Chapter 1

BESIC NETWOR KING

A **computer network** is a digital telecommunications network for sharing resources between nodes, which are computing devices that use a common telecommunications technology.

Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network.The aim of the computer network is the sharing of resources among various devices.In the case of computer network technology, there are several types of networks that vary from simple to complex level.

What Do Networks Do

Computer networks are used to carry out a large number of tasks through the sharing of information.

Some of the things that networks are used for include:

- Communicating using email, video, instant messaging and other methods
- Sharing devices such as printers, scanners and photocopiers
- Sharing files
- Sharing software and operating programs on remote systems
- Allowing network users to easily access and maintain information

Peer-to-Peer

In a Peer-to-Peer network you take the machine currently in existence, install networking cards in them, and connect them through some type of cabling. Each machine is known as Peer and can participate in the sharing of files or resources. No server is required, so there is no additional cost for a dedicated machine, but there is also no real security.

Peer-to-Peer networks require an operating system that can understand networking and function in this (Peer-to-Peer) way. Microsoft Windows 95, Microsoft Windows 98, Windows NT server and Windows NT workstation can all function in Peer to-Peer environment.

If file and print sharing has been enabled on a Windows 95 system, for example, you can create a share by selecting a folder and choosing to share it. By default, no password is associated with it but you can choose to assign one that a user must know in order to access the resource. Access permission can be Read-Only, Full or depend on password this is known as

share level security. Access is gained when a user supplies the correct password to access the share.-

Peer-to-Peer networking works in small environments. If you grow beyond approximately 10 machines, the administrative overhead of establishing shares, coupled with the lack of tight security, creates a nightmare.

Advantages of peer-to-peer network

Server is not required

No additional cost for dedicated-machine

Disadvantages of peer-to peer network

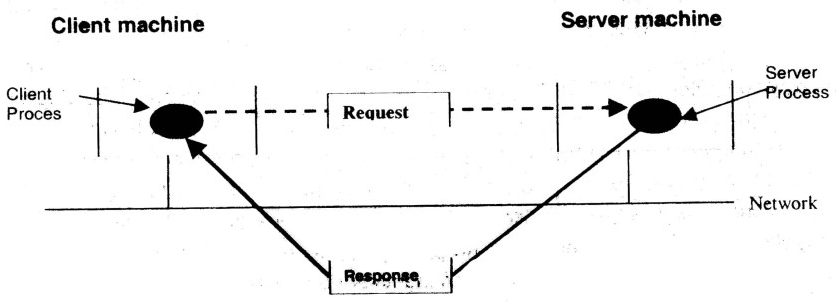
Provides share level security

Can work in small environments only.

CLIENT SERVER MODEL

Normally network should provide high reliability; emergency back up etc. For satisfying this purpose big mainframe computers are required. But this will be not cost efficient. On other side small computers have a much better price/performance ratio than the large Ones. Mainframes (room-Size) computers are roughly a factor of ten faster than personal computers, but they cost thousand times more. This imbalance has cost many system designers to build systems consisting of personal computers, one per user with data kept on one or more shared file server machines.

In this model the users are called clients, and the whole arrangement is called as Client-Server model,



In the client server model communication generally takes the form of a request Message from the client to server asking for some work to be done. The server then does the work and sends back the reply. Usually there are many clients using a small no. of servers.

Types of Network

There are many different types of network, which can be used for different purposes and by different types of people and organization. Here are some of the network types that you might come across:

- **Local Area Networks (LAN)**
  A local area network or LAN is a network that connects computers within a limited area. This might be in a school, an office or even a home.

- **Personal Area Networks (PAN)**
  A personal area network is a network that is based on an individual's workspace. The individual's device is the center of the network, with other devices connected to it. There are also wireless personal area networks.

- **Home Area Networks (HAN)**
  A home area network connects devices within a home environment. It might include personal computers, tablets, smartphones, printers, TVs and other devices.

- **Wide Area Networks (WAN)**
  A wide area network is a network that covers a larger geographical area, usually with a radius of more than a kilometer.

- **Campus Networks**
  A campus network is a LAN or set of connected LANs which is used by a government agency, university, corporation or similar organization and is typically a network across a set of buildings that are close together.

- **Metropolitan Area Networks (MAN)**
  Metropolitan area networks are networks that stretch across a region the size of a metropolitan area. A MAN is a series of connected LANs in a city, which might also connect to a WAN.

- **Enterprise Private Networks**
  An enterprise private network is used by a company to connect its various sites so that the different locations can share resources.

- **Internetworks**
  Internetworks connect different networks together to build a larger network. Internetworking is often used to describe building a large, global network.

- **Backbone Networks (BBN)**
  A backbone is a part of a network that connects different pieces and provides a path for information to be exchanged.

- **Global Area Networks (GAN)**
  A global area network is a worldwide network that connects networks all over the globe, such as the internet.

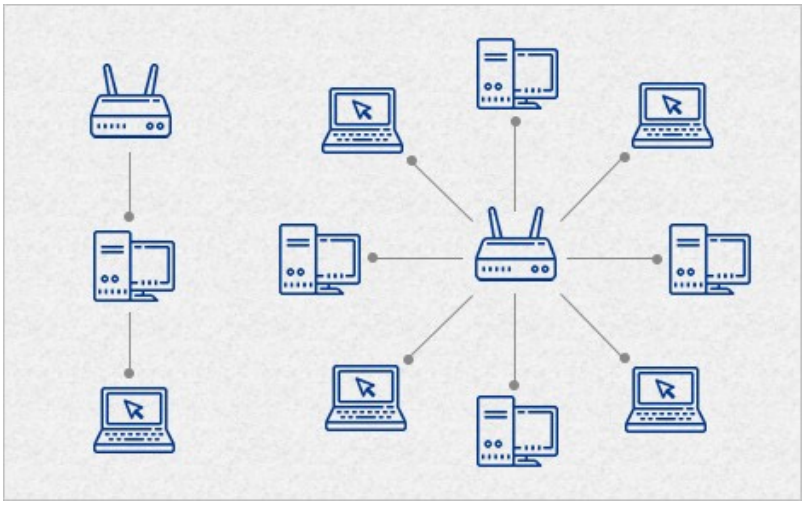
Types of Network Connections

There are also different types of network connections that concern how elements in a network are connected to each other. Topologies are used to connect computers, with a collapsed ring being the most common type due to the Ethernet supporting the internet, local area networks and wide area networks.

The topologies that are used to create networks:

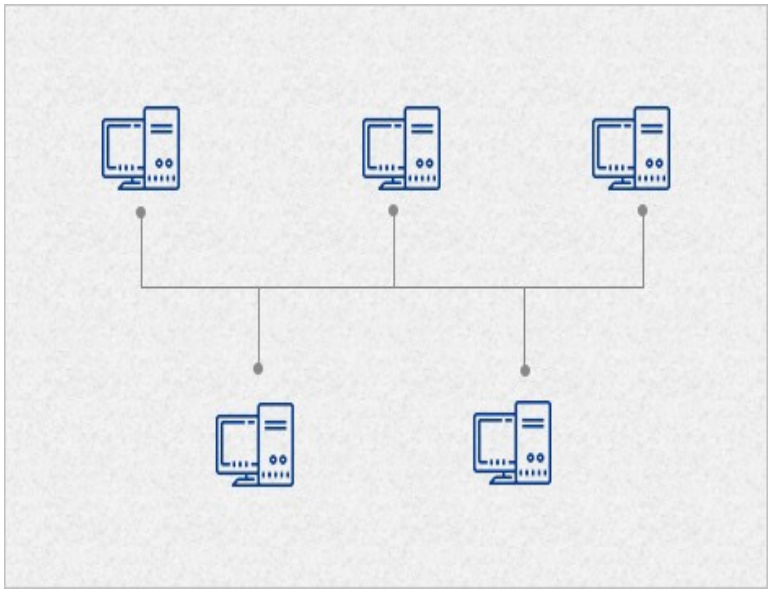
Star Topology

A central node connects a cable to each computer in the network in a star topology. Each computer in the network has an independent connection to the center of the network, and one connection breaking won't affect the rest of the network. However, one downside is that many cables are required to form this kind of network.



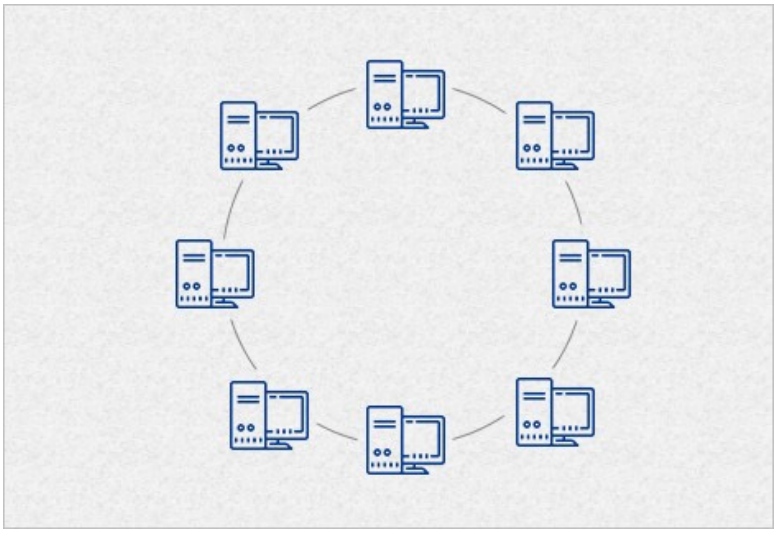
Bus Topology

In a bus topology network connection, one cable connects the computer. The information for the last node on the network has to run through each connected computer. There is less cabling required, but if the cable breaks it means that none of the computers can reach the network.



