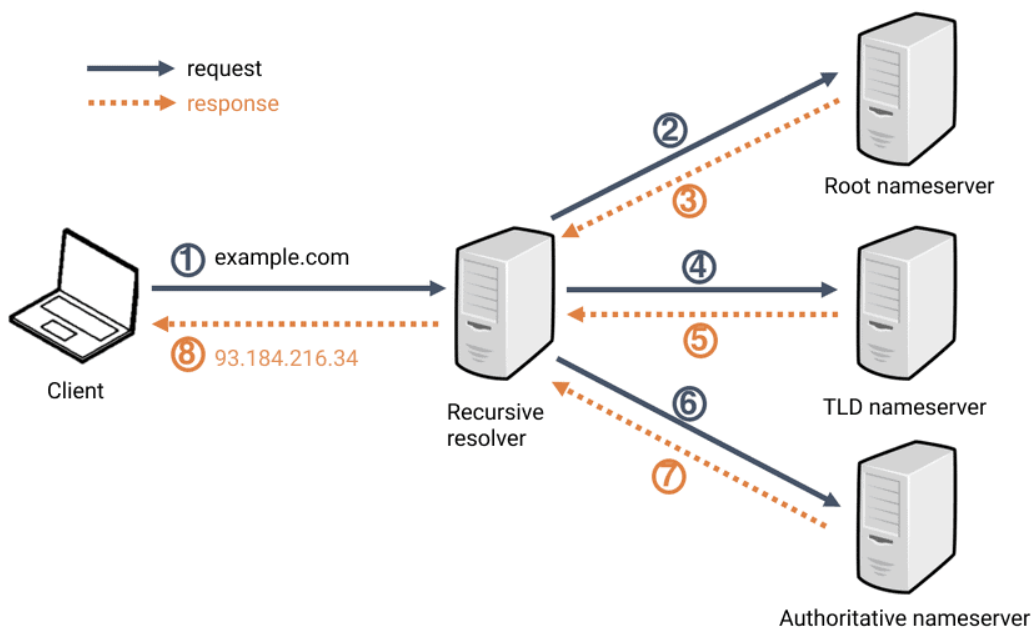


## DNS

- DNS stands for Domain Name System
- Domain name is used as an identification of the website
- It is used in the place of IP address to make it easy for consumers to visit website
- A database is used to store the name of hosts which are available on the internet

## Working of DNS

- When Client sends request, the DNS sends the request to the DNS server to fetch the IP address
- if the server does not contain the IP address with the hostname, it will send request to another DNS server
- when the IP address is fetched the request gets completed



## Root name server

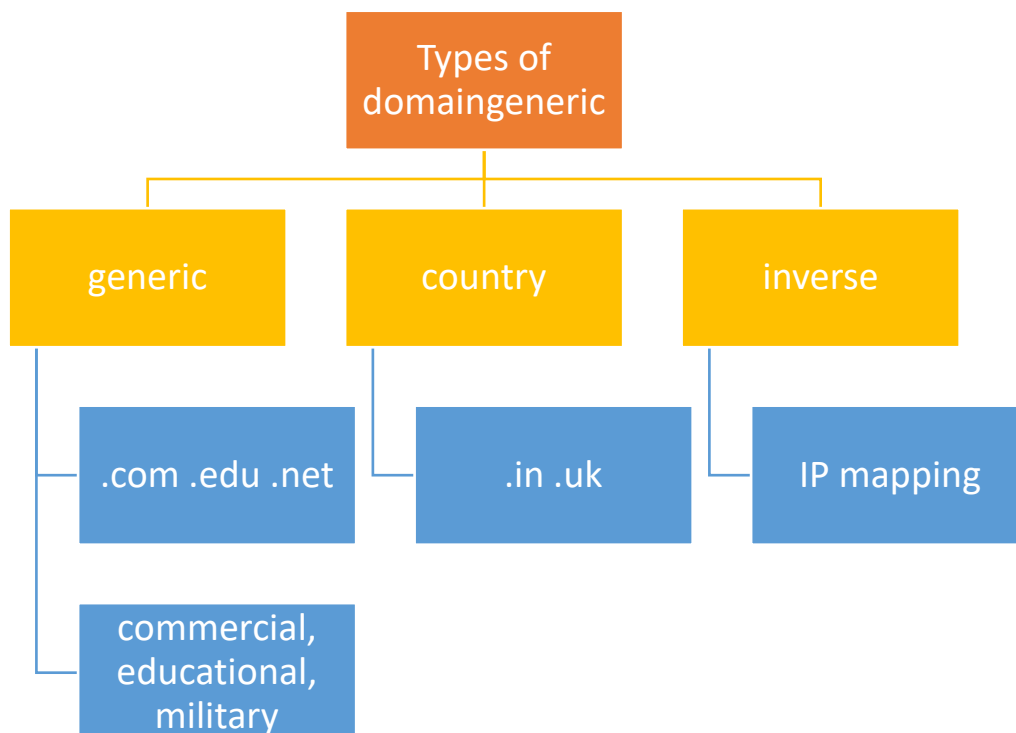
- translates human readable hostnames to IP address

## TLD (Top Level Domain)name server

- it hosts the last portion of hostname (.com, .in)

