Computer Network

A computer network is a set of nodes like computers and networking devices that are connected through communication for the purpose of communication and sharing resources(hardware/software) among the users.

Networks are used to:

(Benefits of computer network)

- Facilitate communication through email / video conferencing / instant messaging or any other mode.
- Share hardware devices like a printer or scanner
- Enable file sharing
- Share software or operating programs
- Share information

Disadvantages of computer network

Lack of robustness, security issue, cost of network

Computer Network

Structure of a network

The geometrical arrangement of computer resources, network devices along with communication channel is known as Network structure or Network topology.

Topology can be physical or logical

- Physical Topology - physical layout of nodes and cables in the network.
- Logical topology - the way information flows between different components.

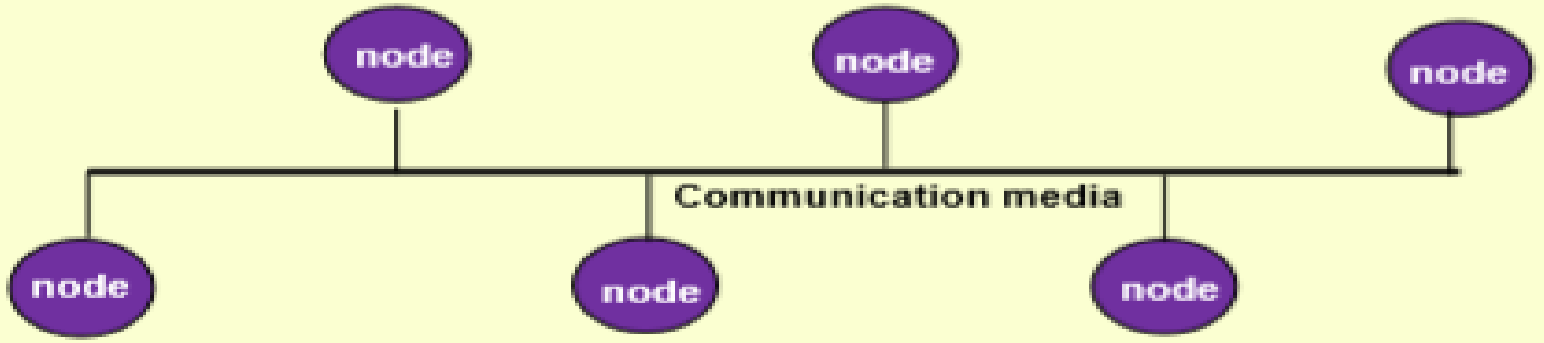
Types of Physical Network Topologies

- Bus Topology
- Star Topology
- Ring Topology
- Mesh Topology
- Tree Topology
- Hybrid Topology

Computer Network

Bus Topology

Nodes are connected through a common communication media like diagram given below.



Advantages of a Bus topology

- Easy to install
- Minimal Cable

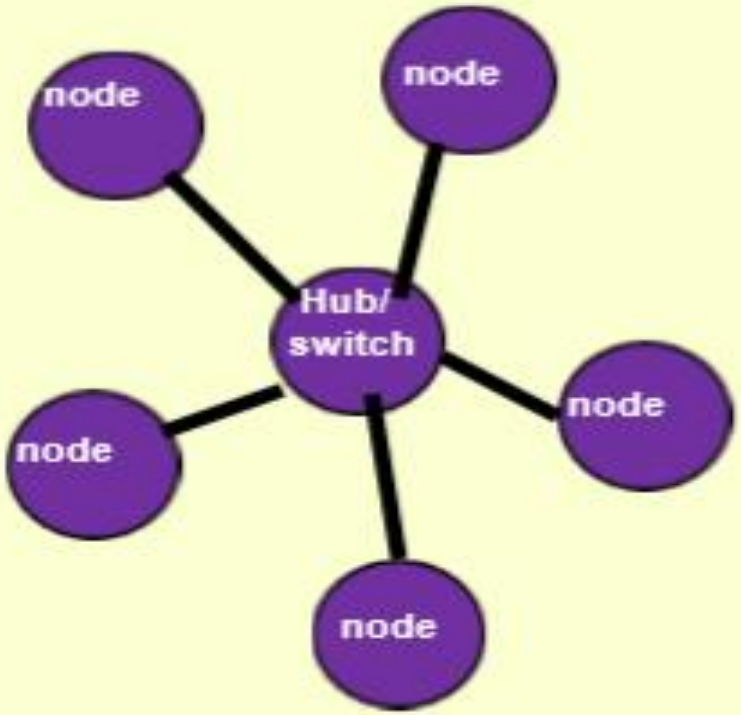
Disadvantages of a Bus topology

- Difficult reconnection
- Difficult to find the problem
- Difficult to add new devices
- Break stops all transmission of data

Computer Network

Star Topology

The star topology uses a separate cable for each node/workstation.The cable connects the node to a central device typically a HUB.



Advantages of a Star topology

- Less expensive than mesh
- Easy to install, easy to configure
- If one link fails the network can still function

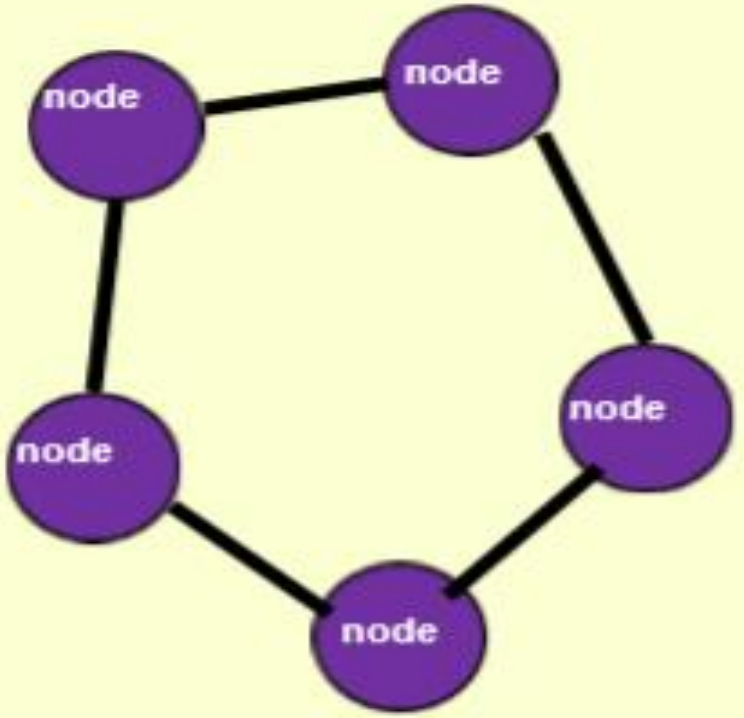
Disadvantages of a Star topology

- Everything depends on the hub

Computer Network

Ring Topology

In ring topology every computer is connected to the next computer in the ring and each transmit the signal ,what it receives from the previous computer. The messages flow around the ring in one direction.



Advantages of a Ring topology

- Easy to install
- Easy to reconfigure
- Easy to detect a problem

Disadvantages of a Ring topology

- Break means the whole system is dead

Computer Network

Mesh Topology

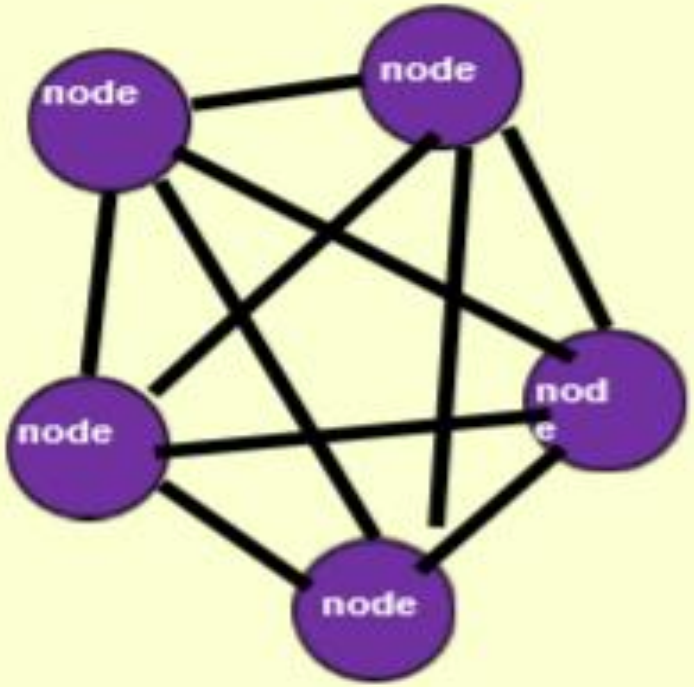
In mesh topology , separate cable is used to connect each device to every other device on the network, providing a straight communication path.

Advantages of a Mesh topology

- Avoid traffic since each link can carry its own data and none are being shared
- If one link breaks, the rest of the network is still functional
- Easy to detect a problem in the network by discovering which device is having problems and examining the link that connects to it.

Disadvantages of a Mesh topology

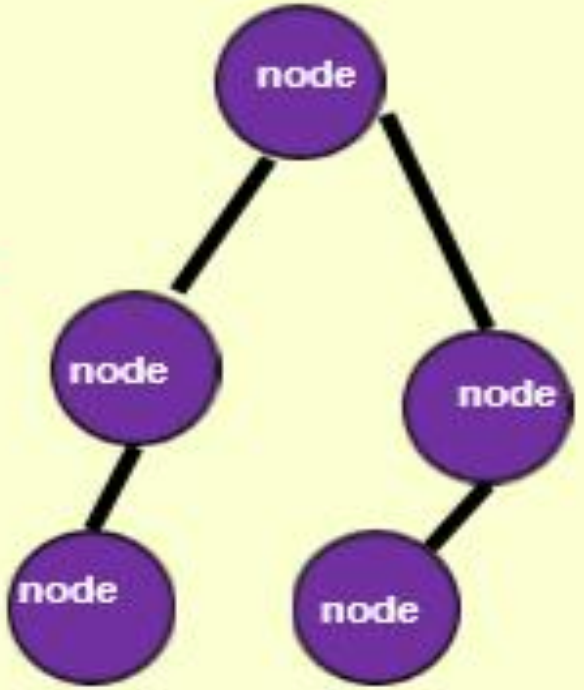
- A lot of cables are needed
- Too many cables means too much cost
- Too many cables means complex network



Computer Network

Tree Topology

In which a central root node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy



Advantages of a Mesh topology

- It is scalable.
- Easier fault identification and isolation.

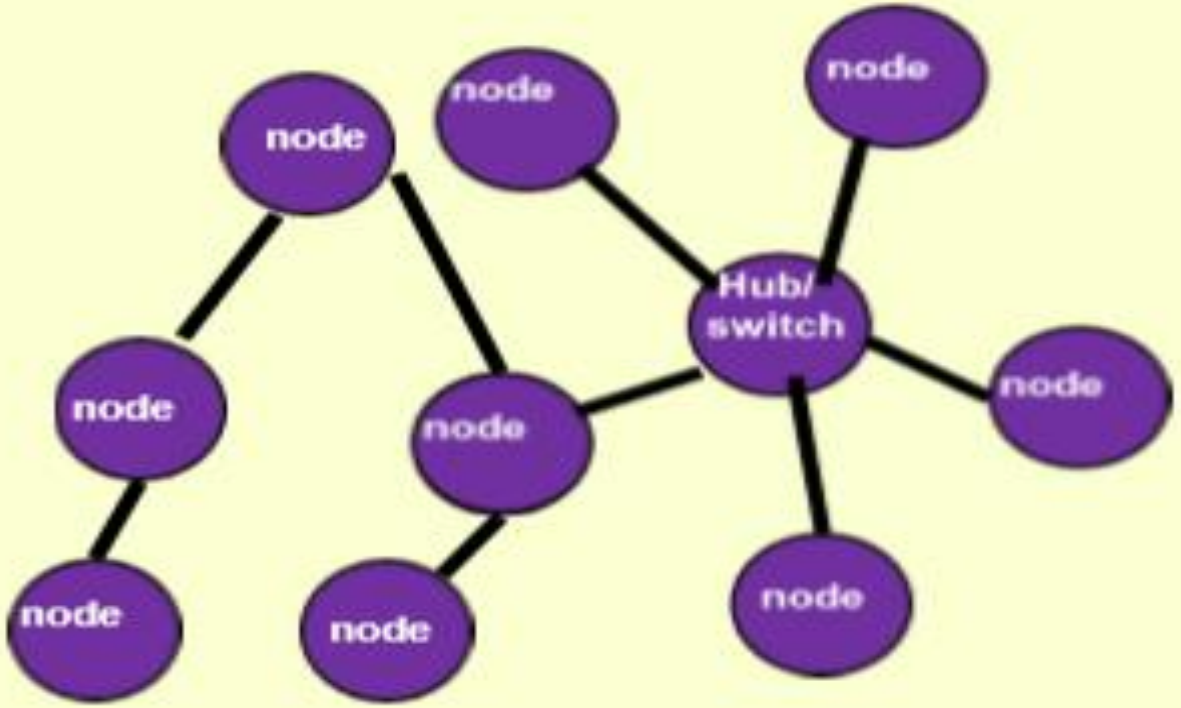
Disadvantages of a Mesh topology

- Maintenance of the network may be an issue when the network spans a great area.
- if the backbone fails, the entire network is crippled.

Computer Network

Hybrid Topology

use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.).



Computer Network

Types of network

1. Local Area Network (LAN) – limited area (within building)
2. Metropolitan Area Network (MAN) – within city
3. Wide Area Network (WAN) – within multiple city/state/ countries

Computer Network

1. **Local Area Network (LAN)** – LANs are the most frequently used/discussed networks.It is one of the most common one of the simplest types of network.It is designed for small physical areas such as an office, group of buildings.Any of different types of topologies can be used to design LAN like Star, Ring, Bus, Tree etc.

Characteristics of LAN

- private networks means no need of regulatory control.
- Operate at relatively high speed.
- Ethernet, Token ring etc type media access controls are used
- Connects computers in a single building, block or campus.

Computer Network

Advantages of LAN

- Resource Sharing
- Software Applications Sharing
- Easy and Cheap Communication
- Centralized Data
- Data Security
- Internet Sharing

Disadvantages of LAN

- High Setup Cost
- Privacy Violations
- Data Security Threat
- LAN Maintenance Job
- Covers Limited Area

Computer Network

2. Wide Area Network (WAN) –Slightly more complex than a LAN, a WAN connects computers across longer physical distances. The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by any single person or owner.

Characteristics of WAN

- Covers large distances(states, countries, continents).
- Communication medium like satellite, public telephone networks etc and routers are used establish connection.

Computer Network

Advantages of WAN

- Long distance business can connect on the one network.
- Shares software and resources
- Messages can be sent very quickly to wide range of nodes
- Hardware devices can be shared.