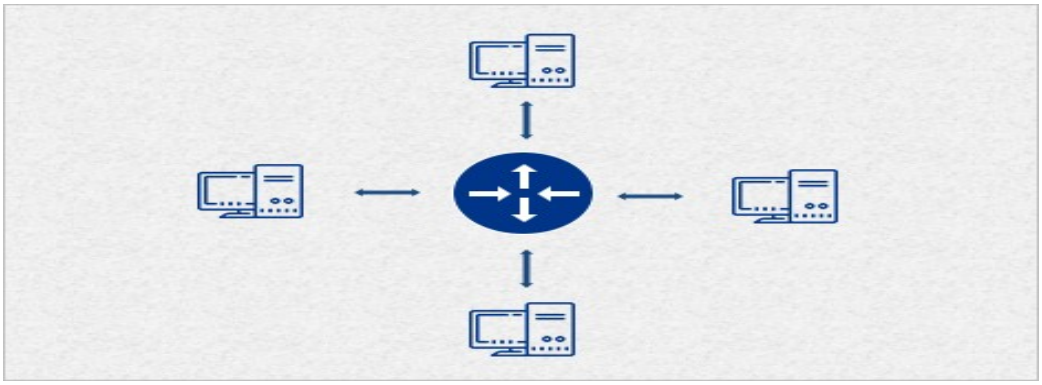
Ring Topology

A ring topology is similar to a bus topology. It uses a single cable with the end nodes connected to each other so the signal can circle through the network to find its recipient. The signal will try several times to find its destination even when the network node is not working properly. A collapsed ring has a central node which is a hub, router or switch. The device has an internal ring topology and has places for cable to plug in. Every computer in the network has its own cable to plug into the device. In an office, this probably means having a cabling closet, where all computers are connected to the closet and the switch.



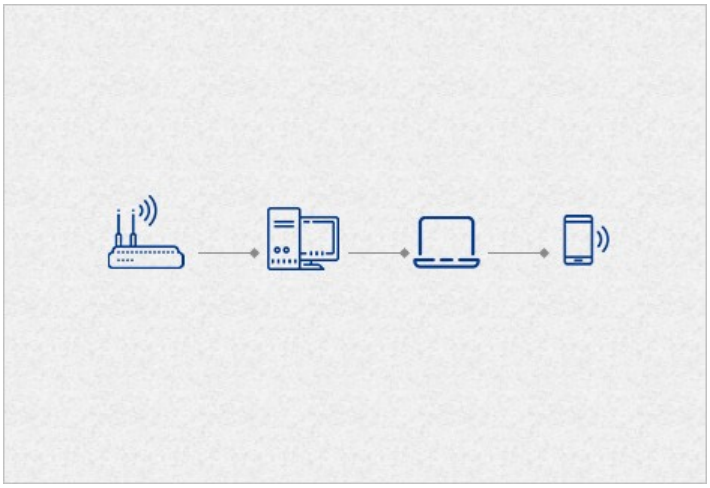
Network Protocols

Network protocols are the languages that computer devices use to communicate. The protocols that computer networks support offer another way to define and group them. Networks can have more than one protocol and each can support different applications. Protocols that are often used include TCP/IP, which is most common on the internet and in home networks.



Wired and Wireless Networks

Many protocols can work with both wired and wireless networks. In recent years, however, wireless technologies have grown and become much more popular. Wi-Fi and other wireless technologies have become the favorite option for building computer networks. One of the reasons for this is that wireless networks can easily support different types of wireless gadgets that have become popular over the years, such as smartphones and tablets. Mobile networking is now an important thing to consider because it's not going to go away anytime soon.



Switching techniques

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- Circuit switching is used in public telephone network. It is used for voice transmission.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- Each and every node stores the entire message and then forwards it to the next node. This type of network is known as **store and forward network.**

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.

- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.

Chapter 2

OSI Model

- The Open System Interconnection (OSI) reference model describes how the information moves from one computer to another computer through a network.
- This model was developed by the International Organization for Standardization (ISO) in 1984.
- This model is used for understanding and designing a network architecture that is flexible, robust and inter-operable.
- OSI model has seven separate but related layers : Physical, Data link, Network, Transport, Session, Presentation and Application.

Each layer defines a part of the process of moving information across the network.

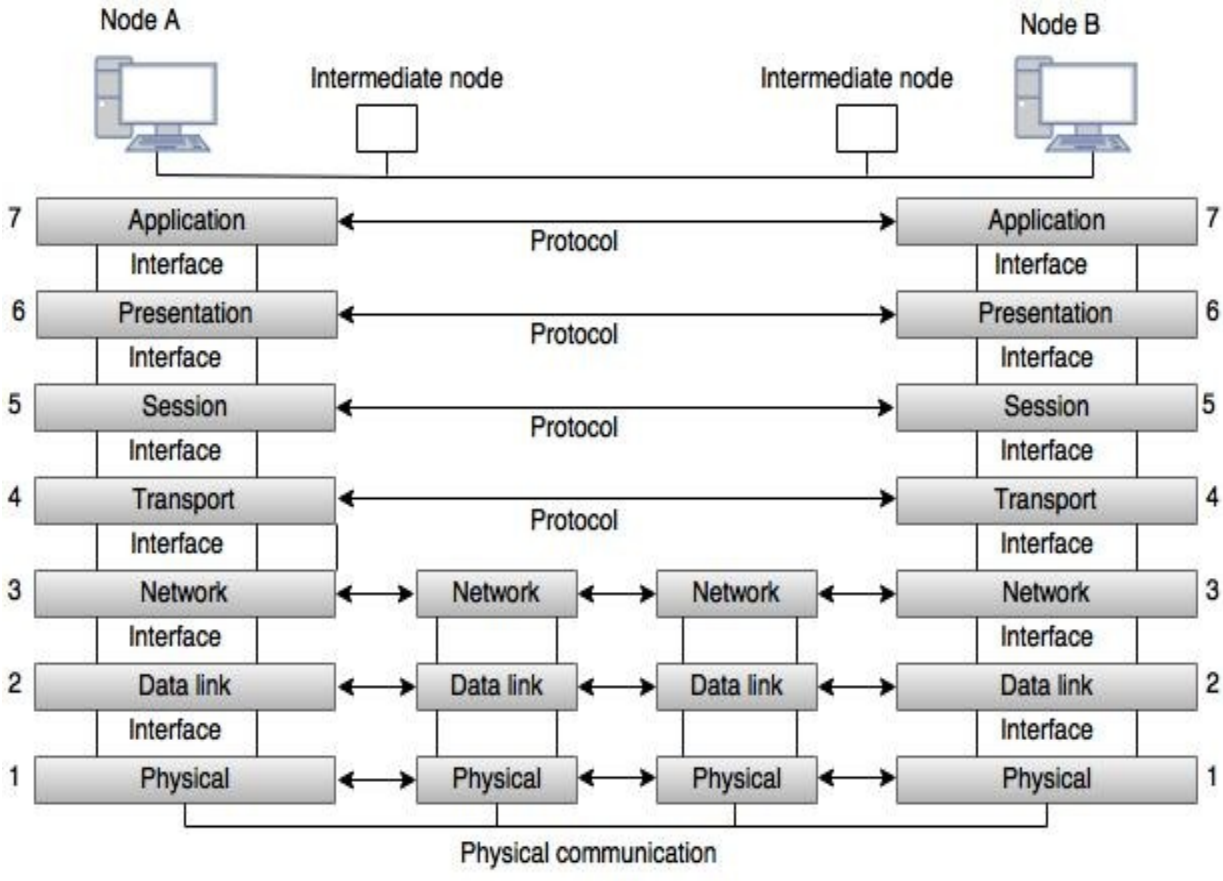


Fig: OSI Model

Interface between layers

Interface is responsible for passing the data and network information down through the layers of the sending device and back up through the layers of the receiving device.

1. Physical layer:

- Physical layer is the lowest layer of the OSI model.
- It coordinates the function required to transmit a bit stream over a communication channel.
- It defines the procedures and functions that physical devices and interfaces have to perform for transmission.
- Physical layer also defines the direction of transmission between two devices. Direction may be simplex, full-duplex and half-duplex.

2. Data link layer

- Data link layer is responsible for transmitting the data over the channels.
- It is used to divide the stream of bits received from the network layer into manageable data units called **frames**.
- It adds a header to the frame to define the sender and receiver of the frame.
- Data link layer detects and corrects the transmission errors using the correction method.