## Authoritative name server

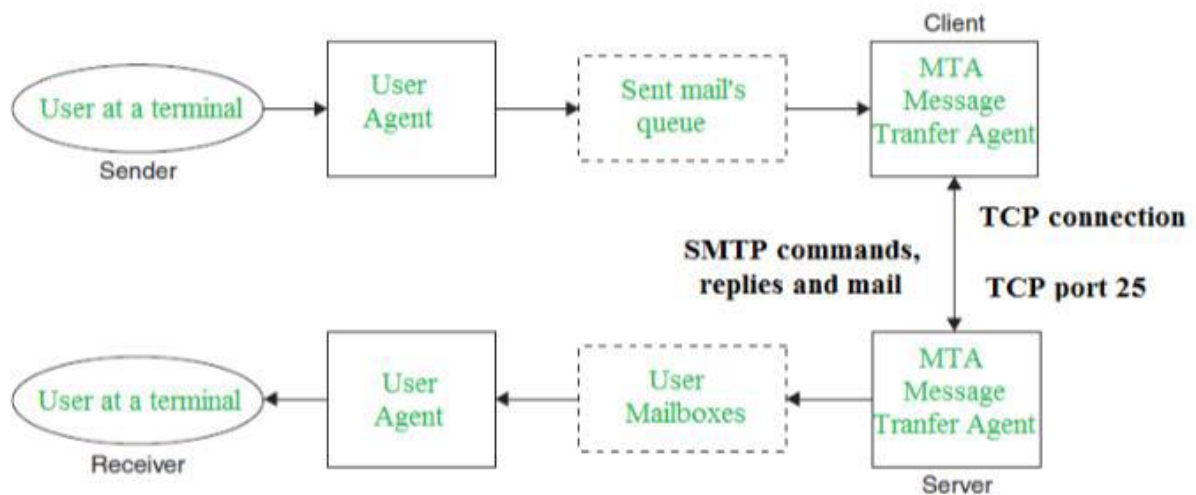
- if this server has the access of the requested record, it will return the IP address of the hostname to the DNS





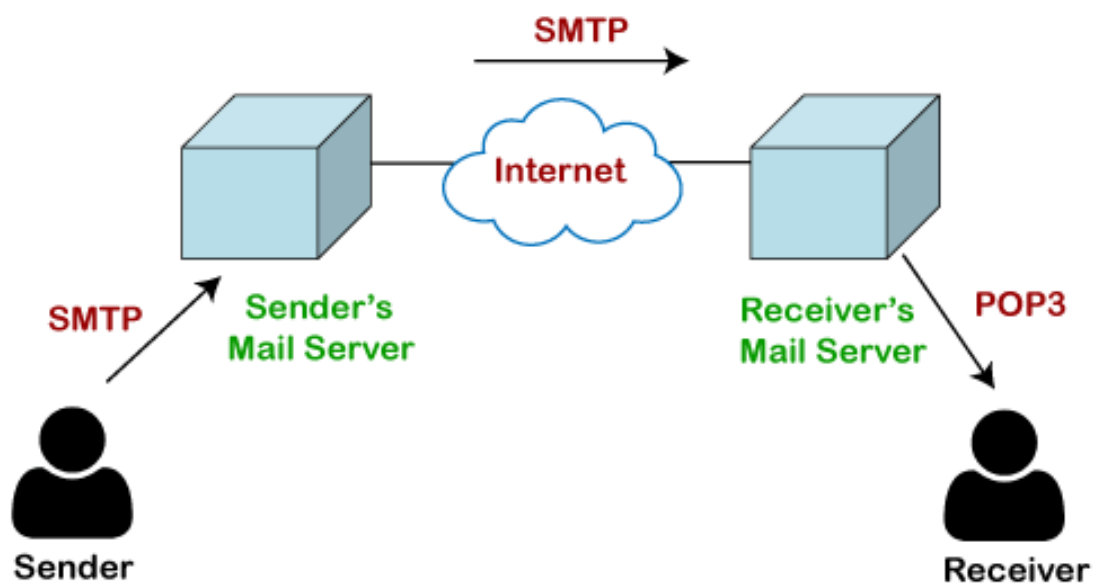
## SMTP (simple mail transfer protocol)

- transfer electronic mails



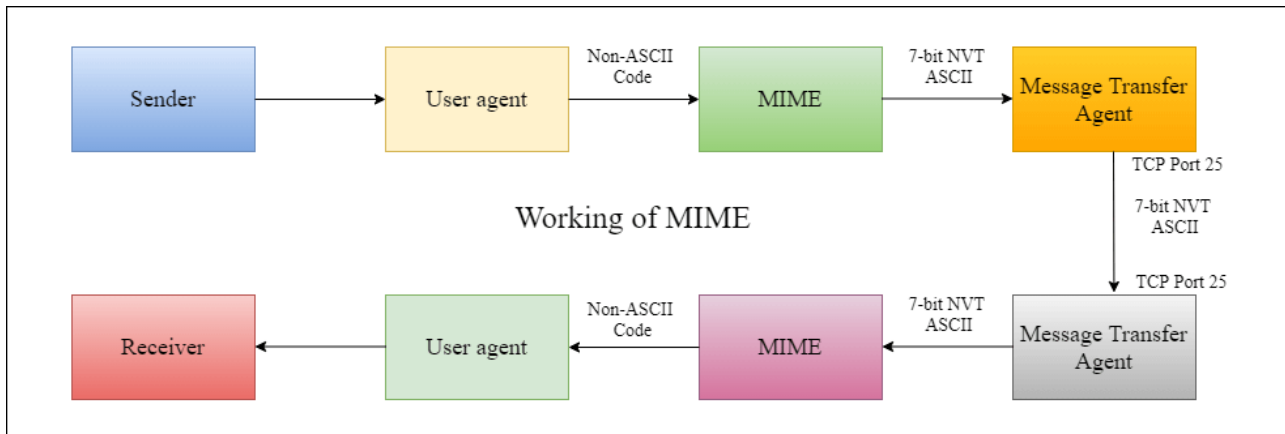
## POP3 (Post Office Protocol 3)

- retrieve emails



## MIME (multipurpose internet mail extension)

- can send images, audio, video etc



## DHCP (Dynamic Host Configuration Protocol)

- it allocates IP address to the user devices