Disadvantages of WAN

- Need a good firewall to restrict unauthorized access
- Setting up a network can be an expensive, slow and complicated.
- Maintaining a network is a full-time job
- Security is a mazor issue when many different people have the ability to use information

Computer Network

Difference between The Internet and The Web

The Internet is a global network of networks while the Web, also referred formally as World Wide Web (www) is collection of information which is accessed via the Internet.

	Internet	World Wide Web
Estimated year of beginning	1969, though opening of the network to commercial interests in 1988	1993
First version	ARPANET	NSFnet
Components	Network of Computers, wires, optical fiber, wireless network	Files/folders/ documents stored in computers
Governed by	Internet Protocol	Hyper Text Transfer Protocol
Dependency	Independent of the World Wide Web	Depends on Internet to work
Nature	Hardware	Software

Cloud computing

Cloud Technologies/Computing

Cloud computing facilitates to access the applications as utilities ,over the internet.It allows us to create , configure and customize applications online.

It is a kind of distributed computing on internet or delivery of computing services over the internet.
e.g. gmail,Hotmail,yahoo etc.

Instead of running an email program on our computer , we log in to a web email account remotely,The software and storage of our account doesn't exist on our computer – it's on the service's computer cloud.

Cloud computing

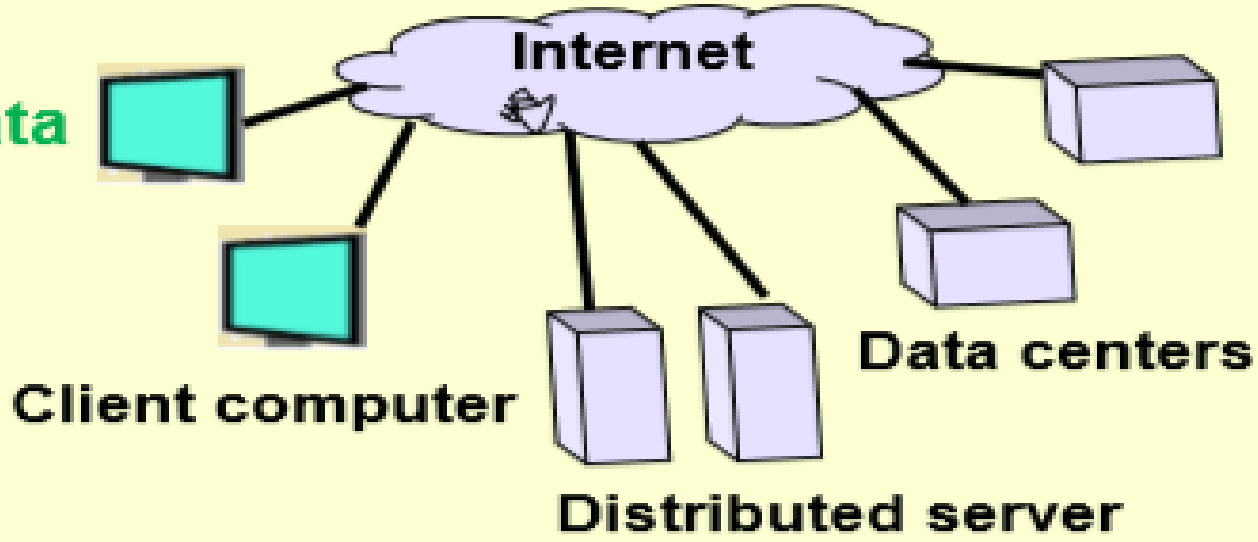
History of Cloud Computing

The concept of cloud computing evolved in 1950(IBM) called RJE (Remote job entry process)

In 2006 amazon provided first public cloud AWS(Amazon web service)

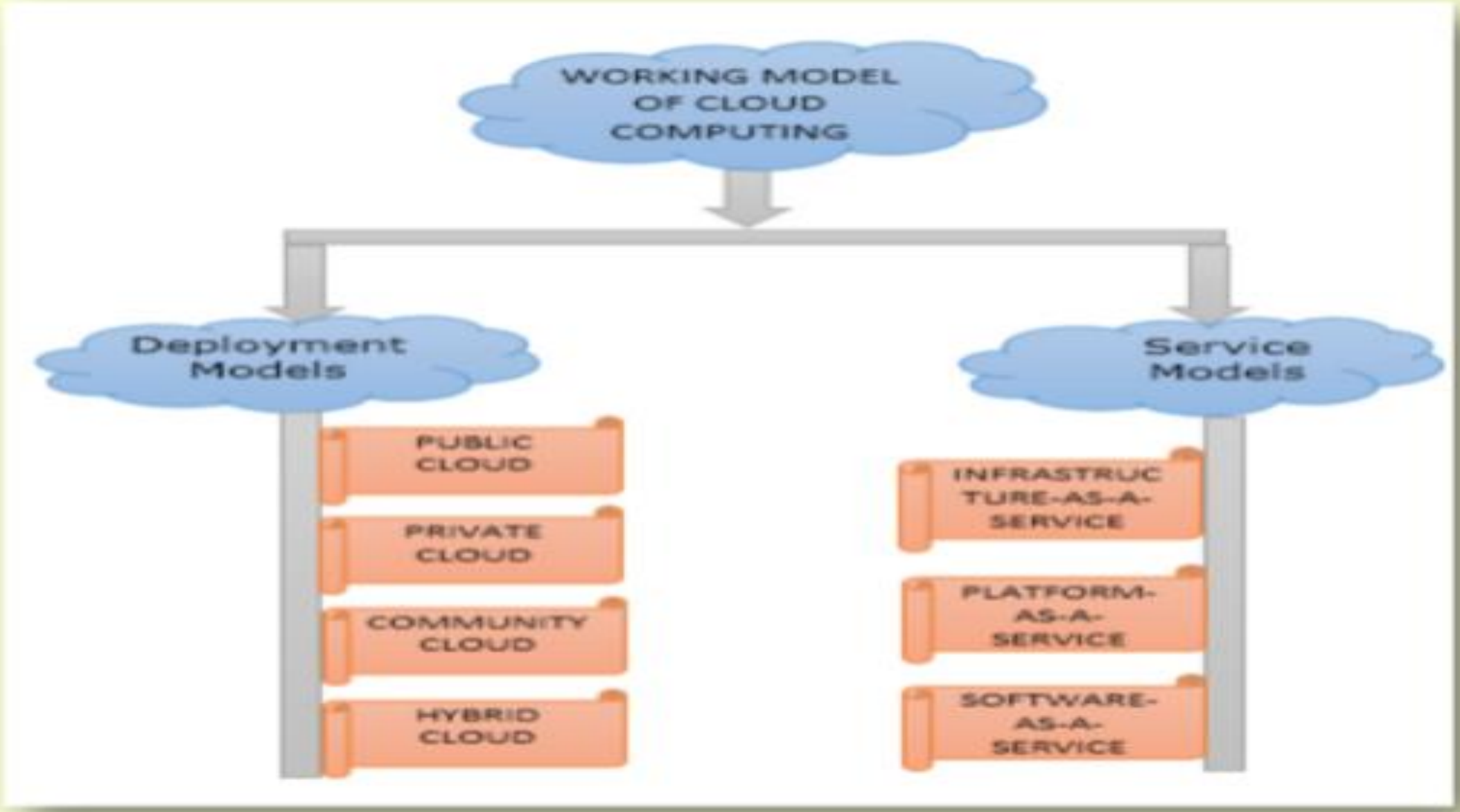
Cloud components

1. **Client** – mobile, pc
2. **Distributed servers** - multiple servers to improve processing
1. **Data centers** – Collection of server where applications/data are stored



Cloud computing

WORKING MODELS FOR CLOUD COMPUTING



Cloud computing

DEPLOYMENT MODEL

- PUBLIC CLOUD –

  For general public.
- PRIVATE CLOUD –

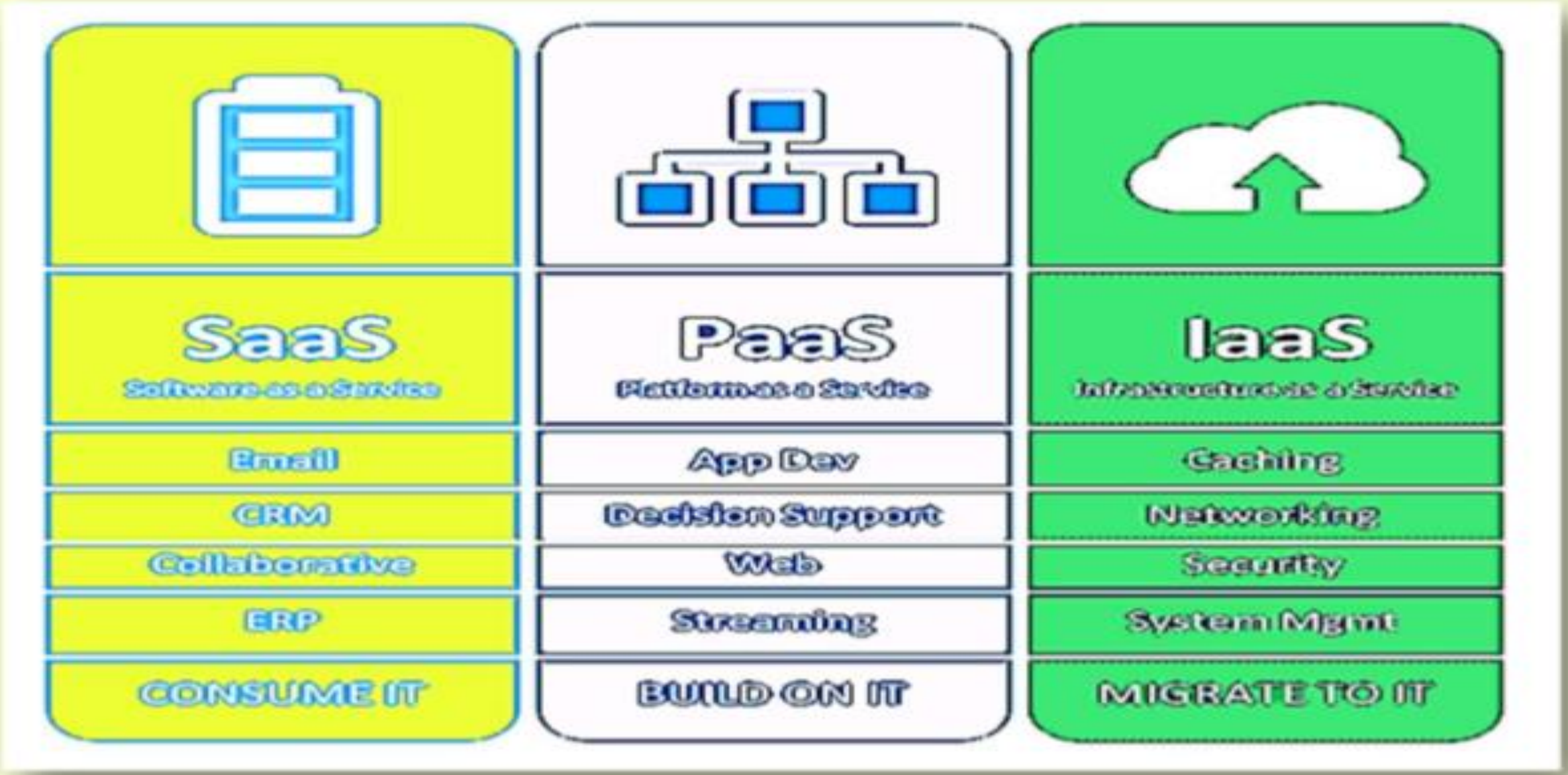
  For an organization only
- COMMUNITY CLOUD -

  For group of organizations.
- HYBRID CLOUD –

  Mixture of public and private cloud

Cloud computing

WORKING MODELS FOR CLOUD COMPUTING



Cloud Computing

Private Cloud Storage

It is a type of storage mechanism that stores an organization's data at in-house storage servers by cloud computing implementation.

It is not publicly accessible and is owned by a single organization and its authorized external partners.

Private cloud storage is also known as internal cloud storage.

Cloud Computing

public cloud storage

It is also called storage-as-a-service, on-line storage or utility storage, is a service model for data storage on a pay-per-use basis.

It is often used for backing up data as disaster recovery plan (DRP) as well as archiving email and static non-core application data. It's Usage is generally charged on a dollar-per-gigabyte-per-month basis.

Provider public cloud is responsible for building and maintaining the storage infrastructure and its associated costs including power, cooling and server maintenance.

Cloud Computing

Features & Benefits	Private Cloud	Public Cloud
Access and Storage	Restricted access and Dedicated storage for one organization	Available to multiple organizations and Data stored on a shared infrastructure.
Location Of The Data Center	dedicated location on the service provider's infrastructure.	Location of the data center varies
Investment	Higher investment	Comparatively lower investment
Security	Superior security mechanism.	Offers a standard security protocol
Customization	Allow companies to customize their cloud	Offers a standard operating procedure for organizations
Costs	1. Expensive	Less expensive

Cloud Computing

Why cloud services are being popular?

- It reduces the complexity of networks
- No need to by software licenses
- Customization
- Scalable and reliable
- Information stored at cloud is not lost easily

Application

- Email sites
- Social media/networking sites
- Search engines etc

IOT

Internet of Things-IOT

The IOT concept was initially proposed by a member of the Radio Frequency Identification (RFID) development community in 1999, and now it has become more relevant to the practical world as the use of mobile devices, embedded devices,communication, cloud computing and data analytics has increased.

Internet connects all people means "Internet of People"
IoT connects all things means "Internet of Things"

Interconnection of Things/Objects/Machines, e.g., sensors, mobilephones, electronic devices, home appliances, any existing items and interact with each other via Internet.

Internet of Things technology can include any sensor, electronic devices or software which are connected to the internet and can be utilized remotely and can exchange data. Here devices works themselves without human intervention for the welfare of humans.

IOT

MAJOR CHARACTERISTICS OF IOT

- Very Large Scale
- Heterogeneity
- Pervasivity - Computing and Communication technologies embedded in our environments

IOT

How Does the Internet of Things Work?

The Internet of Things is an aggregation of internet enabled sensors, smart devices and software that can be manipulated by scripts, applications and user interfaces across long distances.

Applications of IOT

- **Smart house** - Suppose we are not at home and doubts starts in our mind. Did I turn the coffee maker off? Did I set the security alarm? etc.
  With a smart home,we can quiet all of these worries with a quick glance at smartphone/tablet. we can connect the devices and appliances in our home so they can communicate with each other and with us and can work with the commands given over smartphone remotely.

- **Smart car** - the driverless car (now a prototype) where taxis work based on AI and take the passengers safely and accurately to the desired destination.