3. Network layer

- The network layer is responsible for the delivery of a packet, across multiple network.
- It specifies the intra-network operations and different types of addressing and routing devices.
- Network layer also provides the logical and service addressing and switching control.

4. Transport layer

- The transport layer specifies the process to process delivery of the entire message.
- It is responsible for flow control and error control.
- The transport layer of sending device makes sure that the entire message arrives at the transport layer of receiving device without error.

5. Session layer

- Session layer is the network dialog controller.

- It is used to establish, maintain and synchronize the interaction among communicating system.
- Specific responsibility of session layer is dialog control.

6. Presentation layer

- The presentation layer is responsible to translate the information in to bit streams before transmission.
- It is also responsible for data encryption, data decryption and data comprehension.

7. Application layer

- Application layer allows the user, whether human or software, to access the network.
- This layer provides user interfaces and application services for file transfers, e-mail, and other network software services.

Chapter 3

TCP/IP Model

- TCP/IP means **Transmission Control Protocol / Internet Protocol**.
- TCP/IP model is a four layer model and the layers are host-to-network layer, Internet layer, transport layer and application layer.
- The three topmost layers (application, presentation and session) in the OSI model are represented in TCP/IP by a single layer called the **application layer**.
- The host-to-network layer in the TCP/IP model is equivalent to the combination of physical and data link layer in the OSI model.

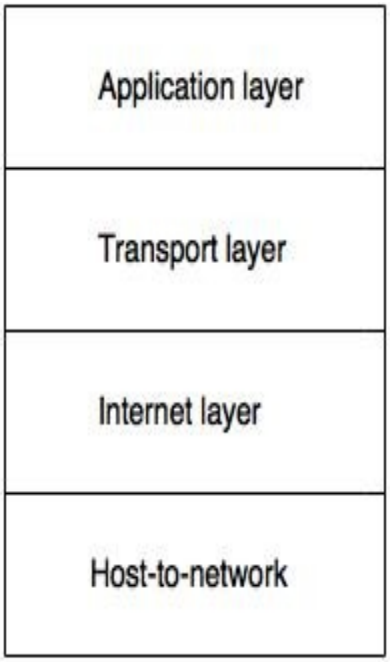


Fig: TCP/IP reference model

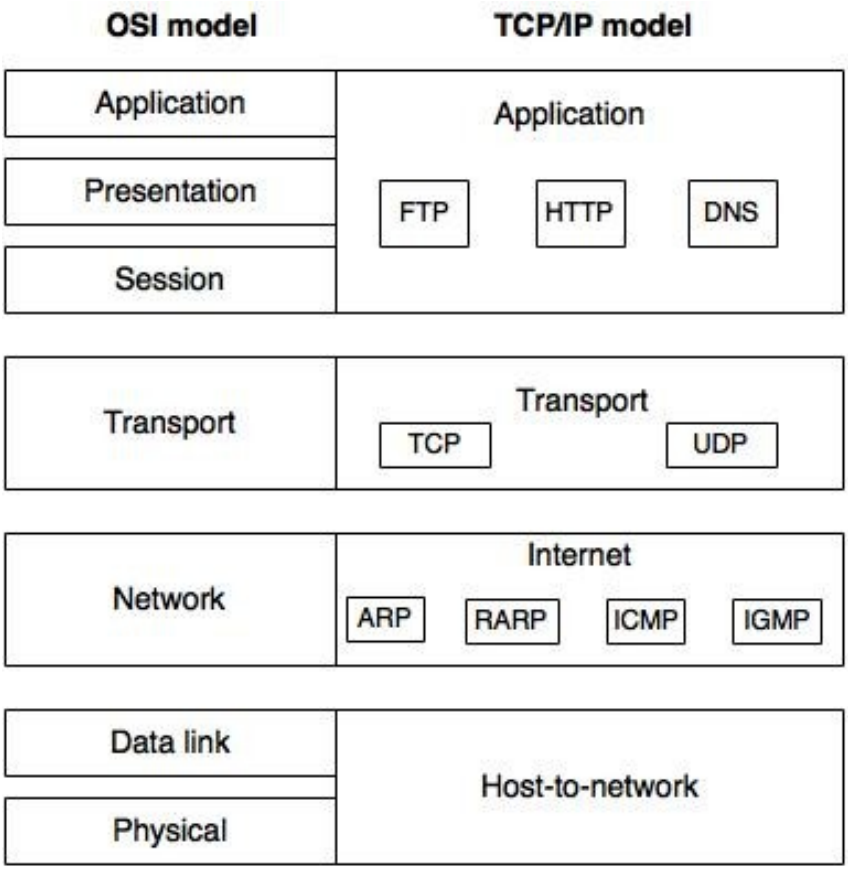


Fig: OSI and TCP/IP model

Host-to-network

- Host-to-network layer does not define any specific protocol.
- It supports all the standard protocols.
- It is responsible for accepting and transmitting IP datagrams.
- The TCP/IP network can be a **Local Area Network (LAN)** or a **Wide Area Network (WAN).**

Internet layer

- At the Internet level, TCP/IP supports IP, ARP, RARP, ICMP and IGMP protocols.
- All these protocols handle machine to machine communication.

IP – IP is the primary protocol, which is used to transport data in packets (datagrams). Each packet is transported separately.

ARP – The **Address Resolution Protocol** is used to associate a logical address with a physical address.

RARP – The **Reserve Address Resolution Protocol** is used to discover host's Internet address when it knows only its physical address.

ICMP – The hosts and gateways use the ICMP (**Internet Control Message Protocol**) mechanism to send notification of datagram problems back to the sender.

IGMP – The **Internet Group Message Protocol** is used for simultaneous transmission of a message to a group of recipients.

Transport layer

- UDP and TCP are the transport layer protocols.
- These protocols are responsible for delivery of a message from one process to another process.

TCP – TCP converts the incoming data stream into smaller units called segments and passes each one into the internet layer.

UDP – This is a connectionless protocol. It adds only port address, checksum error control and length information to the data from the upper layer.

Application layer

- The application layer protocols are: SMTP, FTP, HTTP, DNS, SNMP TELNET and so on.
- TELNET is the Network Terminal Protocol, which provides remote login over the network.
- SMTP is used to deliver the electronic mail.
- FTP is used for interactive file transfer.

Domain Name System

- Domain Name System is an Internet service that translates domain names into IP addresses.

- The DNS has a distributed database that resides on multiple machines on the Internet.
- DNS has some protocols that allow the client and servers to communicate with each other.
- When the Internet was small, mapping was done by using hosts.txt file.
- The host file was located at host's disk and updated periodically from a master host file.
- When any program or any user wanted to map domain name to an address, the host consulted the host file and found the mapping.
- Now Internet is not small, it is impossible to have only one host file to relate every address with a name and vice versa.
- The solution used today is to divide the host file into smaller parts and store each part on a different computer.
- In this method, the host that needs mapping can call the closest computer holding the needed information.
- This method is used in Domain Name System (DNS).

An **IP address** is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. Contrast with IP, which specifies the format of packets, also called datagram, and the addressing scheme.

An IP address consists of 32 bits, often shown as 4 octets of numbers from 0-255 represented in decimal form instead of binary form. For example, the IP address: 168.212.226.204 in binary form is 10101000.11010100.11100010.11001100.

An IP address consists of two parts, one identifying the network and one identifying the node, or host.

IPv4 Address

The common type of IP address (is known as IPv4, for "version 4"). Here's an example of what an IP address might look like:

66.171.248.170

An IPv4 address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255.

Class A Network

In a Class A Network binary address start with 0, therefore the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octet) identify the network and the remaining 24 bits indicate the host within the network. An example of a Class A IP address is 102.168.212.226, where "102" identifies the network and "168.212.226" identifies the host on that network.

Class B Network

In a Class B Network, binary addresses start with 10, therefore the decimal number can be anywhere from 128 to 191. The number 127 is reserved for loopback and is used for internal testing on the local machine. The first 16 bits (the first two octets) identify the network and the remaining 16 bits indicate the host within the network. An example of a Class B IP address is 168.212.226.204 where "168.212" identifies the network and "226.204" identifies the host on that network.

Class C Network

Binary addresses start with 110, therefore the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network and the remaining 8 bits indicate the host within the network. An example of a Class C IP address is 200.168.212.226 where "200.168.212" identifies the network and "226" identifies the host on that network.

Class D Network

In a Class D Network, binary addresses start with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multicasting.

Class E Network

In a Class E Network, binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented or utilized in a standard way.

IPv6 Address

It's called IPv6 and it offers a maximum number of IP address for today and for the future.

Whereas IPv4 supports a maximum of approximately 4.3 billion unique IP addresses, IPv6 supports, in theory, a maximum number that will never run out.

An IPv6 address consists of eight groups of four hexadecimal digits. If a group consists of four zeros, the notation can be shortened using a colon to replace the zeros. Here's an example IPv6 address:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Subnet Masking

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts.

A Class A, B, or C TCP/IP network can be further divided, or subnetted, by a system administrator. This becomes necessary as you reconcile the logical address scheme of the Internet (the abstract world of IP addresses and subnets) with the physical networks in use by the real world.

