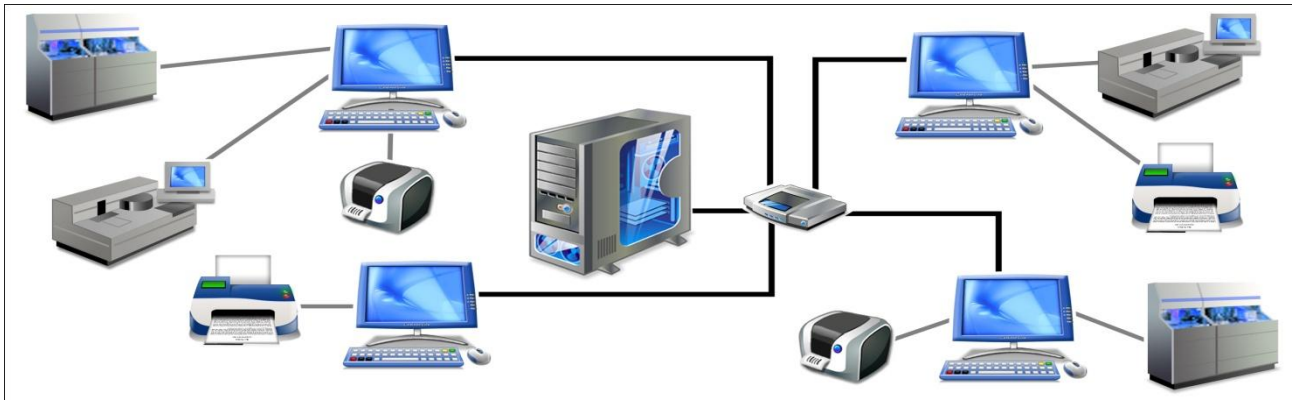
Networking

Networking Introduction

Definition: Networking is the interconnection of two or more devices that makes inter communication among them to share the resource.



Advantages

1) Hardware Sharing: eg – Printer, scanner, web cam, speaker etc.
2) Folder Sharing.
3) Application software sharing.
4) Entertainment: Chatting, video conferencing, etc
5) Increasing Storage capacity.
6) Remote devices access.

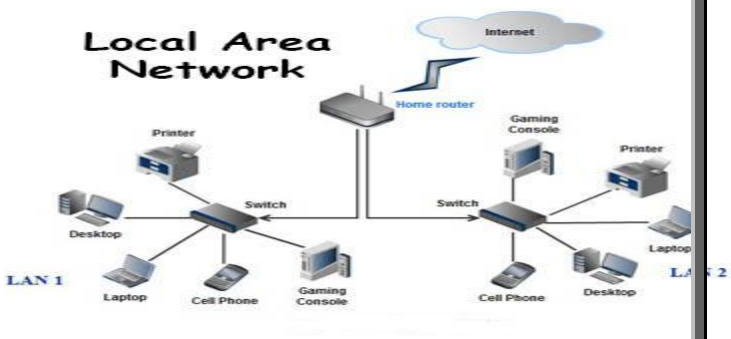
Disadvantages

1) Unauthorised access (hacking problem).
2) Virus can spread easily in network.

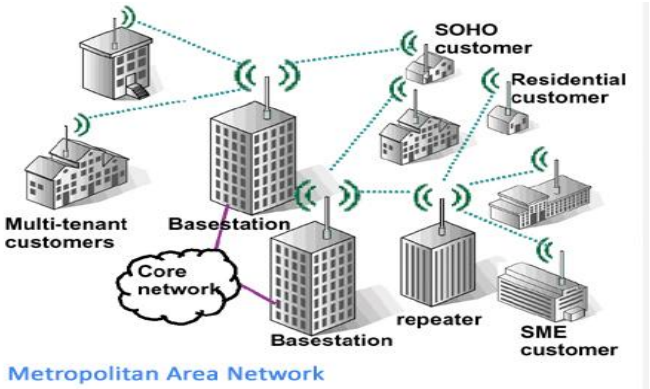
Classification of Network

On the basis of distance

- PAN : Personal Area Network (one to one)
- LAN : Within a room to a office to a building.

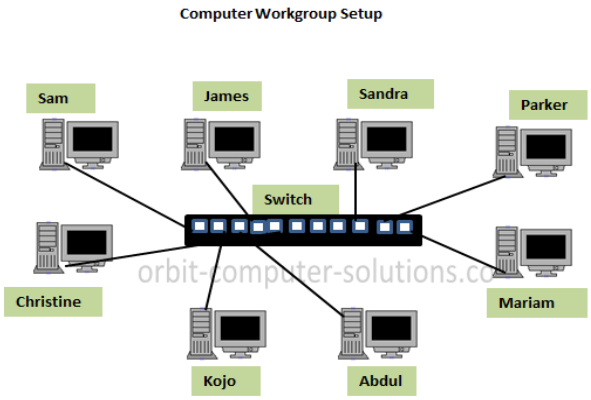


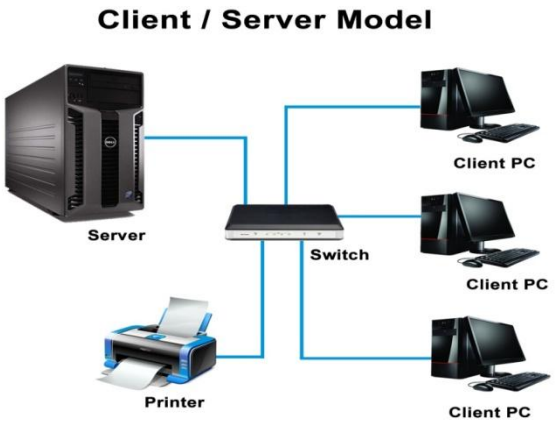
- CAN: Within the campus
- MAN : Within the city
- WAN : All over the world(min two city)



On the basis of use

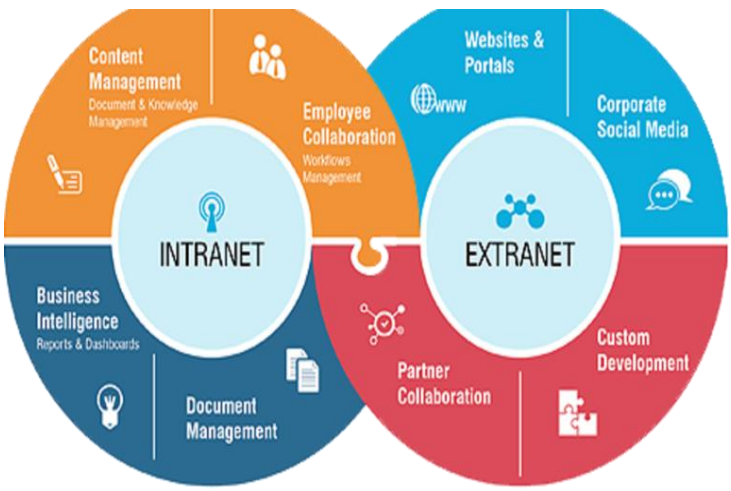
- Peer to peer network (Workgroup)
- Client-server model (Domain)

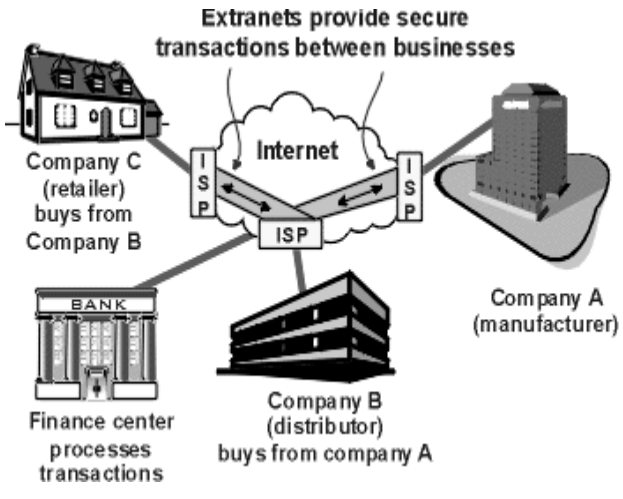




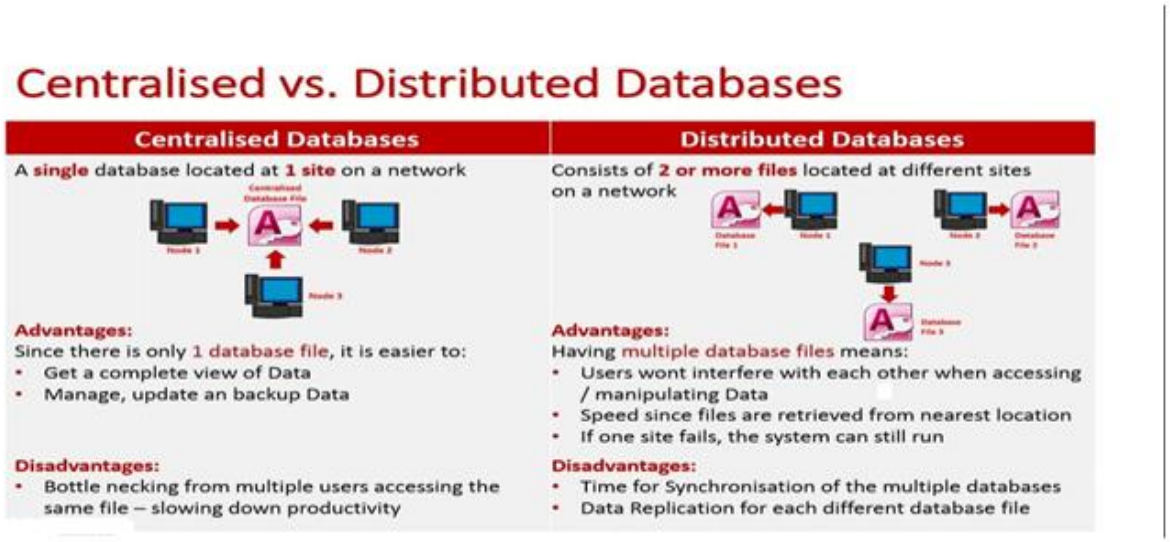
On the basis of connection

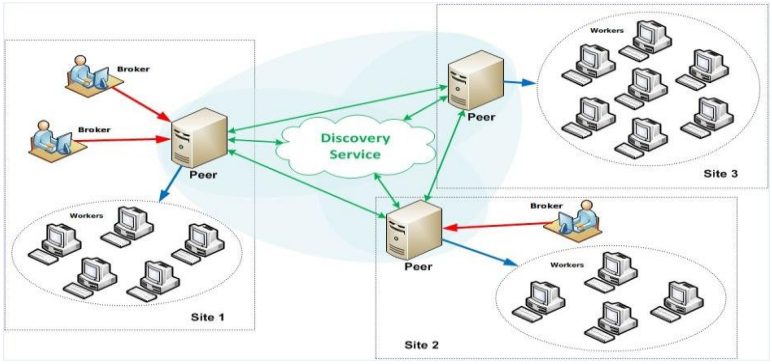
- Intranet: Accessing server within the organization
- Extranet: Accessing server of partner organization
- Internet: Accessing server of all over the world
-





On the basis of Processing





Requirement to create network

1) Computers
2) Operating System that support networking
3) NIC (Network Interface Card) or LAN Card
4) Transmission media
5) Networking Devices
6) Topology
7) Networking Protocol

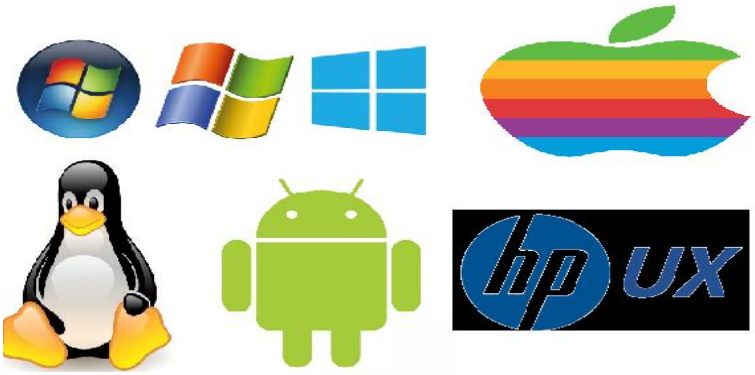
COMPUTERS

1) Laptops 2)Desktops 3)Palmtops

Any types of computers can be connected in network.

O.S (Operating Systems) Family

8) Windows 2)Linux 3)Netware 4)MAC OS 5) BSD



WINDOWS		LINUX O.S
CLIENT O.S	SERVER O.S	
DOS (1980s)	Windows NT Server	Redhat Linux
Windows 1.0	Windows Server 2000	Fedora
Windows 3.0	Windows Server 2003	Centos
Windows 95	Windows Server 2008	Ubuntu
Windows 98	Windows Server 2012	Mandriva
Windows ME	Windows Server 2016	Kali linux
Windows NT		Debian
Windows 2000		Arch Linux
Windows XP (2000)		Free Linux
Windows Vista		Scientific Linux
Windows 7		Mint Linux
Windows 8/8.1		
Windows 10		

Client computers:

- End devices that users use to access the shared resources.
- Usually they run desktop version of OS such as Window 10, Window 7 etc.
- Client computers are also known as **workstations**.

Server computers:

- Computers that provide shared resources.
- Usually they run sever version of OS such as Window Server 2008, Linux etc.
- Server computers run many specialized services to control the shared resources.

Server Type

1) Tower Server

2) Rack Server

3) Blade Server

NIC : Network Interface Card

- NIC is an interface that enables the computer to communicate over the network.
- Every computer must have a NIC in order to connect with the network.
- In earlier time it was a separate card and need to be installed on motherboard.
- All modern computers have it as the integral part of motherboard.

Physical Address or MAC address

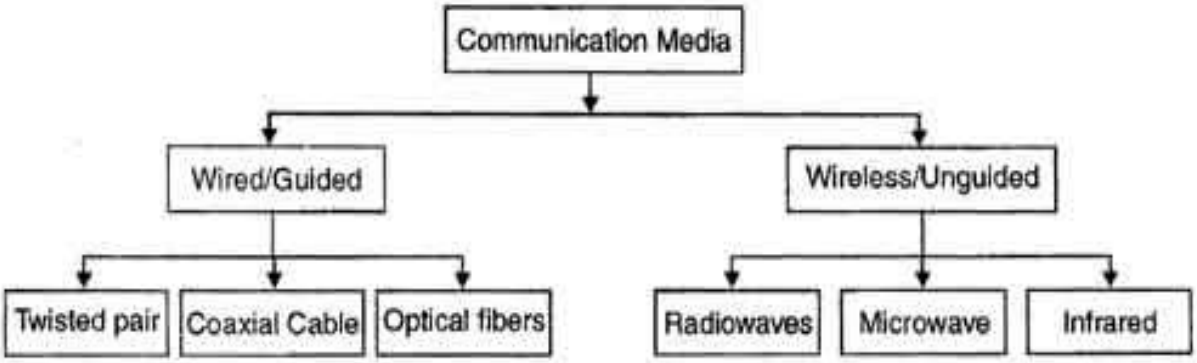
- Fixed address . We can't change it.

- It is already present in NIC Card.
- Given by INTERNIC Organization to manufacturer.
- 48 bits address divided into 24 bits and 24 bits.
- The 1st 24 bits is manufacturer ID and 2nd is unique ID.

Logical Address or IP address

- It can be changed as you like.
- Used for assigning a IP address
- Two types: IPv4 and IPv6
- IPv4 : 32 bits and IPv6 :bits

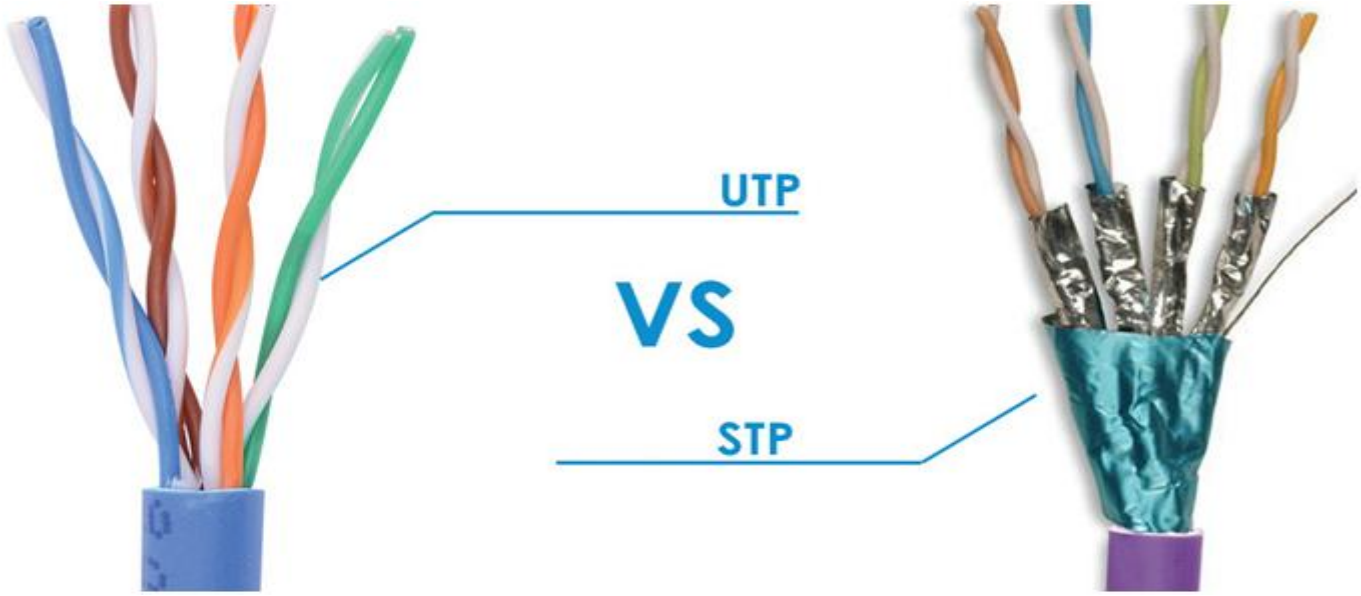
Transmission Media



Twisted Pair Cable

Two Types

UTP (Unshielded Twisted Pair)	STP (Sheilded Twisted Pair)
➢ Less cost	➢ Costly
➢ Normally used everywhere	➢ Used in sensitive places only
➢ Having 8 wires of different colours	➢ same
➢ Only one outer shield	➢ Outer shield as well as separate shield in each pair
	➢ To protect from electromagnetic disturbance in common wiring STP will be used.



Twisted pair categories

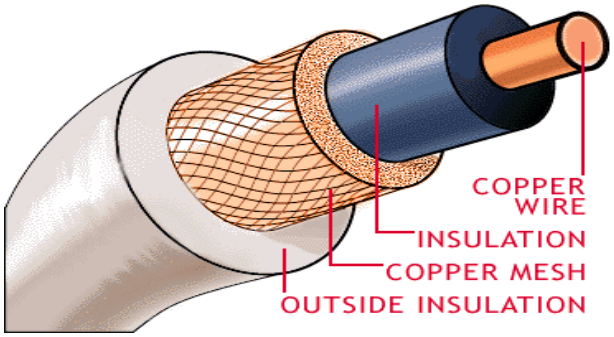
Type	No of Pairs	Transmission Rate	Implementation
Category 1	1	Voice Grade	• used in telephone industry • not suitable for long distance data transmission(used only for short distance)
Category 2	2	4 Mbps	• used for both data and voice transmission
Category 3	4	10 Mbps	• required 3 twist per foot • used for 10 base networks. • used for voice • communication
Category 4	4	16 Mbps	• required 3 twist per foot • used in IBM token ring networks
Category 5	4	100 Mbps	• used in Ethernet and 100 Base-X networks
Category 6	4	100 Mbps and higher	• used in Ethernet and 1000 Base-X networks

Connector used : RJ45 (Resistered jack)

Coaxial Cable

- Coaxial cable is an electrical cable consisting of a round conducting wire, surrounded by an insulating spacer, surrounded by a cylindrical conducting sheath, and usually surrounded by a final insulating layer.

- Most common use of coaxial cable today is in standard cable TV. A copper conductor lies in the center of the cable, which is surrounded by insulation. A braided or mesh outer covering surrounds the insulation. This is also a conductor.



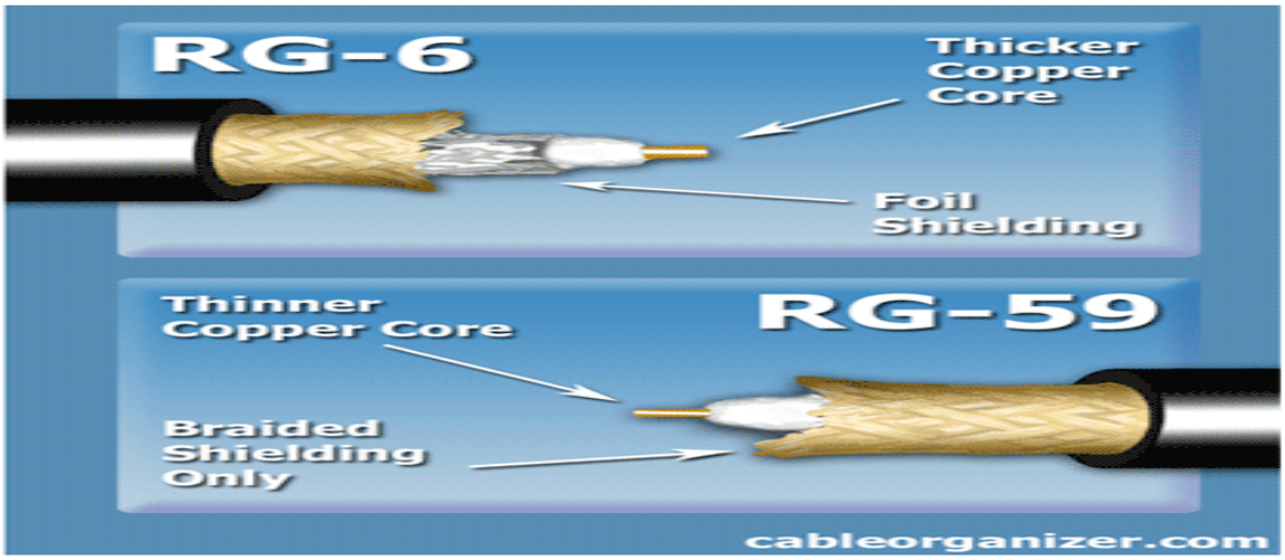
Two Types : Thicknet and Thinnnet

1) ThickNet, or RG-6:

It is older and one of the first types of coaxial cable used in networks. Its thick shielding, very rigid and difficult to work with.

2) ThinNet or RG-59:

It is far more flexible than ThickNet and much easier to work with.



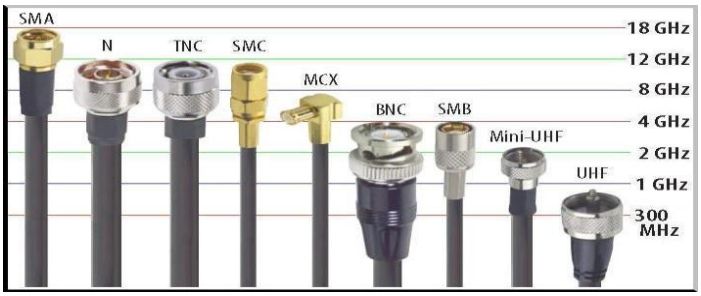
Advantages :

- Sufficient frequency range to support multiple channel, which allows for much greater throughput.
- Lower error rates. because the inner conductor is in a Faraday shield

Disadvantages:

- More expensive to install compare to twisted pair cable.
- The thicker the cable, the more difficult to work with.

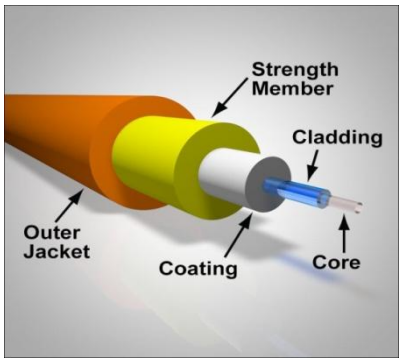
Connector used : BNC (Bayonet Neill Concelman).

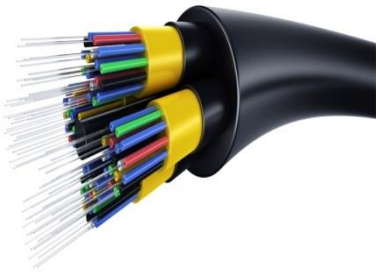


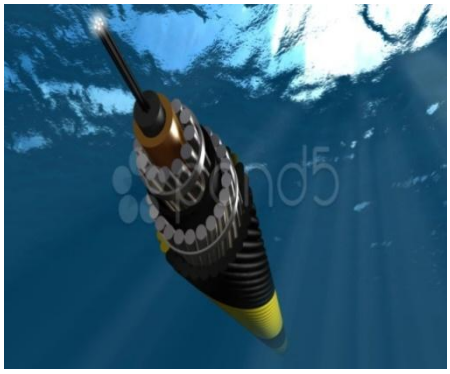
Fiber Optic Cable

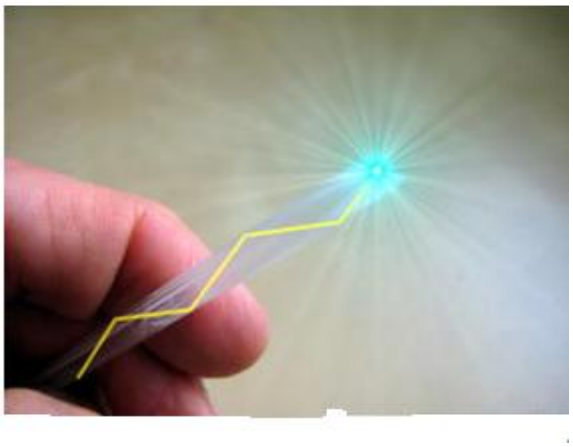
- A technology that uses glass (or plastic) threads (**fibers**) to transmit data.
- Fiber optic cables provide higher bandwidth and can transmit data over longer distances.
- Fiber optic cables support much of the world's internet, cable television and telephone systems.
- Fiber cables rated at 10 Gbps, 40 Gbps and even 100 Gbps are standard.
- Fiber optic cables carry communication signals using pulses of light generated by small lasers or light-emitting diodes (LEDs).
- Speed of light 3 x 10^8 m/s , 30000 km/s.

- In sender side Electrical signal is converted in light signal by the help of transducer and at receiver side light signal is again converted into electrical signal by using transducer.