IOT

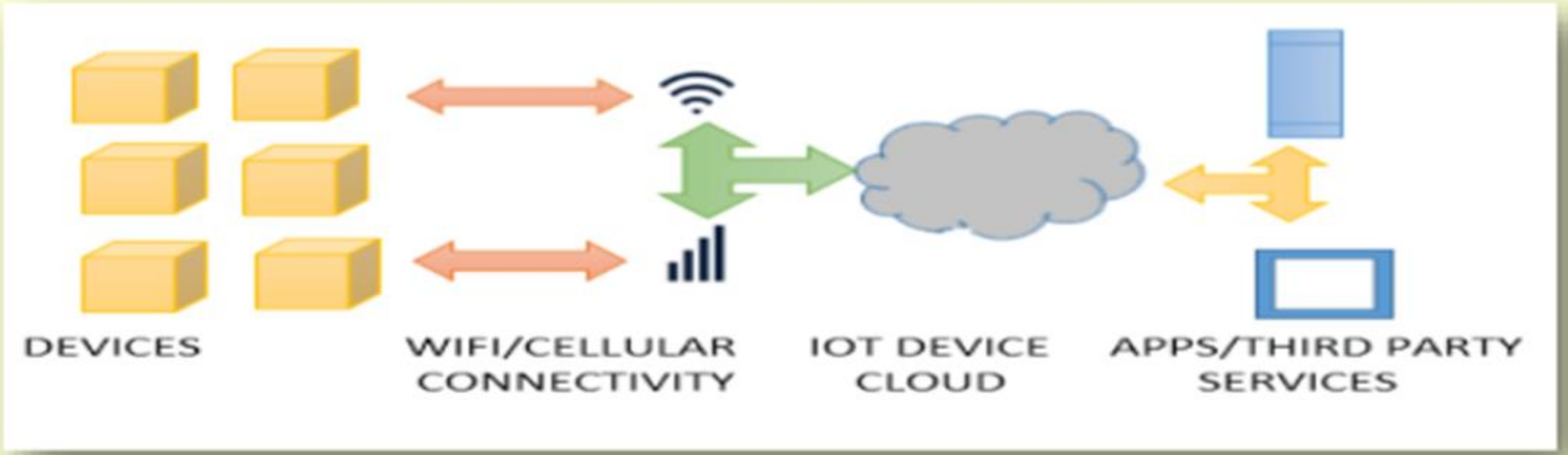
Applications of IOT

- **Elderly care-** Patient surveillance can be life-saving; automatically detecting when someone falls down or when they begin to experience a heart attack so that emergency care can be sent immediately.
- **Disaster warning-** Sensors can collect critical information about the environment, allowing for early detection of environmental disasters like earthquakes, tsunamis, etc., thus saving lives.
- **Delivery Drones** – drones being used to deliver item with the help of smart grid/geospatial data.
- **Smart Toothbrushes** - The smart toothbrushes allow users to visualize the inside of their mouths via mobile app. Users are able to see which areas of their mouth require brushing and can even keep a daily log of their brushing habits.

Many more things are there/under development as under IOT

IOT

What is an IoT Platform?



It is an integrated service which offers the things to bring physical objects online. It easily allow to configure devices for machine-to-machine communication through millions of devices connects simultaneously .

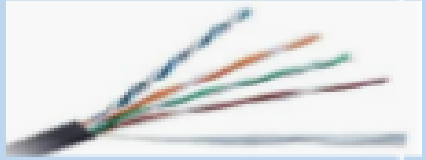
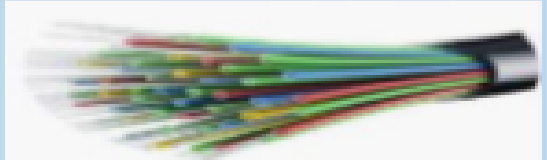
IOT

IoT Platform Types

- **End-to-end IoT Platforms** - provide the hardware, software, connectivity, security, and device management tools to handle connection of millions of concurrent device.
- **Connectivity Management Platforms** – It offer low power and low cost connectivity management solutions through Wi-Fi and cellular technologies.
- **IoT Cloud Platforms** – It's aim to get rid of the complexity of building our own complex network
- **Data Platform** – It deals with data in some way with the tools we need to route device data and manage / visualize data analytics.

wired and wireless networks

Wired Networks - It is also known as Ethernet networks, that is most common type of LAN technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables/ any form of wired media. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Computer must have an Ethernet adapter (sometimes called a network interface card, or NIC) to connect with wire. Most of the network topology uses wired networks

Cable	Twisted pair	Coaxial cable	Fiber optic
Signal form	electricity	electricity	Light
cost	least	moderate	High
speed	low	moderate	High
Ease of use	Easy to install	Professional installation	Professional installation
reliability	low	moderate	High
Real life application	Telephone network	Tv cable	Data transmission & telephone line
Data transmission rate	10Mbps – bps	100Mbps	>100Gbps
Data transfer range	100m	185m - 500m	-
image			

wired and wireless networks

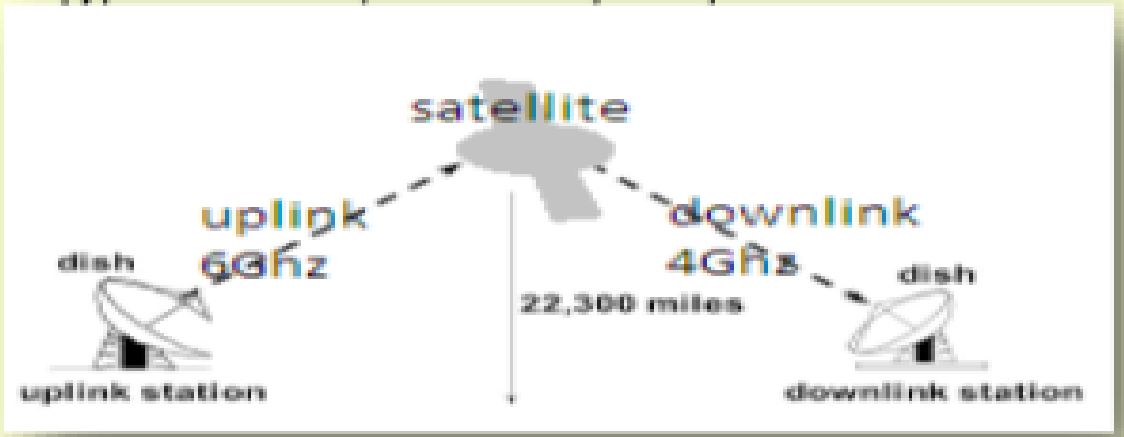
Wireless Networks – It uses high-frequency radio waves rather than wires to communicate. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure.

An peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. An infrastructure wireless network consists of an access point or a base station. Access point acts like a hub, providing connectivity for the wireless computers. There are four basic types of transmissions standards for wireless networking, produced by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps

wired and wireless networks

Satellite Communication

It provide worldwide coverage independent to population density.Satellite ommunication Systems offer telecommunication (Satellite Phones), positioning and navigation (GPS), broadcasting, internet, Mobile, TV, etc.



Microwave radio, a form of radio transmission that use. Ultra-high frequencies. It is a point-to-point, rather than a broadcast, transmission system. Additionally, each antenna must be within line of sight of the next antenna. Frequency Bands Maximum Antenna Separation Analog/Digital 4-6 GHz 32-48 km Analog 10-12 GHz 16-24 km Digital 18-23 GHz 8-11 km Digital.

Bluetooth

It provides data, voice and audio transmission with a transmission range of 10 meters. Almost all mobile phones, tablets and laptops are equipped with Bluetooth devices. They can be connected to wireless Bluetooth receivers.

wired and wireless networks

Wireless Local Area Network (WLAN)

WLAN (Wi-Fi) is an internet related wireless service. Using WLAN, different devices like laptops and mobile phones can connect to an access point and access internet.

WiMAX(Worldwide Interoperability for Microwave Access) - is a telecommunications protocol for mobile Internet access. The protocol is based on IEEE 802.16 Standard.

WiMAX's range is measured in kilometers, while Wi-Fi is measured in meters and local in nature. Wi-Fi uses an unlicensed spectrum, while WiMAX's spectrum could be licensed or unlicensed.

Infrared Communication

Infrared Communication is another commonly used wireless communication in our daily lives. It uses the infrared waves of the Electromagnetic (EM) spectrum. Infrared (IR) Communication is used in remote controls of Televisions, cars, audio equipment etc.

Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs

wired vs wireless networks

Specifications	Wired network	Wireless network
Speed of operation	Higher	lower compare to wired networks,
System Bandwidth	High	Low
Cost	Less as cables are not expensive	More costly wireless routers/access points/ adapters are expensive
Installation	Hard to install,requires more time	easy installation and need less time
Mobility	Limited	Not limited
Transmission medium	copper wires, optical fiber cables, ethernet	radiowaves or EM waves or or infrared
extension	requires hubs and switches	More area is covered by wireless base stations which are connected to one another.
Applications	LAN (Ethernet), MAN	WLAN, WPAN(Zigbee, bluetooth), Infrared, Cellular(GSM,CDMA, LTE)
Interference	Less Interference	Interference is
Quality of Service	Better	Poor due
Reliability	High compare to wireless counterpart, as manufactured cables have higher performance due to existence of wired technology since years.	Reasonably high, This is due to failure of router will affect the entire network.

concept of a client and server

In client/server architecture a client is a consumer of services, and a server is service provider. Thus the term 'client' means 'service requester', and server means 'service provider'.

Web technologies and protocols built around the client-server model are:

- Hypertext Transfer Protocol (HTTP)
- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Telnet

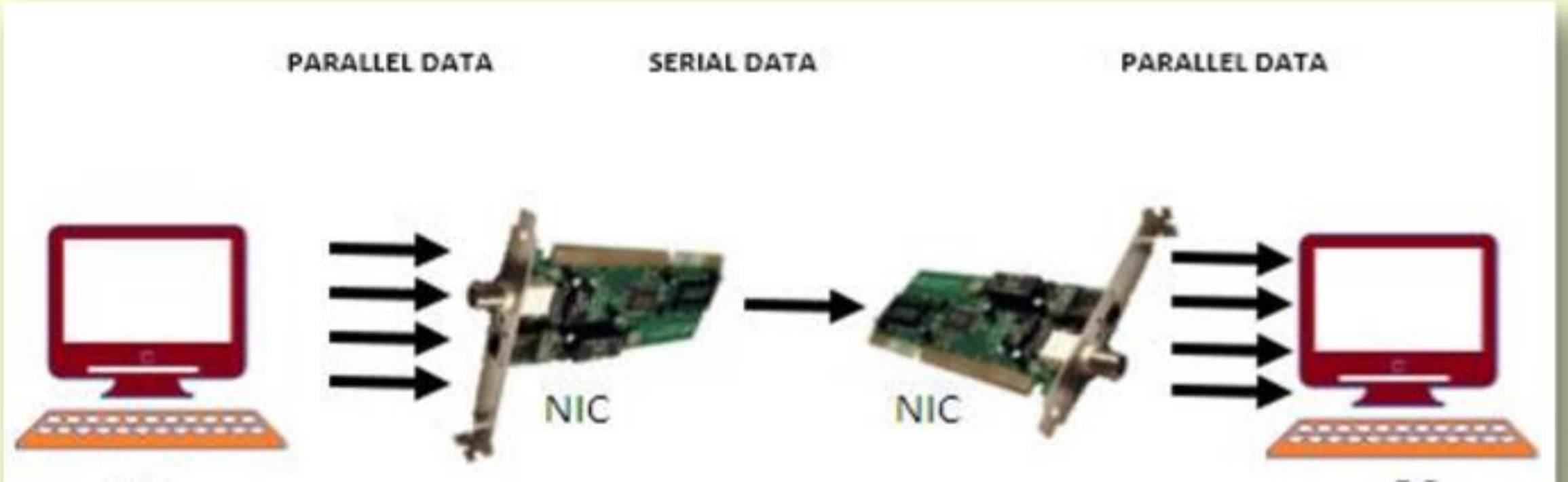
Network devices

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

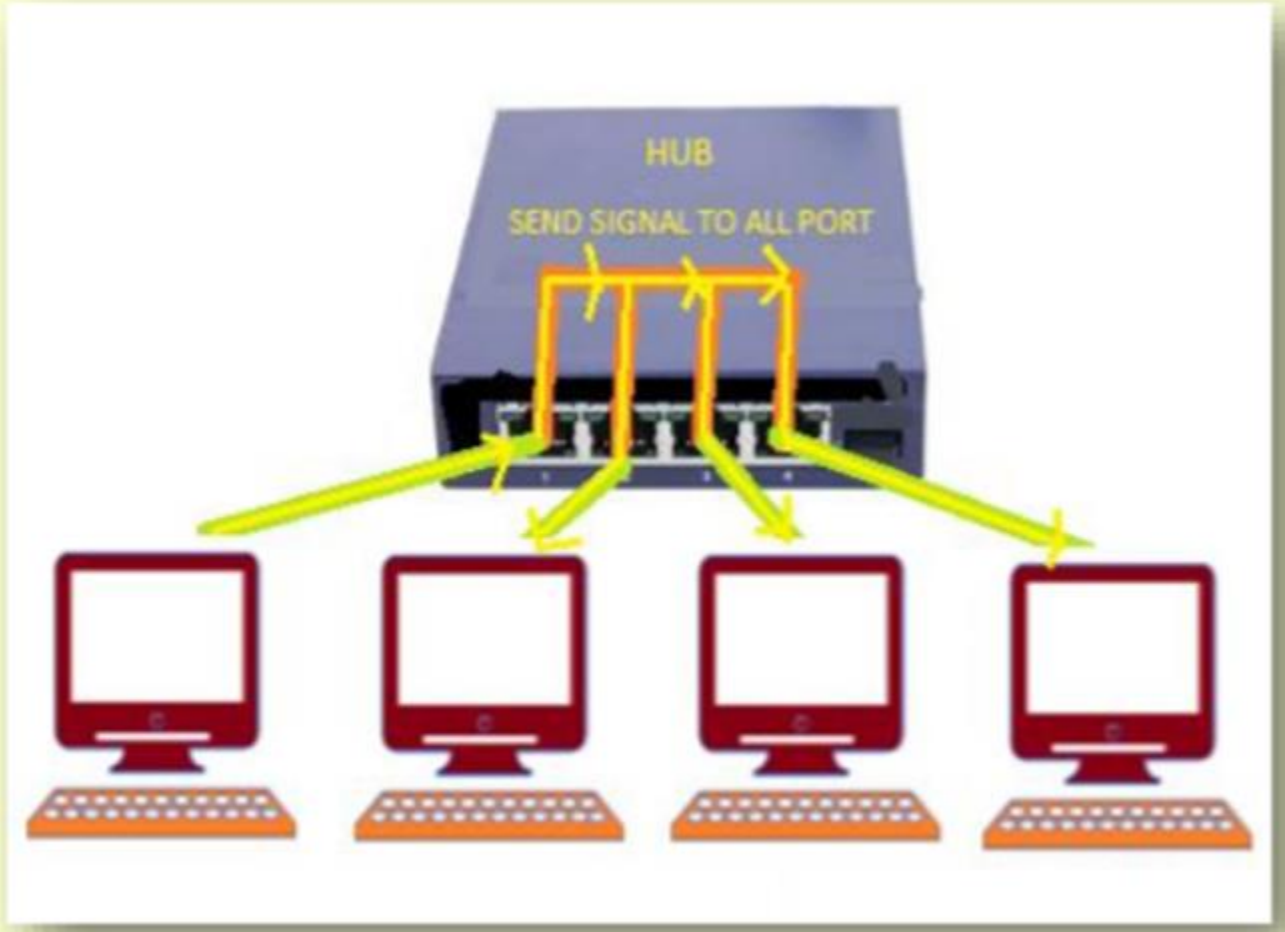
Passive HUB:- It only forwards the signal on all ports without amplifying the signal.