A system administrator who is allocated a block of IP addresses may be administering networks that are not organized in a way that easily fits these addresses. For example, you have a wide area network with 150 hosts on three networks (in different cities) that are connected by a TCP/IP router. Each of these three networks has 50 hosts. You are allocated the class C network 192.168.123.0. (For illustration, this address is actually from a range that is not allocated on the Internet.) This means that you can use the addresses 192.168.123.1 to 192.168.123.254 for your 150 hosts.

Two addresses that cannot be used in your example are 192.168.123.0 and 192.168.123.255 because binary addresses with a host portion of all ones and all zeros are invalid. The zero address is invalid because it is used to specify a network without specifying a host. The 255 address (in binary notation, a host address of all ones) is used to broadcast a message to every host on a network. Just remember that the first and last address in any network or subnet cannot be assigned to any individual host.

You should now be able to give IP addresses to 254 hosts. This works fine if all 150 computers are on a single network. However, your 150 computers are on three separate physical networks. Instead of requesting more address blocks for each network, you divide your network into subnets that enable you to use one block of addresses on multiple physical networks.

In this case, you divide your network into four subnets by using a subnet mask that makes the network address larger and the possible range of host addresses smaller. In other words, you are 'borrowing' some of the bits usually used for the host address, and using them for the network

portion of the address. The subnet mask 255.255.255.192 gives you four networks of 62 hosts each. This works because in binary notation, 255.255.255.192 is the same as 1111111.11111111.1111111.11000000. The first two digits of the last octet become network addresses, so you get the additional networks 00000000 (0), 01000000 (64), 10000000 (128) and 11000000 (192). (Some administrators will only use two of the subnetworks using 255.255.255.192 as a subnet mask. For more information on this topic, see RFC 1878.) In these four networks, the last 6 binary digits can be used for host addresses.

Using a subnet mask of 255.255.255.192, your 192.168.123.0 network then becomes the four networks 192.168.123.0, 192.168.123.64, 192.168.123.128 and 192.168.123.192. These four networks would have as valid host addresses:

192.168.123.1-62
192.168.123.65-126
192.168.123.129-190
192.168.123.193-254

Remember, again, that binary host addresses with all ones or all zeros are invalid, so you cannot use addresses with the last octet of 0, 63, 64, 127, 128, 191, 192, or 255.

You can see how this works by looking at two host addresses, 192.168.123.71 and 192.168.123.133. If you used the default Class C subnet mask of 255.255.255.0, both addresses are on the 192.168.123.0 network. However, if you use the subnet mask of 255.255.255.192, they are on different networks; 192.168.123.71 is on the 192.168.123.64 network, 192.168.123.133 is on the 192.168.123.128 network.

Chapter 4

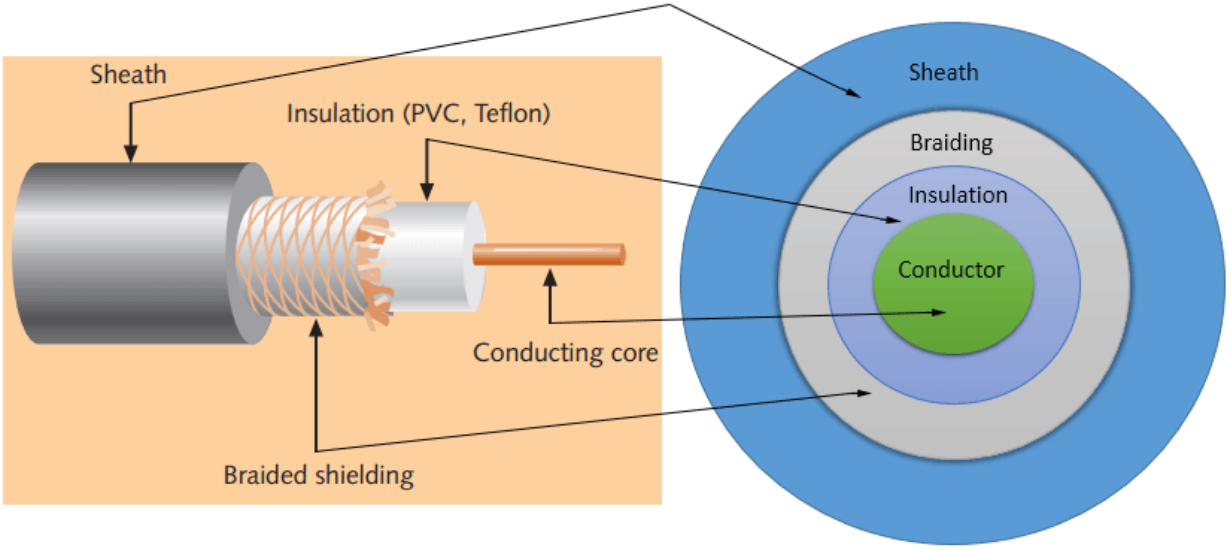
Cable and Connectors

To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables; coaxial, twisted-pair, and fiber-optic.

Coaxial cable

This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.

The following image shows these components.



A **single-core** coaxial cable uses a single central metal (usually copper) conductor, while a **multi-core** coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.

Coaxial cables in computer networks

The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even their use in computer networks has been completely discontinued.

At the beginning of computer networking, when there were no dedicated media cables available for computer networks, network administrators began using coaxial cables to build computer networks.

Because of low-cost and long durability, coaxial cables were used in computer networking for nearly two decades (80s and 90s). Coaxial cables are no longer used to build any type of computer network.

Twisted-pair cables

The twisted-pair cable was primarily developed for computer networks. This cable is also known as **Ethernet cable**. Almost all modern LAN computer networks use this cable.

This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable; UTP and STP.

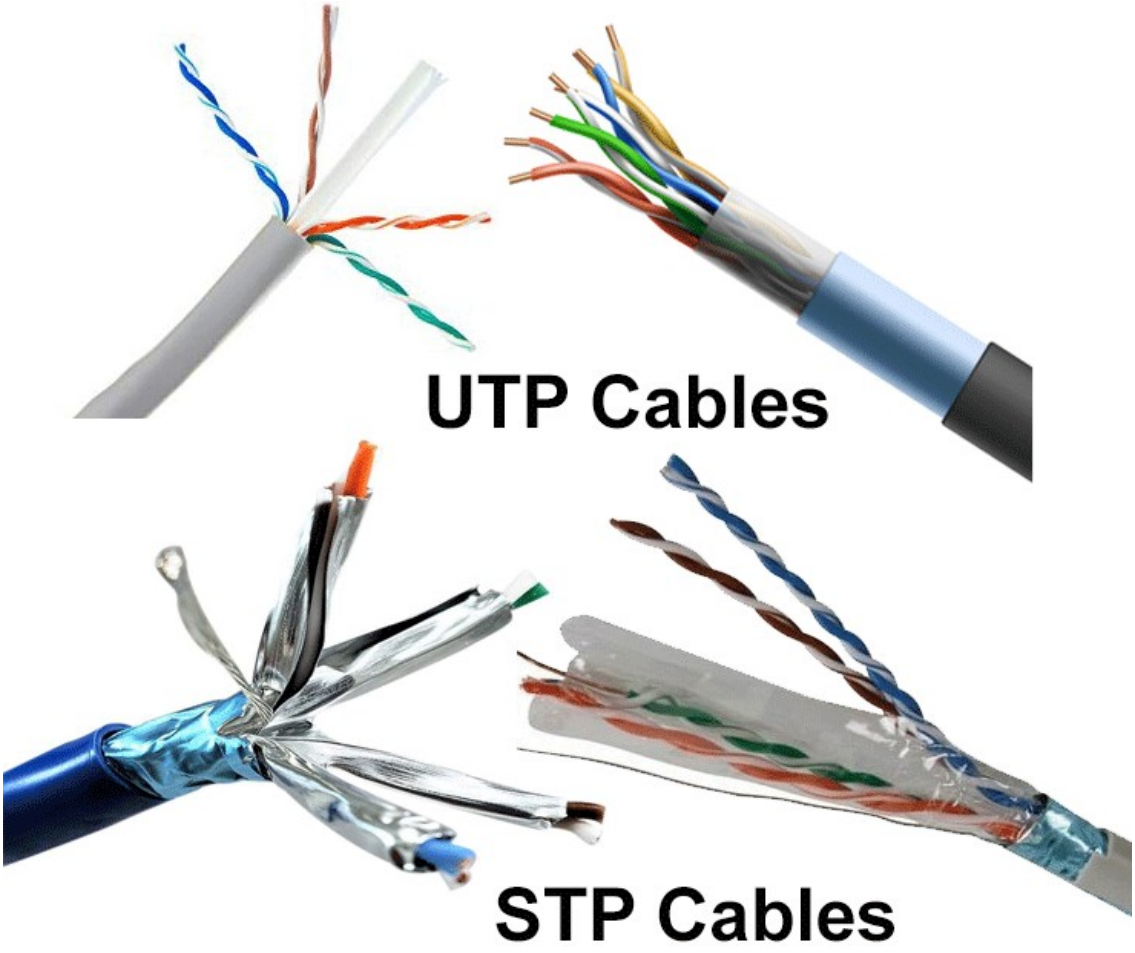
In the **UTP (*Unshielded twisted-pair*) cable**, all pairs are wrapped in a single plastic sheath.