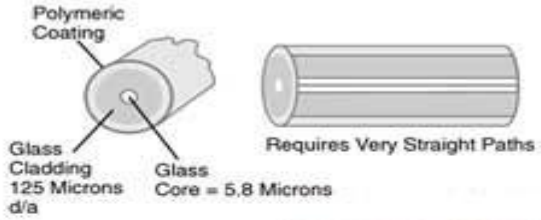
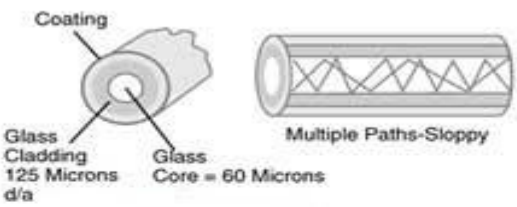
Types of fiber cables

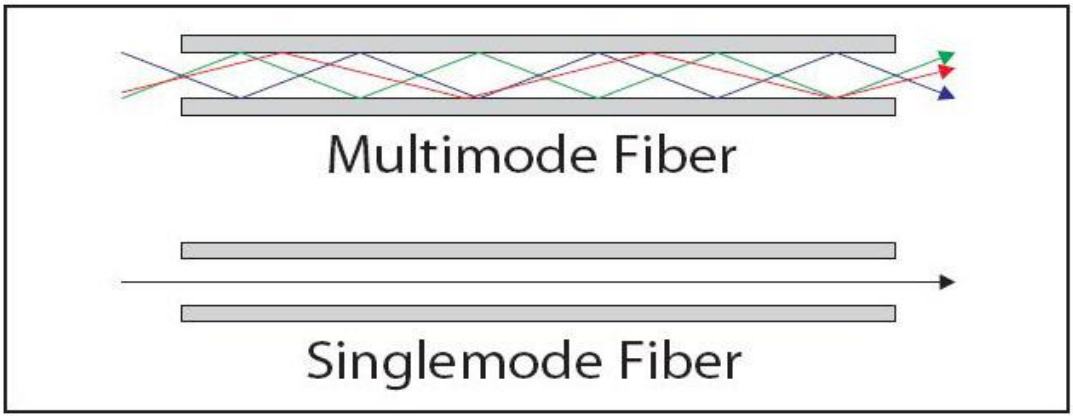
1.) Single Mode:

Single mode fiber is optical fiber that is designed for the transmission of a single ray or mode of light as a carrier and is used for long-distance signal transmission.

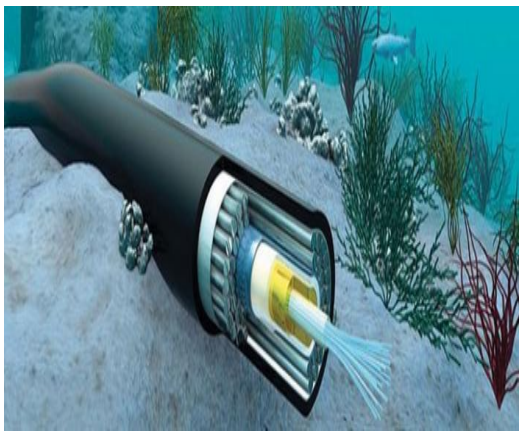
2.) Multimode:

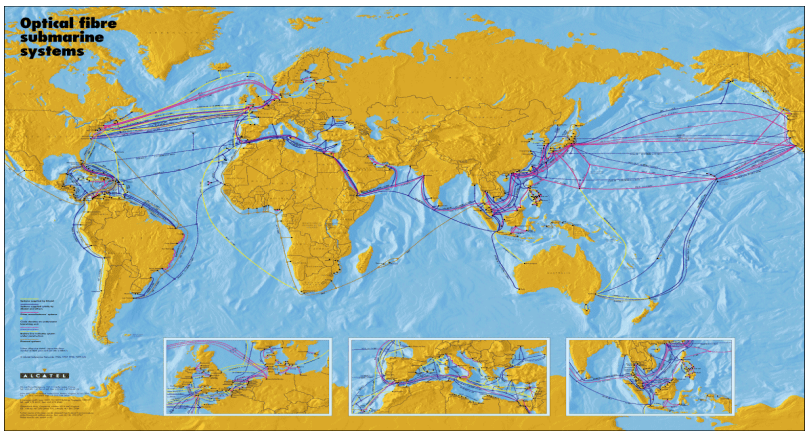
Multi-mode optical fiber is a type of optical fiber mostly used for communication over short distances, such as within a building or on a campus. Typical multi-mode links have data rates of 10 Mbit/s to 10 Gbit/s over link lengths of up to 600 meters (2000 feet).

Single-Mode	Multimode
	
• Small Core • Less Dispersion • Suited for Long-Distance Applications (Up to ~ 3 km) • Uses Lasers as the Light Source Often Within Campus Backbones for Distances of Several Thousand Meters	• Larger Core Than Single-Mode Cable (50 Microns or Greater) • Allows Greater Dispersion and, Therefore, Loss of Signal • Used for Long-Distance Application, but Shorter Than Single-Mode (Up to ~ 2 km • Uses LEDs as the Light Source Often Within LANs or Distances of a Couple Hundred Meters Within a Campus Network



Optical fiber cable under sea





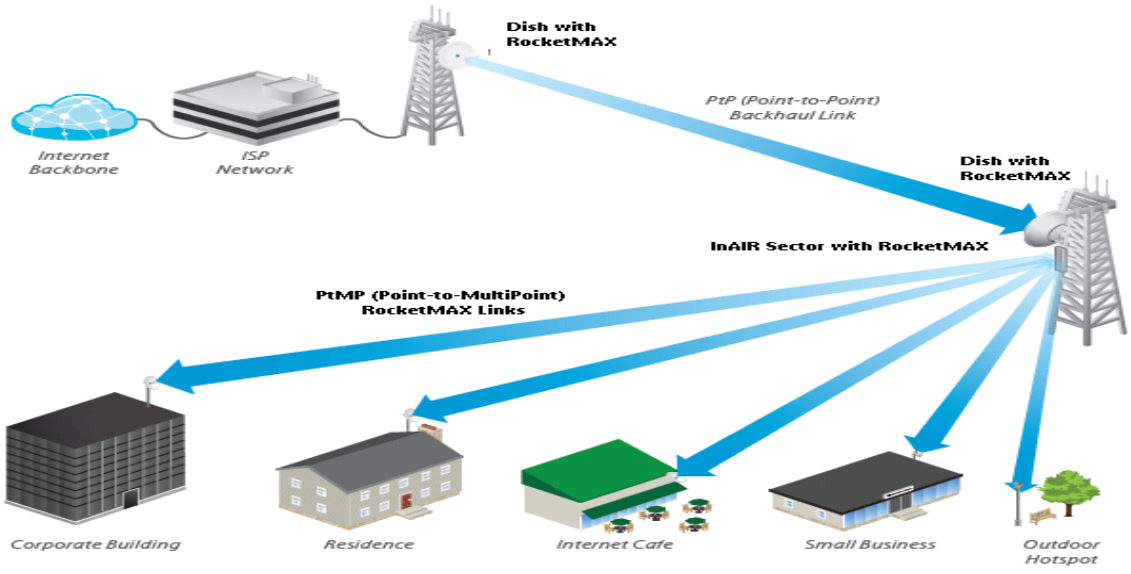
Optical fibre Cable Connectors

Wireless Media

Microwaves:

Microwave link. A *microwave* link is a communications system that uses a beam of radio waves in the *microwave* frequency range to transmit video, audio, or data between two locations, which can be from just a few feet or meters to several miles or kilometers apart.

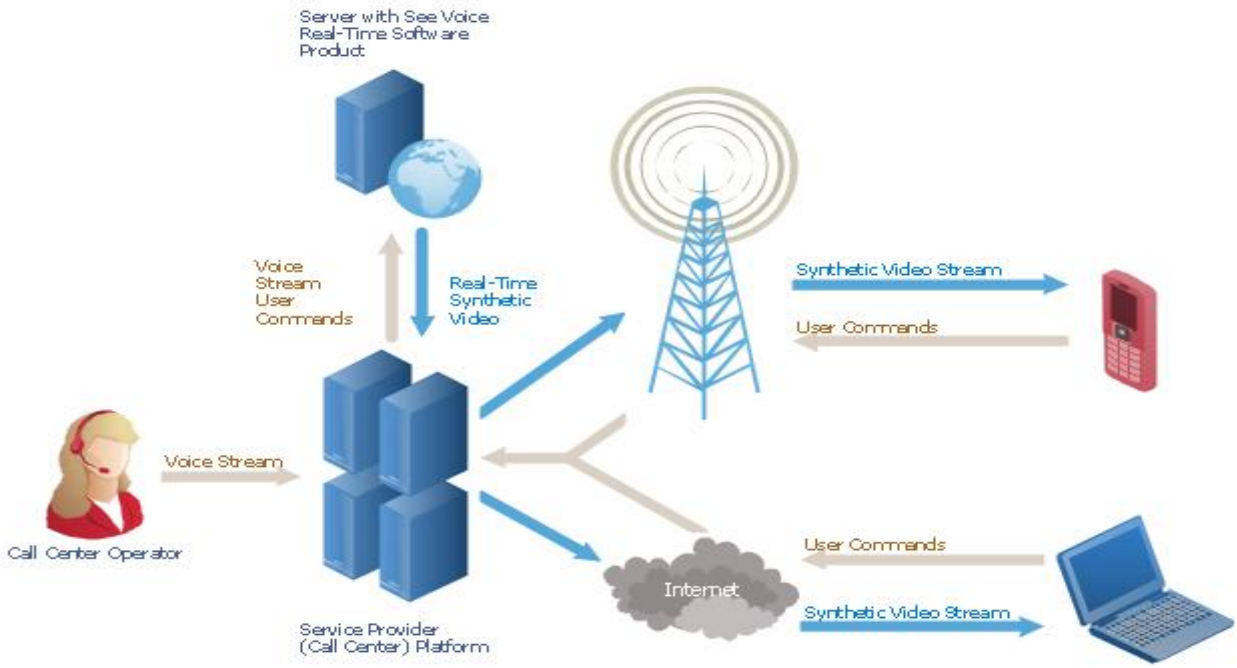
Microwaves travel by line-of-sight;



Radio wave:

Radio waves are a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared light. Radio waves have frequencies as high as 300 GHz to as low as 3 kHz.

A wireless *network* uses *radio waves*, just like cell phones, televisions and radios.



Infrared wave:

Method of transferring data without the use of wires. A common example of an infrared (Ir) device is a TV remote. However, infrared is also used with computers and devices like a cordless keyboard or mouse, wifi routers.

Infrared technology allowed computing devices to communicate via short-range wireless signals in the 1990s. Using IR, computers could transfer files and other digital data bi directionally. The infrared transmission technology used in computers was similar to that used in consumer product remote control units. Infrared was replaced in modern computers by the much faster Bluetooth and Wi-Fi technologies.

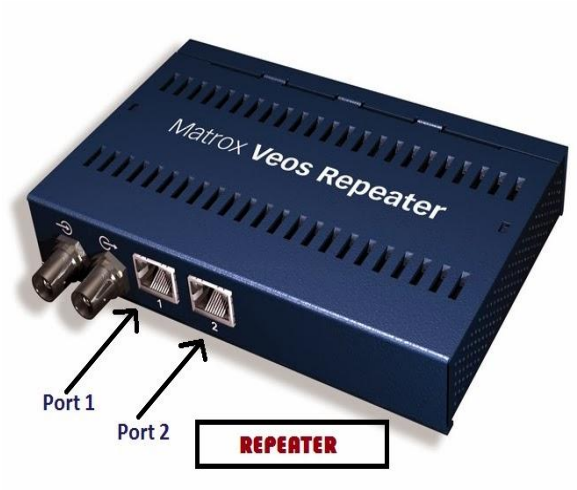
Bluetooth:

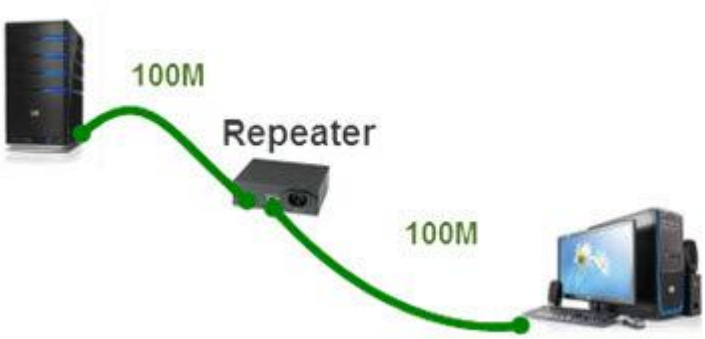
Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks(PANs).

Bluetooth refers to a wireless technology which allows digital devices to easily transfer files at high speed. Bluetooth is common in many portable devices such as laptops, PDAs, mobile phones, smartphones and tablets.

Networking devices

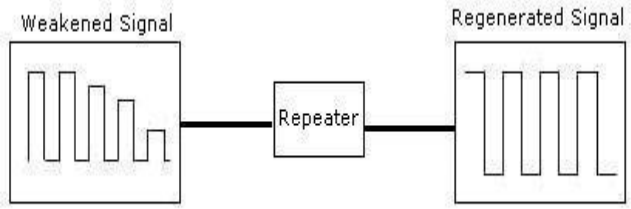
1. **Repeater**: This is used to convert weak signals into strong signals.





Repeater

- Repeater operates on physical layer.
- It receives the signal before it becomes corrupted and regerates the original bit pattern.
- It allows to extend the physical length of the network.
- It doesn't change the functionality of network.



2.Hub: It is used to connect multi devices.

3.**Switch**: It is same as hub but it is smarter and faster.

Two types : Manageable and Non Manageable Switch

Differences between Hub and Switch:

HUB	SWITCH
1. It is layer 1 device of OSI mode.	1. It is layer 2 device of OSI mode. Some switch are layer 3 devices.
2. Max speed 10mbps.	2. Speed = 100Mbps, 1Gbps, 10Gbps, 40 Gbps.
3. Works in half duplex mode.	3. Works in full duplex mode.
4. It broadcast the packet to all its ports.	4.Unicast the packet to its destination(one time broadcast only)

Transmission Modes:

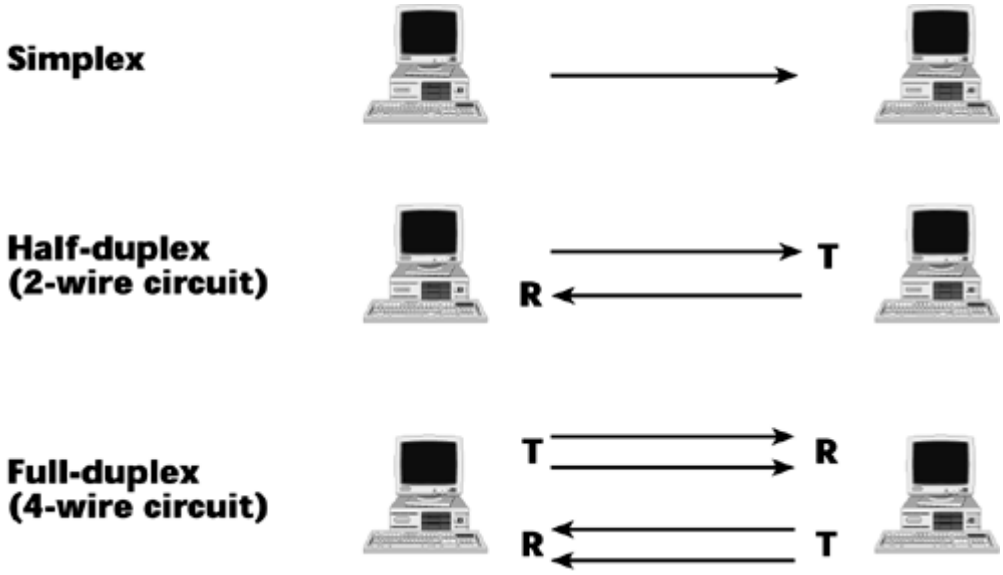
1) **Simplex:-** In this mode, the communication between sender and receiver occur only in one direction.

   That means only the sender can transmit the data to receiver but receive can't.

2) **Half- Duplex:-** In this mode, the communication between sender and receiver occurs in both the directions but, one at a time.

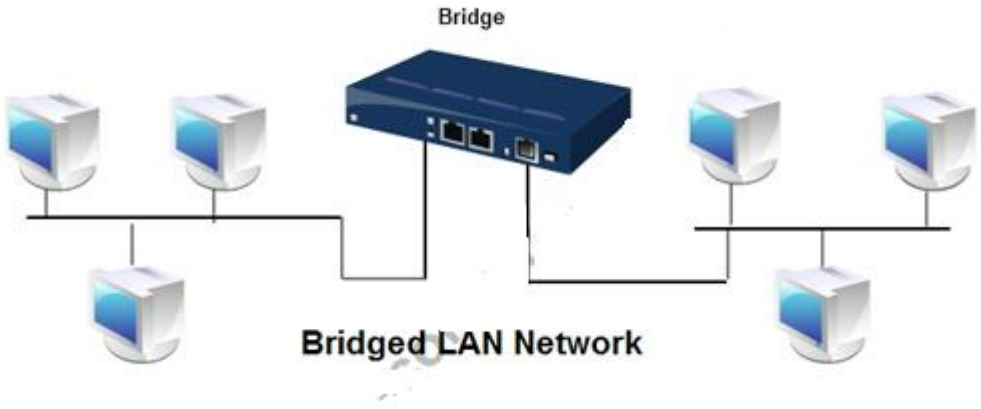
   The sender and receiver both can transmit and receive the information but, only one is allowed to transmit at a time.

3) **Full-Duplex:-** In this mode, the communication between sender and receiver can occur simultaneously.
   Sender and receiver both can transmit and receive simultaneously at the same time.



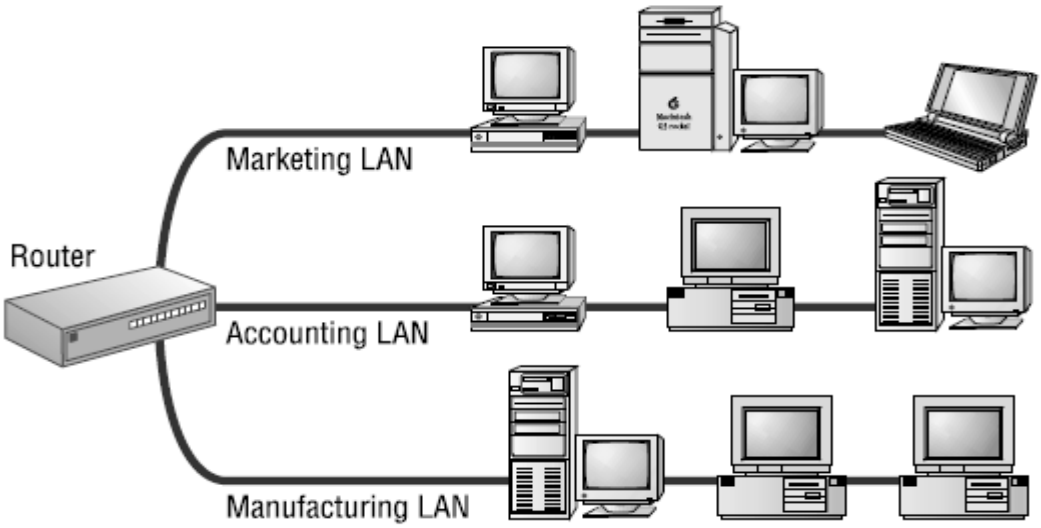
4. Bridge:

It is same as switch but have two or three port only.

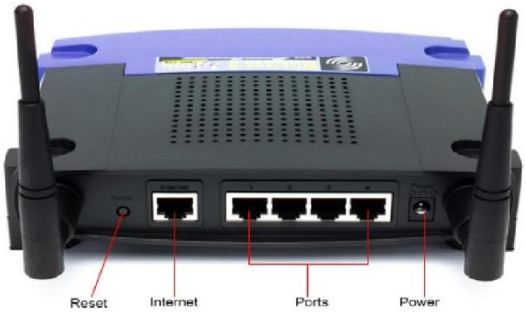


5. Router:

It is used to connect from two different networks.



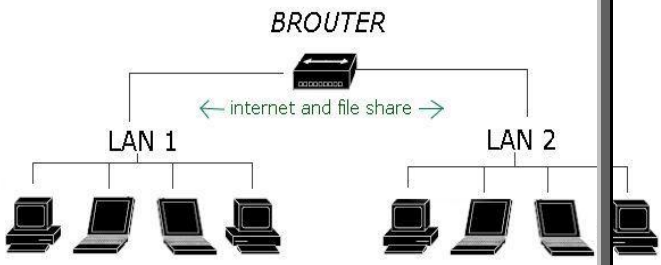
Two types: Home or Office use router and Enterprise router



6. **Brouter:**

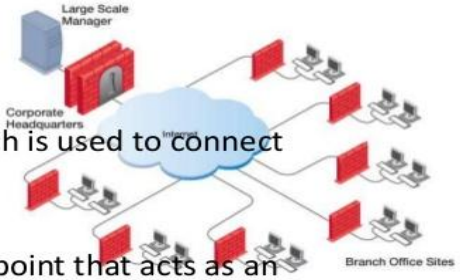
Brouters

- Brouters are a combination of router and bridge.
- Brouters are operated in network layer(routable protocols) & data link layer(non-routable protocols).
- Brouter provides combine features of router for routing protocol & bridge for non-routable protocol.



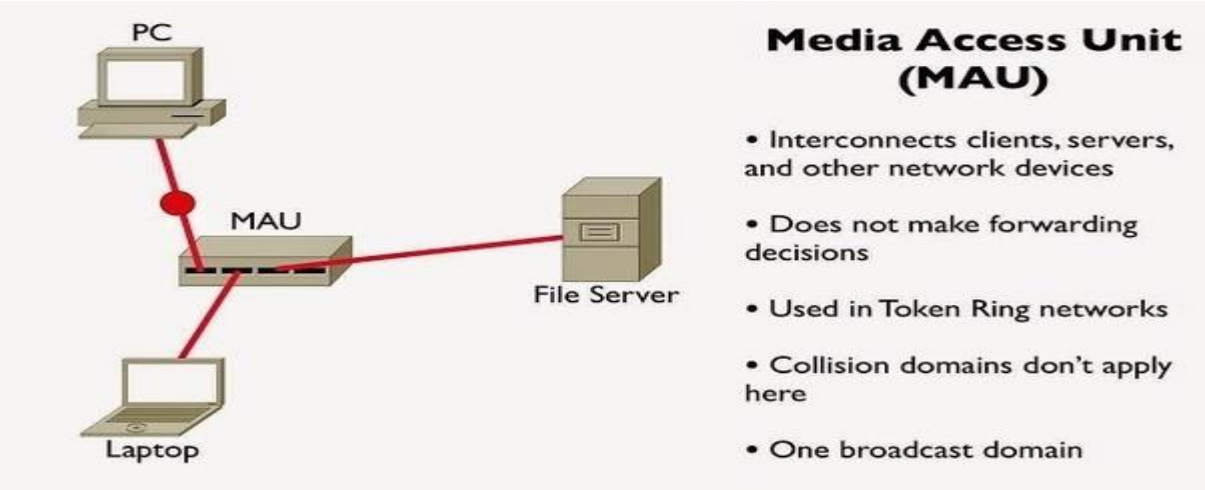
7. **Gateway:**

Gateways



- Gateway is a device which is used to connect multiple networks.
- A **gateway** is a **network** point that acts as an entrance to another **network.**
- It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols.
- A router is also a gateway, since it interprets data from one network protocol to another.

8. **MAU (Multistation Access Unit)**



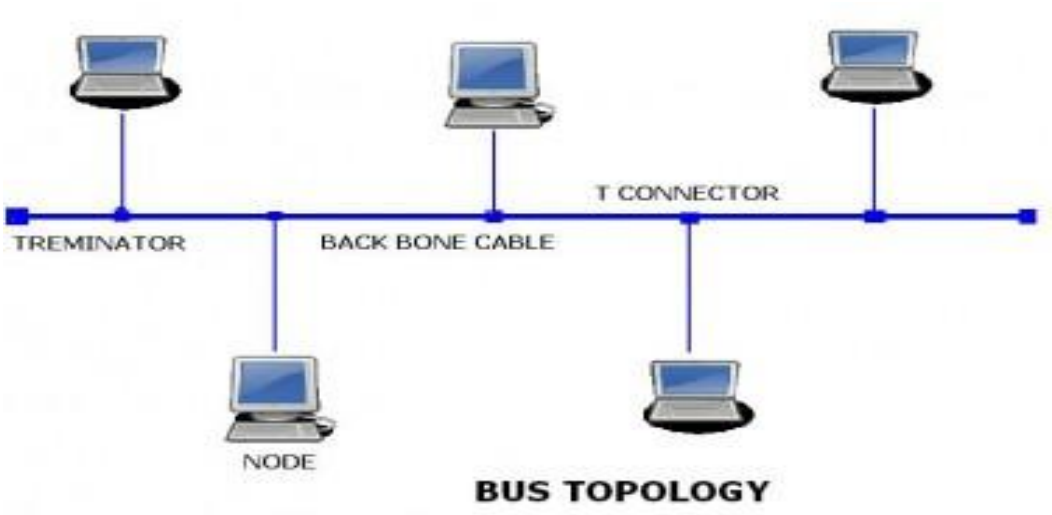
Networking Topology

It is the physical arrangement of networking devices to make a network.

Types of Topology:-

1) Bus **2)** Star **3)**Ring **4)**Mesh **5)**Tree **6)**Wireless

BUS TOPOLOGY:



1. Coaxial cable is used.
2. Now it is absolute.

Advantages of Bus Topology

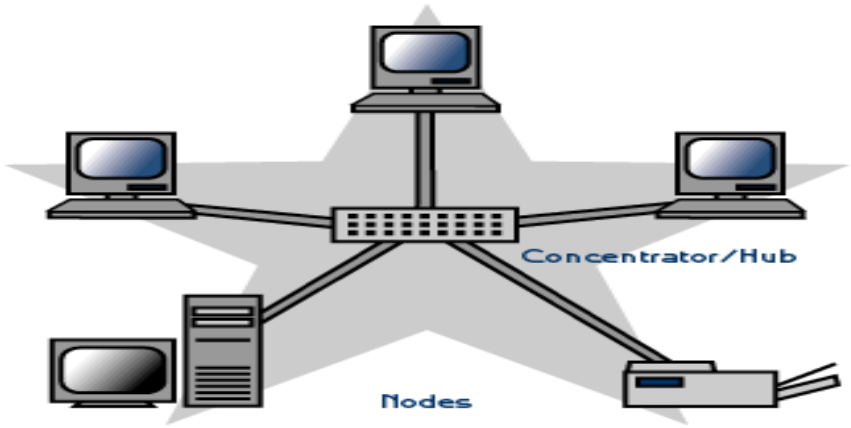
- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution.

Star Topology:

Twisted pair cable is used.