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:-

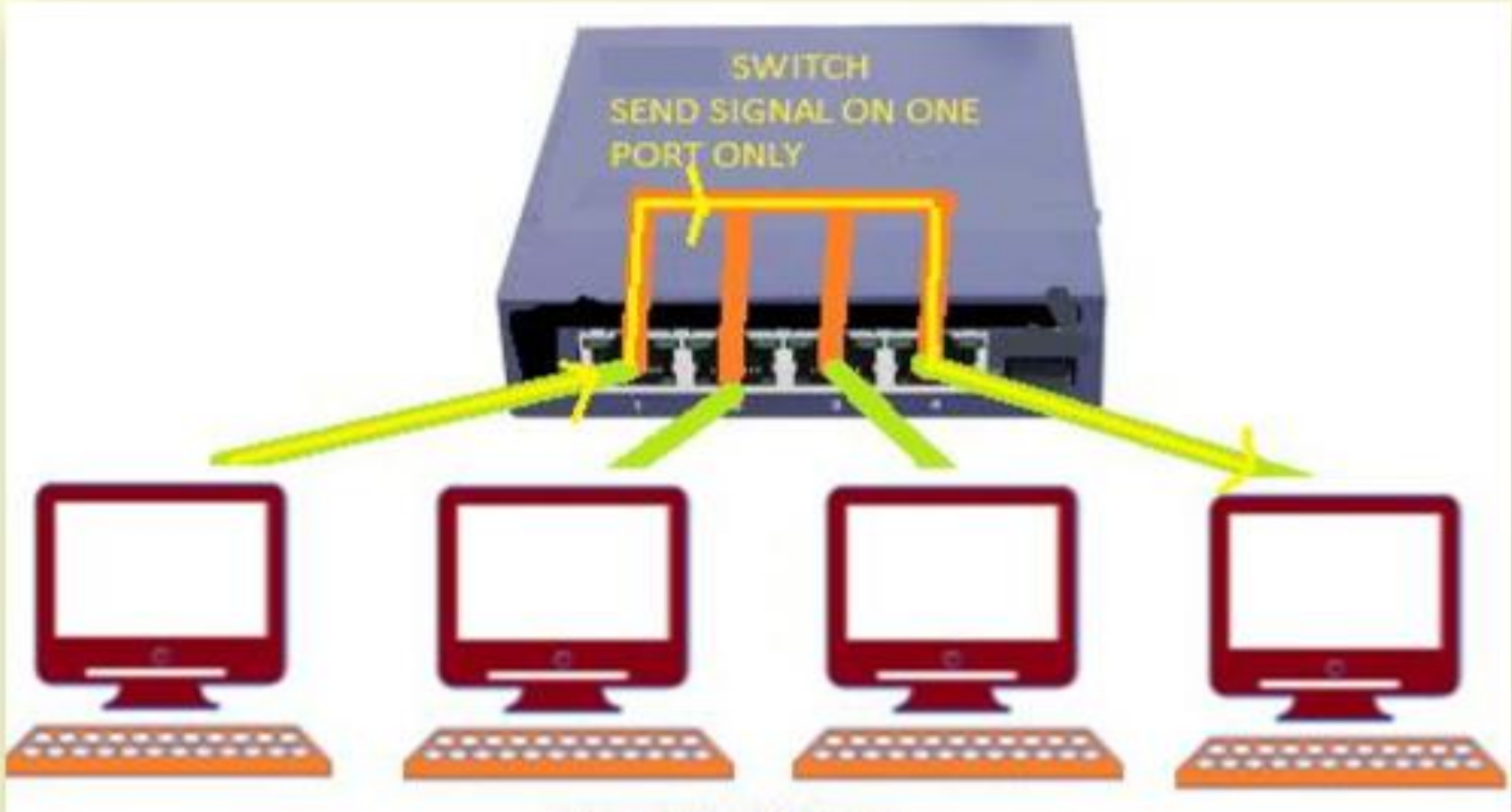
Ethernet HUB :- All ports have RJ-45 connectors.

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



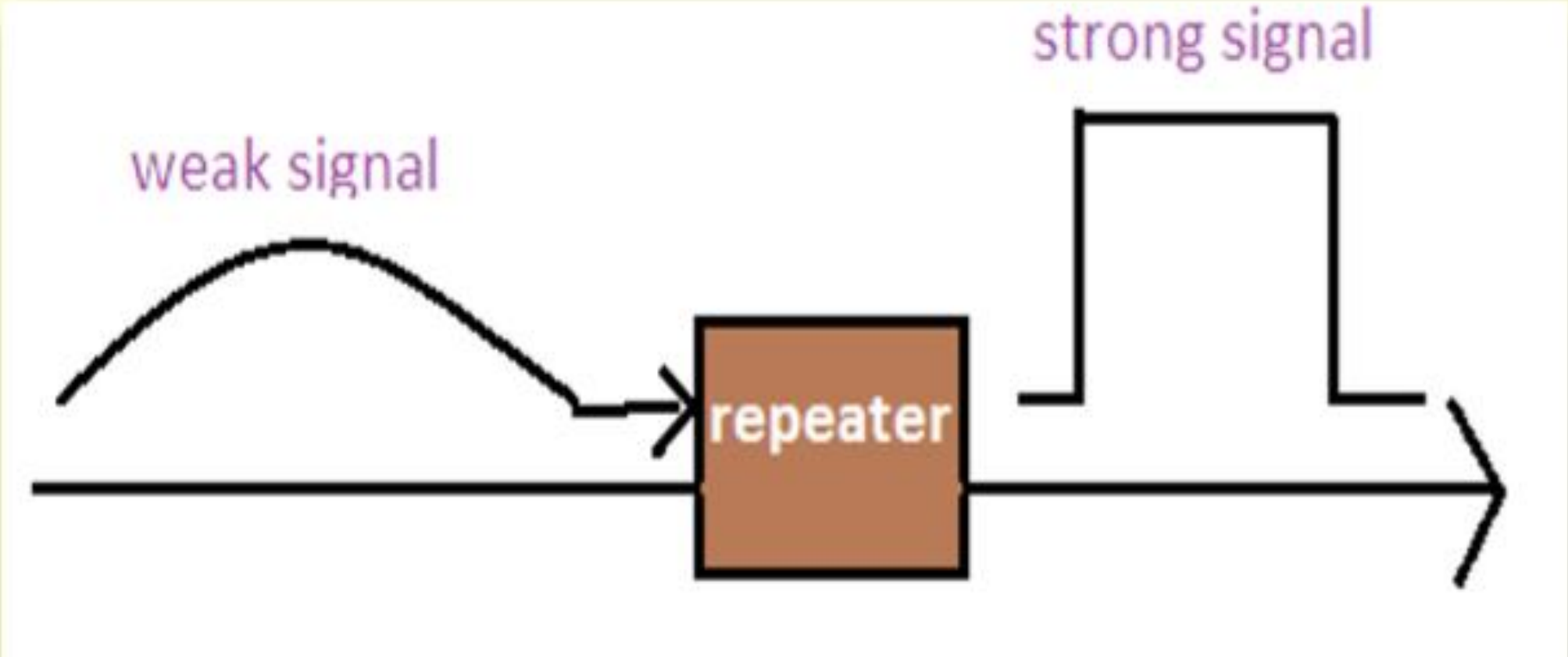
Network devices

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.



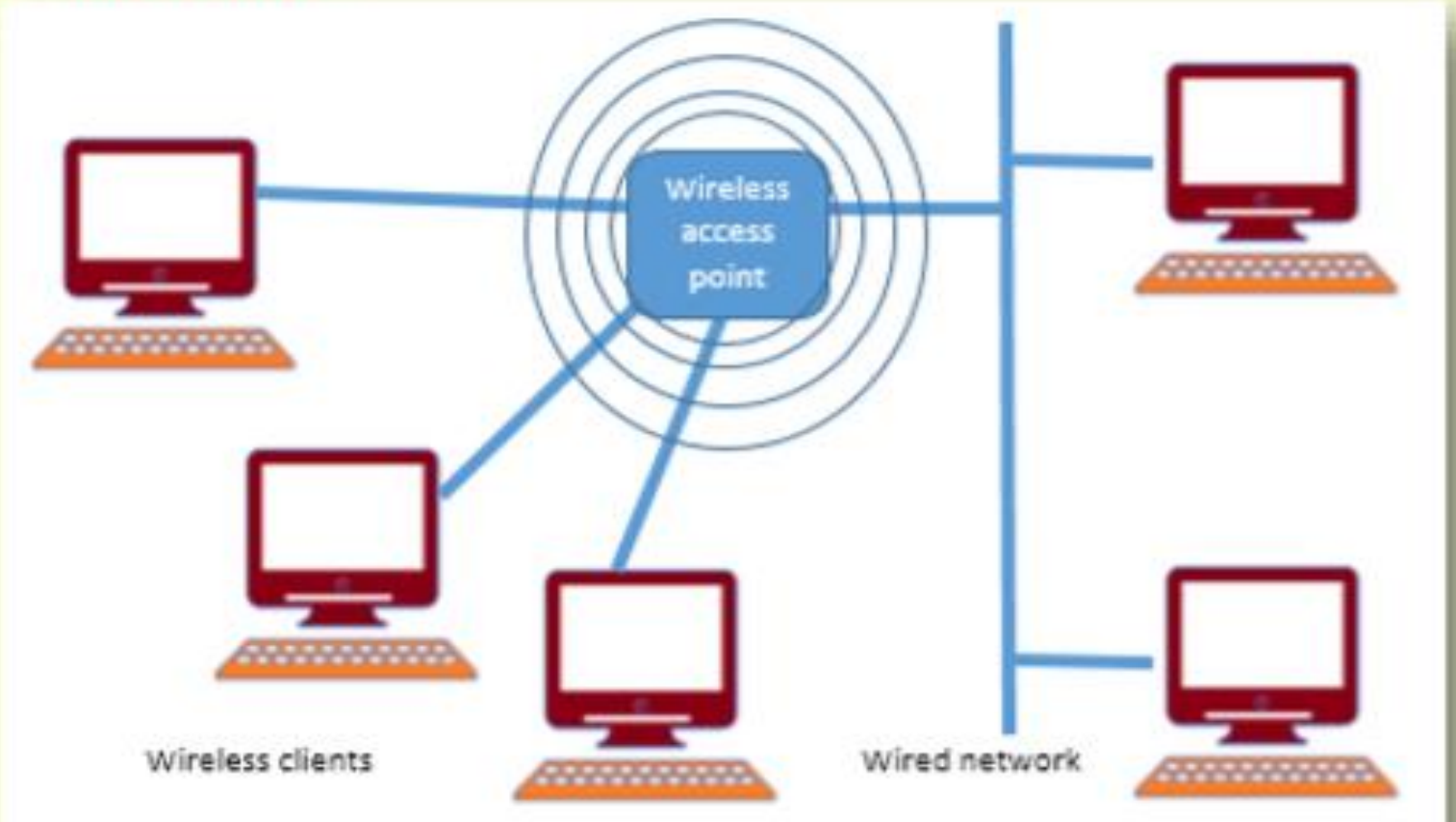
Network devices

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

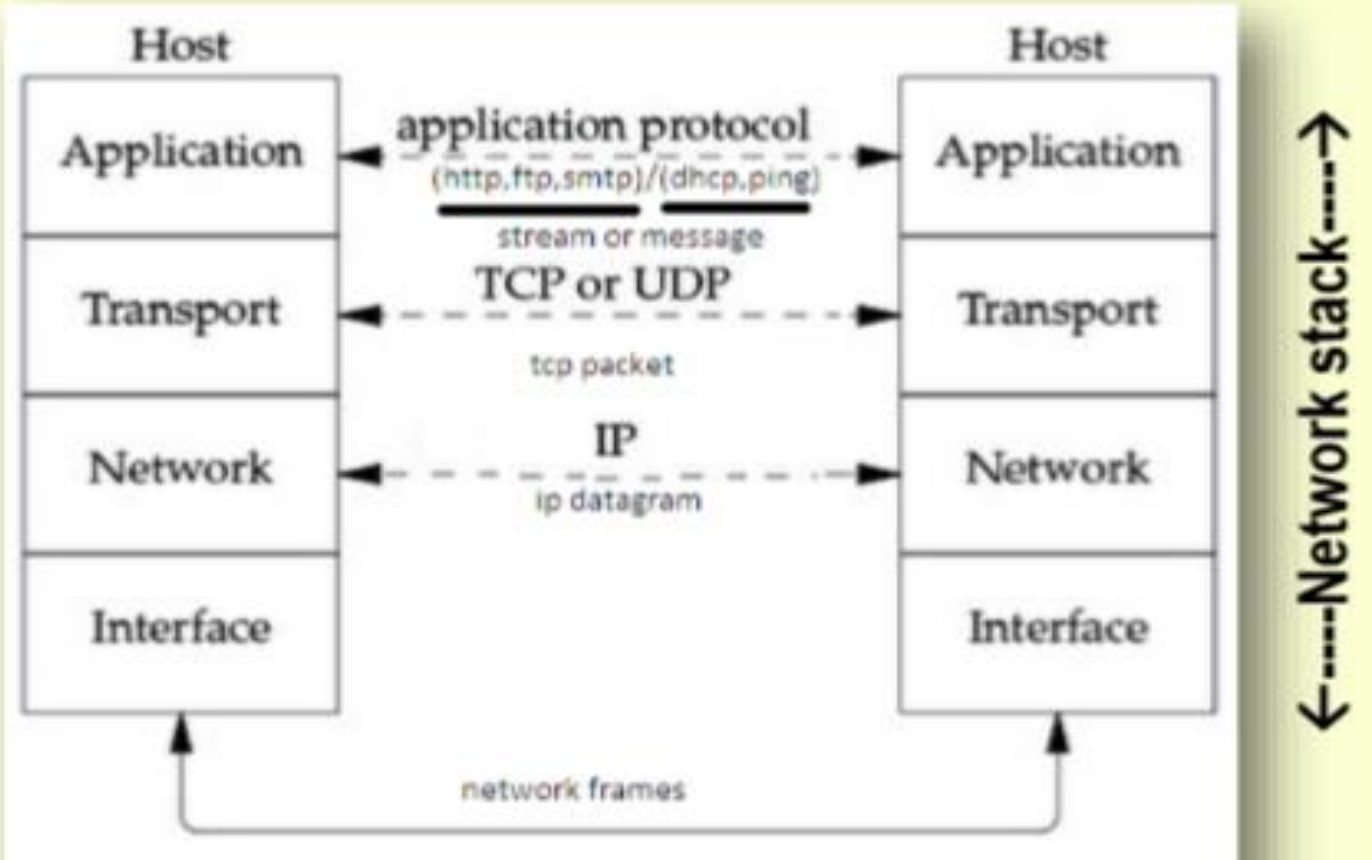
Access Point — Also known as wireless access point. An access point is a station which transmits and receives data (transceiver). It connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network.