In the **STP (*Shielded twisted-pair*) cable**, each pair is wrapped with an additional metal shield, then all pairs are wrapped in a single outer plastic sheath.

Similarities and differences between STP and UTP cables

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Since the STP cable contains more materials, it is more expensive than the UTP cable.
- Both cables use the same RJ-45 (registered jack) modular connectors.
- The STP provides more noise and EMI resistant than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.
- Both cables can accommodate a maximum of 1024 nodes in each segment.

The following image shows both types of twisted-pair cable.



Category / name of the cable	Maximum supported speed	Bandwidth/support signals rate	Ethernet standard	Description
Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4 pairs). This cable was used in the token-ring

				network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.
Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pairs and shields each pair by its own plastic sheath.

- Cat 1, 2, 3, 4, 5 are outdated and not used in any modern LAN network.
- Cat 7 is still a new technology and not commonly used.
- Cat 5e, 6, 6a are the commonly used twisted-pair cables.

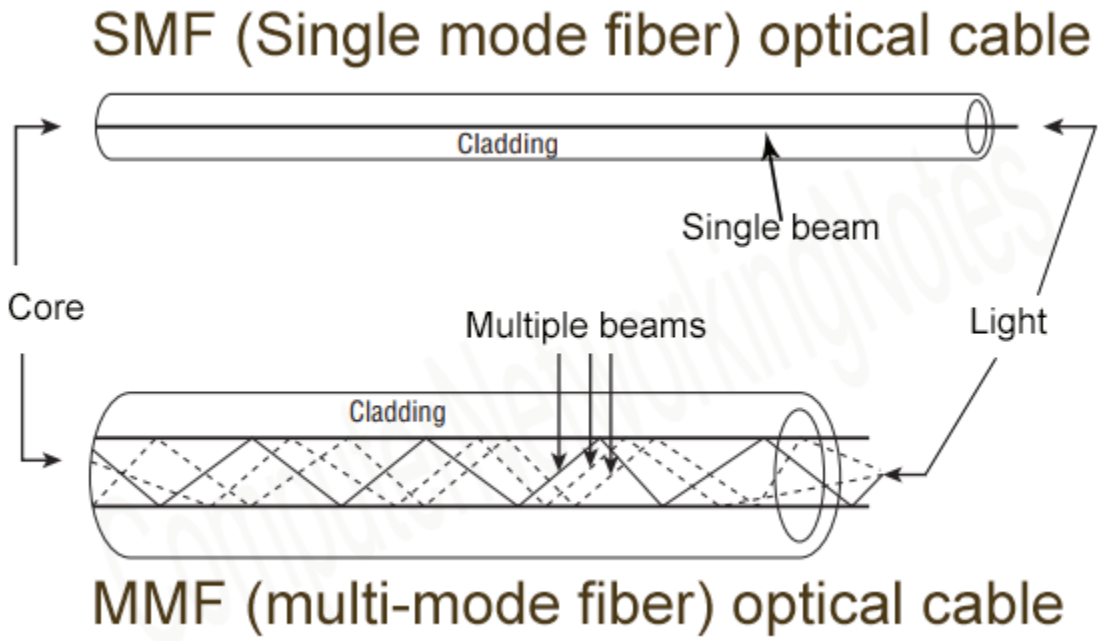
Fiber optic cable

This cable consists of core, cladding, buffer, and jacket. The core is made from the thin strands of glass or plastic that can carry data over the long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

- Core carries the data signals in the form of the light.
- Cladding reflects light back to the core.
- Buffer protects the light from leaking.
- The jacket protects the cable from physical damage.

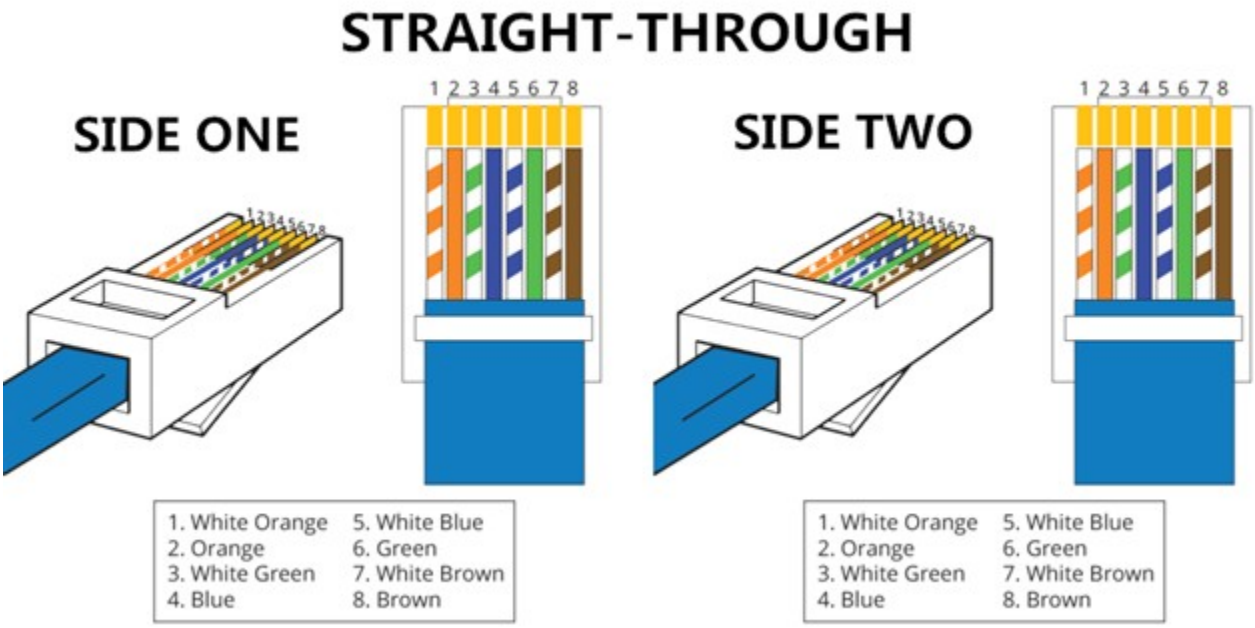
Fiber optic cable is completely immune to EMI and RFI. This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.



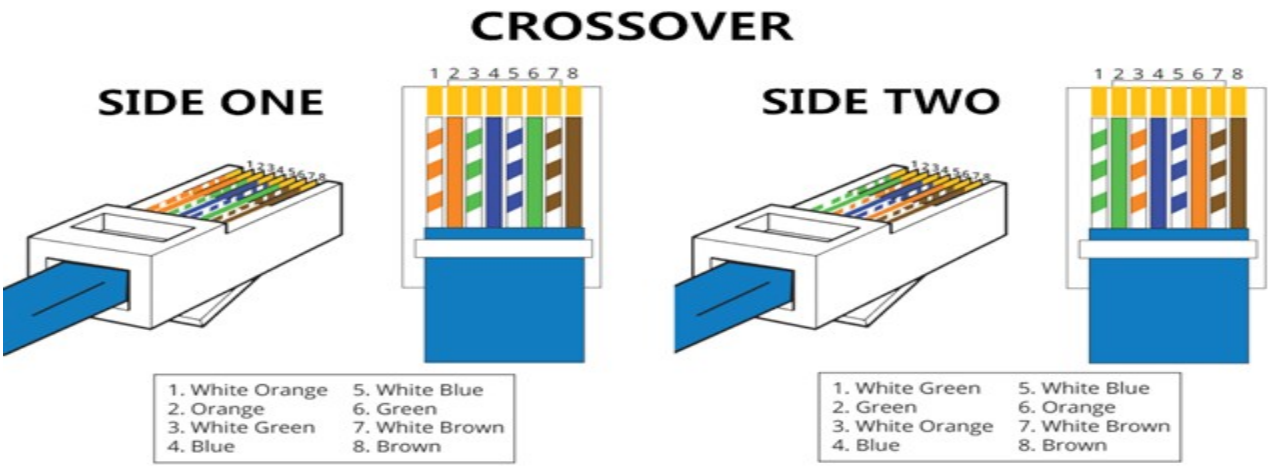
What Is Straight Through Cable?

A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight through cable, the wired pins match. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight through cable of which both ends are wired as the T568B standard.



What Is Crossover Cable?

A crossover Ethernet cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight through cable, the RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other.