Advantages of a Star Topology

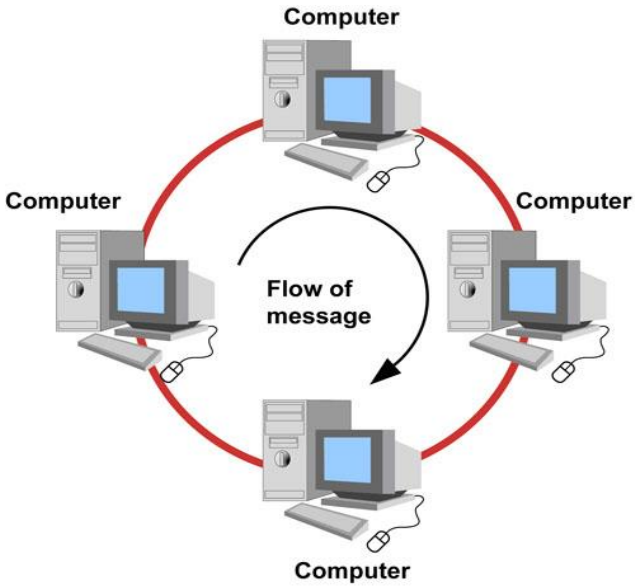
- Easy to install and configure.
- No disruptions to the network when adding or removing devices.
- Easy to detect faults and to remove parts.

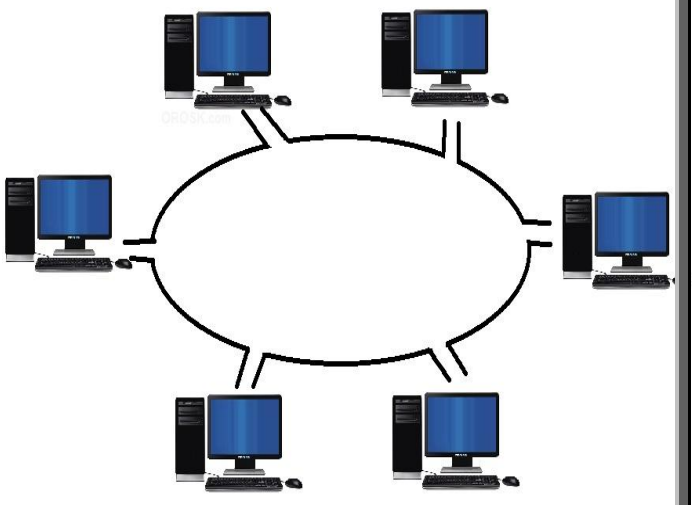
Disadvantages of a Star Topology

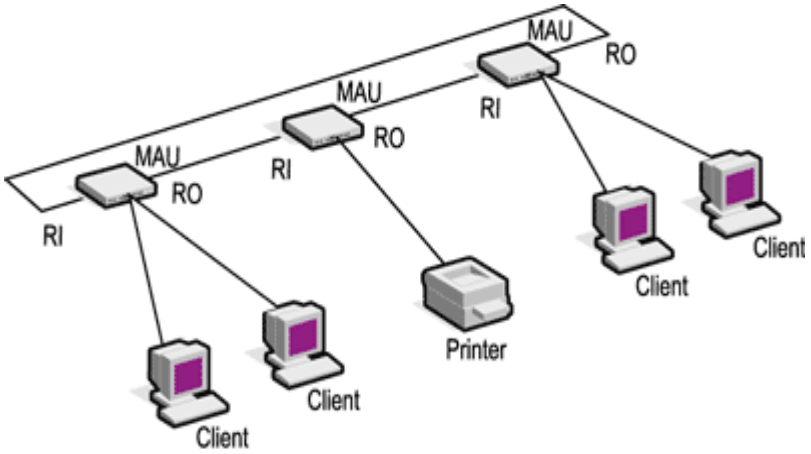
- Requires more cable length than a linear topology.
- If the hub or switch fails the entire network goes down.

Ring Topology

Here we require separate NIC card which supports Ring Topology.







Advantages of Ring Topology

1) This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision.

2) Even when the load on the network increases, its performance is better than that of Bus topology.

4) Additional components do not affect the performance of network.

5) Each computer has equal access to resources.

Disadvantages of Ring Topology

1) Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.

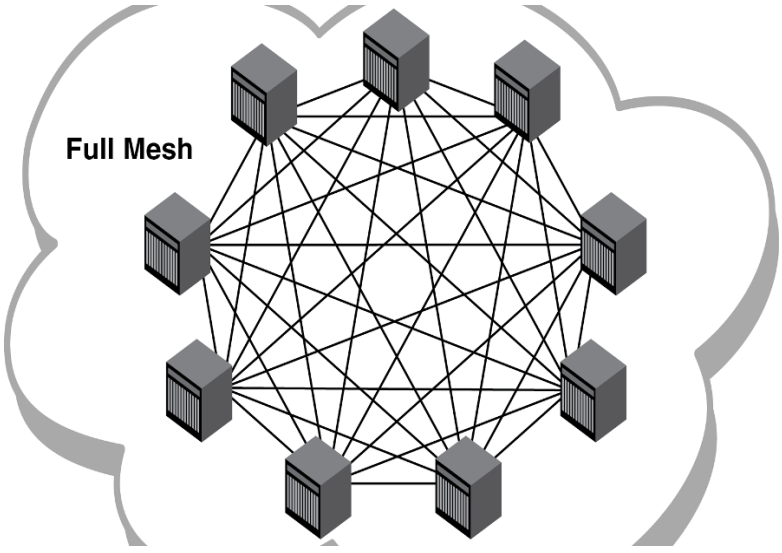
2) If one workstation or port goes down, the entire network gets affected.

3) Network is highly dependent on the wire which connects different components.

4) MAU's and network cards are expensive as compared to Ethernet cards and hubs.

Mesh Topology

A network setup where each computer and network device is interconnected with one another, allowing for most transmissions to be distributed, even if one of the connections go down.



Two types: Full Mesh and Partial Mesh

Full *mesh topology*: Each network

node (workstation or other device) is connected directly to each of the others.

Partial *mesh topology*: Some nodes are connected to all the others, but others are only connected to those nodes with which they exchange the most data.

Advantages of mesh topology:

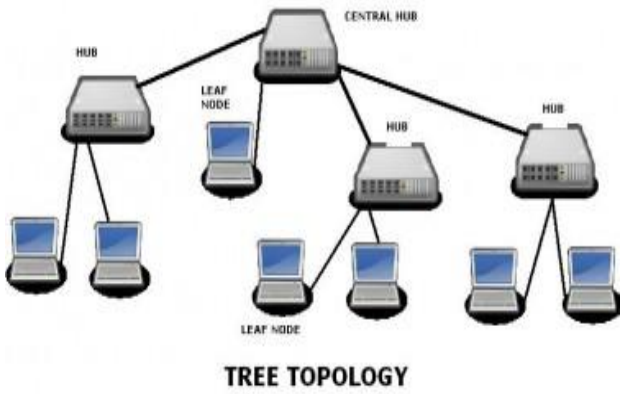
- Each connection can carry its own data load.
- Data transfer rate is high.
- A fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of mesh topology:

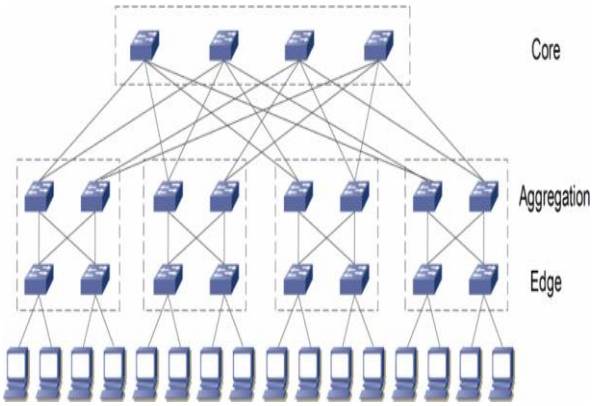
- Installation and configuration are difficult if the connectivity gets more.
- Very very costly.
- Bulk wiring is required.

Tree Topology

It is the combination of multiple topologies.



TREE TOPOLOGY



Advantages of tree topology:

- Scalable as leaf nodes can accommodate more nodes in the hierarchical chain.
- A point to point wiring to the central hub as each intermediate node of a tree topology represents a node in the bus topology
- Other hierarchical networks are not affected if one of them gets damaged.
- Easier maintenance and fault finding.

Disadvantages of tree topology:

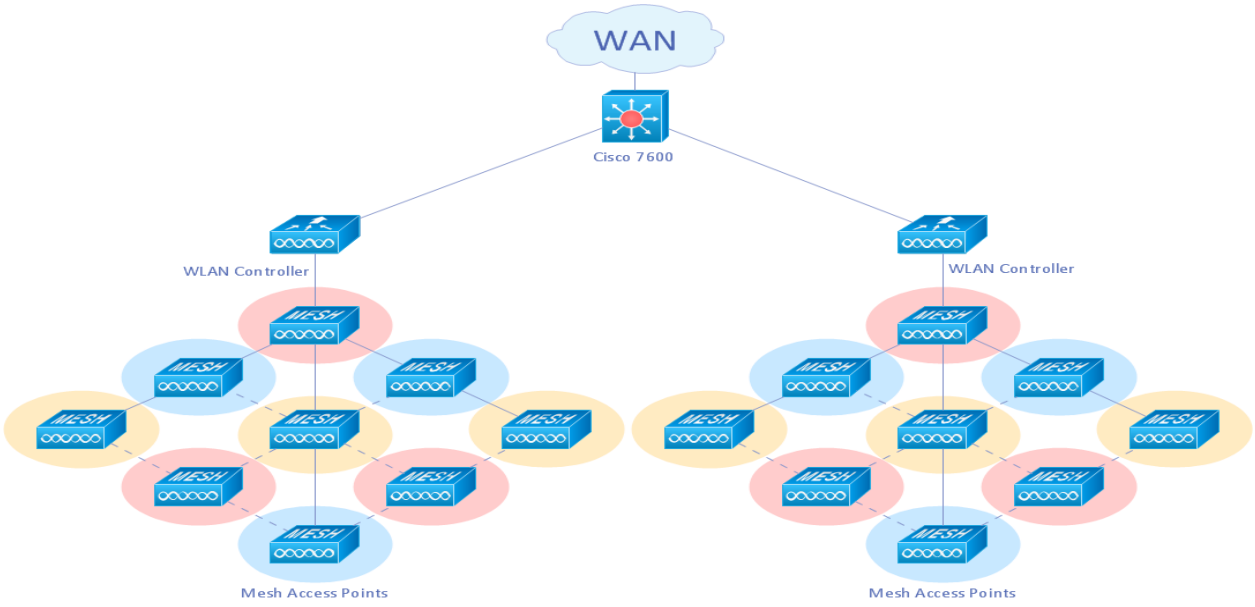
- Huge cabling is needed.
- A lot of maintenance is needed.
- Backbone forms the point of failure.

Wireless Topology

- Wireless network topology is a logical topology.
- It shows how the computers connect and interact each other when there is no physical connection, no cables connecting the computers.
- The computers communicate each other directly, using the wireless devices.
- Wireless networks can have infrastructure or ad hoc topology.

Ad hoc network

- The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks.
- Wireless mobile *ad hoc* networks are self-configuring, dynamic networks in which nodes are free to move.

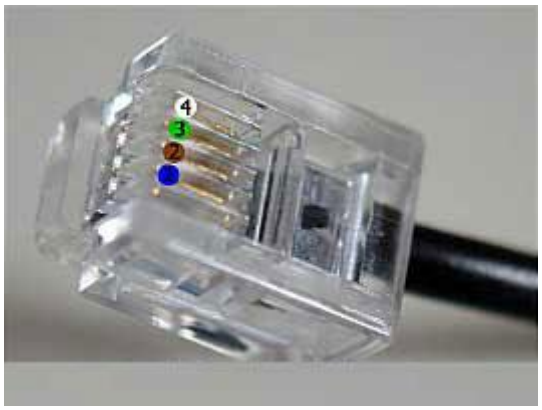


Media Connector

RJ-11 (Registered Jack):

- Standard telephone cable connectors.
- RJ-11 has 4 wires (and RJ-12 has 6 wires).
- A four or six-wire connector primarily used to connect telephone equipment.

RJ-11 Pin	Signal Name
1	VCC (5 volts regulated)
2	Power Ground
3	One Wire Data
4	One Wire Ground



RJ-45 (Registered Jack):

- The RJ-45 connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN).

ST (Straight Tip) :

- ST stands for Straight Tip.
- ST Connectors are among the most commonly used Fiber optic connectors in networking applications.

SC (Subscriber Connector or Standard Connector):

- A fiber-optic cable connector that uses a push-pull latching mechanism similar to common audio and video cables.
- For bi-directional transmission, two fiber cables and two SC connectors (Dual SC) are used.

SC connector

ST connector

BNC Connector:

- The BNC (Bayonet Neill–Concelman) connector is a quick connect/disconnect radio frequency connector used for coaxial cable.
- *BNC connector* commonly used plug and socket for audio, video and networking applications that provides a tight connection.

BNC Tee connector:

- A Tee connector is an electrical connector that connects three cables together.
- It is usually in the shape of a capital T.
- It is usually used for coax cables and the three connector points can be either female or male gender, and could be different or the same standard.

AUI Connector (Attachment Unit Interface):

- A 15 pin connector found on Ethernet cards that can be used for attaching coaxial, fiber optic, or twisted pair cable.

Types of cables used for networking: cabling

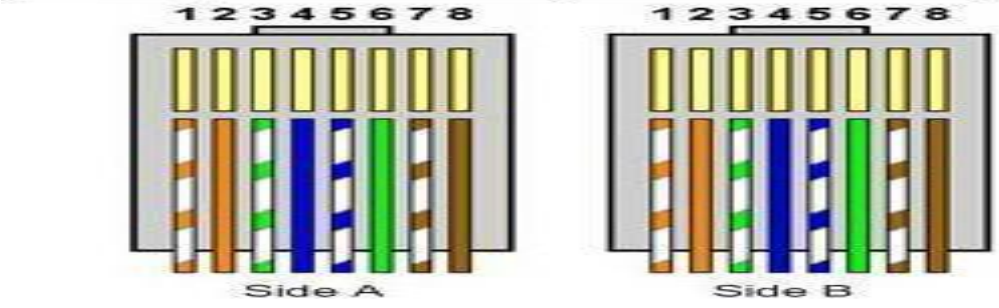
1) STRAIGHT CABLES:

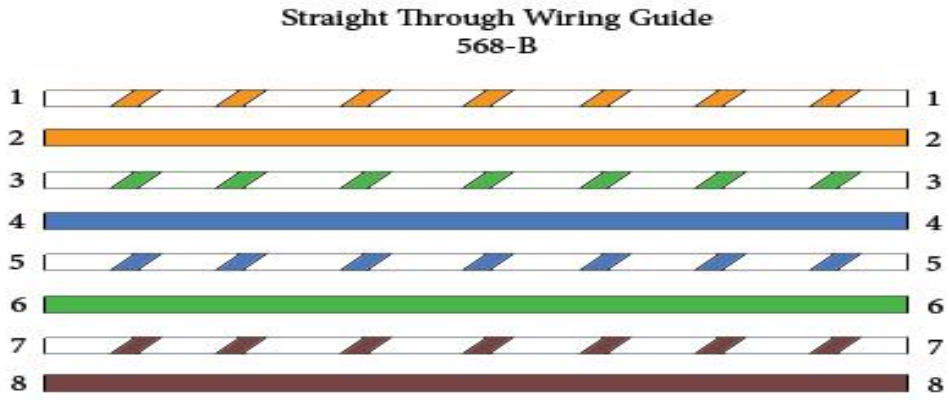
Straight cable is used to connect different type of devices. This type of cable will be used most of the time and can be used to:

1) Connect a computer to a switch/hub's normal port.
2) Connect a computer to a cable/DSL modem's LAN port.
3) Connect a router's WAN port to a cable/DSL modem's LAN port.
4) Connect a router's LAN port to a switch/hub's uplink port. (normally used for expanding network)
5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

If you need to check how straight cable looks like, it's easy. **Both side (side A and side B) of cable have wire arrangement with same color.**

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown





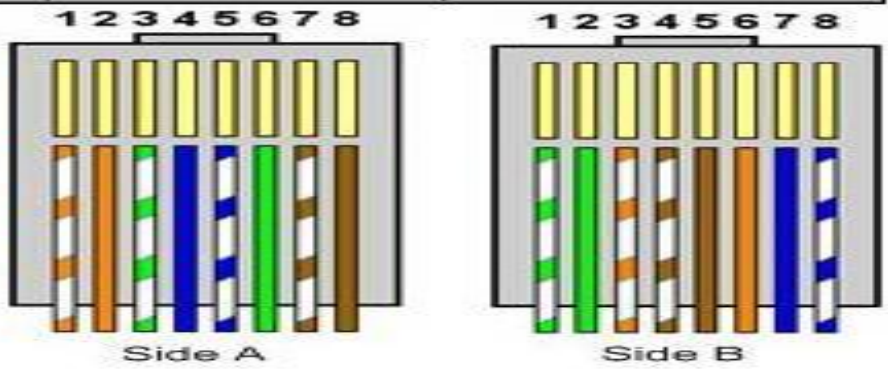
2) Crossover Cable:

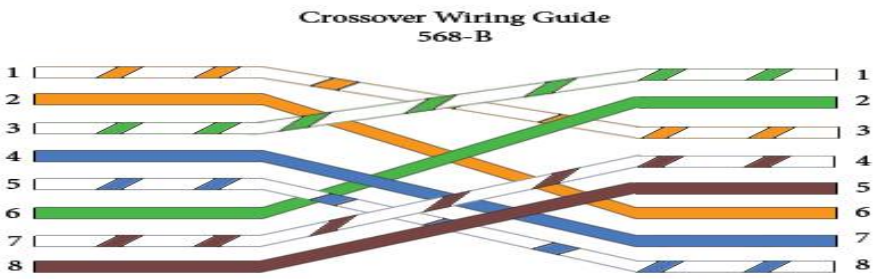
Crossover cable is used to connect same type of devices.

1) Connect 2 computers directly.
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
3) Connect 2 switches/hubs by using normal port in both switches/hubs.

If you need to check how crossover cable looks like, **both side (side A and side B) of cable have wire arrangement with following different color .**

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



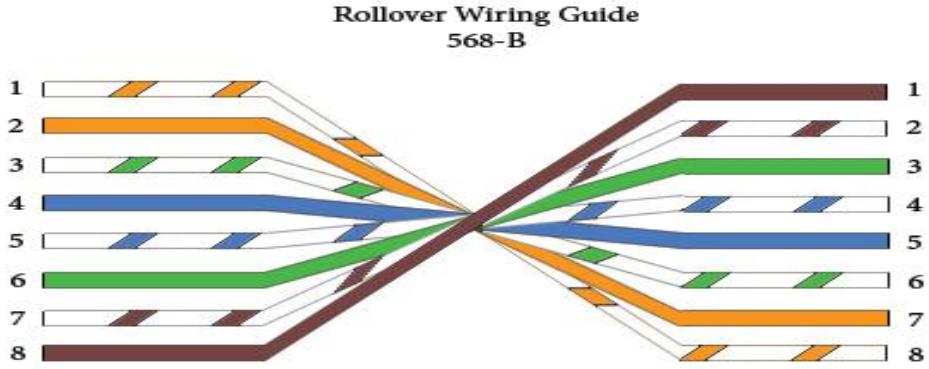


In case you need to make a crossover cable yourself! You can use crimper to do it.

Note: If there is **auto MDI/MDI-X** feature support on the switch, hub, network card or other network devices, you don't have to use crossover cable in the situation. This is because crossover function would be enabled automatically when it's needed.

3) Rollover Cable:

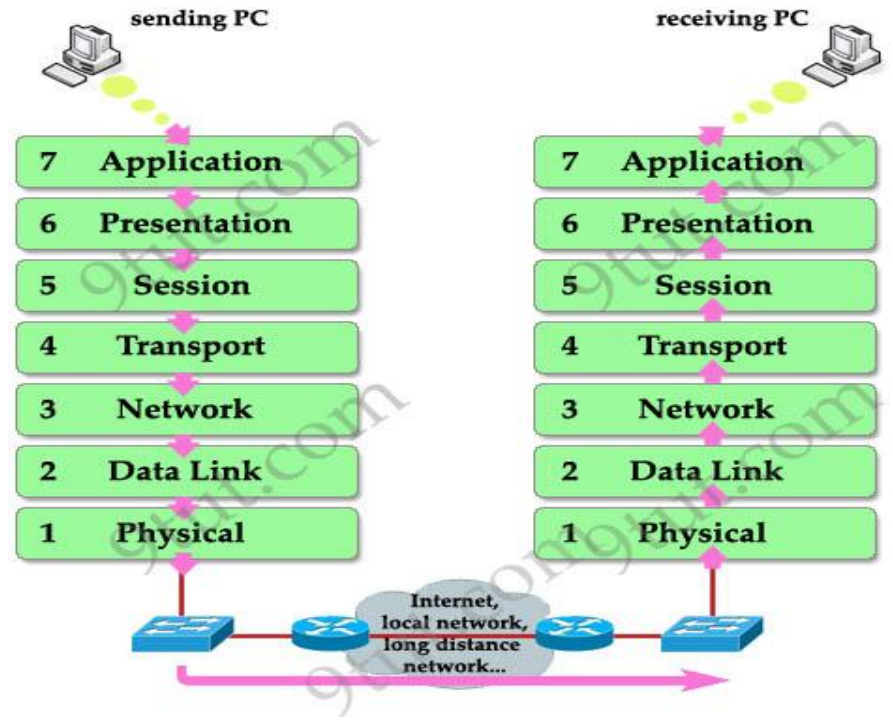
- A rollover cable is a network cable that connects a computer terminal to a network router's console port to make programming changes to the device.
- It is also referred to as a Cisco console cable and is normally flat and light blue so as to distinguish it from other network cable types.
- Rollover cables are also known as Yost cables or Yost Serial Device Wiring Standard connectors.
- Pin 1 of connector A would be connected to Pin 8 of connector B.
- Pin 2 of connector A would be connected to Pin 7 of connector B and so on.



OSI Layer

- Open System Interconnect (OSI) developed by ISO in 1970.
- Defines *a networking framework to implement protocols in seven layers.*
- Communication over network is understandable through this OSI model.
- OSI having 7 layers and each layers has its own responsibilities.
- Hardware and software work together.
- Troubleshooting is easier by separate networks.

Known as	Layer no.	OSI layer	Format of Data	NW devices used
Upper Layer or User access Layer	Layer-7	Application Layer	Data	
	Layer-6	Presentation Layer		
	Layer-5	Session Layer		
Heart/Core of OSI	Layer-4	Transport layer	Segment	
Lower Layer or NW access Layer	Layer-3	Network layer	Packet	Router,
	Layer-2	Data Link Layer	Frame	Switch, Bridge
	Layer-1	Physical Layer	Bits	Hub, Repeater, Networking cable



OSI Layer

Protocol:-

- A **protocol protocol** is a set of rules in which **computers** communicate with each other.
- The **protocol** says what part of the conversation comes at which time.
- It also says how to end the communication.

OSI Layers	Associated Protocol
Application	*WWW browsers, NFS, SNMP, Telnet, HTTP, FTP*
Presentation	*ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI*
Session	*NFS, NetBios names, RPC, SQL*
Transport	*SPX, TCP, UDP.*
Network	*AppleTalk DDP, IP, IPX.*
Data Link	*PPP, FDDI, ATM, IEEE 802.3, HDLC, Frame Relay.*
Physical	*Ethernet, FDDI, B8ZS, V.35, V.24, RJ45.*

Physical Layer responsibilities

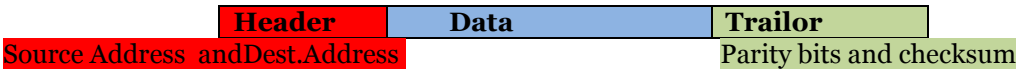
- Type of connection : Physical or Wireless
- Type of signal : Electrical, Light or Radio signal
- Types of communication mode : Simplex, Half duplex or Full duplex
- Transmit a **bit** over the electrical Signals.

Data Link Layer Responsibilities

- Receive bits from physical layer.
- Controls frame synchronization, flow control and error checking.
- Have two sublayer : LLC and MAC
- **Logical Link Control** (**LLC**) For IEEE 802, flow control, error control, and part of the framing duties are all brought together in this **LLC** sub-layer.
- **MAC layer** is responsible for moving data packets to and from one Network Interface Card (NIC) to another across a shared channel.

- MAC address adding(Physical addressing).

Framing : ***Framing*** is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.



- **Data -** The packet from the Network layer
- **Header -** Contains control information, such as addressing, and is located at the beginning of the PDU.
- **Trailer -** Contains control information added to the end of the PDU.
- **PDU -**Protocol Data Unit.
- ***Parity bits*** are used as the simplest form of error detecting code.
- ***Checksum*** is a method of checking for errors in a communications system.

Network Layer responsibilities

- Receive frame from data link layer
- Provides routing and switching
- Error handling, congestion control and packet sequencing.
- Do logical addressing (IP addressing)

Transport Layer responsibilities

- Responsible for end-to-end error recovery and flow control.
- It ensures complete data transfer.
- Two main Protocol : TCP and UDP
- Data segmentation is done here

Session Layer responsibilities

- Establishes, manages and terminates connections between applications.
- It deals with session and connection coordination.
- Dialogue control and session management.

Presentation Layer responsibilities

- Encoding-decoding
- Encryption-decryption
- Compression-decompression
- Changing file format: jpeg, gif, midi, mpe4

Application Layer responsibilities

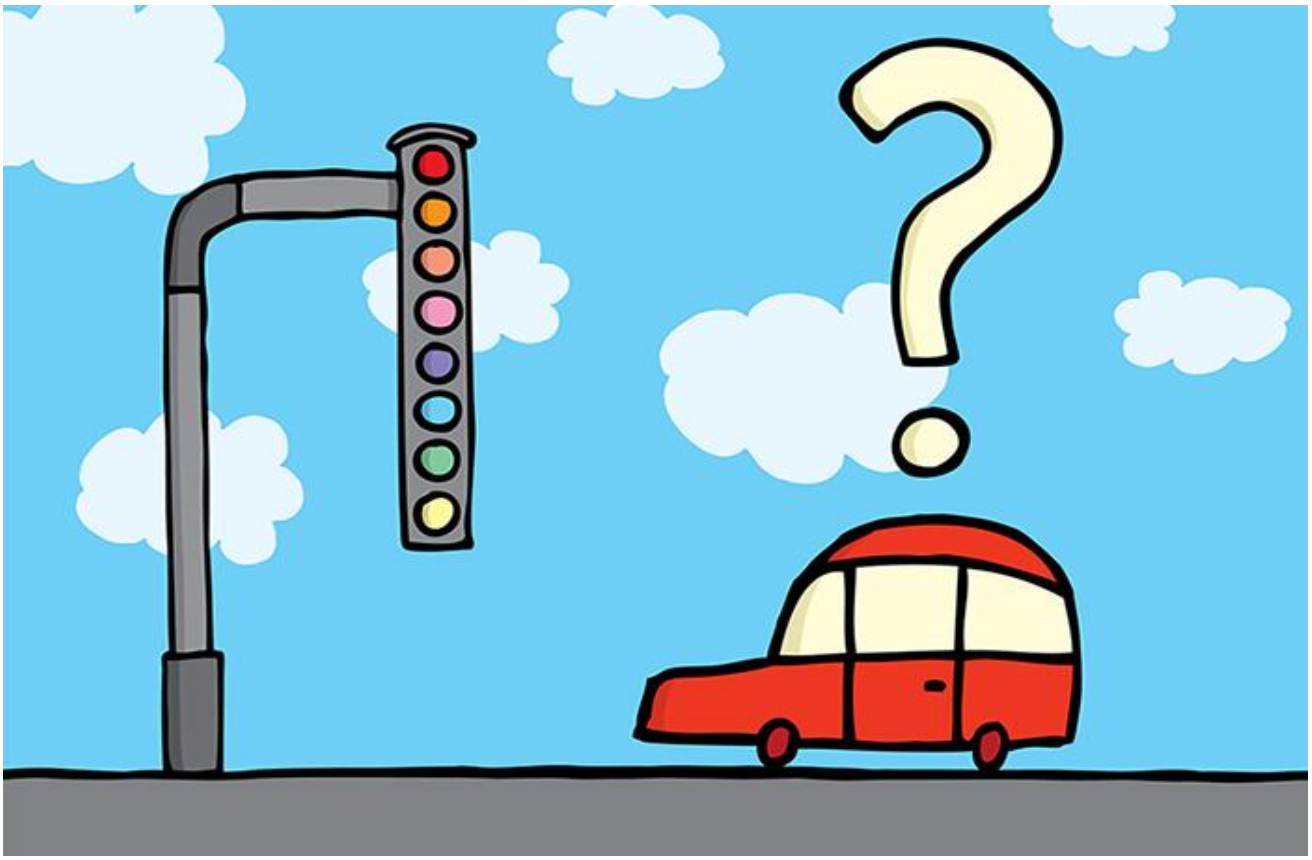
The layer provides an interface for the user interact with the application such as Email, HTTP, FTP, Remote file access.