Network devices

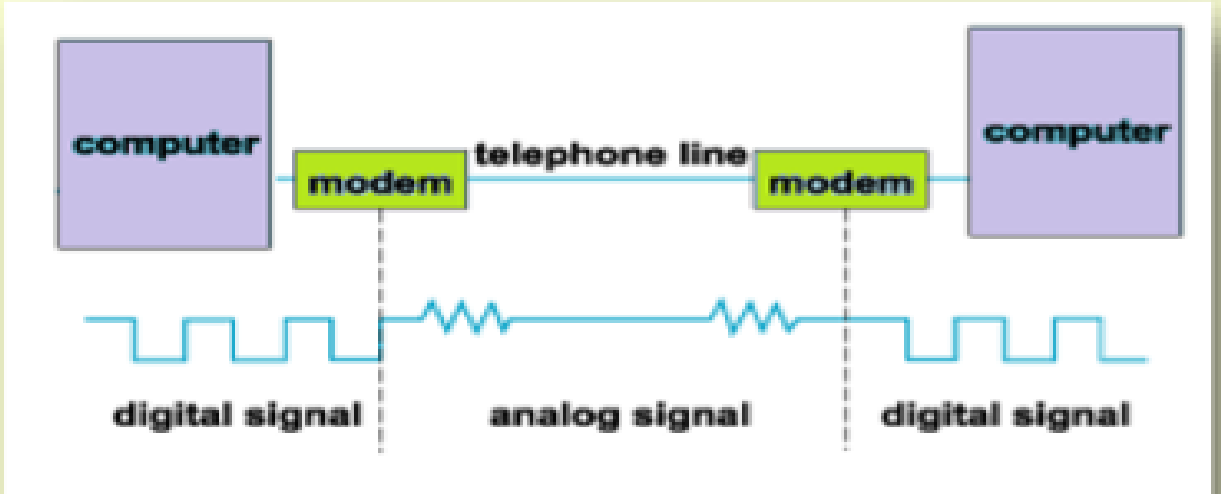
Network stack — It's a sub-system in a computer that deals with networking. In most computers it is TCP/IP stack but there are number of other protocols also. Computer programs only need to know about an IP address or hostname, a tcp or udp port number and the network stack takes care of forming this 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 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.



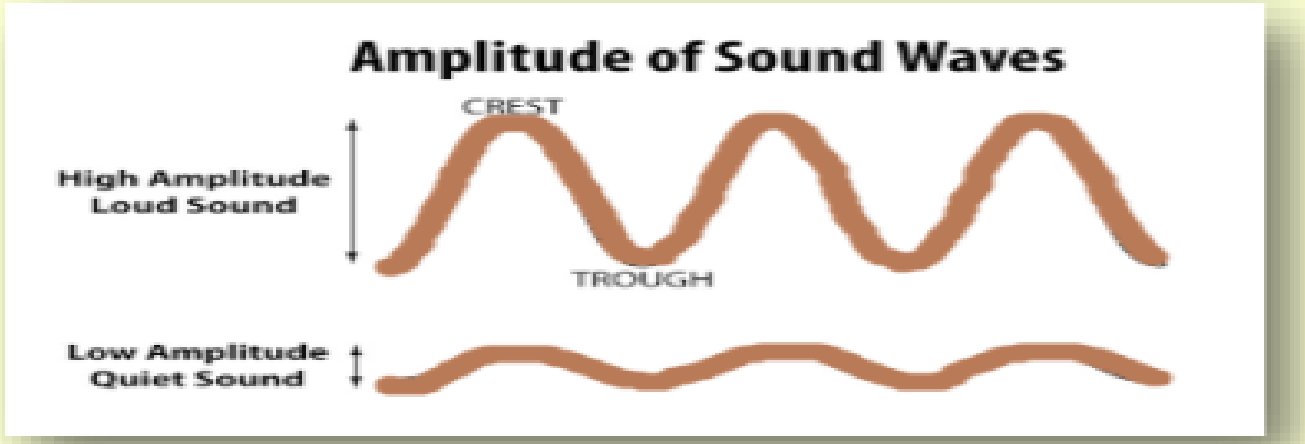
Computer Networking

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.



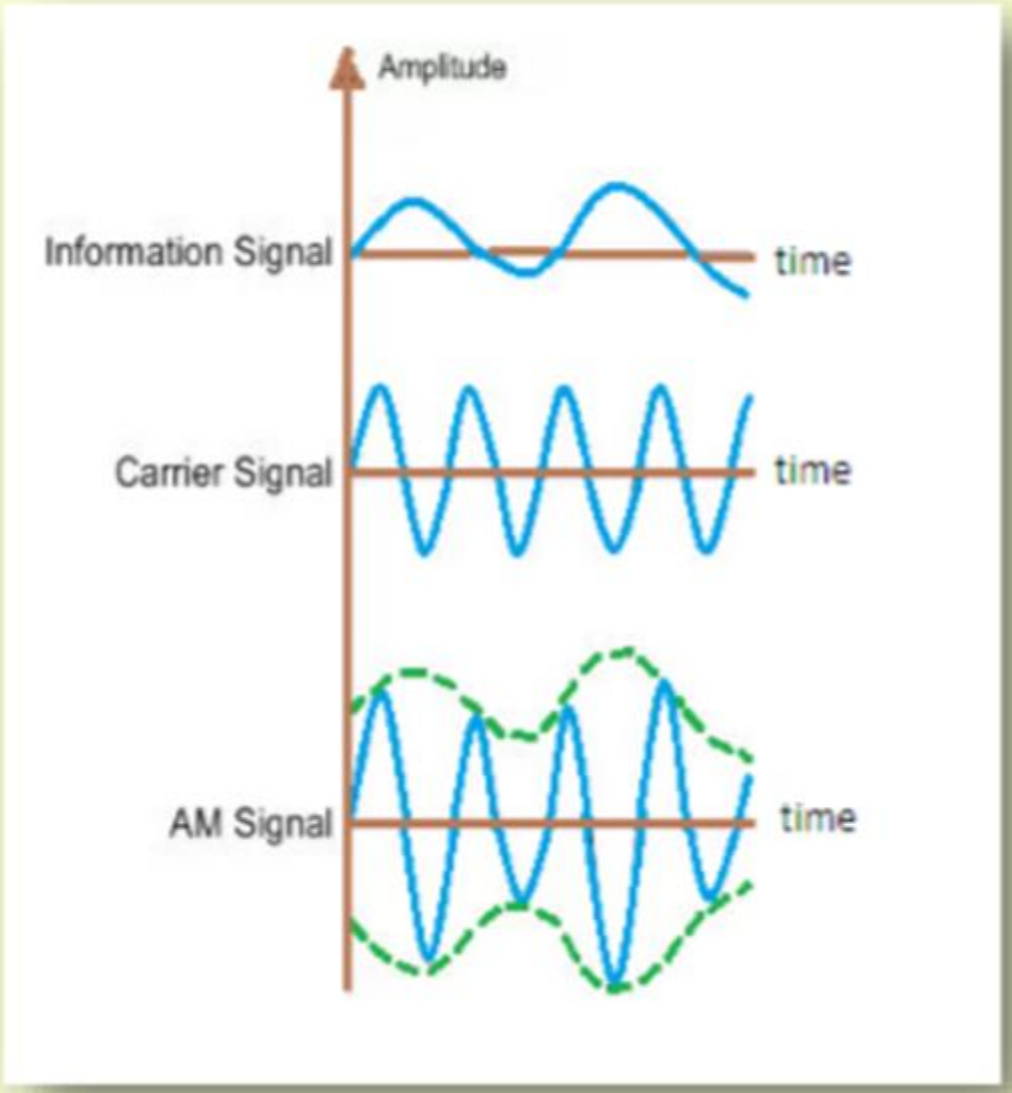
Computer Networking

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.

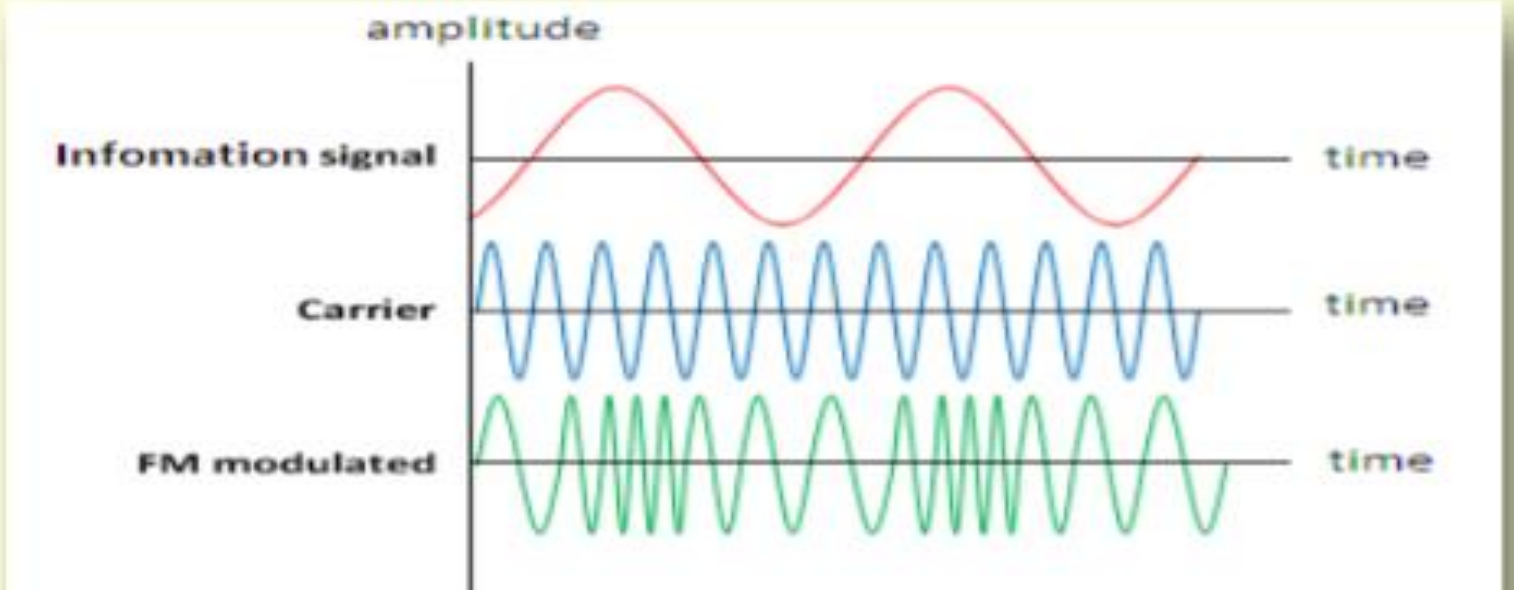


Computer Networking

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.



Computer Networking

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.

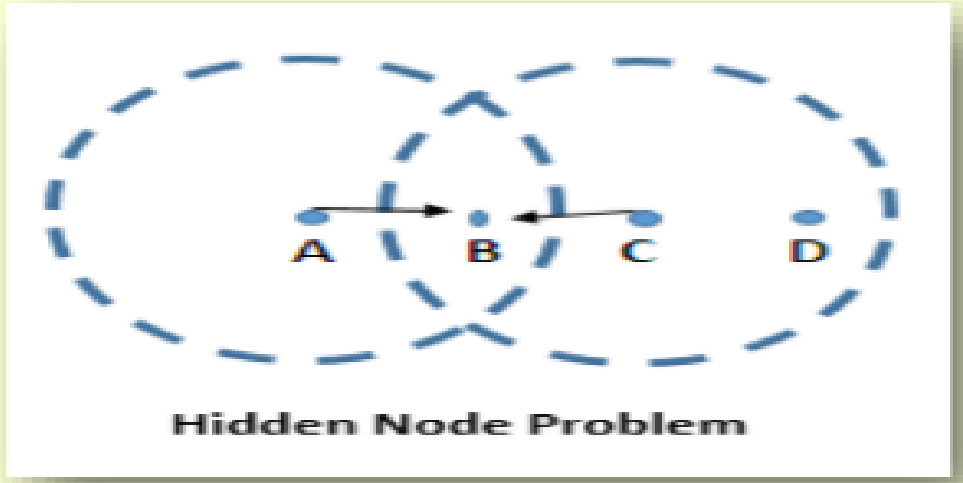
Therefore, CSMA/CA is used on wireless networks. CSMA/CA doesn't detect collisions (unlike CSMA/CA) but rather avoids them through the use of a control message. Should the control message collide with another control message from another node, it means that the medium is not available for transmission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

Computer Networking

Collision in wireless networks –

- **Hidden node problem**

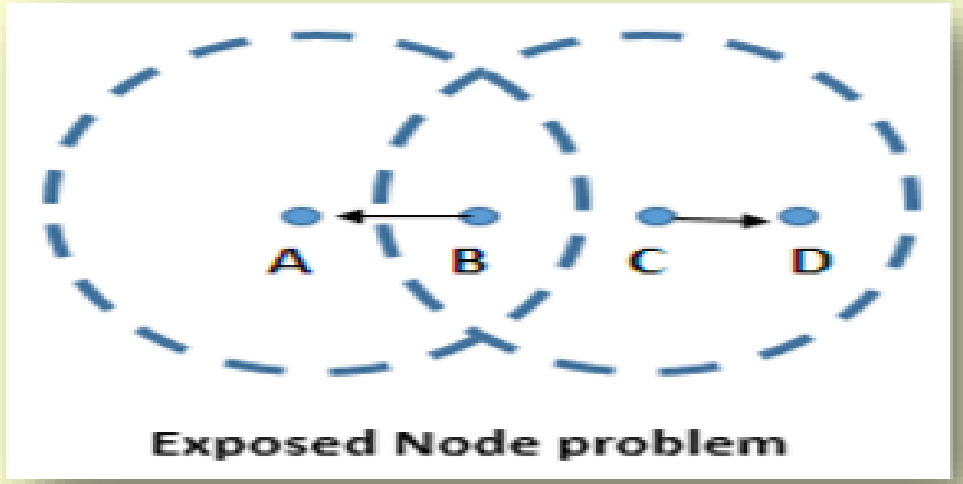
Node A and C send the signal to B at the same time and collision occurs at Node B this can't be detected so CSMA/CA scheme can be used here to avoid collision here.