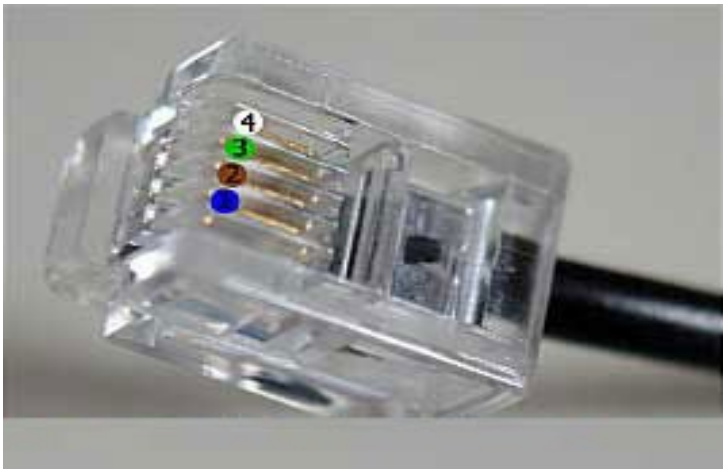
Connectors

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector . A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

An image of RJ45

RJ-11 (Registered Jack)

Standard telephone cable connectors, **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.



SCST

ST (Straight Tip) and SC (Subscriber Connector or Standard Connector)

Fiber network segments always require two fiber cables: one for transmitting data, and one for receiving. Each end of a fiber cable is fitted with a plug that can be inserted into a network adapter, hub, or switch. In the North America, most cables use a square SC connector (Subscriber Connector or Standard Connector) that slides and locks into place when inserted into a node or connected to another fiber cable, Europeans use a round ST connector (Straight Tip) instead.

SC connector

ST connector

BNC

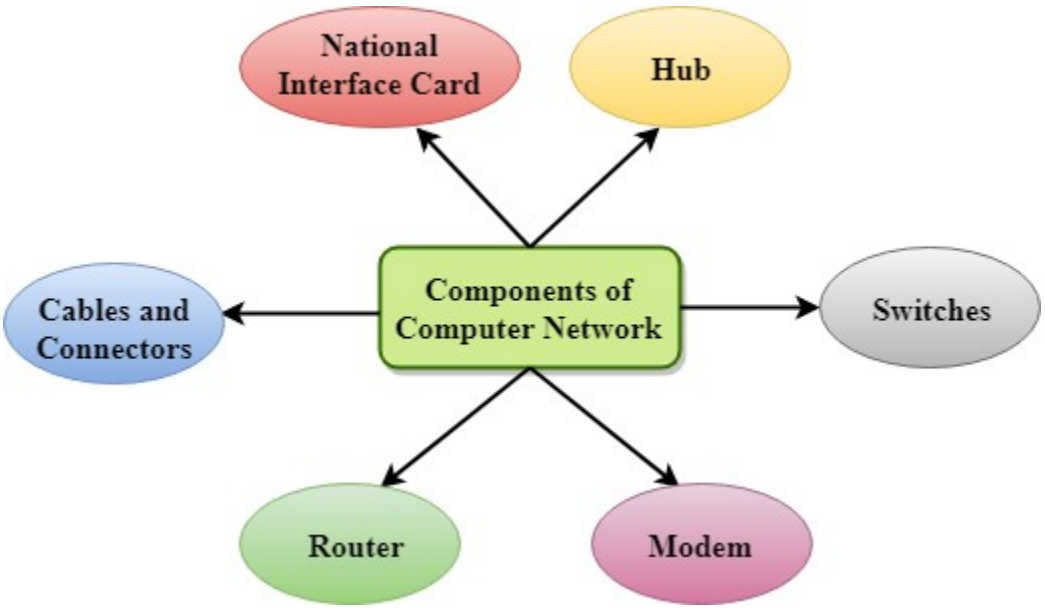
Short for **Bayonet Neill-Concelman** connector, a **BNC connector** is a type of connector used with coaxial Ethernet cable.

The basic BNC connector is a male type mounted at each end of a cable. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.
BNC T-connectors (used with the 10Base-2 system) are female devices for connecting two cables to a network interface card (NIC). A BNC barrel connector allows connecting two cables together.
BNC connectors can also be used to connect some monitors, which increases the accuracy of the signals sent from the video adapter.

Chapter 5

Network Connectivity

If we have to be familiar with the various types of network media and connections, we should learn about some devices commonly found on today's networks. Because these devices connect network entities, they are known as connectivity devices.



Some network connectivity devices are :

- The network interface card (NIC)
- The hub
- The Repeaters
- The switch
- The router
- Other devices

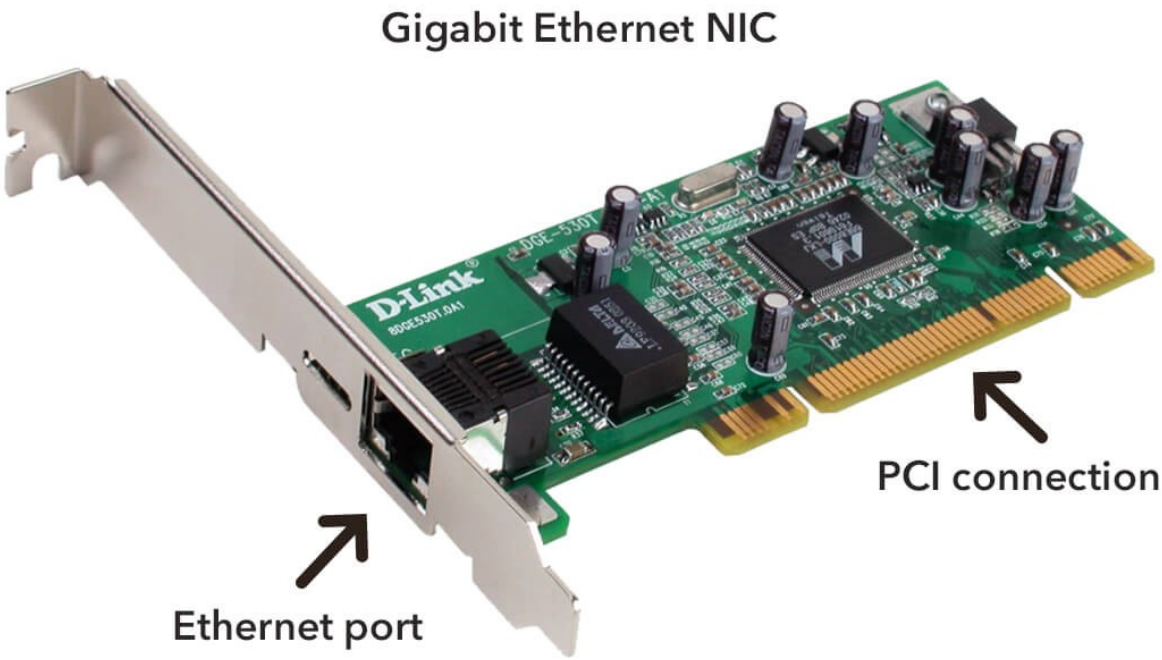
NIC

The *network interface card (NIC),* as its name suggests, is the expansion card you install in your computer to connect, or interface, your computer to the network. This device provides the physical, electrical, and electronic connections to the network media. A NIC is either an expansion card (the most popular implementation) or built in to the motherboard of the computer. In most cases, a NIC connects to the computer through *expansion slots,* which are special slots located on a computer's motherboard that allow peripherals to be plugged directly

into it. In some notebook, NIC adapters can be connected to the printer port or through a PC card slot.

NIC cards generally all have one or two light emitting diodes (LEDs) that help in diagnosing problems with their functionality. If there are two separate LEDs, one of them may be the Link LED, which illuminates when proper connectivity to an active network is detected. This often means that the NIC is receiving a proper signal from the hub/MAU or switch, but it could indicate connectivity to and detection of a carrier on a coax segment or connectivity with a router or other end device using a crossover cable. The other most popular LED is the Activity LED.

The Activity LED will tend to flicker, indicating the intermittent transmission or receipt of frames to or from the network.



Hub

In order to connect various cable segments, we need a central point to plug every thing together. A hub is-a multiport repeater. It provides point-to-multipoint connections, it is basically a shared device and works at physical layer of the OSI model. It is often located in a wiring closet and is a point of concentration for wiring.

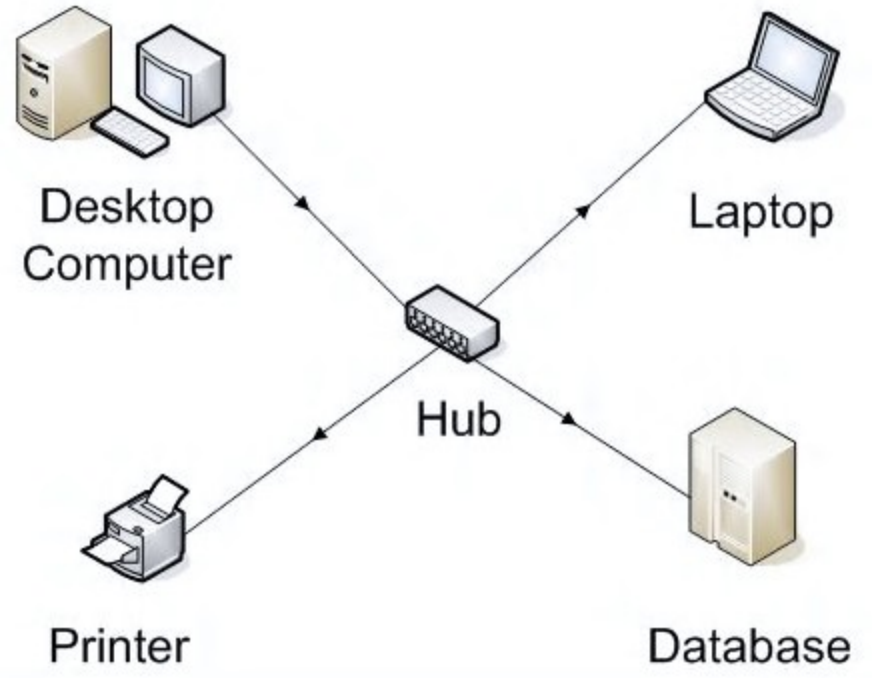
There are three types of hube namely,

Passive hub
Active hub
Intelligent hub

A passive hub connects cable segment together. No signal regeneration is performed. So each segment is allowed to be extended to only half the maximum effective distance.