- Authentication, File access, Management etc.

Networking Protocol

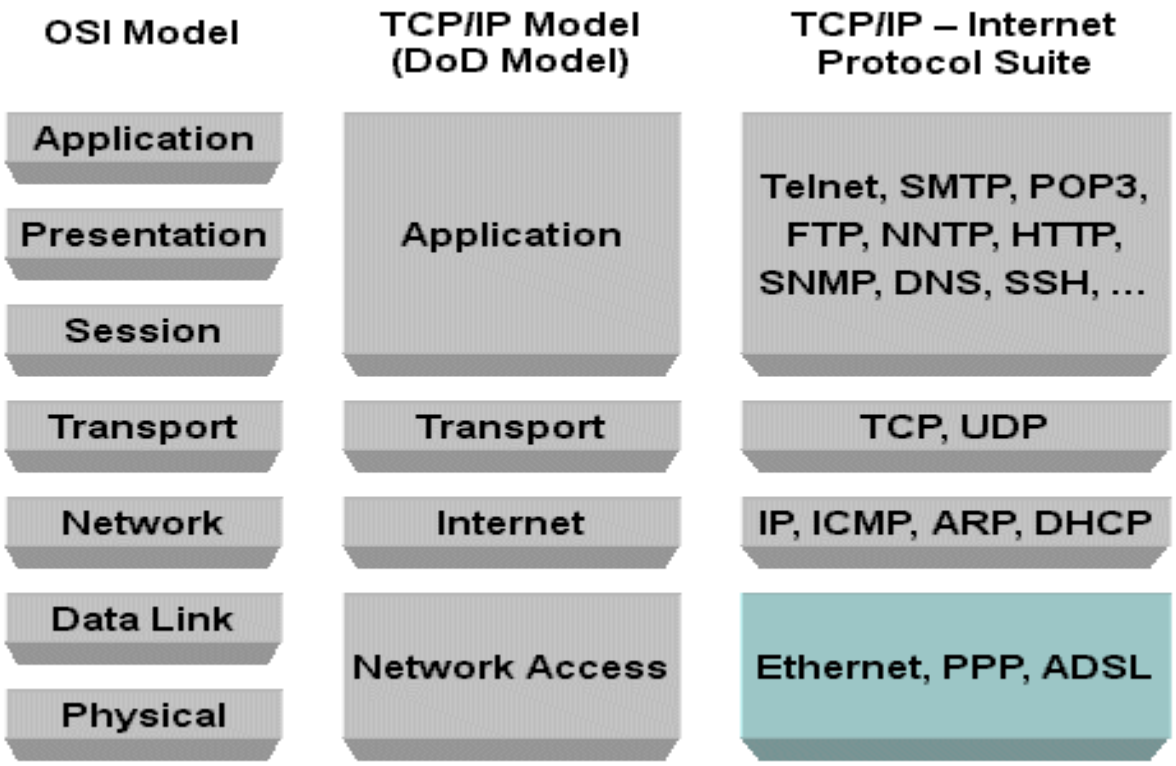
- A protocol is set of rules that must be followed while communicating two networking devices.
- A protocol is the special set of rules that end points in a telecommunication connection use when they communicate.
- Protocols specify interactions between the communicating entities.

Operating System	Network protocol
Windows	TCP/IP
Linux	TCP/IP
Netware	IPX/SPX
Mac os	Apple talk



TCP/IP (Transmission Control Protocol/ Internet protocol)

- ✓ It is the collection of protocols and also called TCP/IP protocol suite.
- ✓ These protocols describe the movement of data between the source and destination or the internet.
- ✓ It consist of 4 layers and each layer having some protocols. Each protocol works independently but some protocol works together depend on the requirement.
- ✓
- ✓ It consist of 4 layers and each layer having some protocols.
- ✓ Each protocol works independently but some protocol works together depend on the requirement.

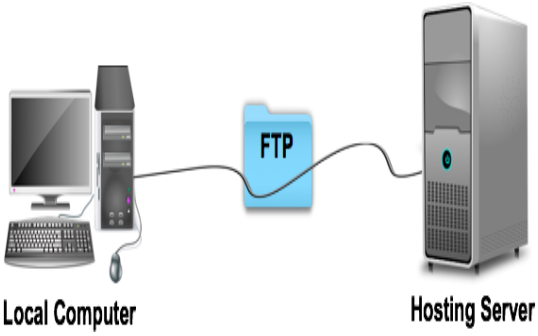


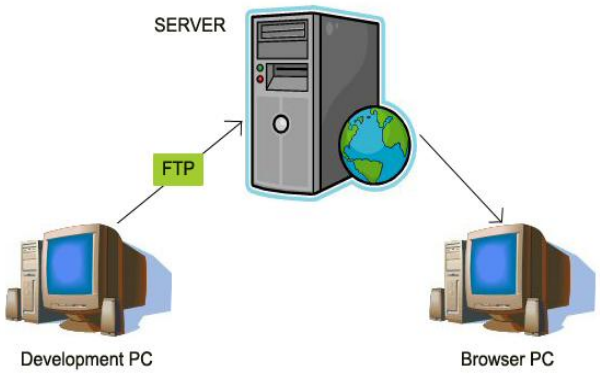
Application Layer Protocols

FTP:File Transfer Protocol

- Organizations use FTP to allow employees to share files across different locations and branch offices.
- Employees use FTP to securely share files with coworkers and external business partners.

- IT teams use FTP to transfer data back to DR (disaster recovery) sites.

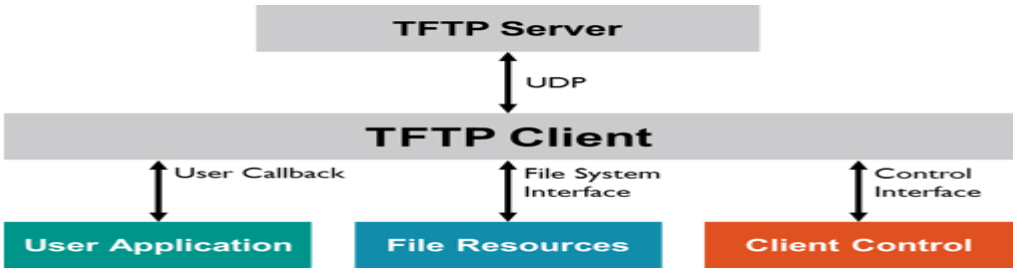




TFTP: Trivial File Transfer Protocol

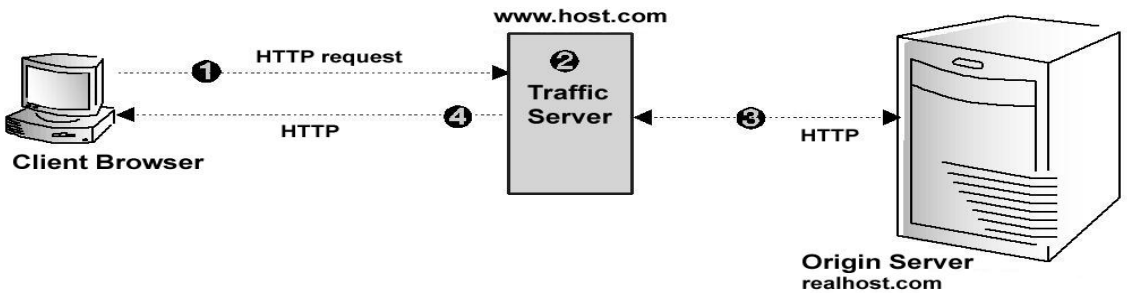
TFTP stands for Trivial File Transfer Protocol. It's a technology for transferring files between network devices, and is a simplified version of FTP (File Transfer Protocol).

TFTP is implemented using UDP, it generally works only on local area networks (LANs).



HTTP:Hyper Text Transfer Protocol

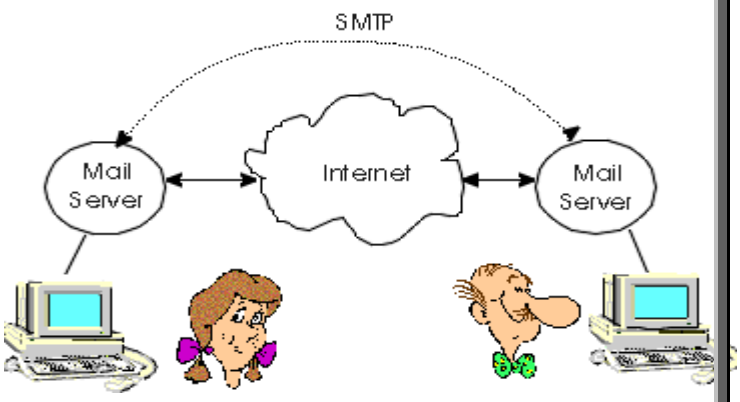
- HTTP means **H***yper* **T***ext* **T***ransfer* **P***rotocol*.
- HTTP is the underlying protocol used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
- When we enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.



HTTPS:Hyper Text Transfer Protocol Secure

It is more secure than HTTP.

SMTP:Simple Mail Transfer Protocol



SMTP stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another.

POP:Post Office Protocol

POP3 stands for Post Office Protocol.

POP3 allows an email client to download an email from an email server.

The POP3 protocol is simple and does not offer many features except for download.

Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects.

We can use only one computer to check your email (no other devices).

IMAP:Internet Message Access Protocol

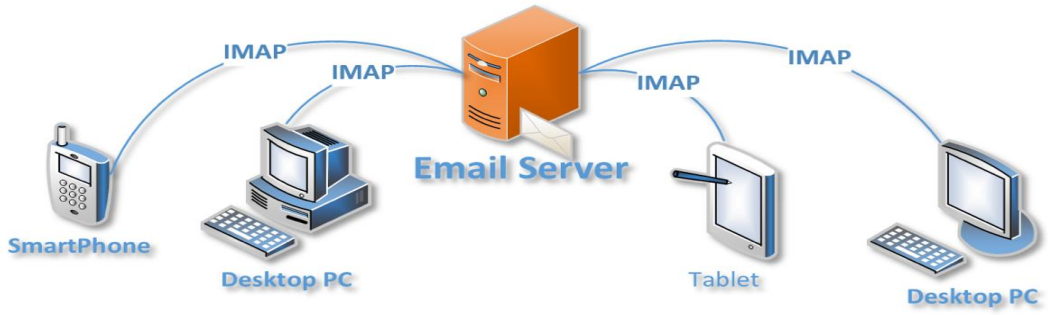
IMAP stands for Internet Message Access Protocol.

IMAP includes many more features than POP3.

The IMAP protocol is designed to let users keep their email on the server.

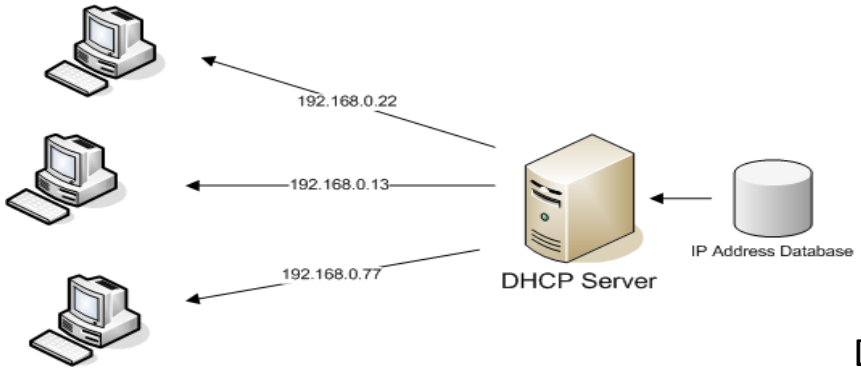
IMAP requires more disk space on the server and more CPU resources than POP3, as all emails are stored on the server

We can use multiple computers and devices to check your email.



DHCP: Dynamic Host Configuration Protocol

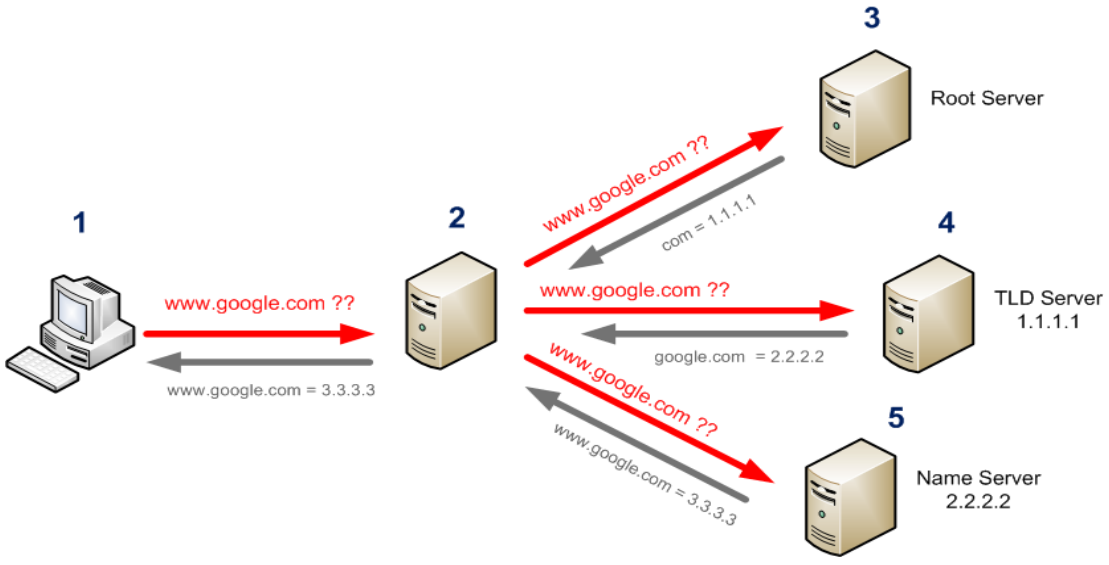
It is used to assign automatic IP address to client PC.

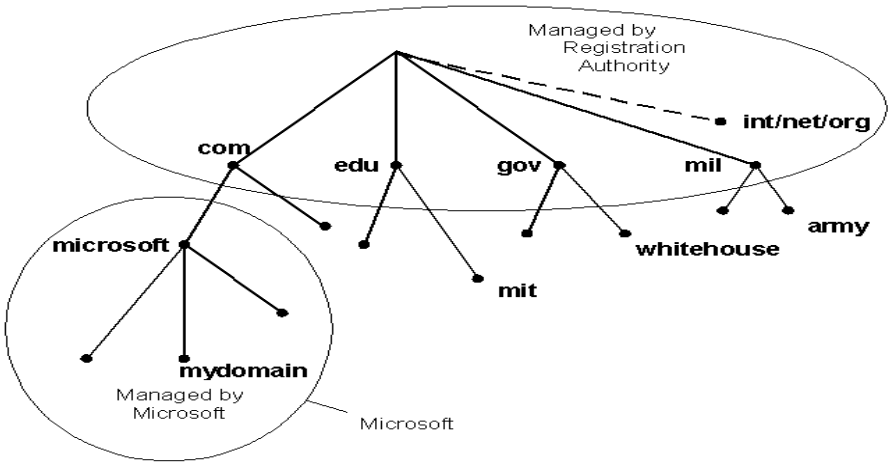


Dynamic Host

DNS:Domain Name System

It resolve name to IP and IP to name (host name).

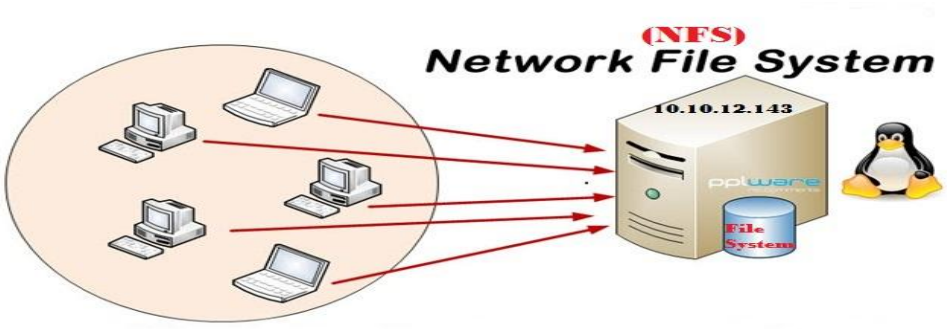




ZONE	DEFINITION	FOR USE BY
.com	Commercial	Businesses
.edu	Education	Universities
.gov	Government	U.S. federal government agencies
.int	International	Organizations established by international treaties
.mil	Military	U.S. military
.net	Network	Network providers, administrator computers, network node computers
.org	Organization	Non-profit and miscellaneous organizations

NFS:Network File Service

Sharing Directory from one place to another in Linux environment



WDS:Windows Deployment Service

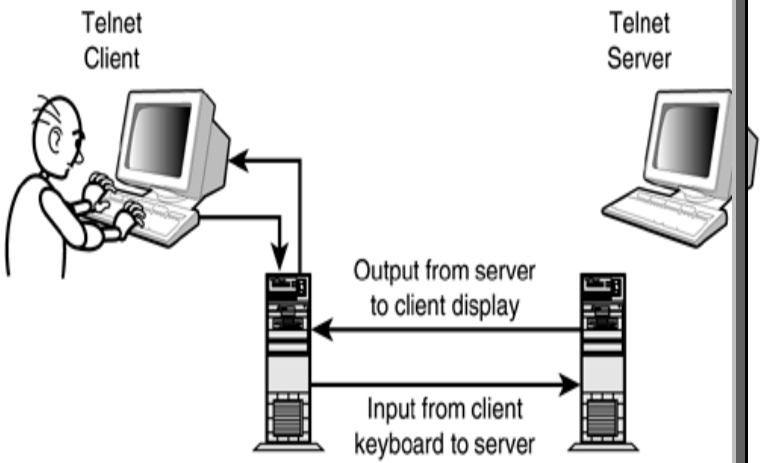
Installing OS in multiple client pc at a time through network .

RIS: Remote Installation Services

Same as WDS but used with windows server 2003.

Telnet:Terminal Network

It is used to access remote device through command mode.



SSH:Secured Shell

Same as Telnet but it is a Secured Communication.

Transport layer

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

Protocols using TCP: HTTP, HTTPS, FTP etc.

Protocol using UDP: DHCP, TFTP, VOIP etc

Which protocol use both TCP and UDP: DNS

INTERNET PROTOCOL

IP: Internet protocol

- It is the method or protocol by which data is sent from one computer to another on the internet.
- Each Computer (known as host) on the internet has at least one IP address that uniquely identifies it from all other Computers on the internet.

ARP:Address Revolution Protocol

To collect Physical Address from the given Logical address.

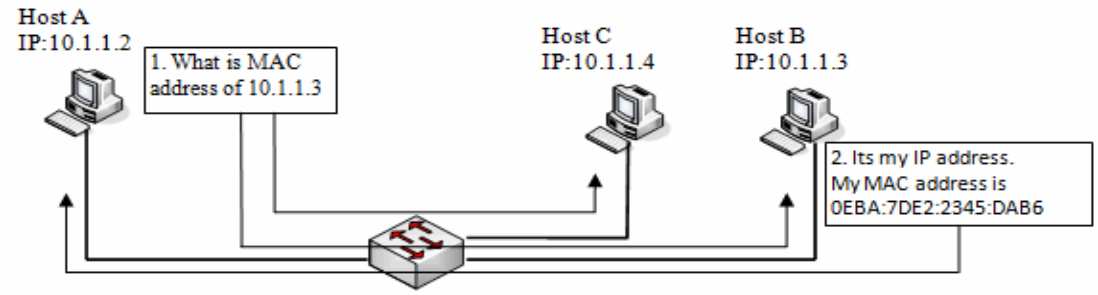
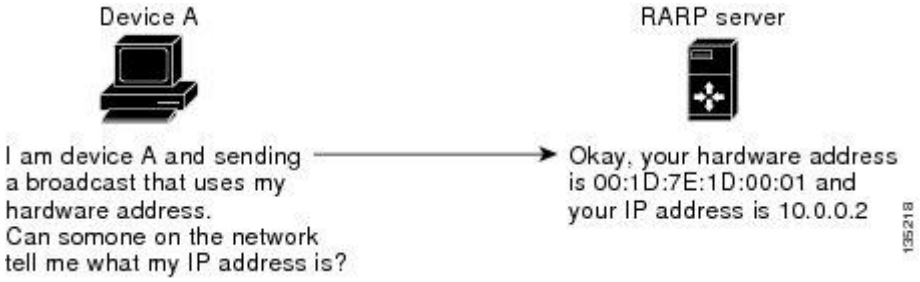


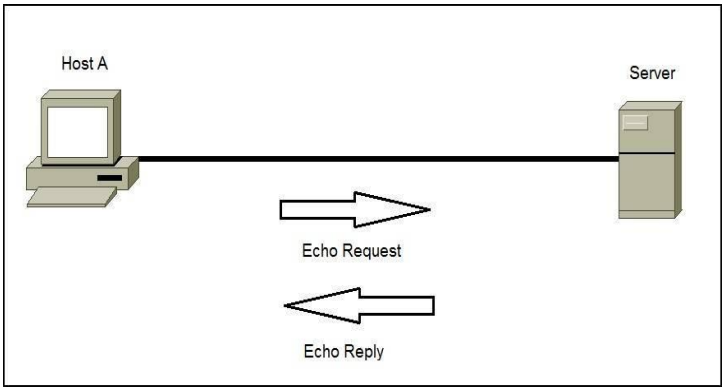
Figure 2.5. ARP operation on the LAN

RARP: Reversed Address Resolution Protocol



ICMP:Internet Control Message Protocol

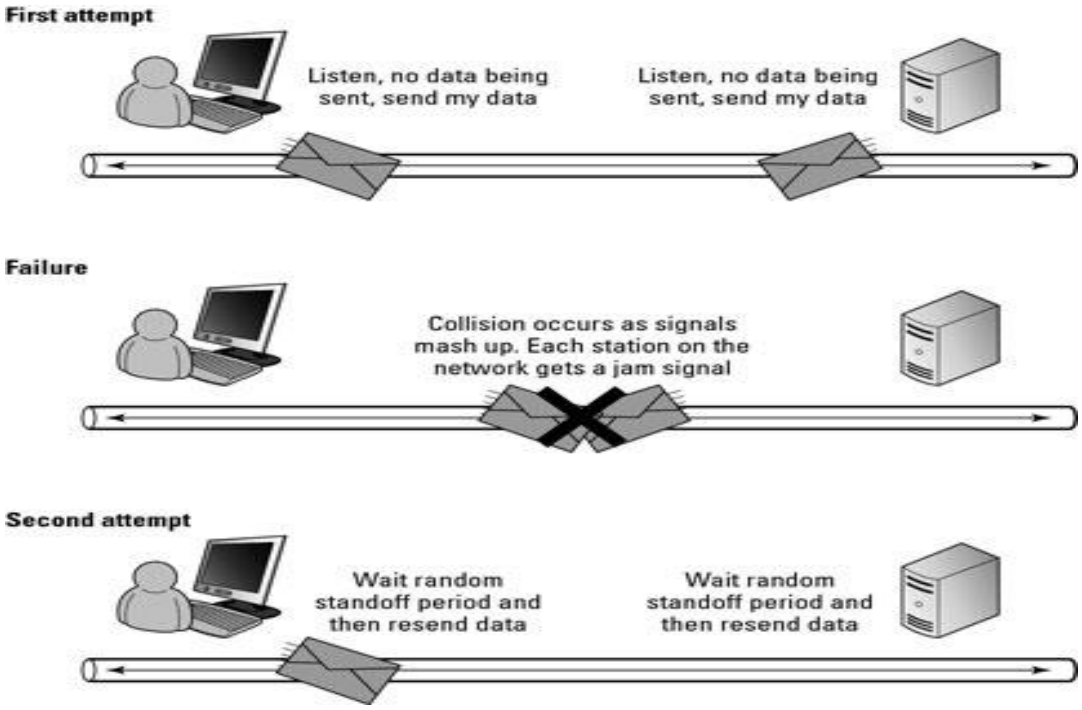
Behind Ping Command ICMP Protocol works to check connectivity.



NETWORK ACCESS LAYER

(CSMA/CA).Carrier-sense multiple access with collision avoidance

In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent. If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear.



FRAME DELAY

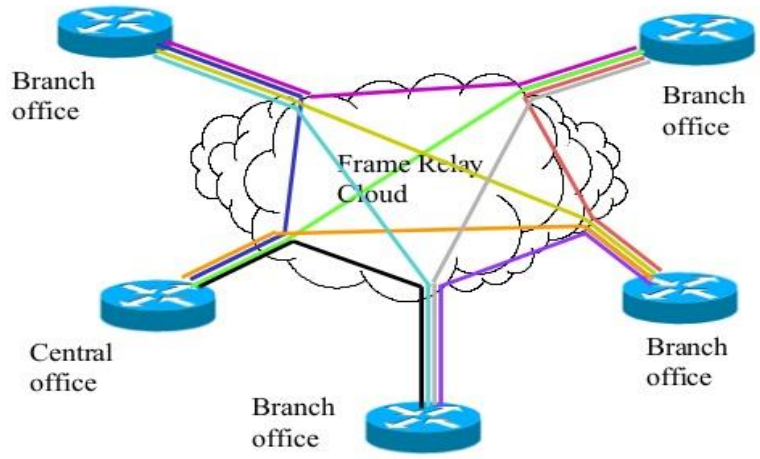
- **Frame relay** is a data link layer, digital packet switching network protocol technology designed to connect Local Area Networks (LANs) and transfer data across Wide Area Networks (WANs).
- It also supports variable-length packet sizes for more efficient utilization of network bandwidth.
- Frame Relay operates over fiber optic or ISDN lines and can support different higher level network protocols including Internet Protocol (IP).