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.
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.



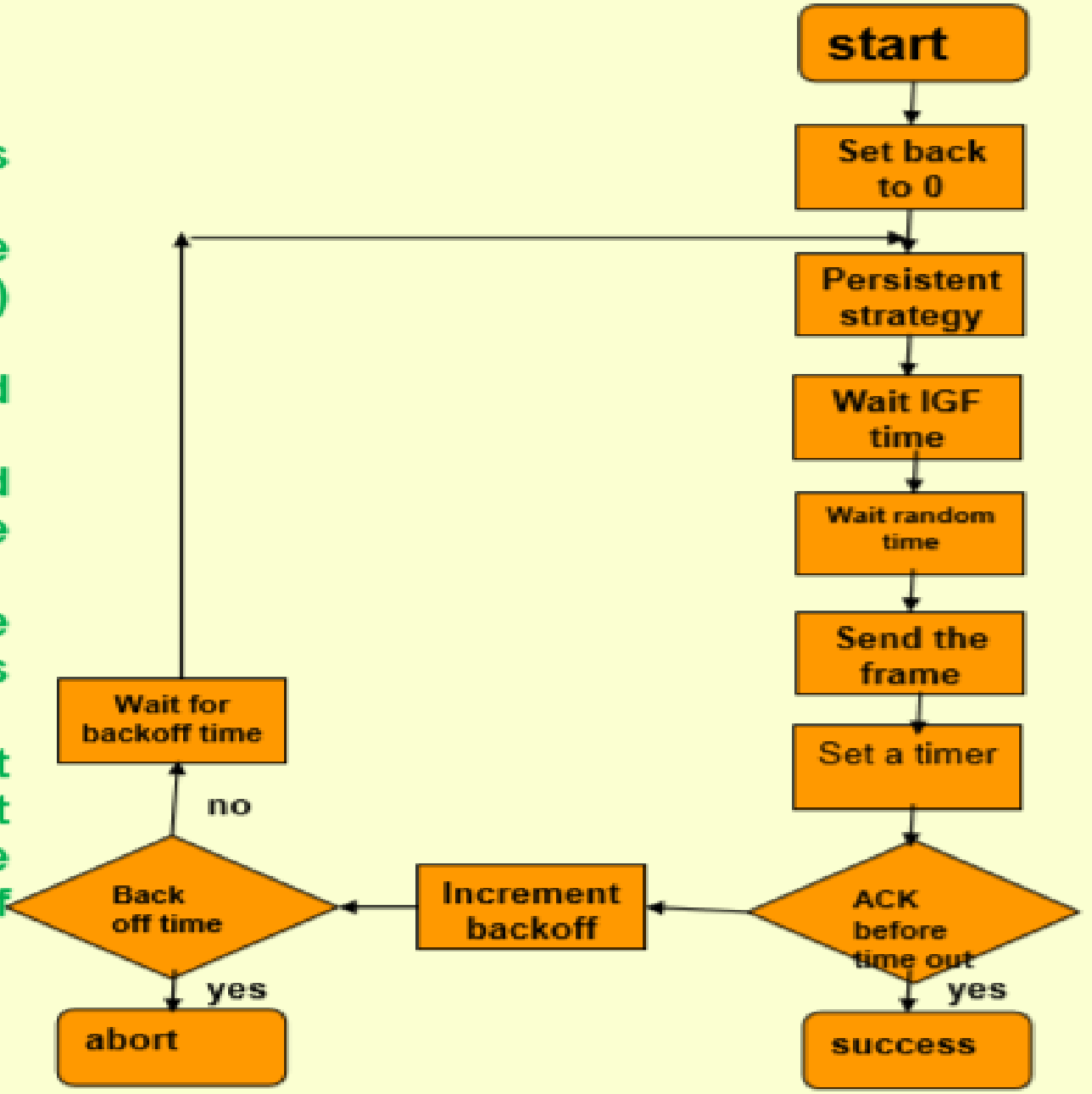
Exposed Node problem

Computer Networking

How CSMA/CA Works

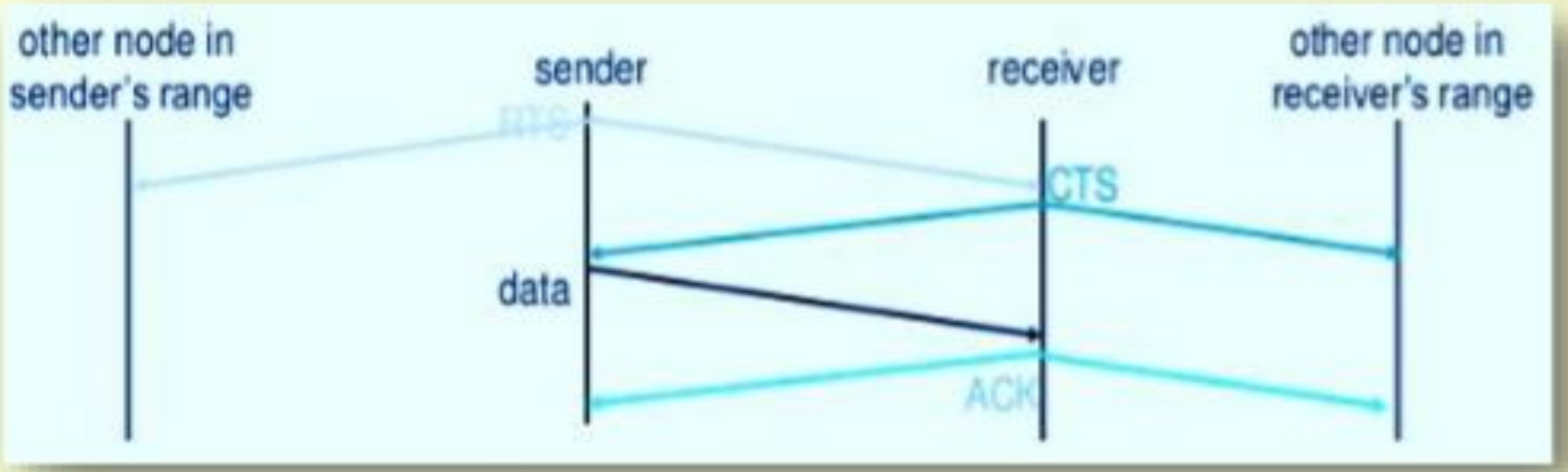
The station ready to transmit signal, senses the line by persistent strategies.

- 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.

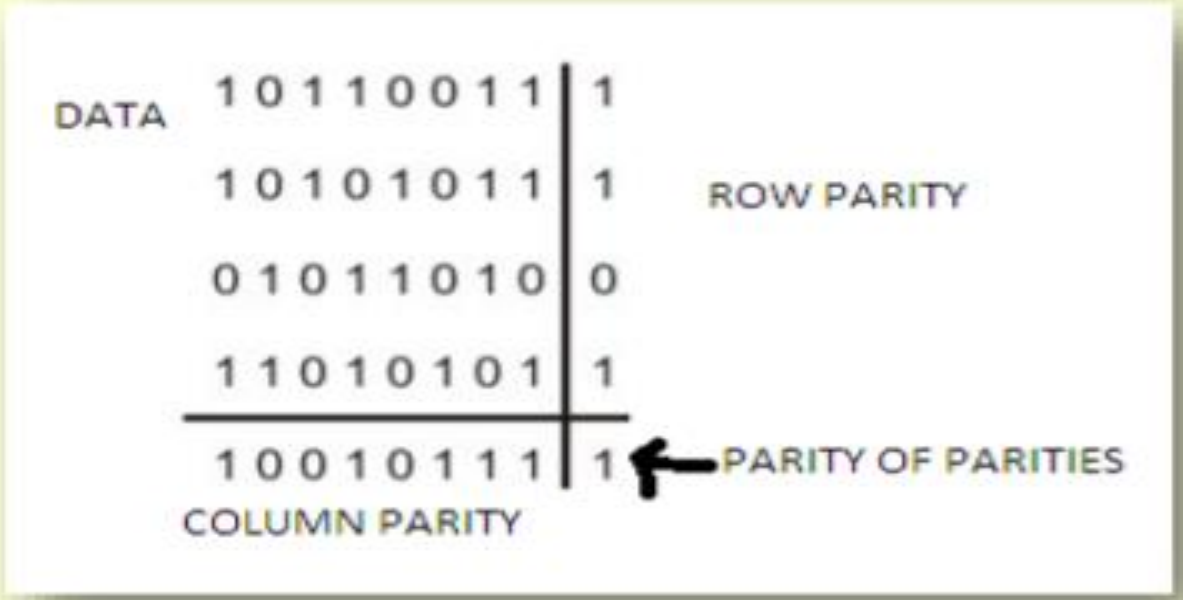
11111110 11011110 11101100 11001001

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.



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.

00:1B:f4:11:fA:B7 is an example of a MAC address.

Manufacturer id Card no

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 191.255.255.254
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

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)

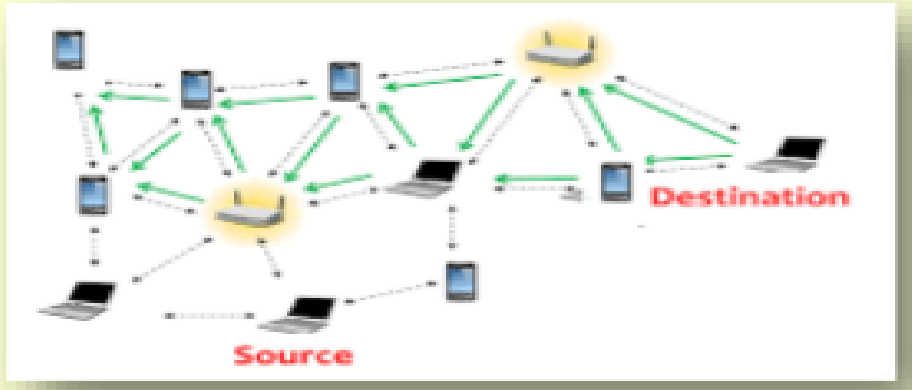
Where to route to **192.168.1.30**?

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 ✓

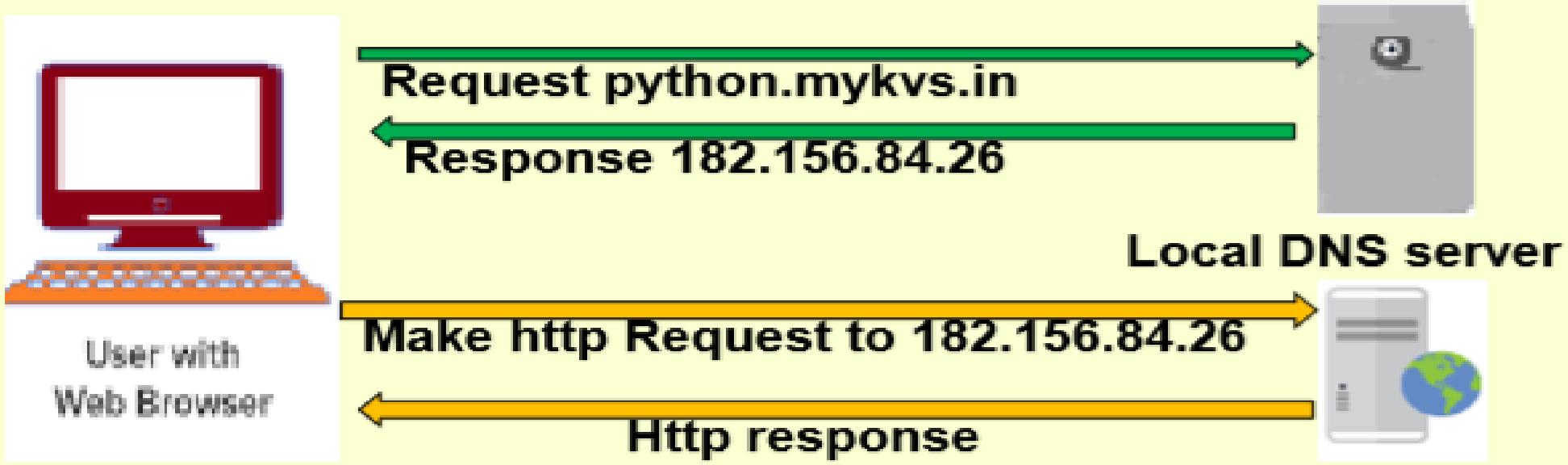
192.168.1.20/32 via 10.254.2.1



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.