An active hub is like a passive hub except it regenerates or amplifies signals. The main drawback of active hub is that some active hubs amplify cable noise as well as signal.

An intelligent hub, in addition to signal regeneration, also helps in performing network management functions. The SNMP (simple network management protocol) agents must be embedded in a hub to carry out network related functions.

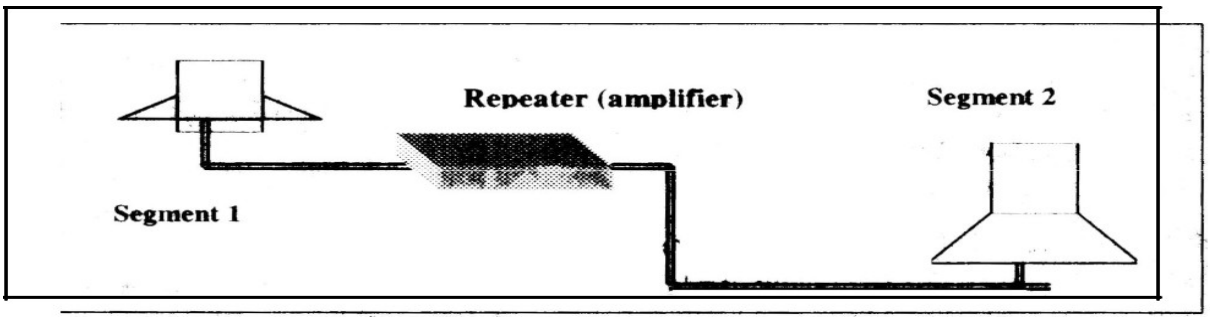


Repeaters

When an electrical signal is sent across a medium, It fades along the distance (known as attenuation) as a result of resistance from the medium itself. Naturally the longer the distance that it travelled, the more the signal fades. Eventually tie signal fades to a, point where the receiving station cannot recognise the original message (Or has trouble doing so).

In short each transmission medium can be used for a certain distance. However you can exceed the physical medium's maximum effective distance by using amplification, device called as Repeater. It works at OSI physical layer. A repeater operates as at the physical layer of the OSI model and takes a signal from one LAN and sends it to another LAN- reconditioning and retiming it in the process. The reconditioning usually amplifies and boosts the signal's power. If the signal has travelled a distance it is weak, and so on, the amplification can also be done on noise receivers.

The repeaters job is simple: it detects the signal, amplifies and retimes it, and sends it through all the ports except the one on which the signal was seen. It is important to note that since the repeater has no real knowledge of the data it is carrying, no error checking is performed. Therefore any error are passed from one segment to the next without any ability to stop it. Many networks limit the number of repeaters between the transmitting and receiving stations. On other side, by not performing any filtering, the -repeater does not slow down the network's speed or performance. The signal has travelled a distance is weak, and so on, the amplification can also be done on noise received.



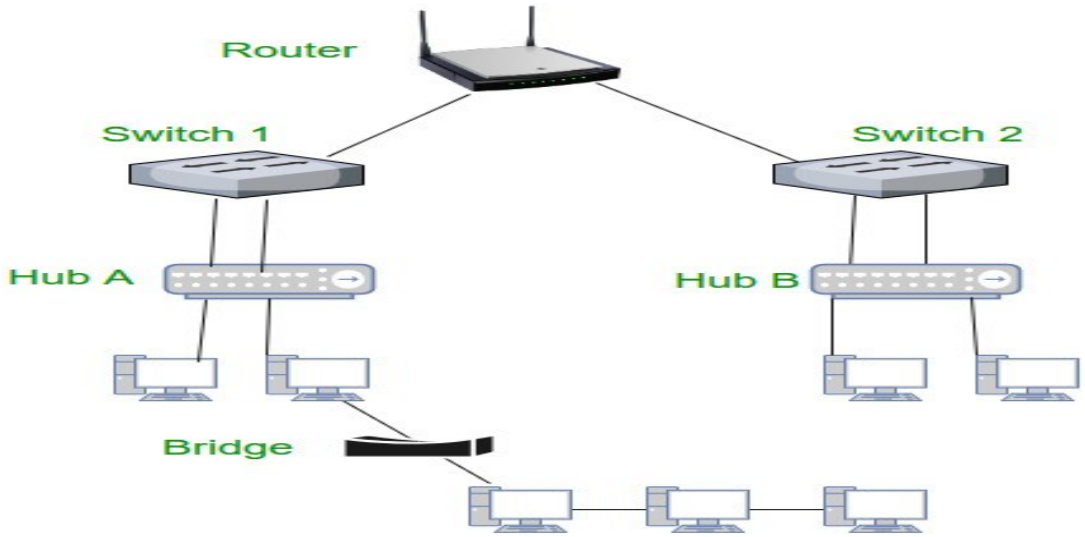
Switch

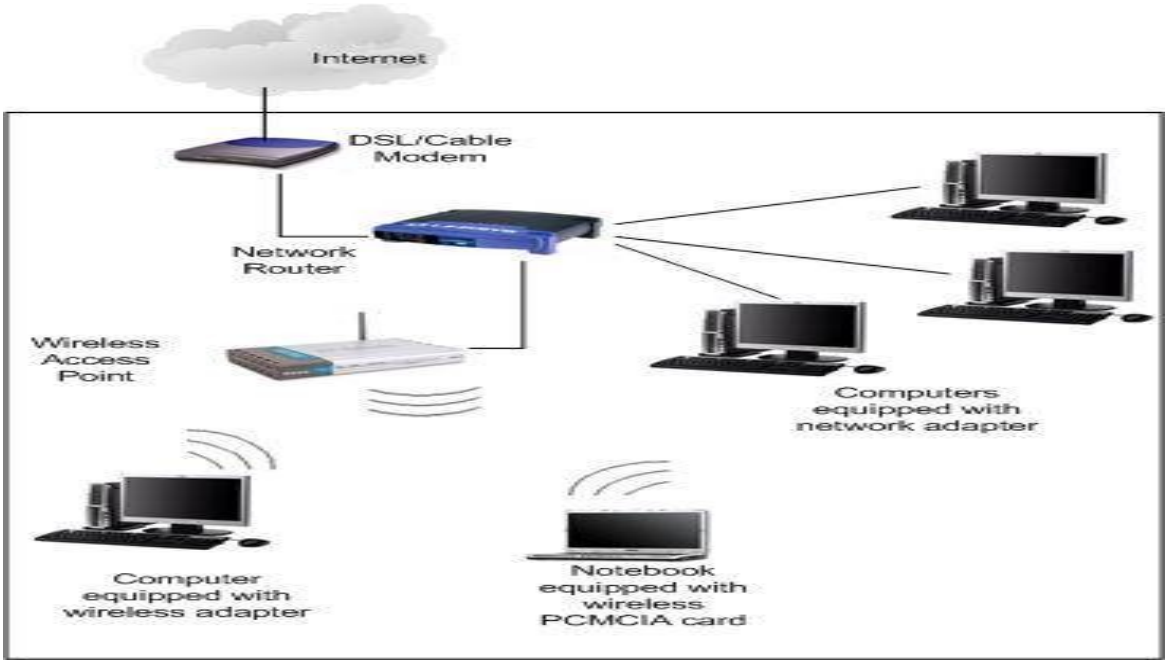
Like a hub, a switch connects multiple segments of a network together, with one important difference. Whereas a hub sends out anything it receives on one port to all the others, a switch recognizes frame boundaries and pays attention to the destination MAC address of the incoming frame as well as the port on which it was received. If the destination is known to be on a different port than the port over which the frame was received, the switch will forward the frame out over only the port on which the destination exists.

Otherwise, the frame is silently discarded. If the location of the destination is unknown, then the switch acts much like a hub in that it floods the frame out every port, except for the port over which it was received, unlike a hub. The only way any party not involved in that communication will receive the transmission is if it shares a port with the transmitter or receiver of the frame. This can occur if a hub is attached to the switch port, instead of in a 1:1 relationship of end devices and switch ports. The benefit of a switch over a hub is that the switch increases performance because it is able to support full wire speed on each and every port with a non blocking backplane, meaning the electronics inside the switch are at least equivalent in speed to the sum of the speeds of all ports.