Two types of connections:

1.Permanent Virtual Circuits(PVC): For persistent connections intended to be maintained for long periods of time even if no data is actively being transferred.

2.Switched Virtual Circuits(SVC): For temporary connections that last only for the duration of a single session.

Typical frame relay Diagram:-



FDDI:Fiber Distributed Data Interface

- A Higher Speed Backbone technology.
- Optical fiber transmission.
- Dual ring LAN.
- Thousand stations of network Security.
- 100Mbps token passing.
- Connect Equipment to the ring over long distance.

IP ADDRESSING

It is a unique address used to identify a device (like computer, smart phone, router, IP based phone, network printer etc) in network.

IP Address	
IP v4	IP v6
Decimal Format	Hexadecimal Format
32 Bits address	128 Bits address

What happened to IPv1, IPv2, IPv3 and IPv5 ?

- IPv1, 2, & 3 would actually be part of the TCP/IP protocols, of which there were 3 versions.

- ❖ IPv5 is an experimental TCP/IP protocol called the Internet Stream Protocol that never really went anywhere because increases in bandwith made streaming over IPv4 feasible. So IPv5 was never finalized and they skipped to IPv6.

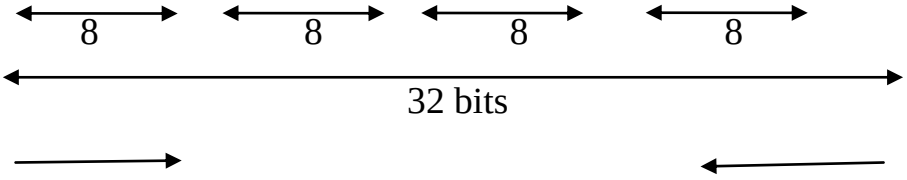
IP V4

- It is 32 bits address divided into 4 octet.
- This 32 bits address is having Network ID and Host ID.

Example:-

192 . 168 . 1. 1

11 00 00 00 .10 10 10 00 .00 00 00 01 . 00 00 00 01



Network ID Host ID

8 bits = 2^8= 256

Therefore the value we can write in each octet is from 0 – 255 only.

32-bits = 2^{32} = Around 4.2 billions numbers.

IP v4	
Classful	Classless
1) Class A – Used for large network	Subnetting and Supernetting
2) Class B – Used for medium network	
3) Class C – Used for small network	
4) Class D – Used for multicasting	
5) Class E – Reserved for Research and Development	

Q: Where we can assign the IP Address?

Ans: NIC card

Q: Which organization is responsible for managing IP addresses **?**

IANA (Internet Assigned Number Authority) : IANA created some range to distribute the IP bsed on use.

Range of IPv4

Class	Starting	Ending
A	1.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

Note : 127.0.0.1 is reserved for local host and called loopback address.
Range: 127.0.0.1 – 127.255.255.254

To Remember	
Class	Range
A	1 - 126
B	128 – 191
C	192 – 223
D	224 – 239
E	240 – 255

Network bits and Host bits

Class A: Network bits: 08, Host bits: 24

Subnet Mask

11111111	00000000	00000000	00000000
255	0	0	0

Class B: Network bits : 16, Host bits: 16

Subnet Mask

11111111	11111111	00000000	00000000
255	255	0	0

Class C: Network bits : 24, Host bits: 08

Subnet Mask	11111111	11111111	11111111	OOOOOOOO
	255	255	255	O

Types of IP Address:

- Unicast Address
- Multicast Address
- Broadcast Address

- Unicast is communication between One to One receiver.[A, B, C – Unicasting]
- Multicast is communication between one-to-many
  [D, E – Multicasting]
- Broadcast is Communication between one-to-all.

Loop-back Address:

It is a special class A IP address (127.0.0.1-127 255.255.255.0),reserved for loopback or diagnostic functions.

Link-Local Address:

DHCP is automatically assign the IP Address to a computer.

Condition for Pinging / Communicating:

Class	PC-1				PC-2			
Class - A	A	B	C	D	A	X	Y	Z
Class - B	A	B	C	D	A	B	X	Y
Class - C	A	B	C	D	A	B	C	X

Note:- To communicate two PC the network ID must be same in both PC.

Calculation of IP Address:

Formula:-

No. of Network = 2^{n-r} **No. of Host Network = $2^{h}-2$**

Where, n = Network bits r = Reserved bits h = Host bits

Reserved bits :

Class	Reserved bits	No of bits
A	0	1
B	10	2
C	110	3

1) **Class - A :**
   n = 8, h = 24 , r = 1
   No. of network = $2^{n-r} = 2^{8-1} = 2^7 = 128$
   No. of host network = $2^h-2 = 2^{24}-2 = 16,777,214$

2) **Class – B :**
   n = 16, h = 16 , r = 2
   No. of network = $2^{n-r} = 2^{16-2} = 2^{14} = 16384$
   No. of host network = $2^h-2 = 2^{16}-2 = 65,536-2 = 65,534$

3) **Class – C :**
   n = 24, h = 8 , r = 3
   No. of network = $2^{n-r} = 2^{24-3} = 2^{21} = 2,097,152$
   No. of host network = $2^h-2 = 2^8-2 = 256-2 = 254$

How to configure Class-C IP address for 600 Computers ?

Ans:

192.168.1.0 → **Network ID**

192.168.1.1

192.168.1.2

.

.

192.168.1.254

Valid host = 254

192.168.1.255 **Broadcast ID**

192.168.2.0 → **Network ID**

192.168.2.1

192.168.2.2

. → **Valid host = 254**

.

192.168.2.254

192.168.2.255 → **Broadcast ID**

192.168.3.0 → **Network ID**

192.168.3.1

192.168.3.2

. → **Valid host = 92**

.

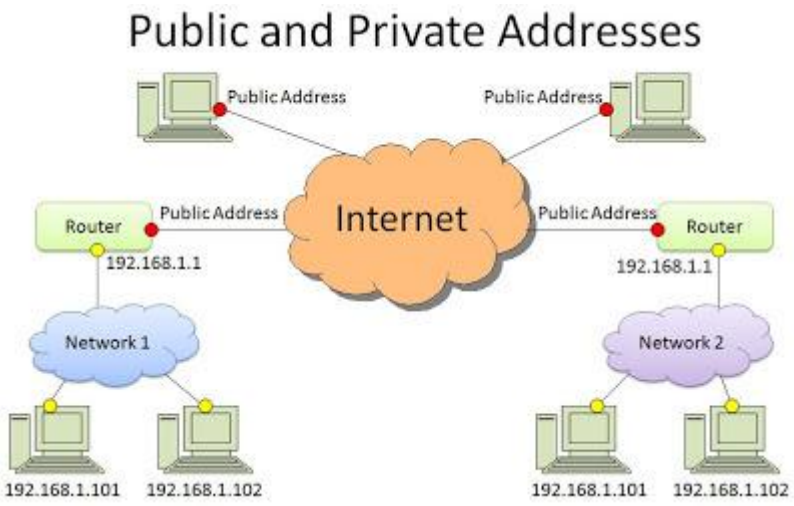
192.168.3.92

192.168.2.255 → **Broadcast ID**

Therefore total valid host (Computers) = 254+254+92 = 600

Two router require to communicate all systems here.

Public IP and Private IP:



Differences between Public IP and Private IP:

Public IP	Private IP
Assinged by ISP	Assigned by user from a given range
Used to Connect Internet	Used to Share Internet Connection
It can be directly accessed through Internet	It cannot be accessed through Internet

Private IP Range:

Class	Private IP address range	Subnet mask	No. of hosts
A	10.0.0.0 – 10.255.255.255	255.0.0.0	16,777,212
B	172.16.0.0 – 172.16.31.255	255.255.0.0	8190
C	192.168.0.0 – 192.168.255.255	255.255.255.0	65,534

Private IP Addresses

Note:- Total IP Address = 2^{32} = 4.2 Billions

3.7 billions used by Public IP

0.5 billions used by Private IP, Lookback address and APIPA address.

SUBNETTING

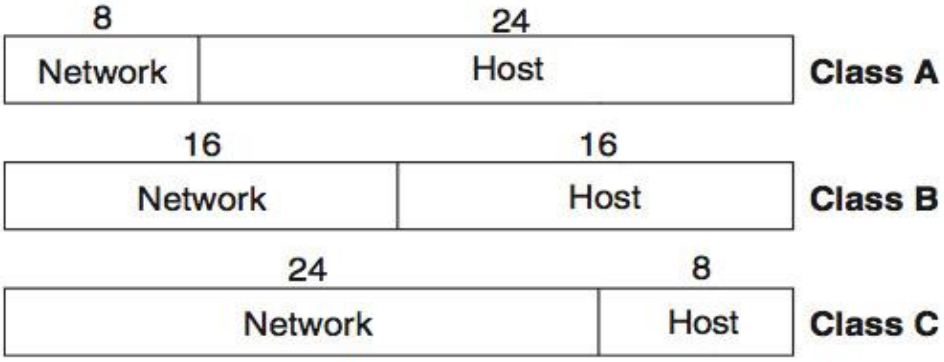
- Subnetting enables the network administrator to further divide the host part of the address into two or more subnets.
- Subnet mask is a mask used to determine what subnet an IP address belongs to.
- The subnetting process allows the administrator to divide a single Class A, Class B, or Class C network number into smaller portions. The subnets can be subnetted again into sub-subnets.

Subnetting advantages

- Reduces the network traffic by reducing the volume of broadcasts
- Saving unused IP addresses
- Enables users to access shared data within their network.
- Security can be maintained
- Easy to troubleshoot network problems.

The default subnet mask is as follows:

Class	Subnet mask	CIDR notation
A	255.0.0.0	X.X.X.X/8
B	255.255.0.0	X.X.X.X/16
C	255.255.255.0	X.X.X.X./24



Subnetting is the process of Dividing a Single Network into Multiple Networks.
Converting Host bits into Network Bits i.e. Converting 0's into 1's

Subnetting can be perform in two ways.
1. FLSM (Fixed Length Subnet Mask)
2. VLSM (Variable Length subnet mask)

Subnetting can be done based on requirement .

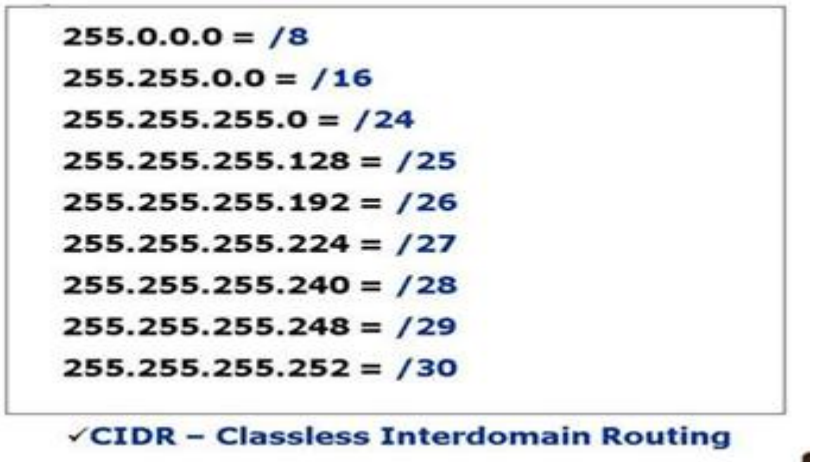
Requirement of Hosts ? **2h - 2 >= requirement**
Requirement of Networks ? **2n >= requirement**

What is Supernetting or CIDR?

- Classless Inter-Domain Routing (CIDR) merges or combine network addresses of same class into one single address to reduce the size of the routing table.
- It is done on core router to reduce the size of routing table.
- It is implemented by ISP (internet service providers).

For subnetting calculation number of bits is borrowed from host ID

No of Bits	No of networks	No of n/w or host
1	2	128
2	4	64
3	8	32
4	16	16
5	32	8
6	64	4
7	128	2



FLSM : Example-- 1
Req = 40 hosts using C-class address network 192.168.1.0/24
1. 2h - 2 >= req
26 – 2 >= 40
64 – 2 >= 40
62 >= 40
Host bits required **(h) = 6**
2.Converted network Bits (n) = Total. H. Bits -- req. H. Bits
= 8 --- 6 **= 2 (n)**
4.Total . Network Bits =total network bits + converted bits = 24 + 2 = /26
subnet mask = (/26)= 255.255.255.192
5.Blocksize = 2h = 26 = 64
6.Subnets = 2n = 22 = 4 Subnets
7.Range :
Network ID --- Broadcast ID
192.168.1.0/26 ----- 192.168.1.63/26
192.168.1.64/26 ----- 192.168.1.127/26
192.168.1.128/26 ----- 192.168.1.191/26
192.168.1.192/26 ----- 192.168.1.255/26

FLSM : Example-- 2
1.Req = 500 hosts using B-class address network 172.16.0.0/16
2h - 2 >= req
29 – 2 >= 500
512 – 2 >= 500
510 >= 500
2.Host bits required **(h)= 9**
3. **Converted network Bits** (n) = Total. H. Bits -- req. H. Bits
= 16 --- 9 = **7 (n)**
3. Total . Network Bits = total network bits + converted bits = 16 + 7 = /23
subnet mask = (/23)= 255.255.254.0
6. **Blocksize** = = 2h = 29 = 512
7.**Subnets** = 2n = 27 = 128 Subnets
Range
Network ID --- Broadcast ID
172.16.0.0/23 ---- 172.16.1.255/23
172.16.2.0/23 ---- 172.16.3.255/23

172.16.4.0/23 ---- 172.16.5.255/23
172.16.6.0/23 ---- 172.16.7.255/23

FLSM : Example-- 3

1.Req = 2000 hosts using A-class address network 10.0.0.0/8
2h - 2 >= req
211 – 2 >= 2000
2048 – 2 >= 2000
2046 >= 2000
2.Host bits required (h)= 11
3.Converted network Bits (n) = Total. H. Bits -- req. H. Bits
= 24 --- 11 = **13 (n)**
4. Converted network Bits (n)= 13
5.Total . N. Bits = 8+ 13 = /21
subnet mask = (/21) = 255.255.248.0
6.blocksize = 2h = 211 = **2048**
7.Subnets = 2n = 213 = 8192 Subnets
8.Range:
Network ID --- Broadcast ID
10.0.0.0/21 … 10.0.7.255/21
10.0.8.0/21 … 10.0.15.255/21
10.0.16.0/21 … 10.0.23.255/21
…
…
10.0.248.0/21 … 10.0.255.255/21
10.1.0.0/21 --- 10.1.7.255/21
10.1.8.0/21 --- 10.1.15.255/21
10.1.16.0/21 --- 10.1.23.255/21
10.1.248.0/21 … 10.1.255.255/21
10.2.0.0/21 --- 10.2.7.255/21
10.2.8.0/21 --- 10.2.15.255/21
10.2.16.0/21 --- 10.2.23.255/21
…
…
10.2.248.0/21 … 10.2.255.255/21
….
…
….
10.255.0.0/21 --- 10.0.7.255/21
10.255.8.0/21 --- 10.0.15.255/21
10.255.16.0/21 --- 10.0.23.255/21
….
…
10.255.248.0/21 … 10.255.255.255/21

WIRELESS NETWORK

- Wireless network allows to a communication between 2 or many computers without using physical wire.

Wireless Network Categories

	PAN	LAN	MAN	WAN
Coverage	Reach within a person	Reach within a Building or campus	Reach within a city	Reach within a world wide
Performance	Moderate	high	high	Low
Standard	IEEE 802.15 Bluetooth	802.11 wifi	Preparatory IEEE 802.16, Wimax	Cellular, broadband, 2G, 3G, 4G

What is IEEE ?

- Institute of Electrical and Electronics Engineers
- Its objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering and allied disciplines.

IEEE 802 : IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks.

IEEE 802 Standard

802.1–Higher layer LAN protocol
802.2– LLC Link Local Control
802.3 –Ethernet
802.4 –Token bus
802.5 –Token Ring
802.6 –MAN
802.11 –Wi-Fi
802.15 –PAN
802.16 –MAN [Wimax]

IEEE 802.11 Standard

STANDARD	FREQUENCY	SPEED	RANGE-METER
802.11	2.4 GHz	2 Mbps	20/100
802.11a	5 GHz	54 Mbps	35/120
802.11b	2.4 GHz	11 Mbps	35/140
802.11g	2.4 GHz	54 Mbps	38/140
802.11n	2.4/5 GHz	150 Mbps	70/250
802.11 ac	5 GHz	1 Gbps	35/.....
802.11 ad	60 GHz	7 Gbps	60/100

Mobile Network Generation

Parameters	1G	2G	3G	4G
Image				
Name	1st Generation Mobile Network	2nd Generation Mobile Network	3rd Generation Mobile Network	4th Generation Mobile Network
Introduced in year	1980s	1993	2001	2009
Location of first commercialization	USA	Finland	Japan	South Korea
Technology	AMPS (Advanced Mobile Phone System), NMT, TACS	IS-95, GSM	IMT2000, WCDMA	LTE, WiMAX
Multiple Address/Access system	FDMA	TDMA, CDMA	CDMA	CDMA
Switching type	Circuit switching	Circuit switching for Voice and Packet switching for Data	Packet switching except for Air Interface	Packet switching
Speed (data rates)	2.4 Kbps to 14.4 kbps	14.4 Kbps	3.1 Mbps	100 Mbps
Special Characteristic	First wireless communication	Digital version of 1G technology	Digital broadband, speed increments	Very high speeds, All IP

Full Form

NMT - Nordic *Mobile* Telephone

AMPS - Advance *Mobile* Phone System

GPRS – General Packet Radio Service

GSM – Global System for Mobile communication

CDMA– Code Division Multiple Access

TDMA - Time Division Multiple Access

WCDMA – Wide Band Code Division Multiple Access

EDGE – Enhanced Data for Global Evolution

UMTS – Universal Mobile Telecommunications Service

HSDPA – High-Speed Downlink Packet Access

LTE – Long Term Evolution

Wireless LAN Security

Wireless security is the prevention of unauthorized access or damage to computers using **wireless** networks.

1) **WEP** (Wired Equivalent Privacy):

- WEP is a weak security standard.
- The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools.

2) **WPA** (Wi-Fi Protected Access):

- WPA was a quick alternative to improve security over WEP.

3) WPA2

- The current standard is WPA 2, some hardware cannot support WPA2 without firmware upgrade or replacement.
- WPA 2 uses an encryption device that encrypts the network with a 256-bit key, the longer key length improves security over WEP.

Encryption and authentication

1) WPA2-TKIP

- TKIP is actually an older encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time.
- TKIP is actually quite similar to WEP encryption.
- TKIP is no longer considered secure, and is now deprecated.

2) WPA2-AES

- AES is a more secure encryption protocol introduced with WPA2.
- AES isn't some creaky standard developed specifically for Wi-Fi networks, either.
- It's a serious worldwide encryption standard that's even been adopted by the US government

How to configure new wi-fi router

1) See the back side of router

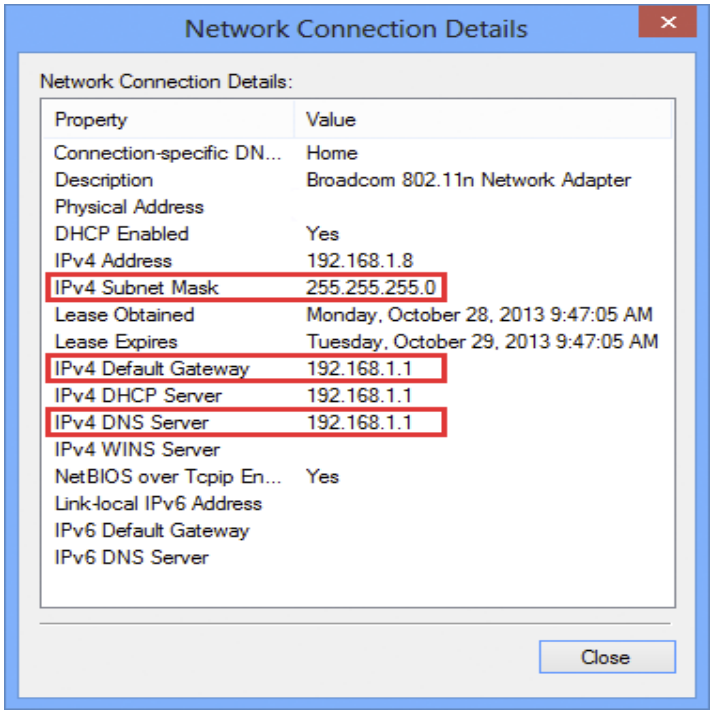
IP = 192.168.1.1

User = admin , Password =admin

2) Connect router to PC directly through network cable

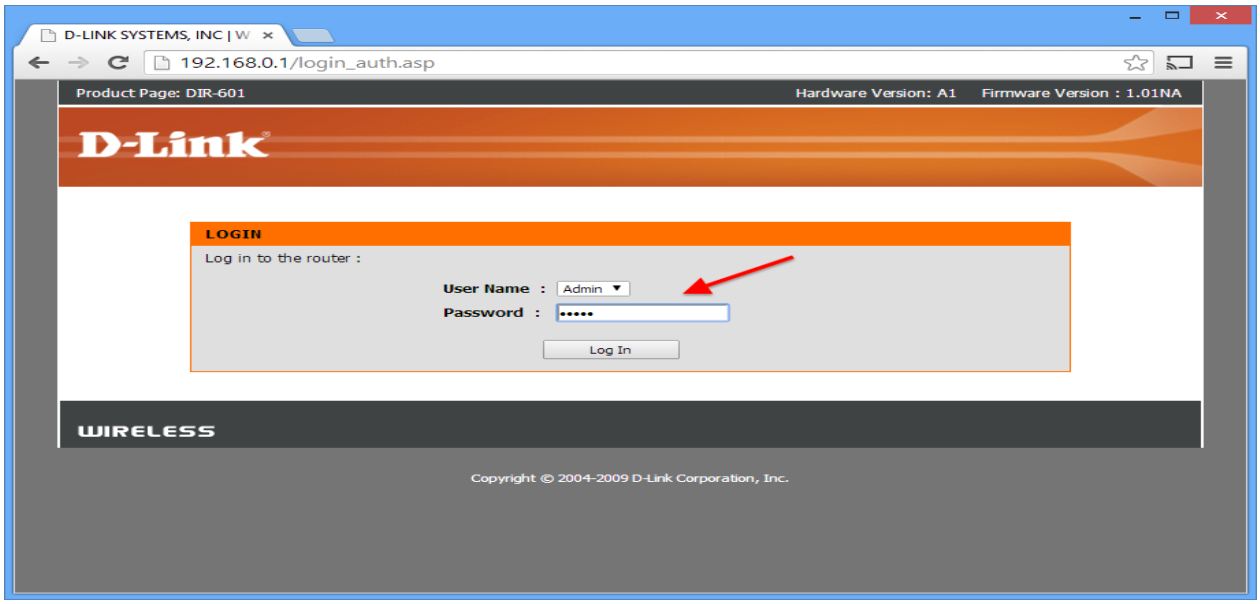
3) In PC configure IP address to obtain automatically

4) Check IP in PC (specially gateway address)



5) Open any web browser in PC and type -- 192.168.1.1

User =admin, Password = admin



A) Internet setup : Static IP or Dynamic IP or User/Password or Bridged

B) Wireless Security

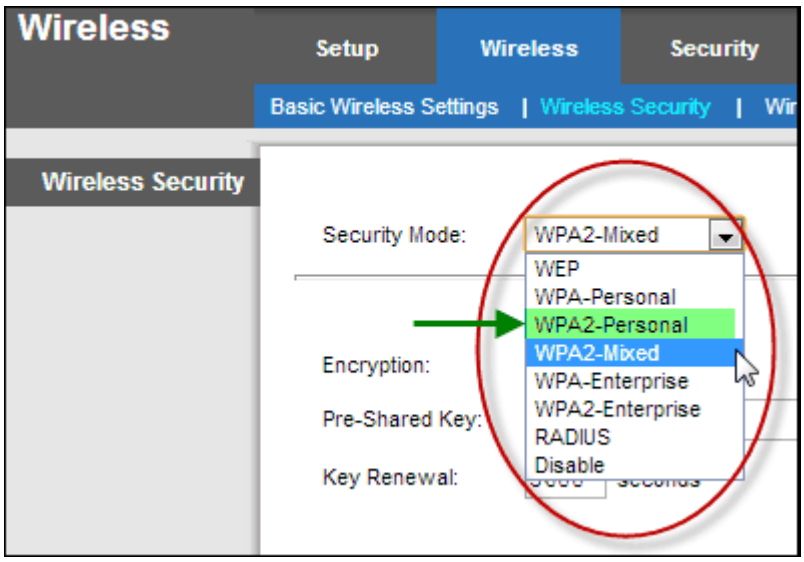
SSID = RTS

Mode: 802.11n

Security option = WPA2

Encryption = AES

Pre shared key = 123456



C) LAN setting

IP = 192.168.1.1

SM= 255.255.255.0

DHCP mode Enabled

DHCP IP Pool : 192.168.1.2 - 192.168.1.254

Lease time = 3600 sec

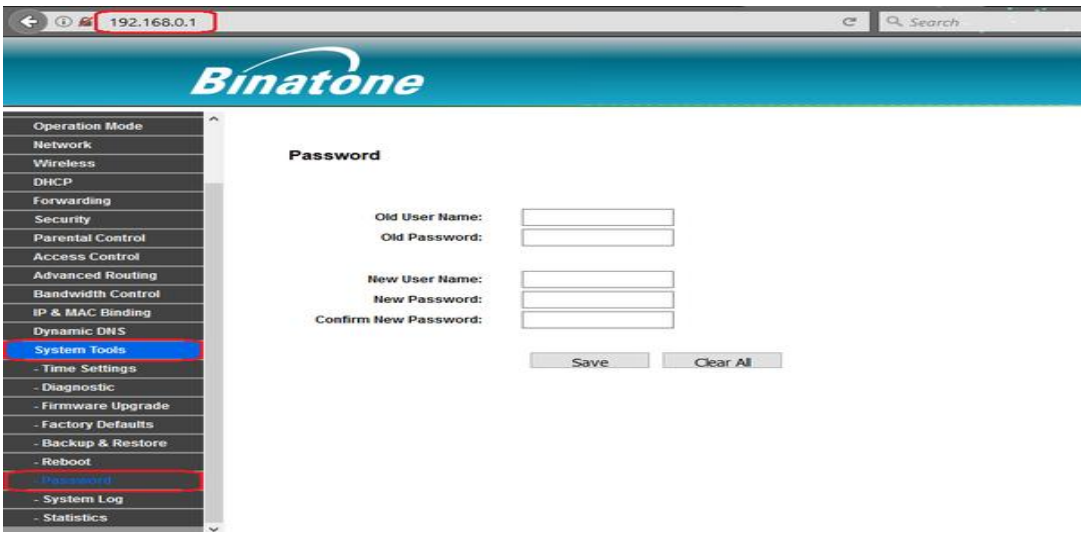
D) MAC Address filtering: To fix specific system to access Internet

E) Parental Control

-Blocking web sites

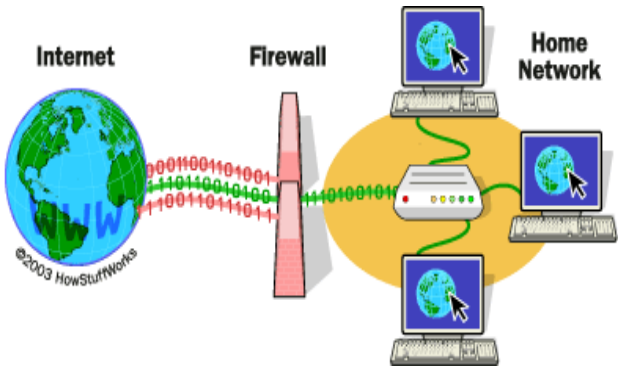
- Blocking services(like http, https, ftp etc)

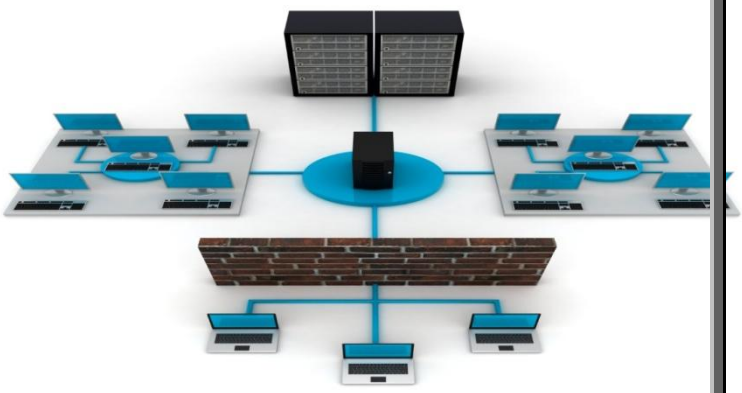
F) Change router login password -- This is one time work



Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network.