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

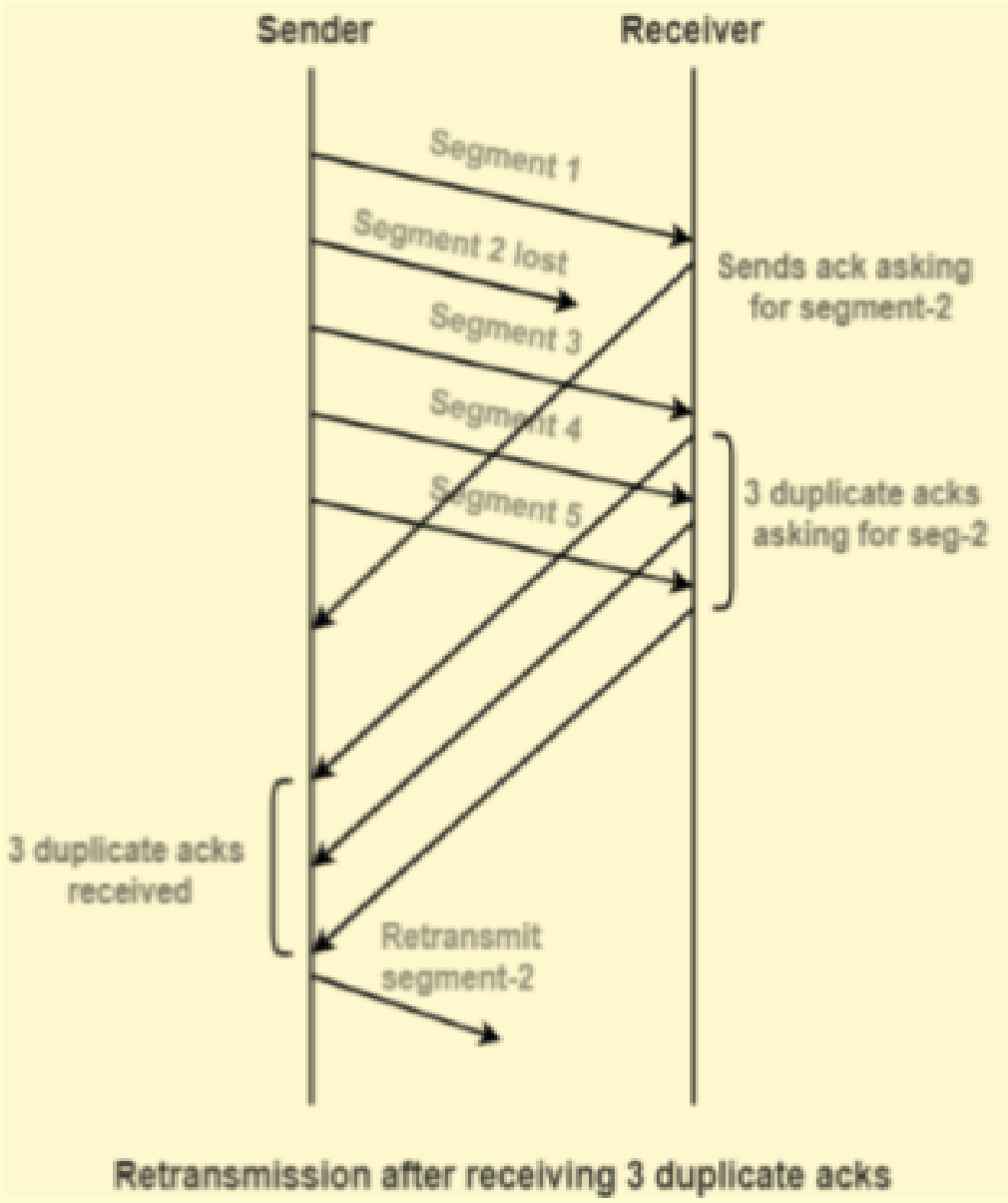
Computer Networking

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.

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.



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.

Basic Network tools

Traceroute -

Traceroute is a network diagnostic tool initially developed by Van Jacobson to determine whether routing problems exist on the network. Traceroute can be used to determine which path IP packets are taking to get from our computer to the remote computer. It should not be used in the network where there are no routers in between. It is not really useful unless there are at least two routers in the network. The Internet has thousands of routers so traceroute is perfect for the Internet. Traceroute was designed to reveal when network failures such as routing loops and black holes occur and displays roughly where those failures exist.In windows environment we have to use the **tracert** (tracerout) command.

Basic Network tools

Traceroute –

Following are the characters may be displayed during tracing of remote computer while traceroute command is under process.

IP Traceroute Text Characters	
Character	**Description**
*	The probe timed out
A	Administratively prohibited
Q	Source quench
I	User interrupted test
U	Port unreachable
H	Host unreachable
N	Network unreachable
P	Protocol Unreachable
T	Timeout
?	Unknown packet type

Basic Network tools

ping –

The ping command is the basic troubleshooting tool for TCP/IP. We can use it to determine whether basic TCP/IP connectivity has been established between two computers or not.

It is a simple, widely used, cross-platform networking utility for testing if a host is reachable on an Internet Protocol (IP) network.

It works by sending a series of Internet Control Message Protocol (ICMP) echo_request messages to the target host and waiting for response.Most of the network administrator use this utility/protocol to check that two computers are properly connected with each other or not on network.

Basic Network tools

ipconfig –

Ipconfig is a useful networking troubleshooting command in windows. It is often used to display the basic networking information (addresses etc.) on a given computer but it can do much more than that. It can release and renew IP addresses for any adapter, it can refresh DHCP leases for dynamic adapters, it can also flush the DNS cache, and more.Open command prompt and type.

>ipconfig

It will display networking information of the computer we are using.

ipconfig - Briefly show you the configured network adapter's information, such as IP address, subnet mask and gateway.

ipconfig /all - Show detailed information of network adapter that includes IP address, subnet mask, gateway, DNS, DHCP, MAC address, etc.

ipconfig /release - Release the IP address of network adapter, mainly used for network adapter that relies on DHCP server to obtain IP address.

ipconfig /renew - Renew the IP address of network adapter, mainly used for network adapter that relies on DHCP server to obtain IP address.

ipconfig /displaydns - Display the contents of the DNS Resolver Cache.

ipconfig /flushdns - Clear the DNS Resolver cache.

ipconfig /? - Display detailed command usage info/manual.

Basic Network tools

nslookup –

Nslookup is a command line utility supplied as part of most of operating systems that can reveal information related to domain names and the Internet Protocol (IP) addresses associated with them.

In simple terms, it is a tool which provide information by interrogating DNS servers either locally or remotely assuming the required DNS server responsible (or knowledgeable) about the requested domain is contactable from where you are operating - over the Internet.

Basic Network tools

whois –

Whois is a service/protocol that provides basic information about a registered domain like domain owner, contact information, domain availability status and the company with which the domain is registered (known as Registrar). Whois also provides registration and expiration dates of a domain along with the nameservers the domain is using.Open the command prompt and type

Speedtest –

- **Speedtest.net** is a web service which provides free analysis of Internet access performance metrics like connection data rate and latency. It was founded by Ookla in 2006, and is based in Seattle, Washington.
- **FAST.com** speed test gives you an estimate of your current Internet speed. You will generally be able to get this speed from leading Internet services, which use globally distributed servers.
- **ping-test.net** - is fast and accurate tool for quality measurements of the Internet connection. It checks delays in millisecond between your computer and selecter remote server. The ping value strongly depends on the distance to the server - the bigger distance the ping value is higher. Your connection is stable if the chart is like straight horizontal line.

Network Protocols

OSI —

Open System Interconnection (OSI) is a network model developed by ISO (International Standard Organization) in 1978 where peer-to-peer communications are divided into seven layers for the purpose of standardization of development of network hardware or software by different software/hardware companies, which can interact with each other in heterogeneous environment. Each layer performs a specific task or tasks and builds upon the preceding layer until the communications are complete.

7. APPLICATION LAYER	Human interaction through application which access network services(HTTP,FTP,Telnet etc.)	Software layer
6. PRESENTATION LAYER	Data encryption to present those data to be displayed over application(IMAP,SSL,JPEG etc.)	
5. SESSION LAYER	To maintain session to deliver data over network(API,Socket etc.)	
4. TRANSPORT LAYER	Transmit data using TCP (TCP,UDP)	Heart of OSI
3. NETWORK LAYER	Decide network path to move over data(IP,ICMP,IPsec)	Hardware layer
2. DATALINK LAYER	Defines format of data for network (Ethernet,SWITCH,BRIDGE,PPP)	
1. PHYSICAL LAYER	Transmit raw bit stream over physical medium(FIBER,COAX,HUB etc.)	

Network Protocols

Application Layer –

The application layer is at the topmost position of the protocol hierarchy. It is the layer where actual communication is initiated. It uses the services of the lower layer as proposed in OSI reference mode to transfer data to a remote host. Following are some of the protocols used under Application Layer.

- HTTP
- working of email
- secure communication: encryption and certificates (HTTPS),
- network applications: remote desktop, remote login, HTTP, FTP, SCP, SSH, POP/IMAP, SMTP, VoIP, NFC

Network Protocols

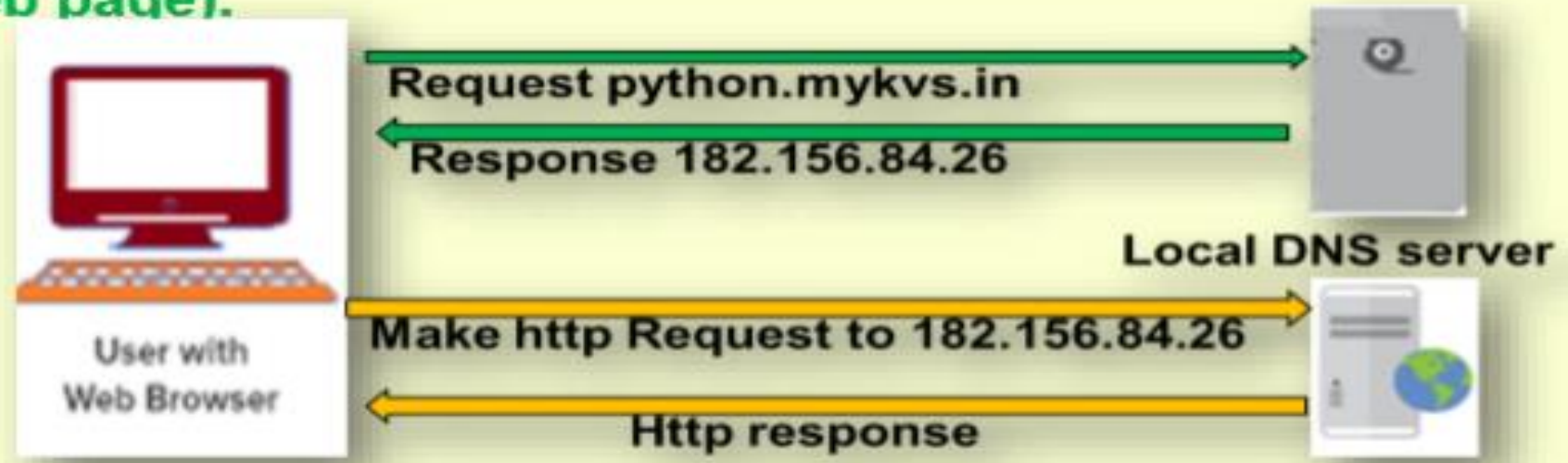
Application Layer —

HTTP - HTTP stands for hypertext transfer protocol and is used to transfer data across the Web. It allow users of the World Wide Web to exchange information found on web pages. When accessing any web page entering http:// in front of the address tells the browser to communicate over HTTP.

How It Works-

It is a connectionless text based protocol. Clients (web browsers) send requests through *request object* of http to web servers for web pages / images etc.Web server respond accordingly through *response object* of http After this cycle(request – response), the connection between client and server across the Internet is disconnected. A new connection must be made for each request(means for each web page).

This diagram shows the working of http protocol. Working with dns server and working with web Server both.

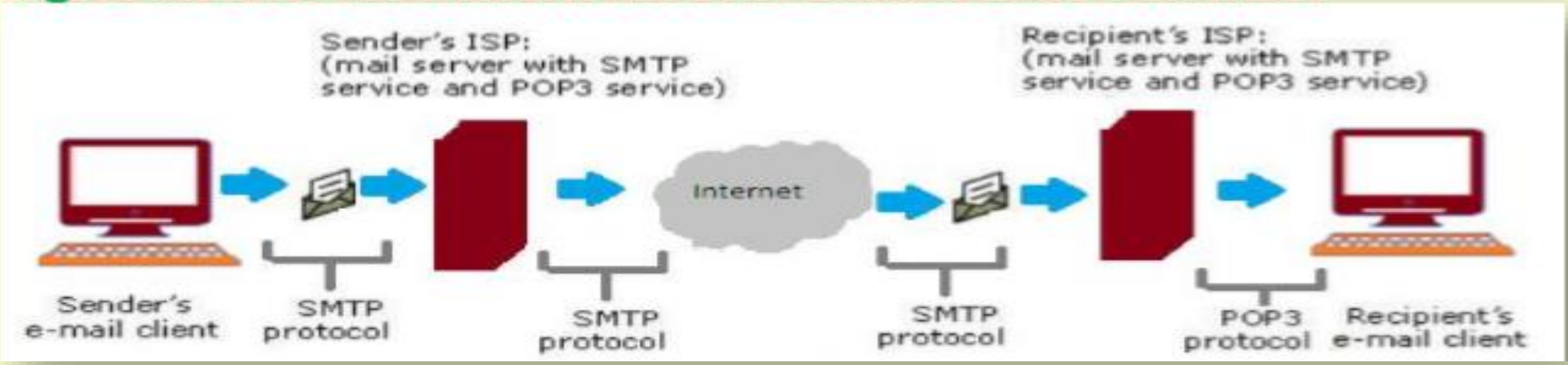


Network Protocols

Application Layer –

Working of email

Email –Electronic mail is a facility that allows users to transmit messages across the internet in fast and secure manner.



Email created using email client program->on press of send button ,it is delivered to sender's mail server through SMTP(Simple mail transfer protocol)->which further transmit the same through internet to recipient's mail server->whenever recipient's email client program's inbox is opened,that email is delivered to inbox through POP3 (post office protocols 3rd version)->which user will read in email client program.

Network Protocols

Application Layer –

Secure communication –

Secure communication is when sender and receiver are communicating and do not want a third party to listen it. For that they need to communicate in a way not susceptible to eavesdropping or interception(message stolen from the media).Generally encryption techniques are used to secure the message.
Encryption - to change electronic information or signals into a secret code (= system of letters/numbers/symbols) that people cannot understand .
Decryption It is the process of decoding the data which has been encrypted.
Encryption is done at sender's site where as decryption is done at receiver site.

Network Protocols

Application Layer –

Secure communication – HTTPS

HTTPS(Hyper text transfer protocol secure) scramble the messages using that "code" so that no one in between can read the message. It keeps our information safe from hackers.

Https uses the "code" on a **Secure Sockets Layer (SSL)**, sometimes called Transport Layer Security (TLS) to send the information back and forth.

Essentially, we need three things to encrypt data:

- The data to be sent/encrypted
- A unique encryption key
- An encryption algorithm (a math function that garbles the data)

asymmetric encryption is used in https. Asymmetric means we are using two different keys, one to encrypt and one to decrypt.

This encryption is now done at TLS rather than SSL.

Network Protocols

Application Layer –

Network applications:

Remote desktop – A computer program/utility that enable us to connect our computer across the Internet virtually with any other computer, Pocket PC, or smartphone.