Firewalls can be implemented in both hardware and software, or a combination of both.

Hardware Firewall	Software Firewall
The firewall is a dedicated hardware appliance protecting all your computers, also reffered to as a network or gateway firewall.	Software firewalls are installed on your computer and you can customize it; allowing you some control over its function and protection features.
A hardware firewall is more secure, can protect more computers and runs on its own processing power and so does not affect a computer's performance.	A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall.

Windows Firewall Rule

1) Inbound Rule
2) Outbound Rule

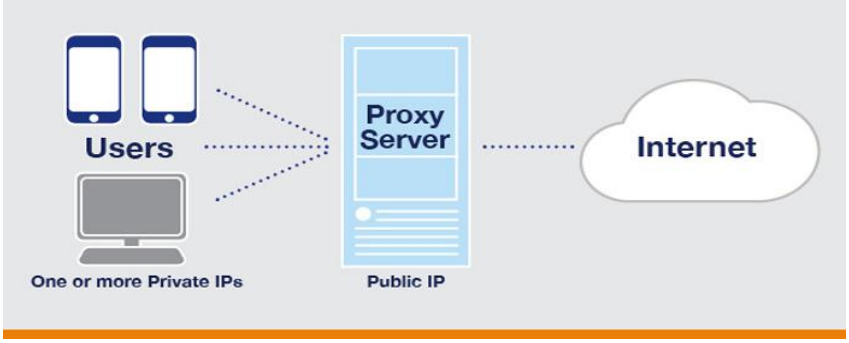
- Inbound rules: These are to do with other things accessing your computer. If you are running a Web Server or RD server on your computer then you will have to tell the Firewall that outsiders are allowed to connect to it.
- Outbound rules: These are so that you can let some programs use the Internet, and Block others. You will want to let your Web Browser (Internet Explorer, Firefox, Safari, Chrome, Opera...) have access to the Internet, so you will tell Windows Firewall that it's allowed.

Some Firewall Software

1) Zone Alarm
2) Comodo free firewall 3) Peer Block 4)Tiny wall

Internet connection Management

- A proxy server, also known as a "proxy" or "application-level gateway", is a computer that acts as a gateway between a local network and a larger-scale network such as the Internet.
- A proxy server works by intercepting connections between sender and receiver.
- A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services.
- Proxy servers provide increased performance and security. All incoming data enters through one port and is forwarded to the rest of the network via another port.



How to Configure Proxy Server to manage Internet Connection ?

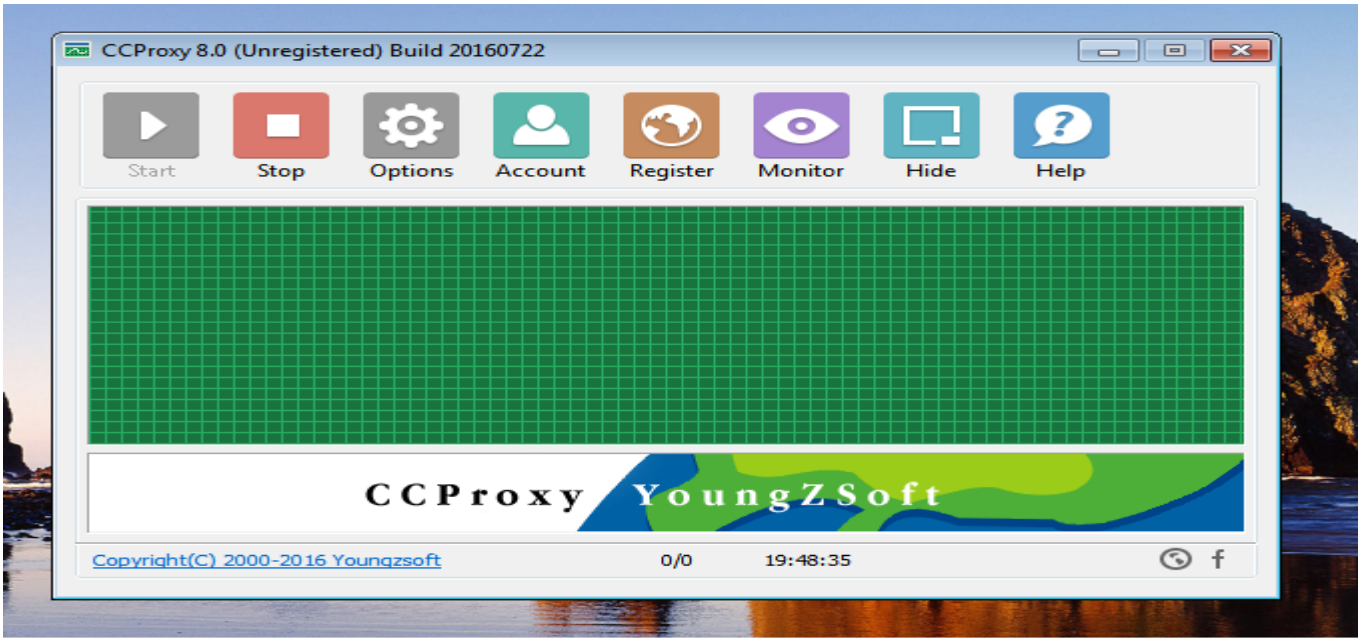
a) In Proxy Software install Internet connection management proxy server
b) Available Softwares :CCProxy, Interguard, Verioto 360, iMonitor Soft etc.

CCProxy Software advantages:

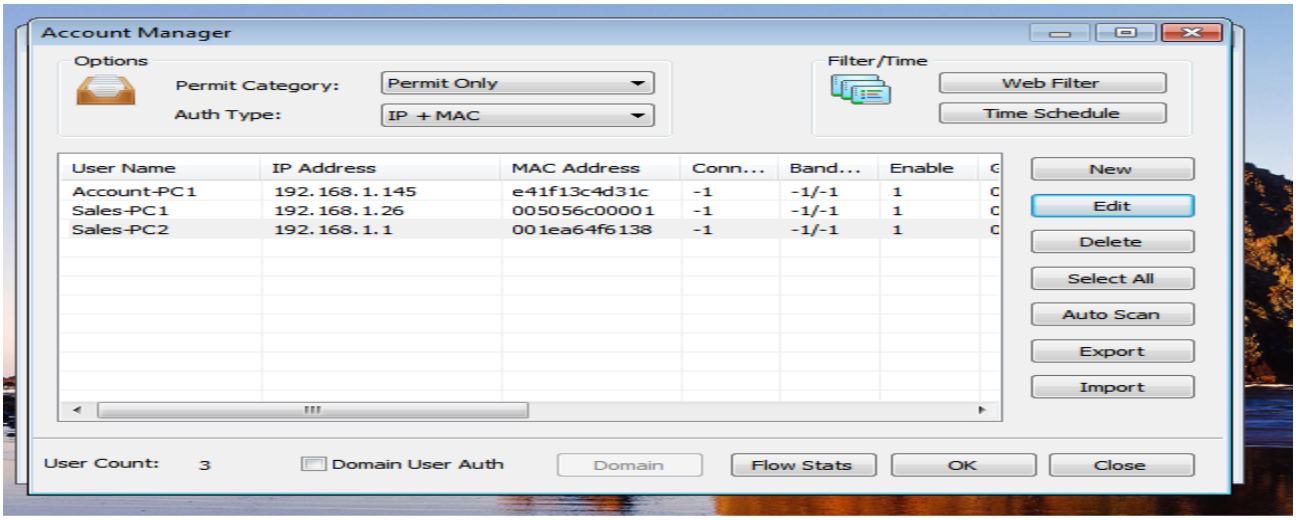
a) Different method to give authorization.
b) Web Site ,URL, Web Content Filtering
c) Time Setting to use Internet
d) Data Usage setting based on per user.
e) Download and upload speed setting

Here we are configuring CCProxy Software:

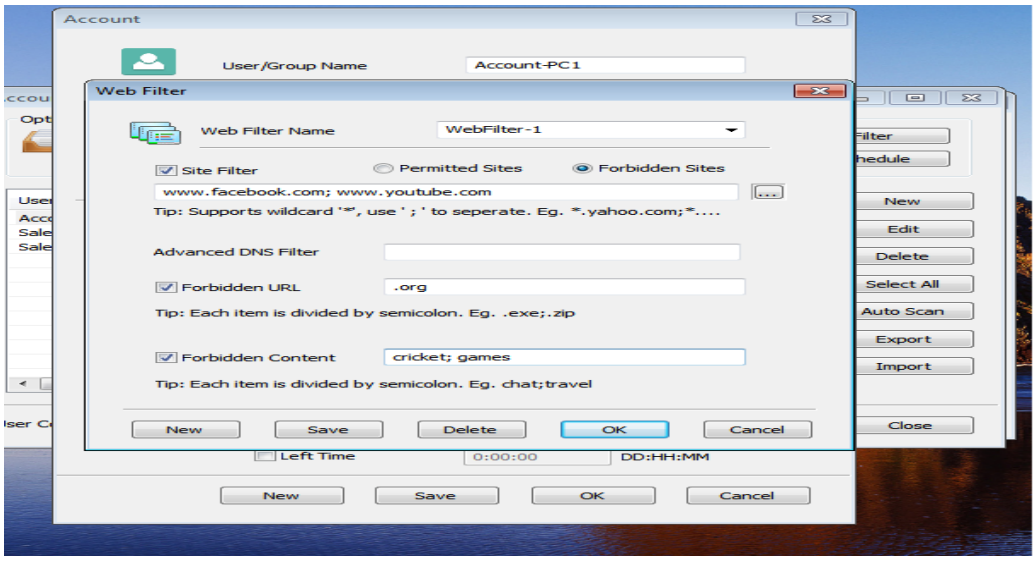
1) Install this Software Normally and add users one by one and configure it.



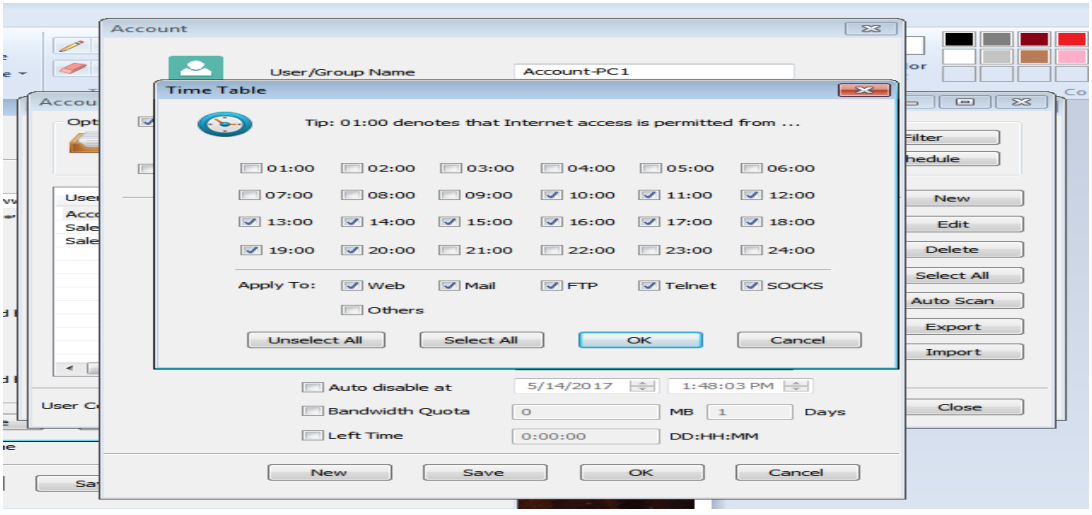
Select permit category and Auth Type then click on new to add new user



Restrict to use facebook and youtube



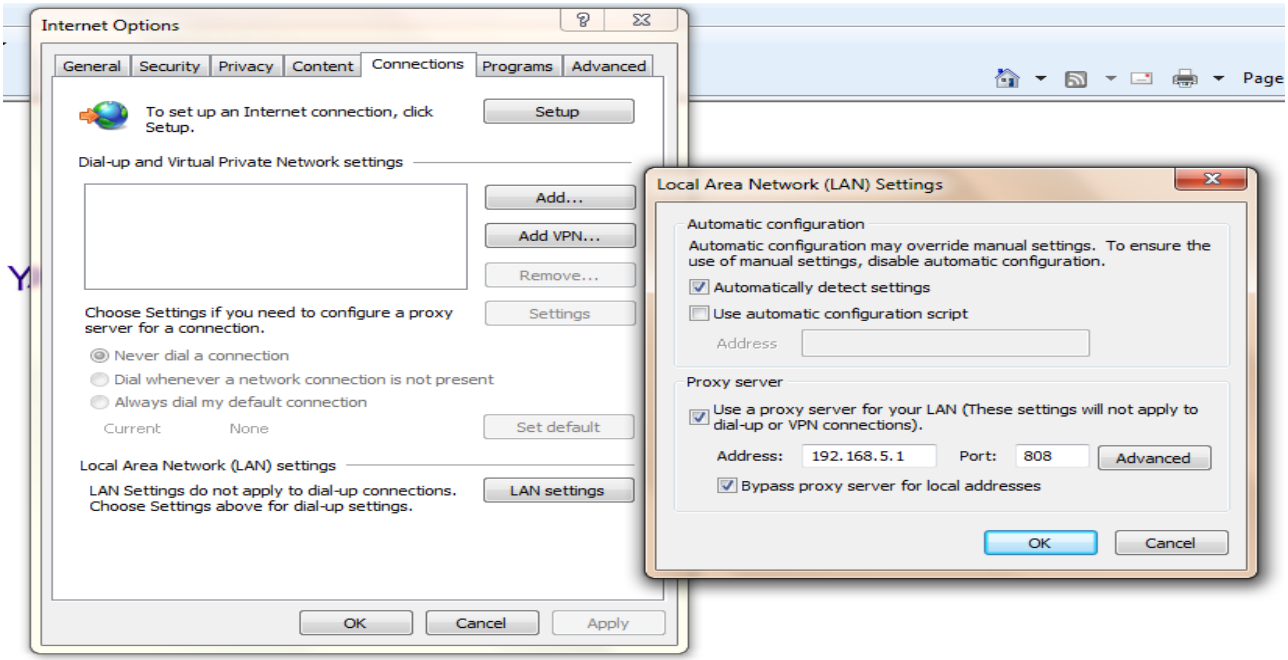
Set time to use Internet in that time only



How to add or configure Client PC to get Internet through Proxy Server ?

Sol:- Open Internet Explorer – Go to tools – Internet options—Connection—LAN Setting--- Select " Use a Proxy Server for Your LAN" and put Proxy Server address here as well as Port no-808 then Apply –OK

This configuration will work with Chrome browser also.



TCP/IP UTILITY

1) Ping:

- The PING utility tests connectivity between two hosts.
- PING uses a special protocol called the Internet Control Message Protocol (ICMP)to determine whether the remote machine (website, server, etc.) can receive the test packet and reply.
- Pinging the loopback address (127.0.0.1) to verify that TCP/IP is installed and configured correctly on the local computer.
- Open cmd mode → ping 127.0.0.1 or ping espn.com (any pc IP)

2) Tracert:

- Tracert is very similar to Ping, except that Tracert identifies pathways taken along each hop, rather than the time it takes for each packet to return (ping).
- If we have trouble connecting to a remote host we will use Tracert to see where that connection fails.

- Open cmd mode → tracert espn.com (or any IP of PC).

3) ARP:

- The ARP utility helps diagnose problems associated with the Address Resolution Protocol (ARP).
- TCP/IP hosts use ARP to determine the physical (MAC) address that corresponds with a specific IP address. Type **arp** with the **– a** option to display IP addresses that have been resolved to MAC addresses recently.
- Open cmd mode →arp -a

4) Netstat:

- Netstat (Network Statistics) displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics.
- It is a helpful tool in finding problems and determining the amount of traffic on the network as a performance measurement.
- Open cmd mode →netstat (it shows connection) or netstat –s (it shows traffic)

5) Nbtstat:

- Nbtstat (NetBios over TCP/IP) enables you to check information about NetBios names.
- It helps us view the NetBios name cache (nbtstat -c) which shows the NetBios names and the corresponding IP address that has been resolved (nbtstat -r) by a particular host as well as the names that have been registered by the local system (nbtstat –n).
- Open cmd mode →nbstat

6) NSLookup:

- NSLookup provides a command-line utility for diagnosing DNS problems. In its most basic usage, NSLookup returns the IP address with the matching host name.
- Open cmd mode →nslookup

7) IPConfig:

- Not part of the TCP/IP utilities but it is useful to show current TCP/IP settings.
- The IPConfig command line utility will show detailed information about the network you are connected to. It also helps with reconfiguration of your IP address through release and renew.
- Open cmd mode →ipconfig or ipconfig /all

CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

There are five primary functions of cryptography :

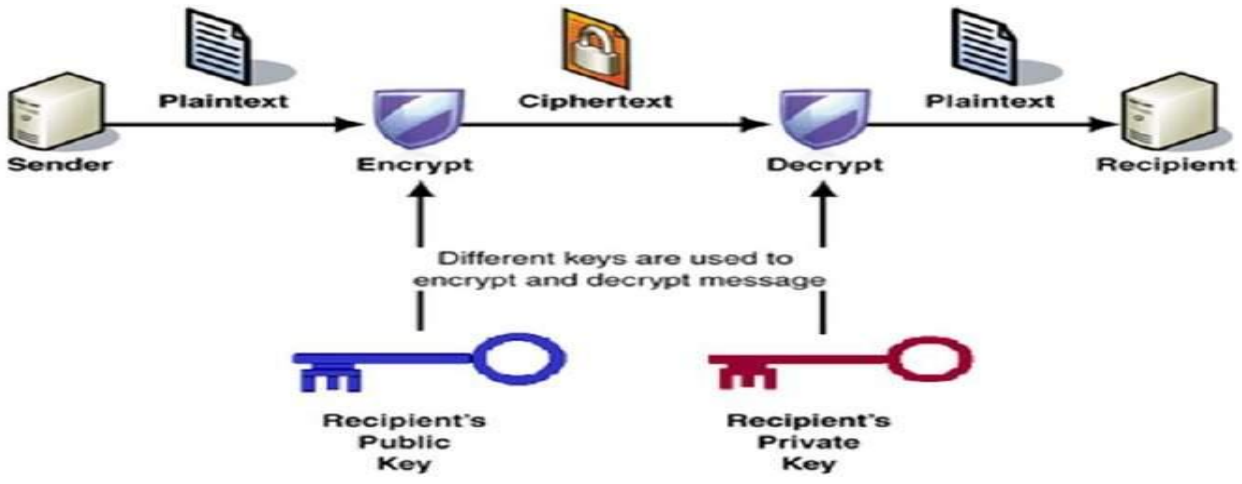
1. **Privacy/confidentiality**: Ensuring that no one can read the message except the intended receiver.
2. **Authentication:** The process of proving one's identity.
3. **Integrity:** Assuring the receiver that the received message has not been altered in any way from the original.
4. **Non-repudiation:** A mechanism to prove that the sender really sent this message.
5. **Key exchange:** The method by which crypto keys are shared between sender and receiver.

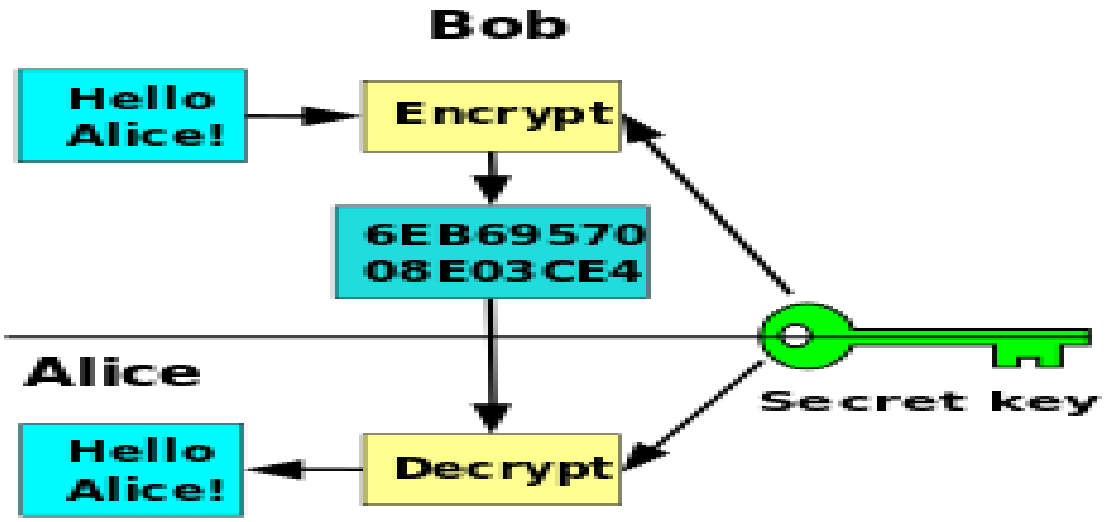
Plain Text:

The unencrypted data, referred to as *plaintext*.

Ciphertext:

Plaintext is encrypted into *ciphertext*.

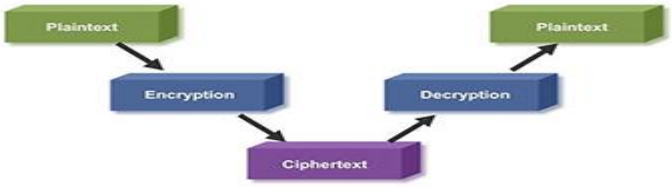




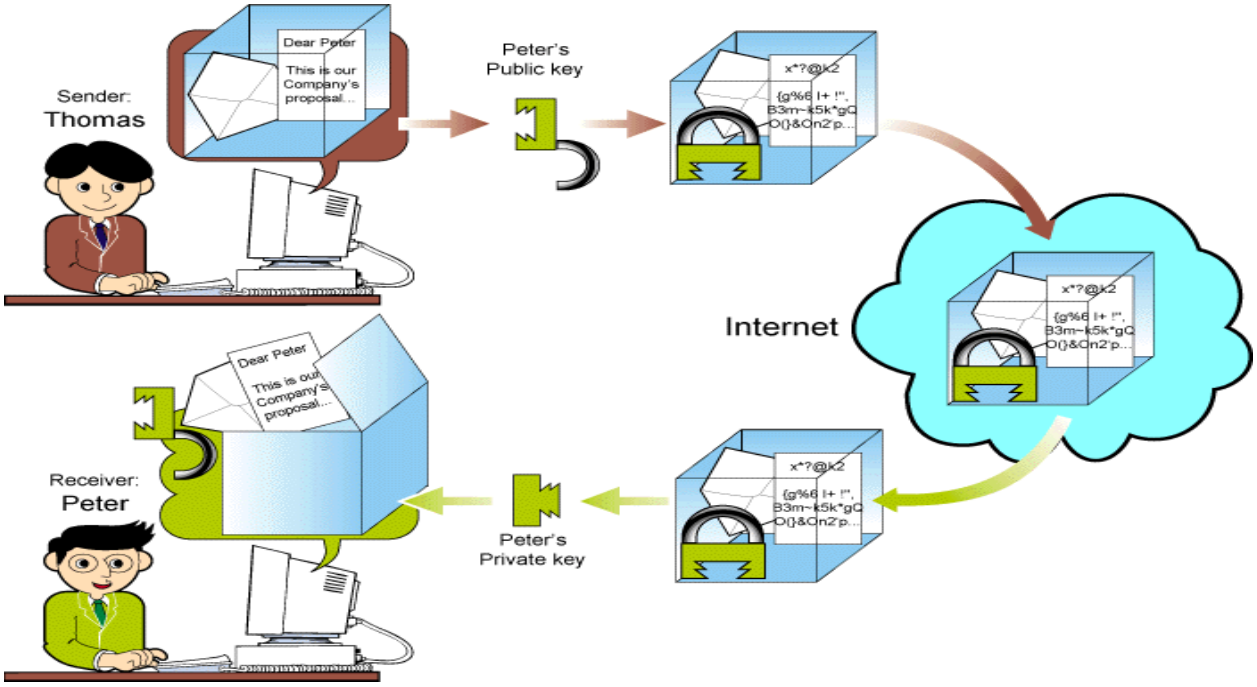
Cryptography definitions

Plaintext
Readable format.
Non-encrypted data.

Ciphertext
Non-readable format.
Encrypted data.



Cryptology
Study of cryptography and cryptanalysis



TYPES OF CRYPTOGRAPHIC ALGORITHMS

1) ***Secret Key Cryptography (SKC):*** Uses a single key for both encryption and decryption; also called *symmetric encryption*. Primarily used for privacy and confidentiality.

2) ***Public Key Cryptography (PKC):*** Uses one key for encryption and another for decryption; also called *asymmetric encryption*. Primarily used for authentication, non-repudiation, and key exchange.

3) ***Hash Functions:*** Uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity.