To start Remote Desktop on the computer we want to work from in windows

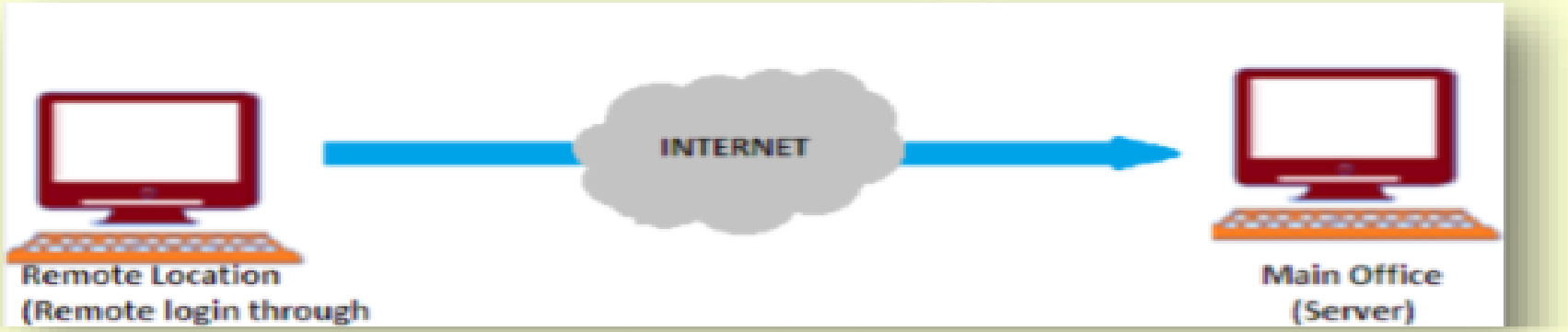
- Open Remote Desktop Connection by clicking the Start button Start button icon. In the search box, type Remote Desktop Connection, and then, in the list of results, click Remote Desktop Connection.
- In the Computer box, type the name of the computer that we want to connect to, and then click Connect. (we can also type the IP address instead of the computer name.)

Network Protocols

Application Layer –

Network applications:

Remote login – A remote login facility permits a user who is using one computer to login to remote computer or interact with a program on another computer. Command given at remote location is processed by server and result displayed over remote location.



Telnet – Telnet is most popular protocol for accessing remote site/server. Using telnet client software on our computer, we can make a connection to a telnet server (that is, the remote host). Once our telnet client establishes a connection to the remote host, our client becomes a virtual terminal, allowing us to communicate with the remote host from our computer. In most cases, we need to log into the remote host, which requires that we have an account on that system. Occasionally, we can log in as guest or public without having an account.Generally it is used in unix based client server system to interact.

Network Protocols

Application Layer –

Network applications:

How to Enable telnet in Windows –

1. Open Start menu and select Control Panel.
2. Click on Programs.
3. Click on "Turn Windows features on or off."
4. Put a checkmark next to Telnet Client then click OK.
5. Wait for Windows to update your system then close the Control Panel.

Working on telnet

Working on telnet is very easy we have to type following in run dialog box of windows to connect to remote server telnet hostname port or telnet ipaddress port

e.g.

we can even use Telnet to talk to an artificially intelligent psychotherapist named *Eliza*.(one of the game,there are no of games on internet)

Type telnet telehack.com in run dialog box .it will open command prompt with list of telehack commands to communicate.some of command like you may type

>.eliza

Auto response will be given

>hi, my name is python

Auto response will be given

Network Protocols

Application Layer –

Network applications:

FTP – FTP, or File Transfer Protocol, is one of the standard internet protocols used to transfer data files between a client(FTP client) and a server(FTP server) over a computer network. It was developed in the early 1970s by Abhay Bhushan (alumni IIT Kanpur),while he was a student at MIT. FTP was initially created to allow for the secure transfer of files between servers and host computers over the ARPANET Network Control Program (a precursor to the modern internet).Nowadays it is being used for uploading files on webserver after non anonymous ftp(means username and password available with you).downloading is possible as anonymous ftp(no password is required).FTP is available in two mode –text mode ftp(where user have to give commands in text form) and GUI ftp(graphical interaction is possible)

Some of the more popular, and reliable, FTP Clients currently operating in the industry are FileZilla,WinSCP,Cyberduck,gFTP

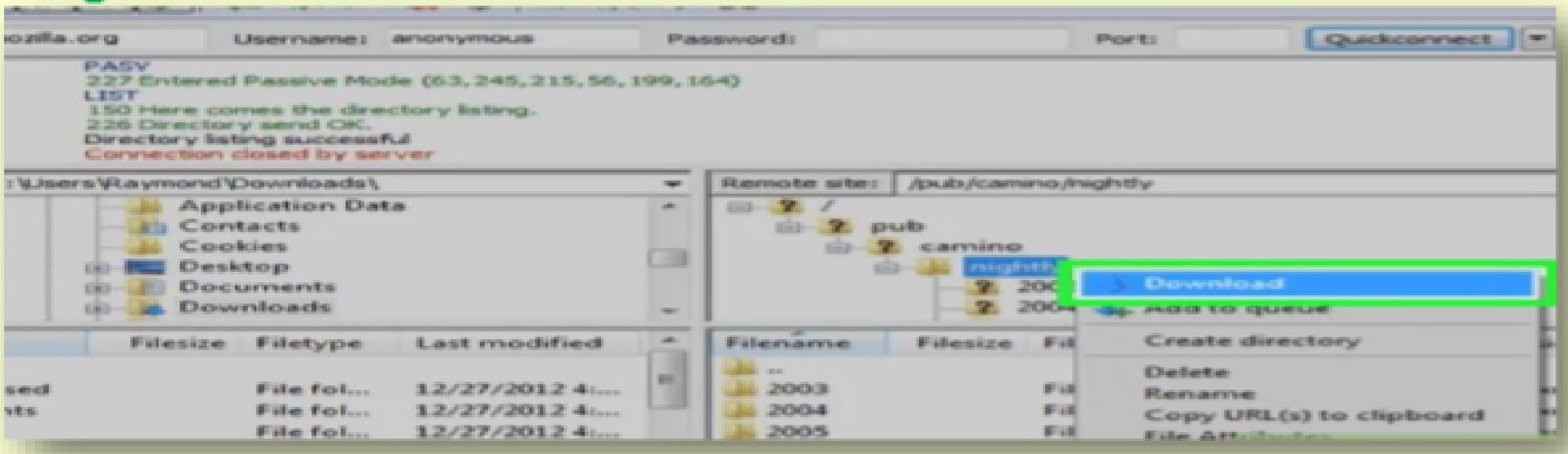
Network Protocols

Application Layer –

Network applications:

How to work on FTP – Here we are using Filezilla.

1. Download filezilla
2. Install filezilla
3. Open site manager from file menu and click on new site button
4. Type credential available of any domain
5. Press ok, It will connect our computer with remote computer ,screen will be something like this



6. Left side pan will display the folder/files of our computer and right side pan will display the file structure of remote computer.through simple drag and drop we can download upload(receive file from remote computer to local computer) or upload(sending file to remote computer from local computer) the files.

Network Protocols

Application Layer –

Network applications:

SSH – It is referred to as Secure Shell is a method for secure remote login from one computer to another with strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).

The protocol is used in corporate networks for:

- providing secure access for users and automated processes
- interactive and automated file transfers
- issuing remote commands
- managing network infrastructure and other mission-critical system components.

Network Protocols

Application Layer –

Network applications:

SCP – It is the abbreviation of 'secure copy protocol'. SCP is better designed for a one-time transfer between two computers on the same network, though it can be used remotely over the Internet as well.

The SCP command can be used to send a file to a server or retrieve a file from a server. Because it uses the SSH protocol for authentication SCP is more secure than FTP which transmits passwords in plain text. We can use PSCP utility in windows that is available at PuTTy.org. download and install it ,open the command prompt and set the path.

To receive

pscp free@example.com:/etc/hosts c:\temp\example-hosts.txt

To send

pscp c:\documents\myfile.txt free@example.com:/tmp/foo

Network Protocols

Application Layer –

Network applications:

POP3 – Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows us to download email messages on our local computer and read them even when we are offline. Note, that when we use POP3 to connect to our email account, messages are downloaded locally and removed from the email server. This means that if we access our account from multiple locations, that may not be the best option for us. On the other hand, if we use POP3, our messages are stored on our local computer, which reduces the space of email account uses on your web server.

IMAP - Internet Message Access Protocol is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s). This allows users to organize messages into folders, have multiple client applications know which messages have been read, flag messages for urgency or follow-up and save draft messages on the server.

Network Protocols

Application Layer –

Network applications: Difference between POP3 and IMAP

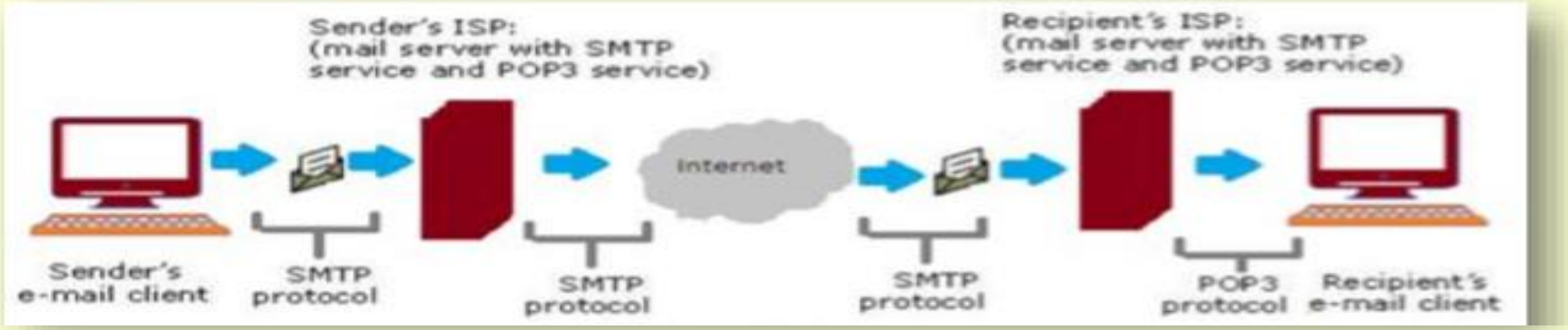
BASIS FOR COMPARISON	POP3	IMAP
Basic	To read the mail it has to be downloaded first.	Email content can be checked partially before download.
Organize	Mails can't be organized in mailbox of mail server by user.	User can organize the mails on the server.
Folder	User cannot create, delete or rename mailboxes on a mail server.	User can create, delete or rename mailboxes on the mail server.
Content	User cannot search the content of mail for prior downloading.	User can search the content of mail for specific string of character before downloading.
Partial Download	User has to download the mail for accessing it.	User can partially download the mail if bandwidth is limited.
Functions	POP3 is simple and has limited functions.	IMAP is more powerful and has more features over POP3.

Network Protocols

Application Layer –

Network applications:

SMTP – Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail to email server. it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server.An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail.



The SMTP model is of two type :

- End-to- end method
- Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method is used within an organization.

Network Protocols

Application Layer –

Network applications:

VOIP – Voice over Internet Protocol (VoIP), is a technology that allows us to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.

VoIP services convert our voice into a digital signal that travels over the Internet. If we are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination. VoIP can allow us to make a call directly from a computer, a special VoIP phone. In addition, wireless "hot spots" in locations such as airports, parks, and cafes allow us to connect to the Internet and may enable us to use VoIP service wirelessly.

Advantages:

- Less Cost
- Accessibility
- Flexibility
- Voice Quality
- Extra/Less Expensive Features

Disadvantages:

- Reliable Internet Connection Required
- Power Outages/Emergencies
- Latency

Network Protocols

Application Layer –

Network applications:

Services provided by VOIP – Phone to phone,pc to phone ,phone to pc,voice to email,ip phone,toll free number,call center applications,vpn,unified messaging etc.

Protocols used for VOIP are

- **Session Initiation Protocol (SIP)- connection management protocol developed by the IETF**
- **H.323 - one of the first VoIP call signaling and control protocols that found widespread implementation.**
- **Real-time Transport Protocol (RTP)- transport protocol for real-time audio and video data**
- **Real-time Transport Control Protocol (RTCP)- sister protocol for RTP providing stream statistics and status information**
- **Secure Real-time Transport Protocol (SRTP) - encrypted version of RTP**
- **Session Description Protocol (SDP) - file format used principally by SIP to describe VoIP connections**

Network Protocols

Application Layer –

Network applications:

NFC – Near field communication is a standards-based technology to provide short range wireless connection technology to carry secure two-way interactions between electronic devices.For Communication,it is not required to set-up by users as in the case of many other wireless communications.

It provides contactless communication up to distances of 4 or 5 centimeters. so communications are inherently more secure because devices normally only come into contact and hence communication when the user intends to do so.

The connection is more reliable as no physical connectors are used in NFC and does not suffer problems of contact wear, corrosion and dirt experienced by systems using physical connectors.

NFC applications

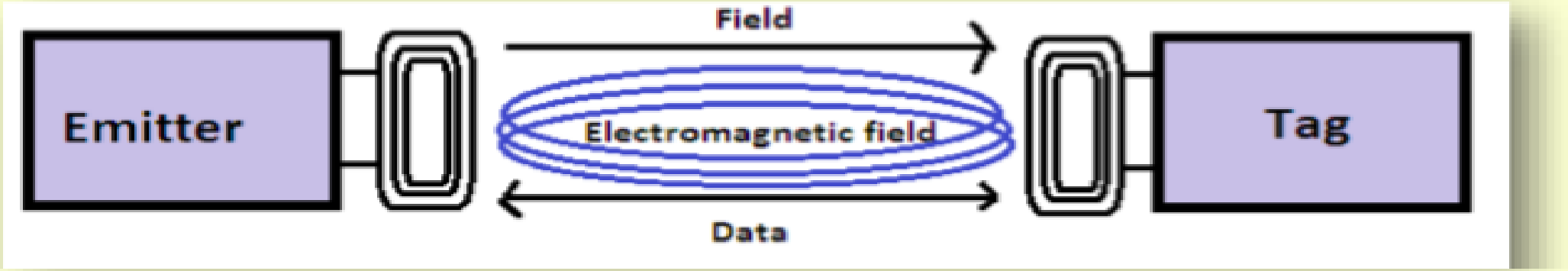
- **Payment cards**
- **Ticketing**
- **Mobile phones, PDAs, etc**
- **Check-out cash registers or "point-of-sale" equipment**
- **Vending machines**
- **Parking meters etc.**

Network Protocols

Application Layer –

Network applications:

How NFC works –



The antennas of the Emitter and Tag are coupled via an Electromagnetic Field known as Air-Core Transformer. An alternating current passes through the primary coil (Emitter) and this current induces a field thru the air, inducing current in the secondary coil (Tag). The Tag may use the current from the field to power itself. In general, inductive coupling thru air is very inefficient, and therefore, the read/write range is quite limited. tag contain an antenna(Inlay) & small amount of memory. A tag is a passive device, and the power the device needs to operate comes from the electromagnetic field, generated by the emitter. RFID Inlays are attached to the EEPROM Memory for the antenna. These inlays are customized for the antenna design and application.