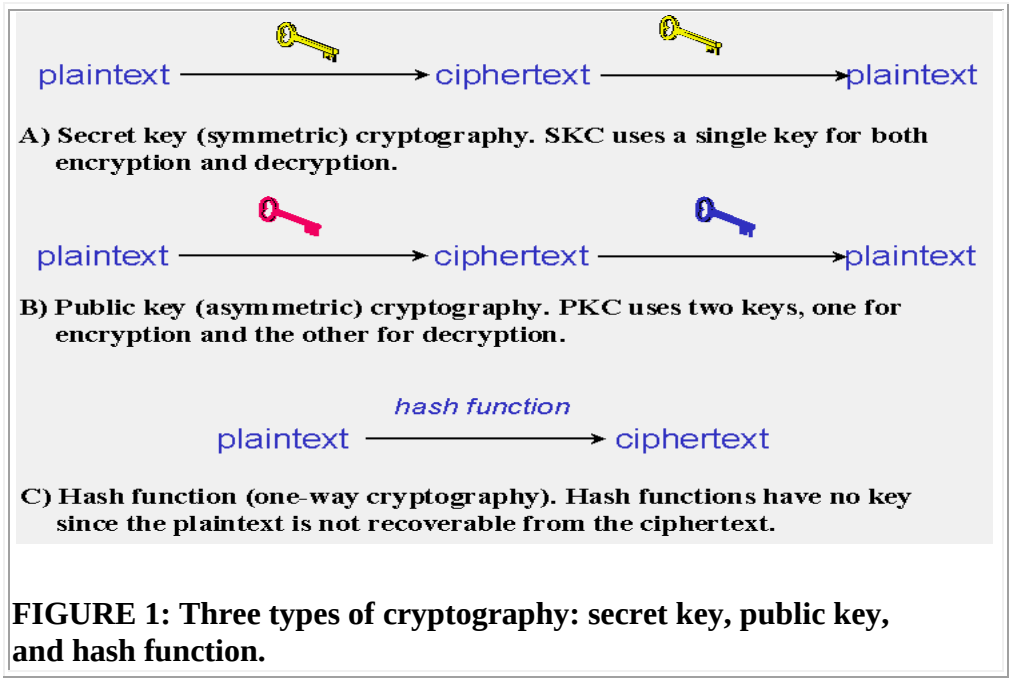


FIGURE 1: Three types of cryptography: secret key, public key, and hash function.

Windows OS Networking Practical

1. IP address configuration:-

PC 1	PC 2
1. Open network setting Local area connection tcp/Ipv4 IP= 192.168.2.1 S.M= 255.255.255.0	1. Open network setting Local area connection tcp/Ipv4 IP= 192.168.2.2 S.M= 255.255.255.0
2. Turn off firewall	2 . Turn off firewall
3. Start → Run → ping 192.168.2.2→ ok	3 Start → Run → ping 192.168.2.1 → ok

2. Remote Desktop:-

PC1	PC2
Right click on my computer→ Properties → Remote setting → Allow connection from computer running any version of remote desktop → Apply → Ok.	Start - Remote Desktop connection: Type PC1 IP --connect --then type user and password of PC1
User must have password on PC.	
Windows firewall must be off.	

3. Folder Sharing:-

PC1	PC2
Right click on folder → Properties → Sharing → Advance sharing → Select share this folder → Permissions → Select full control → Apply → Ok → Apply → Ok.	Start → Run →\\192.168.2.1(IPaddress of PC1).
Security→ Edit → Add → Advanced → Find now → Select Everyone → Ok → Ok → Apply → Ok → Close.	We can get the share folder of PC1.
Open to advance Network Sharing→ Turn all options → only turn off password protected option.	

4. Drive Mapping:-

It will create shortcut drive to access share folder.

PC1	PC2	PC3
Share the folder(song) normally.	Right click on computer → Map network drive →\\PC1 IP address\song	Right click on computer → Map network drive →\\PC1 IP address\song
	Open my computer you get shortcut folder drive.	Open my computer you get shortcut folder drive.

5. Remote Assistance:-

Same as remote desktop but has three extra features.

1. We can set time duration for session.
2. Both user can see the desktop.
3. Both user can chat through remote assistance.

PC1	PC2
Start→ Type Remote → Windows remote assistance →Invite someone your trust to help you → Save this invitation as a file in a folder → share the folder.	Open the share folder → Double click on invitation file → Enter the password.
Note down the password.	Click on request control.
Right click on computer →Properties → Remote setting →allow remote assistance → Advance → Set time duration → Ok.	

Note:- To open remote assistance in windows 8, 10 use (msra.exe) command in run option.

FTP (File Transfer Protocol)

It used to share our data to all other users in same network.

Any user can download the shared data by using web browser.

IIS (Internet Information Services) Installation:

Process:-

- Create a folder and store data.
- Open programs and features → turn windows features on or off → Internet information services (IIS) → Expand IIS and Select all options →Ok.
- Start → Control panel →Administrative tool → IIS Manager → double click PC Name →Right click on sites → Add ftp sites→ give ftp site name → Select Physical path of created folder → Next → Give server IP Address → Select No SSL → Next → Authentication (select Anonymous) → Allow access to (All users) → Permission (Read) → Finish.
- Now right click on created FTP link → Edit permission → Security → Edit → Add → Advanced → Find now → Everyone → OK →OK→ Full control → Apply → OK.

- In other PC open any browser and type ftp://192.168.5.2/

HTTP (Hyper Text Transfer Protocol)

1) Install IIS
2) After Installing IIS . It create a default path in "c:/" drive. (c:/inetpub/wwwroot), keep your html web page here.
3) Open IIS manager → Right click on sites → Add website → site name (Test 1) → Physical path (C:\inetpub\wwwroot) → IP address (192.168.5.1 or server IP address) → Ok.
4) Now in client PC open any web browser and write http://192.168.5.1 (server IP).

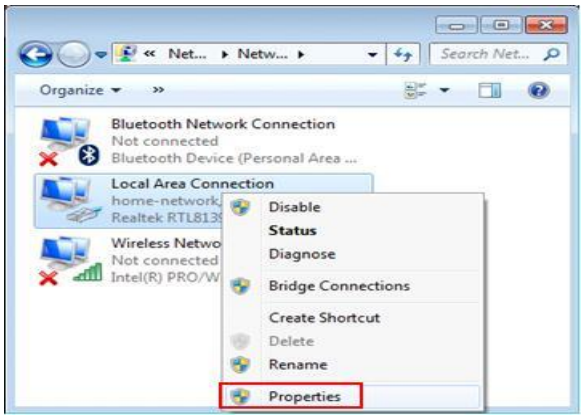
Internet connection Sharing

Windows 7 Internet Connection Sharing (ICS) feature on computer (host computer) in order to share Internet connection with other computers.

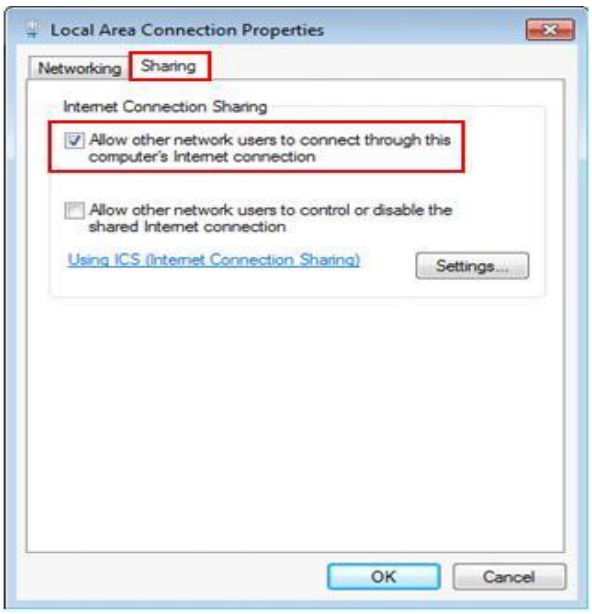
The benefit of this approach is no router is required to share Internet, but the drawback is this host computer needs to be on for other computers to access Internet.

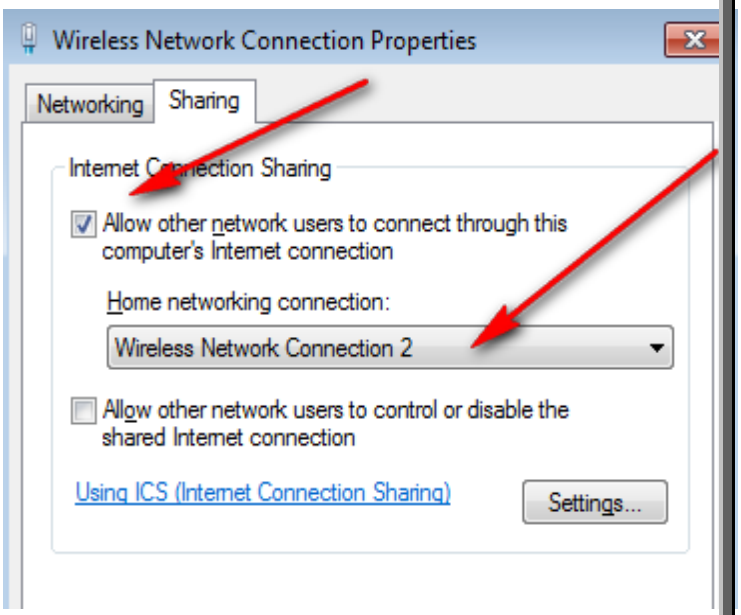
1) Open Network and Sharing Center will appear, click on **Change adapter settings**.

2) Right click on the network adapter that has Internet connection and click **Properties**.

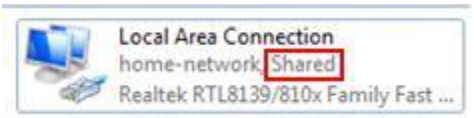


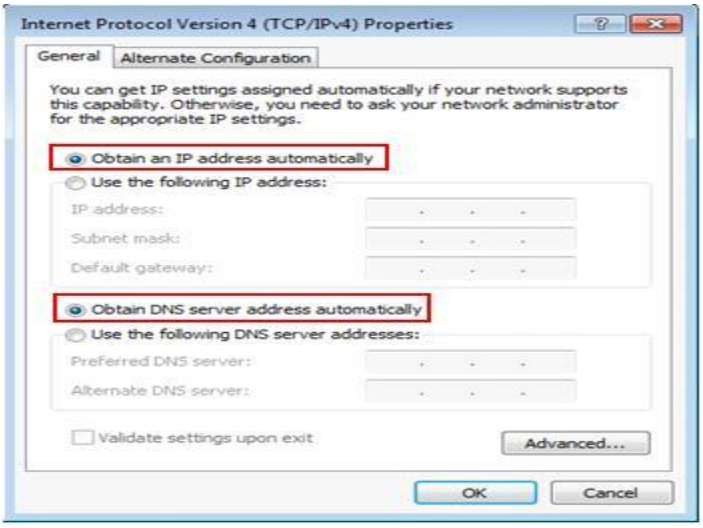
3) Click on **Sharing** tab and then tick on **Allow other network users to connect through this computer's internet connection.**





4) You will see there is a **Shared** wording on that network adapter after the sharing.





5) After enabling Windows 7 Internet connection sharing feature, the network card connected to the home network (wired or wireless) would be assigned a **static IP address 192.168.137.1 with netmask 255.255.255.0** (It would be that wireless adapter in this case). This ICS host will act as a DHCP server and assign other IP addresses in the **192.168.137.x/24** range to other client computers.

6) In order to access Internet, other client computers (Windows Vista, XP, 2000, etc) should configure TCP/IP on their local area connection to obtain an IP address

automatically. Then those computers will be assigned IP address in the **192.168.137.x** range and able to access Internet through this ICS host computer. Good luck!

ACTIVE DIRECTORY

1) Active directory is the directory Service provided by Microsoft.
2) It is the centralize data base used to manage and control the users and computers of whole organization.
3) It is the collection of objects (users, computers, group, OU, printers, contact etc)
4) It authenticates users to log on in network PC.

Elements of AD	
Logical Elements	Physical Elements
Domain	Domain Controller
Users	Sites
Organizational Unit	
Forest	

Q : What is Active Directory Database File
Ans: C:\Windows\NTDS\ntds.dit

Ntds.dit = New Technology Directory Service. Directory Information Tree

Q: What is AD Partitions ?

Ans: Directory partition is where the AD information is segregated and logically stored.
Schema information Configuration information
Domain information Application Partition.

ACTIVE DIRECTORY STRUCTURE

a. **Domain:** It a logical group of network objects (computers, users, devices) that share the same Active Directory database.

b. **Domain Controller:** a) A Machine which hold AD Database.

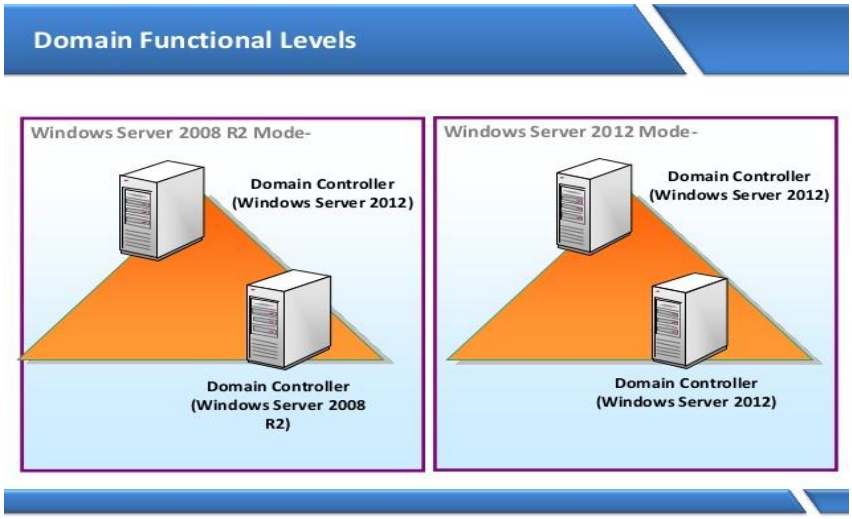
b) A machine where AD is installed.

c. **Parent Domain Controller (PDC):** Main Server or root server
d. **Child Domain Controller (CDC):** Branch Server
e. **Additional Domain Controller (ADC):** Backup Server
f. **Tree :** Domain trees are collections of domains that are grouped together in hierarchical structures.
g. **Forest** :A group of Active Directory trees is known as a forest.

h. **Sites :** It is a collection of Subnets.
i. **Objects :** It is the main resource which need to manage or control. Eg: users, computers, group, Organisational unit, Printer, contact etc.

Active Directory Domain Services (AD DS) Functional Levels

- Functional levels determine the available Active Directory Domain Services (AD DS) domain or forest capabilities.
- They also determine which Windows Server operating systems you can run on domain controllers in the domain or forest.
- The functional level of a domain or forest controls which advanced features are available in the domain or forest.
- If W.S. 2003 is selected as domain or forest functional level then all higher version of server 2003 will be supported.



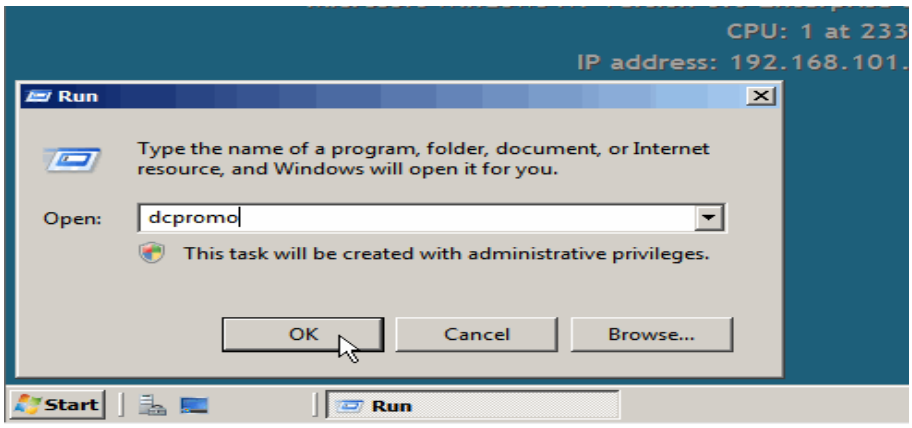
Active Directory Installation

Prerequisite

1) System must have user friendly name.
2) System must have Static IP with DNS IP configured.
3) NIC port must be connected to network cable.

Installation Process

Start→ Run→dcpromo→ ok→ next→Select " Create a new domain in new forest - ....Finish



How to uninstall AD ?

Ans: Start→

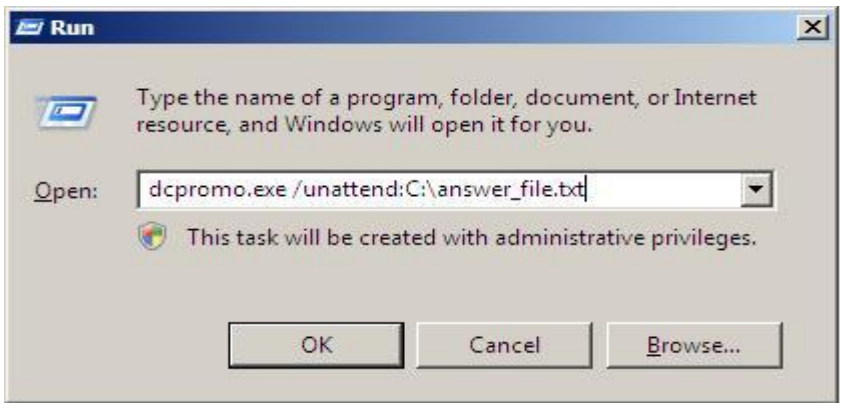
Run→dcpromo→ ok→ next→ select " delete this domain controller" ----------finish

How to perform Unattended AD installation ?

Ans: 1) Download the AD unattended scrip from google and edit it according to requirement.

2) Save this file(ad.txt) in c drive or in any location

3) Start - Run - dcpromo /unattend:c:\ad.txt

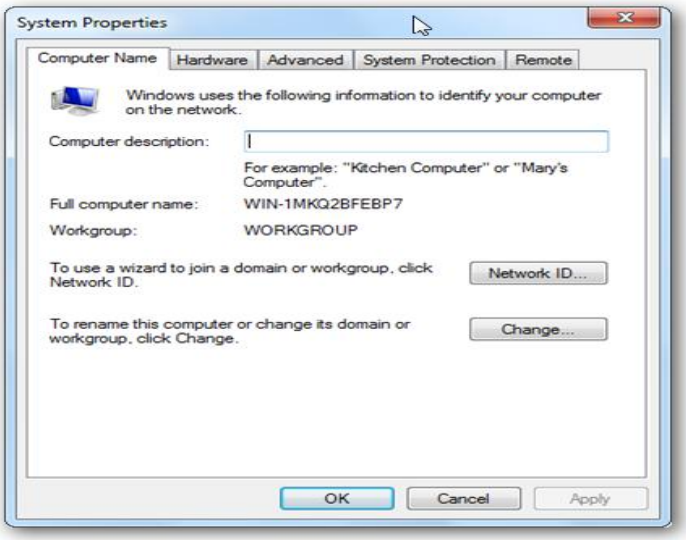


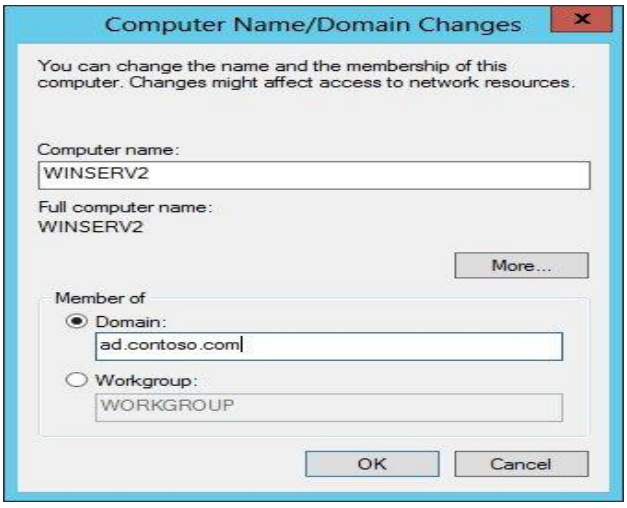
How to add Client PC to Server.(Adding workstation to domain)

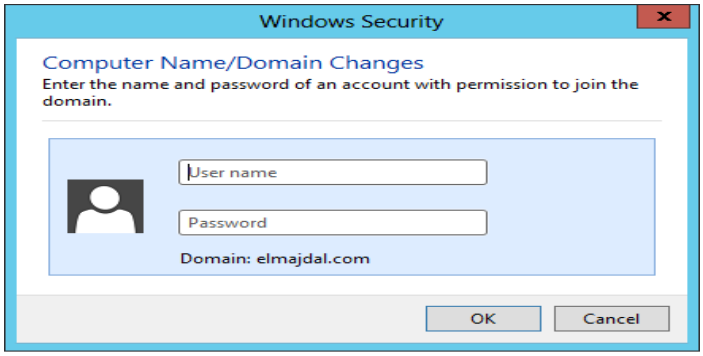
Ans: 1) Check proper connectivity with server and having same DNS address as server.

2) Right Click on Computer – Properties – Change setting – change – select domain and type domain name – ok – Type Server user name (administrator) and password – ok – ok --------

Restart the PC







Now restart the PC and Log on with domain user

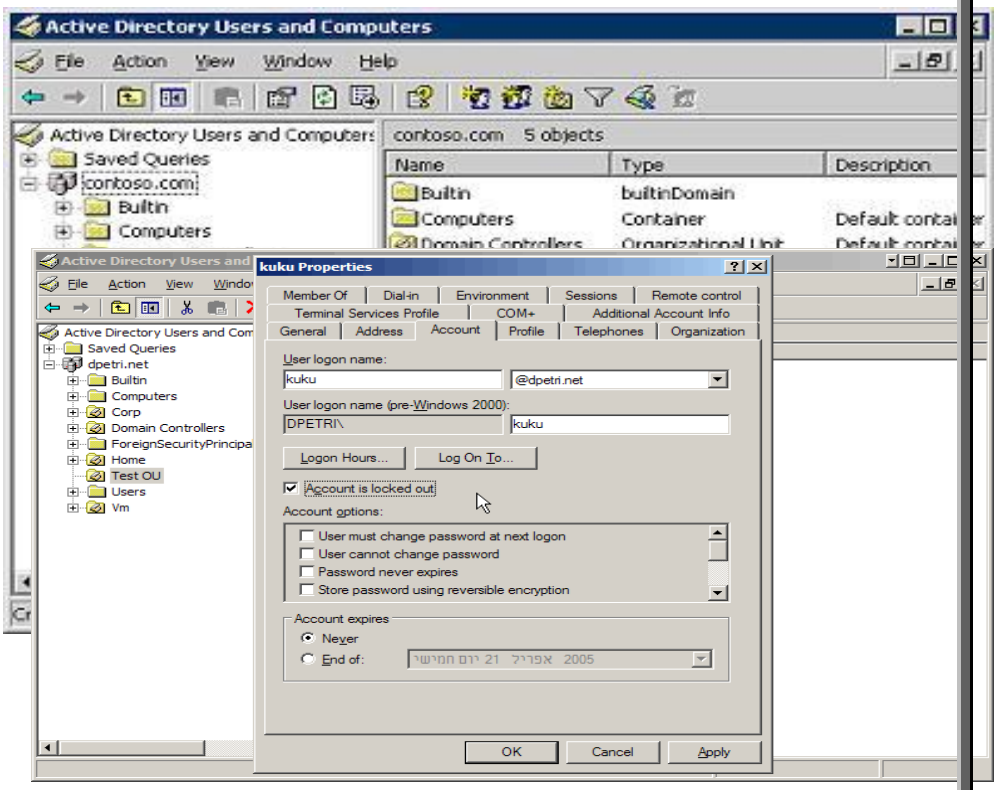
Working with Active directory Users and Computers(ADU and C)

Active Directory Users

1) AD user is created for employ names, branch office name etc.
2) AD users can log on in any machine in the entire network accept domain controller(server).
3) AD user having limited access or power only.
4) After logon in client pc the user can save his data but it will be saved in his local machine.

A) Creating User

Ans: Open AD U and C -- R.C. on Users - New- User - .



Now we can log on in client PC with this user

B) Modifying User properties

- **How to set time limitation for user to logon in PC.**

Ans: Right click user(e.g. prabhas) → proprerties → account → logon → hour → set time hour→ok

Note:- By default an user can logon at any pc of the network.

- **How to fix a user to logon in one machine only ?**

  Ans:-Right click on user→properties→account→logon to→select the following computer and fix the IP address.

- **How to reset any user password from server ?**

  Ans: Right click on user→reset password→give password→ok.

- **How to disable any user in case he has gone for long leave or he left the company ?**

  Ans: Right click on user →disable account.

- **How to auto disable any account after a fix time ?**

  Ans: Right clickon user→properties→account→account expire→select end off→give the time→ok.

User Profile Types

- Local profile
- Roaming profile
- Mandatory profile

1) Local profile:

a) All users created in AD is having local profile only.
b) His created data and desktop setting will be saved in local machine only.
c) This is good for the user who always use same PC.

2) Roaming profile:

a) We can create roaming profile from the local profile.
b) The user can logon in any machine of network and everywhere , he will get same desktop setting and his created data also.
c) This is good for user who always uses different machines.

3) Mandatory Profile:

Mandatory user logon in client PC and can do any changes with the local PC data and settings , when he Logoff , all changes will be restored(previous state).

Now log on in client PC – Do any changes with settings and data and log off

ACTIVE DIRECTORY GROUPS

1) It is the collection of same types of objects(users).
2) Some user can be connected in a group and some permissions and restrictions can be given to the group. All users of that group will get the same permission or restrictions.

GROUPS

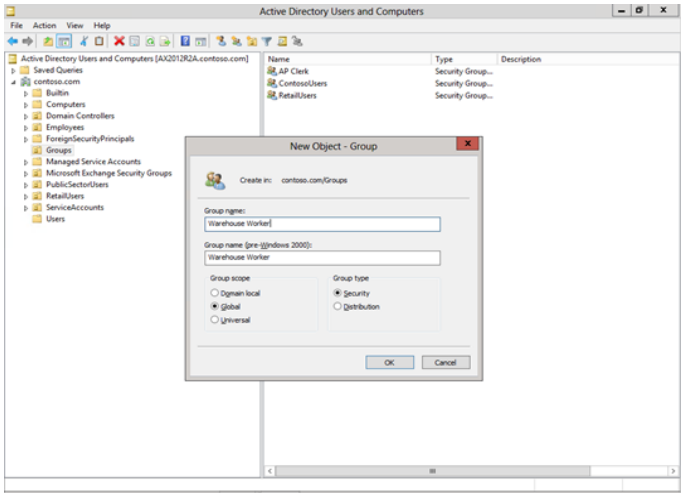
TYPE	SCOPE
Security (Full access of network resource)	Domain
Distribution(Limited access)	Global
	Universal

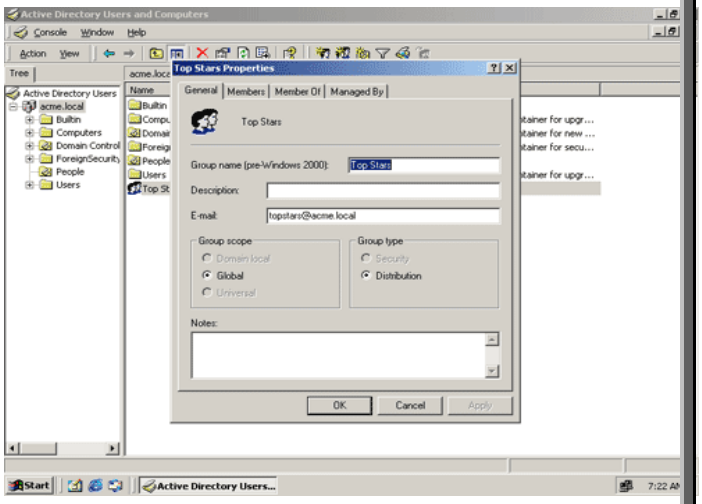
How to create Group ?

Ans: - Open active directory user and computers→ Expand domain name→Right click on created users→New→Group→give group name(e.g. "Technical") →OK.

How to add users in a group ?

Ans:-Right click on created group→Properties→Members→Add→Advanced→Find now→Selected required users→OK→OK→Apply→OK.





Builtin Group:-

These groups are already created with active directory, each group have its own power.

Some special Built-in group (Powerful group):

a) Administrator
b) Domain Admin
c) Enterprise Admin

Domain User:

Limited access. All A.D users are by default member of this group.

Remote Desktop Users:

The users of this group can take remote desktop connection of server.

How to give full power to any A.D user (to make admin user) ?

Ans: Add the required users to any powerful group.

Right click on required user →properties→member of→add→advanced→find now→select administrators and domain admin→ok→ok→apply→ok.

Now with this user logon to any client PC and do some system setting changes.

In the same way we can add our created group to built-in group to give special permissions.

Organizational Unit (OU)

- This is the collection of multiple type of object.
- It is mainly created for department name and office branch name.

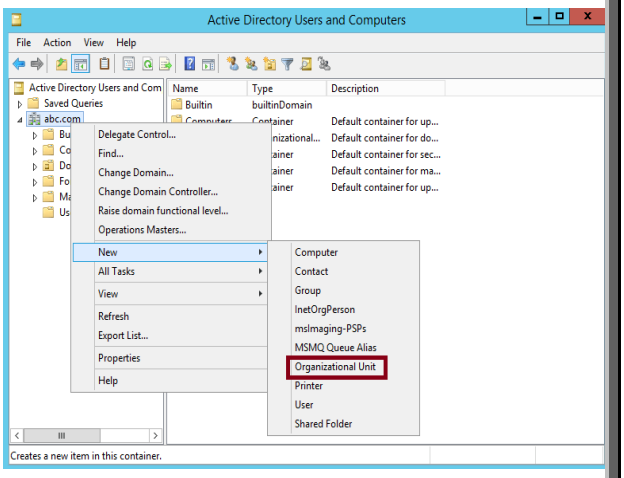
Domain →	**RTS.COM**		
O.U. →	**TRAINING**	**MARKETING**	**SALES**
OBJECTS →	User	User	User
	Group	Group	Group
	Computer	Computer	Computer
	Printer	Printer	Printer

OU creation way

How to Create O.U ?

Open AD users and computers→right click on domain name→organisational unit.

Create some users and groups in each O.U.



How to move a user from one O.U to other O.U ?

Ans: Right click on required user→move→select destination O.U→ok.

How to delete any O.U ?

Ans: 1) Open AD user and computer→view→click advanced features.

2) Right click on required O.U→properties→object→uncheck protect object from accidental deletion→apply→ok.

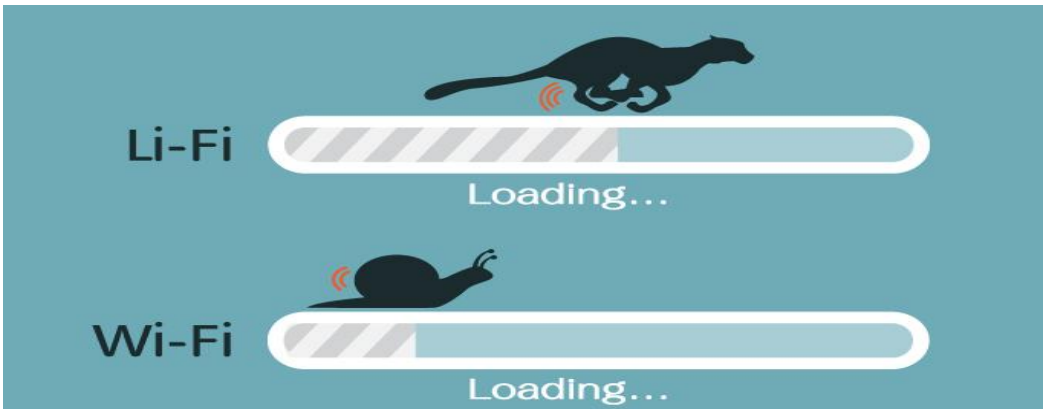
3) Delete the O.U normally.

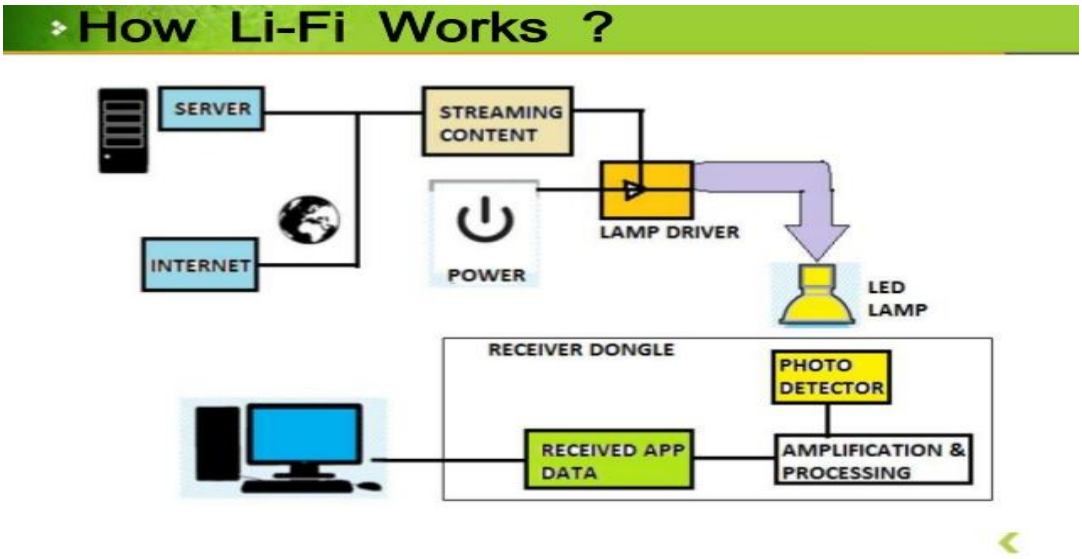
Li-Fi

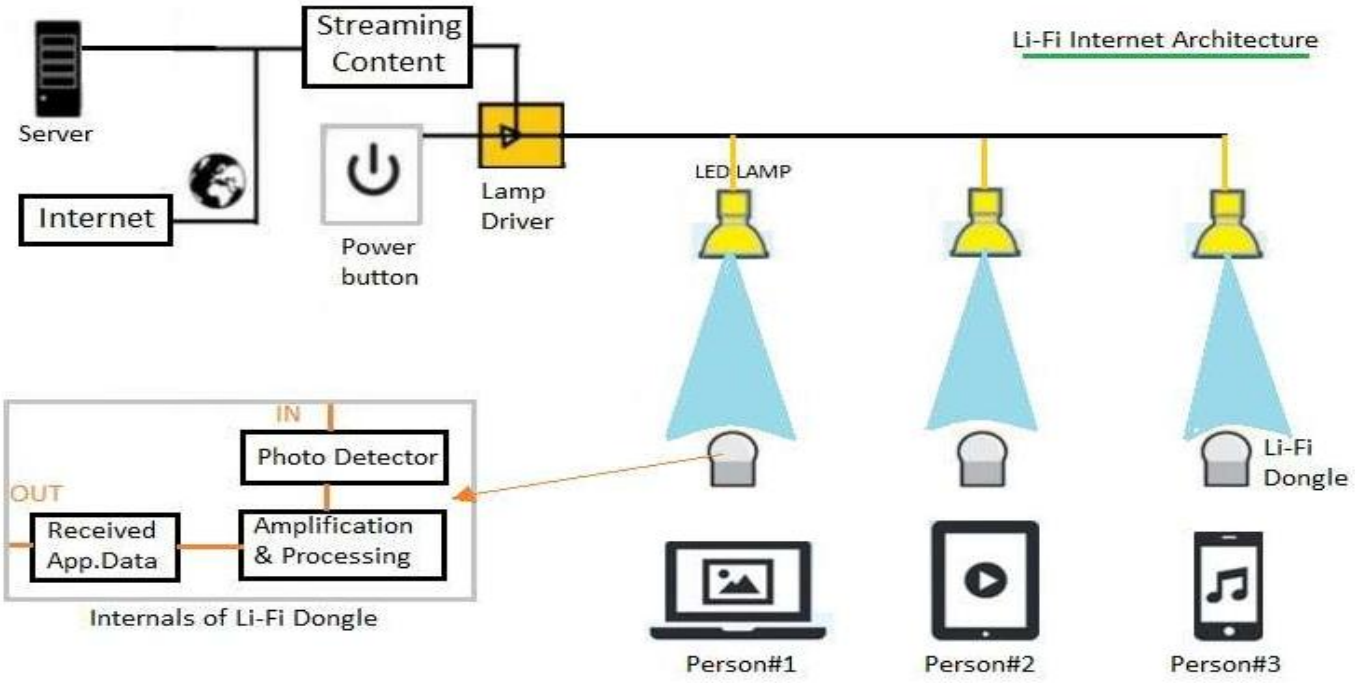
Introduction

- LiFi is a wireless optical networking technology that uses light-emitting diodes (LEDs) for data transmission.
- LiFi is designed to use LED light bulbs similar to those currently in use in many energy-conscious homes and offices.
- However, LiFi bulbs are outfitted with a chip that modulates the light imperceptibly for optical data transmission.
- LiFi data is transmitted by the LED bulbs and received by photoreceptors.

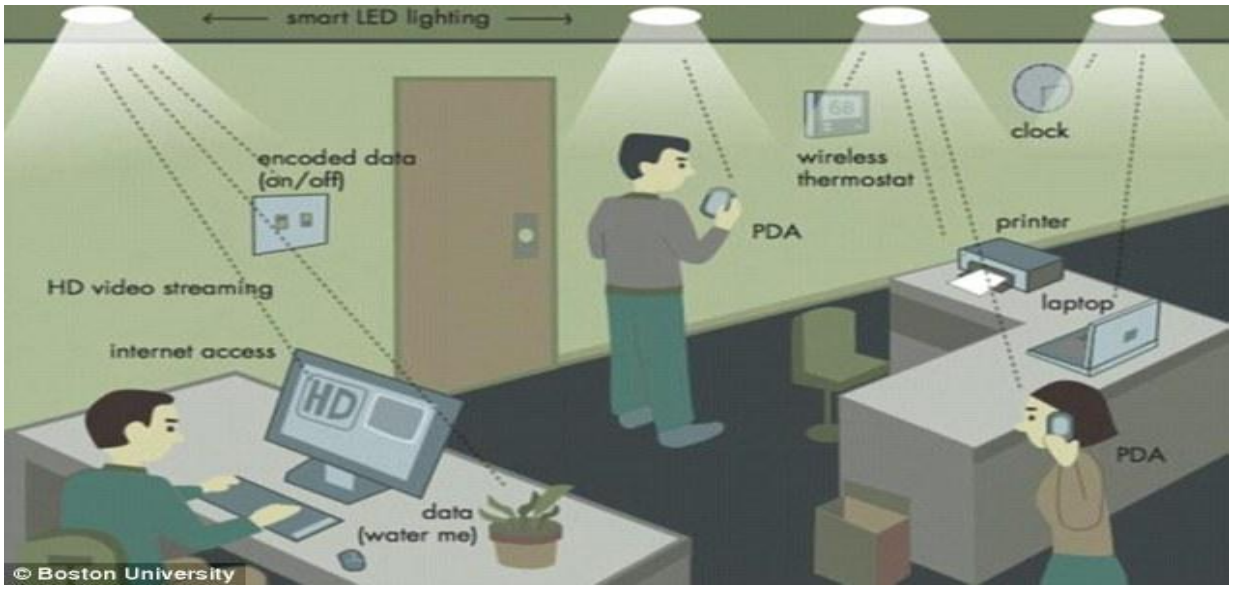
- The LiFi is the short form of Light Fidelity.
  This technology is based on visible light communication (VLC).
- **Li-Fi** is a bidirectional, high-speed and fully networked wireless communication technology similar to Wi-Fi.
- LiFi comprises of multiple light bulbs that form a wireless network, offering a substantially similar user experience to Wi-Fi except using the light spectrum.




How Li-Fi Works ?
SERVER
STREAMING CONTENT
INTERNET
POWER
LAMP DRIVER
LED LAMP
RECEIVER DONGLE
PHOTO DETECTOR
RECEIVED APP DATA
AMPLIFICATION & PROCESSING


Li-Fi Internet Architecture
Server
Internet
Streaming Content
Power button
Lamp Driver
LED LAMP
Li-Fi Dongle
IN
Photo Detector
OUT
Received App.Data
Amplification & Processing
Internals of Li-Fi Dongle
Person#1
Person#2
Person#3


Li-fi



Advantages of LiFi

1) The data transfer rate for internet application is higher.

2) It provides high amount of security as data communication is line of sight (LOS). Moreover lifi signal covers low region does not pass through the walls. This will avoid unwanted access of lifi signal by unauthorized persons.

3) The lifi devices consume low power for operation and hence used in IoT applications.

4) It uses optical spectrum and hence avoids already crowded RF spectrum.

5) As it operates on optical bands which are not harmful like RF spectrum. Hence there is no health concerns in LiFi based system.

6) There is great amount of energy reduction in lighting industry which uses LiFi based devices.

7) It is easy to install.

Disadvantages of LiFi

1) Internet can be used only where light of source device is available. Moreover light can not penetrate from walls and it works only in line of sight path. This limits access of internet whereever one requires. Moreover its range is limited.

2) It cannot be used in outdoor environment like RF signal. This is because of interference caused by sunlight and other optical sources present nearby. Moreover it can be intercepted by the unwanted people if used outdoors.

3) Though the installation is simple, Lifi system requires whole new infrastructure. This will add cost to the companies/people wanting to take LiFi Internet service.

4) Though it draws low power, in order to avail lifi internet services, lights need to be kept ON throughout day and night. As internet is need of the hour, this will waste energy more than any other internet system.

5) One cannot watch games and videos on internet in the dark during night before sleeping on the bed.

Li-Fi / Wi-Fi comparison

Parameter	Li-Fi	Wi-Fi
Speed	***	***
Range	*	**
Data density	***	*
Security	***	**
Reliability	**	**
Power available	***	*
Transmit/receive power	***	**
Ecological impact	*	**
Device-to-device connectivity	***	***
Obstacle interference	***	*
Bill of materials	***	**
Market maturity	*	***

* low ** medium *** high

purelifi

Port Number

Network ports are provided by the TCP or UDP protocols at the Transport layer.

They are used by protocols in the upper layers of the OSI model.

Port numbers are used to determine what protocol incoming traffic should be directed to.

Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN). By ICANN there are three categories for ports:

- From **0 to 1023** – **well known ports** assigned to common protocols and services
- From 1024 to 49151 – registered ports assigned by ICANN to a specific service
- From 49152 to 65 535 – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by any service on an ad hoc basis. Ports are assigned when a session is established, and released when the session ends.

Port	Service name	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name Server (DNS)	TCP and UDP
67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	Post Office Protocol (POP3)	TCP

123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP

IPv4 vs IPv6

IPv4 Address	IPv6 Address
x.x.x.x A set of 4 octet. 1 octet contain 8 bits . 8x4 = 32 bits	xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx. A set of 8 octet. 1 octet contain 16 bits. 8x16 = 128 bits
Multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IP addresses	Aggregatable global unicast addresses
Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/48)
APIPA addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
Dotted decimal notation	Colon hexadecimal format

- IPv6 addresses use eight sets of four hexadecimal addresses (16 bits in each set), separated by a colon **(:)**,like this: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (x would be a hexadecimal value).** This notation is commonly called string notation.

- Hexadecimal values can be displayed in either lower- or upper-case for the numbers A–F.

- A leading zero in a set of numbers can be omitted;
  for example, you could either enter 0012 or 12 in one of the eight fields—both are correct.

- If you have successive fields of zeroes in an IPv6 address, you can represent them as **two colons (::).** For example, **0:0:0:0:0:0:0:5**could be represented as **::5**;
  and **ABC:567:0:0:8888:9999:1111:0** could be represented
  as **ABC:567::8888:9999:1111:0**

Dual Stack Transition Mechanism (DSTM) : Used to make communication between IPv4 to IPv6

Q: How to get IPv4 Address of any hostname ?

Ans: open cmd and type : nslookup www.google.com

For tracing : tracert www.google.com

For pinging : ping www.google.com

Q: How to get IPv6 Address of any hostname ?

Ans: open cmd and type : nslookup www.google.com

For tracing : tracert -6 ipv6.google.com

For pinging : ping -6 ipv6.google.com

Q: How can you view all of the ipv4 and ipv6 addresses of your workstation from cmd ?

Ans: netsh interface ipv6 show address

netsh interface ipv4 show address

OSI QUESTIONS

1. How many OSI layers are there?

A.5 B.6 C.7 D. 8 E. 9

2. At which layer do router devices operate?

A. Data Link Layer B. Network Layer C. Transport Layer D. Physical Layer

3. The Session layer communicates with which other layers?

A. None B. Application and Transport

C. Transport and Network D. Transport and Presentation

4. What devices operate at the Data Link Layer?

A. Hubs B. Switches C. Repeaters D. Hubs and Repeaters

5.The OSI reference model is a seven-layer reference model that originated from the

A. ISO standards committee B. ITU standards committee

C. IEEE standards committee D. ANSI standards committee

6.What are the seven-layers of the OSI reference model?

A. Application, presentation, dialog, transport, network, datalink, bit

B. Application, data format, dialog, transport, network,datalink, bit

C. Application, data format, dialog, end-to-end connection, network, datalink, bit

D. Application, presentation, session, transport, network, data link, physical

7. What is the function of the Application Layer as described by the OSI reference model?

A. Provides network services to user applications B. Provides desktop connectivity to the LAN

C. Provides desktop connectivity to the WAN D. None of the above

8. Data is referred to as _____ at the Application Layer?

A. Data B. Packets C. Segments D. Bits

9. What are some of the common standards that are implemented at the Application Layer?

A. SMTP, TELNET, FTP, CMIP B. NetBIOS, LAT, DDP, SNA

C. IP, IPX, DDP D. SDLC, LAT, NETBIOS

10. What is the function of the Presentation Layer, as described by the OSI reference model?

A. Provides data representation and format to the Application Layer

B. Provides presentation services to the Presentation Layer.

C. Converts application data to binary.

D. Converts application data to EBCDIC.

11. The *upper layers* of the OSI model are, in correct order -

A. Session, application, presentation B. Session, presentation, application

C. session, application, presentation, physical D. Application, presentation, session, physical

12. True or False: The network layer uses physical addresses to route data to destination hosts.

A. True B. False

13. Application layer provides basis for

A. Email services B) Directory services. C)File transfer, access, and management.

2) Network virtual terminal.

14. Segmentation and reassembly is responsibility of

A. 7th Layer B)6th Layer C)5th Layer D)4th layer

15. Layer that are used to deal with mechanical and electrical specifications are

A. Physical Layer B)Data Link Layer C)Network Layer D)Transport Layer

16. Network layer is responsible for the

A. Node to node communication B)Source to destination
B. Hop to hop communication D) Both b and c

17.TCP/IP model does not have _____ layer but OSI model have this layer.
a) Session layer b) presentation layer
c) Application layer d) both (a) and (b)

18. Which layer links the network support layers and user support layers

a) session layer b) data link layer c) transport layer d) network layer

19.Which address is used in an internet employing the TCP/IP protocols?
a) physical address and logical address b) port address
c) specific address d) all of the mentioned

20.Which layer is responsible for process to process delivery?
a) network layer b) transport layer c) session layer d) data link layer

21. Which layer provides the services to user?
a) application layer b) session layer c) presentation layer d) none of the mentioned

22. Transmission data rate is decided by
a) network layer b) physical layer c) data link layer d) transport layer

23. On _____ layer every device has a logical address know as IP address.

a) Network layer b) Physical layer c) Data link layer d) Application layer

24. _____ defines the protocol to set up and terminate a connection between two directly connected nodes over a link/medium.

a) Network layer b) Physical layer c) Data link layer d) Presentation layer

25. OSI model was introduced by ISO (International Organization for Standardization) in

a) 2001 b) 1985 c) 1999 d)1970

26._____ provides for full-duplex, half-duplex, or simplex operation.

a) Network layer b) Session layer c)Data link layer d) Presentation layer

27. Switch is _____ Layer device.

a) Transport b) Datalink (layer-2) c) Physical layer (layer-1) d) Network layer

28._____ layer establishes, manages and terminates the connections between the local and remote application.

A)Network b) Session layer C)Data link layer d) Transport layer

29. The addresses use for communication on data-link layer is _____

a) MAC b) IP Address c) Frames d) Bits

30. The layer deals with electrical and specifications of the data connection is

a) Network layer b) Physical layer C)Data link layer d) Presentation layer

31. On which layer of OSI model, information/data is form of bits?

a) Network layer b) Physical layer C)Data link layer d) Presentation layer

32. The network layer protocol of internet is
a) Ethernet b) internet protocol c) hypertext transfer protocol d) none of the mentioned

33.The network layer concerns with
a) bits b) frames c) packets d) none of the mentioned

34. Transport layer protocols deals with
a) application to application communication b) process to process communication
c) node to node communication d) none of the mentioned

35. Which one of the following is a transport layer protocol?
a) stream control transmission protocol b) internet control message protocol
c) neighbor discovery protocol d) dynamic host configuration protocol

TCP/IP QUESTIONS

1) What is the basic unit of data transfer across an IP internetwork?

A.The Data Link Layer frame B. The IP Layer Packet

C. The TCP Layer Packet D. The Application layer Packet

2. Which of the following components of the TCP/IP protocol stack are end to end layers (also know as host to host layers) ?

A.ARP B. IP C. TCP and UDP D. All the above

3. Which of the following does not describe the IP packet delivery layer?

A. Connectionless B. Best Effort C. Unreliable D. Streaming

4. Which of the following fields in the header of an IP packet will be decremented by one at each router?

A. The Header Checksum B. The Type of Service (TOS)

C. The Time to Live (TTL) D. The Protocol Number

5. Which of the following fields in the IP header identifies the type of data (payload) that the IP packet is carrying?

A. The Header Checksum B. The Type of Service (TOS

C. The Time to Live (TTL) D. The Protocol Number

6. Which of the following is not true about an IP address?

A. An IP address is a logical address B. An IP address is globally unique in an internetwork

C. An IP address can be considered to consist of a Network Part and a Host Part

D. An IP address is usually represented in Hex Format for the user

7. Which of the following IP addresses is a class A number?

A. 126.1.1.1 B. 128.1.1.1 C. 191.1.1.1 D. 192.1.1.1

8. Which of the following default masks for the major class numbers is incorrect?

A. Class A mask 255.0.0.0 or /8 B. Class B mask 255.255.0.0 or /16

C. Class C mask 255.255.255.0 or /24 D. Class D mask 255.255.255.255 or /32

9) Given the IP address 199.74.239.1 /24, what is the network number?

A. 199.0.0.0 B. 199.74.0.0 C. 199.174.239.0 D. 199.74.239.1

10. What does the ARP (Address Resolution Protocol) do?

A. Resolves IP addresses to MAC addresses B. Resolves MAC addresses to IP addresses

C. Resolves the TYPE field to the MAC address D. Resolves the MAC address to the TYPE field

11. Which of the following services use TCP?

1.DHCP 2)SMTP 3)HTTP 4)TFTP 5)FTP

A. 1 and 2

B. 2, 3 and 5

C. 1, 2 and 4

D. 1, 3 and 4

12.What layer in the TCP/IP stack is equivalent to the Transport layer of the OSI model?

A. Application

B. Host-to-Host

C. Internet

D. Network Access

13.You want to implement a mechanism that automates the IP configuration, including IP address, subnet mask, default gateway, and DNS information. Which protocol will you use to accomplish this?

A. SMTP

B. SNMP

C. DHCP

D. ARP

14. Which of the following is private IP address?

A. 12.0.0.1

B. 168.172.19.39

C. 172.15.14.36

D. 192.168.24.43

15.Which of the following allows a router to respond to an ARP request that is intended for a remote host?

A. Gateway DP

B. Reverse ARP (RARP)

C. Proxy ARP

D. Inverse ARP (IARP)

15.The DoD model (also called the TCP/IP stack) has four layers. Which layer of the DoD model is equivalent to the Network layer of the OSI model?

A. Application

B. Host-to-Host

C. Internet

D. Network Access

16.Which class of IP address provides a maximum of only 254 host addresses per network ID?

A. Class A

B. Class B

C. Class C

D. Class D

17.If you use either Telnet or FTP, which is the highest layer you are using to transmit data?

A. Application

B. Presentation

C. Session

D. Transport

18.Which of the following is the decimal and hexadecimal equivalents of the binary number 10011101?

A. 155, 0x9B

B. 157, 0x9D

C. 159, 0x9F

D. 185, 0xB9

19.Which statements are true regarding ICMP packets?

1.They acknowledge receipt of a TCP segment.

2.They guarantee datagram delivery.

3.They can provide hosts with information about network problems.

4.They are encapsulated within IP datagrams.

A. 1 only

B. 2 and 3

C. 3 and 4

D. 2, 3 and 4

20.Which of the following are layers in the TCP/IP model?

1.Application

2.Session

3.Transport

4.Internet

5.Data Link

6.Physical

A. 1 and 2

B. 1, 3 and 4

C. 2, 3 and 5

D. 3, 4 and 5

21.Which layer 4 protocol is used for a Telnet connection?

A. IP

B. TCP

C. TCP/IP

D. UDP

Although Telnet does use TCP and IP (TCP/IP), the question specifically asks about layer 4, and IP works at layer3. Telnet uses TCP at layer 4

23.What protocol is used to find the hardware address of a local device?

A. RARP

B. ARP

C. IP

D. ICMP

24.Which of the following protocols uses both TCP and UDP?

A. FTP

B. SMTP

C. Telnet

D. DNS

---------- Finish ----------