Routers

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.





Configure a Router

Configure your router to make your network complete. You need to configure the router so that it can communicate with your network components. Fortunately, the configuration steps are rather straightforward.

After you connect the router to the network, or simply turn on a wireless router, you connect to the router by using your PC's Web browser, such as Internet Explorer. The documentation that came with the router gives you the router's Web page address. Usually, it's numerical, such as

```
http://192.168.0.1/
```

After accessing the router, and (optionally) entering its password, you see a Web page displayed. The Web page is really the router's configuration program. Follow the directions that came with the device for the basic configuration of the router. In addition to those directions, consider the following points:

- Enable the router's firewall. You don't need to adjust the firewall; most routers set things up just as you need them.
- Set a *Service Set Identifier,* or *SSID,* for your wireless network. This is the name by which the wireless network is known.
- Set the encryption for the network, known as the WEP, or Wired Equivalent Privacy. Make sure that you note the password! It's a long string of numbers and letters, and you must enter it exactly to access the network.
- You may hear or read that the password is optional, but generally, it's not. Don't compromise your network by omitting the password. In fact, Windows may not even connect to a wireless network that lacks a password.
- (Optional) Configure the base station to allow connections only from known computers. You specify this setting by listing the MAC address of the wireless Ethernet adapter in each PC.

- Tell the wireless router to provide IP addresses dynamically for all computers on the network. This is also known as Dynamic Host Configuration Protocol (DHCP).

What is Internet Telephony (VoIP Telephony)?

A category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls. For users who have free, or fixed-price Internet access, Internet telephony software provides free telephone calls anywhere in the world.

Internet telephony can be any means of transmitting the human voice (real time or close to real time) over the internet. There are several components. On the client side, a multimedia-equipped PC with special client software will digitize your voice. This can be done with a voice modem or other voice encoding method; second, a direct or dial-up connection to the internet allows your voice to be transmitted in packet form to its destination. Third, a connection with the far side is achieved by IP address search, common servers or beacons to identify the called party (and to "ring" that person's phone). Fourth, a similar arrangement on the far end completes the call and allows both parties to speak.

There are also PSTN/Internet gateways that allow regular telephone callers to make Phone-to-Internet-to-Phone connections. There are PC-to-Phone connections and Phone-to-PC connections. To date, however, Internet telephony does not offer the same quality of telephone service as direct telephone connections.

Chapter 6

Network Administrator / Securities

Client-server Technology

Client-server is a computer model that separates client and server, and usually interlinked using a computer network. Each instance of a client can send data requests to one of the servers online and expect a response. In turn, some of the available servers can accept these requests, process them and return the result to the client. Although the concept be applied to various uses and applications, the architecture is almost the same.

Often clients and servers communicate through a computer network with separate hardware, but the client and server can reside on the same system. The machine is a host server that is running one or more server programs that share their resources with clients.

A client does not share its resources, but requests content from a server or service function. Clients, therefore, initiate communication sessions with the servers that wait for incoming requests.

Features of the Client

- Always start applications servers;
- Waits for responses;
- Get answers;
- Usually connects to a small number of servers at once;
- Normally, interacts directly with end users through any user interface, such as graphical user interface.

Server Features

- Always wait for a request from a client;
- Serves clients' requests, then responds with the requested data to clients;
- A server can communicate with other servers in order to meet a client's request.

What is Server Management

Server management is the process of monitoring and maintaining servers to operate at peak performance. Server management also encompasses the management of hardware, software, security, and backups. The primary goals of an effective server management strategy are to:

- Minimize—and hopefully eliminate—server slowdowns and downtime
- Build secure server environments
- Ensure servers continue to meet the needs of an organization as it evolves

At its base, server management entails system administration duties. They include initial server setup tasks, service monitoring, regular server maintenance and optimisation, and security. Whilst a larger corporation can staff an IT department, pay salaries and manage employees who complete these tasks, it is usually not a viable option for a smaller business. Using a server management company instead is a great way to alleviate the headaches that come with the growth of your business. Your systems will be monitored for health and serviced on a regular basis without having to find and pay for full time employment of an onsite systems administrator.

Benefits of Using a Server Management

- **Monitoring** – Your hardware gets monitored so that small issues are caught and corrected before they become big problems. We implement scheduled preventative maintenance to more effectively conduct advanced performance monitoring, key application maintenance and OS & 3rd party patch management.
- **Optimisation** – Your equipment gets the attention it needs to perform at its best. Management technicians examine your servers and find ways to increase performance to keep your customers delighted with your service whether you're at one location or have several different branches.
- **Security** – Server management teams are responsible for keeping your systems secure. They keep the bad guys out by implementing managed anti-virus software and monitoring. You should be able to trust a good server management team so that your customers can trust you. Advanced Technology also supply a managed backup of your servers at regular intervals so none of your important data is lost in case of an emergency.
- **Cost** – One of the greatest benefits of contracting Advanced Technology for your server management duties is cost. You no longer have to worry about maintaining a large staff. A good server management provider will charge a fair price, and for that you'll get a number of techs available to handle your needs any time, day or night.

RAID (redundant array of independent disks)

RAID is a way of storing the same data in different places on multiple hard...

Originally is was known as *Redundant Array Of Inexpensive Disks.* RAID management is a storage technology that combines multiple disk drives into logical units. RAID is a disk management tool which works with most of the operating systems like Windows and Linux. It is a special kind of method which uses drive signature. Disk Drives are configured as dynamic disks for implementation of RAID management which enables us to enlarging a partition without deleting it or losing its data. RAID management can be considered as an example of storage virtualization and the operating system can access array by the one single drive.

Disk Mirroring

Disk Mirroring is a fault tolerance method which simultaneously writes the same information on various hard disks using same disk controller. This is very good method as if one of them disks got crashed or does not work then the data can be retrieved from the other disk and the work will be continued without any delay. So it is useful when any of the disks got crashed. Disk Mirroring is provided by the most NOS that is Network Operating Systems.

Disk Mirroring is pretty useful in case of disk crashes or non availability of a disk. But when two or both of the disks are fail or crashed then it is not any useful because then there will be no substitute for getting data.

Cryptography

Cryptography is a method of protecting information and communications through the use of codes so that only those.

Definition: Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It 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. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.

Three types of cryptographic techniques used in general.

1. Symmetric-key cryptography

2. Hash functions.

3. Public-key cryptography

Ethical Hacking

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.
- **Protect the privacy of the organization** been hacked.
- **Transparently report** all the identified weaknesses in the computer system to the organization.
- **Inform** hardware and software vendors of the **identified weaknesses**.

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking.

Chapter 7

Wireless networking

A *wireless network* is a network that uses radio signals rather than direct cable connections to exchange information. A computer with a wireless network connection is like a cell phone. Just as you don't have to be connected to a phone line to use a cell phone, you don't have to be connected to a network cable to use a wireless networked computer.

Basic wireless network:

- A wireless network is often referred to as a *WLAN,* for *wireless local area network.* Some people prefer to switch the acronym around to *local area wireless network.* The term *Wi-Fi* is often used to describe wireless networks, although it technically refers to just one form of wireless networks: the 802.11b standard.
- A wireless network has a name, known as a *SSID.* SSID stands for *service set identifier.* Each of the computers that belong to a single wireless network must have the same SSID.
- Wireless networks can transmit over any of several channels. In order for computers to talk to each other, they must be configured to transmit on the same channel.
- The simplest type of wireless network consists of two or more computers with wireless network adapters. This type of network is called an *ad-hoc mode network.*
- A more complex type of network is an *infrastructure mode network.* All this really means is that a group of wireless computers can be connected not only to each other, but also to an existing cabled network via a device called a *wireless access point,* or WAP.

How Wi-Fi Works

Wi-Fi (wireless fidelity) is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet. It allows these devices--and many more--to exchange information with one another, creating a network.

Internet connectivity occurs through a wireless router. When you access Wi-Fi, you are connecting to a wireless router that allows your Wi-Fi-compatible devices to interface with the Internet.

On the technical side, the IEEE 802.11 standard defines the protocols that enable communications with current Wi-Fi-enabled wireless devices, including wireless routers and wireless access points. Wireless access points support different IEEE standards.

A wireless access point (AP) allows wireless devices to connect to the wireless network. An access point takes the bandwidth coming from a router and stretches it so that many devices can go on the network from farther distances away. But a wireless access point does more than simply extend Wi-Fi. It can also give useful data about the devices on the network, provide proactive security, and serve many other practical purposes.

A wireless router is sometimes referred to as a wireless local area network (WLAN) device. A wireless network is also called a Wi-Fi network.

Wi-MAX IEEE 802.16 technology

WiMAX technology is a wireless broadband communications technology based around the IEE 802.16 standard providing high speed data over a wide area.

The letters of WiMAX stand for Worldwide Interoperability for Microwave Access (AXess), and it is a technology for point to multipoint wireless networking.

WiMAX technology is able to meet the needs of a large variety of users from those in developed nations wanting to install a new high speed data network very cheaply without the cost and time required to install a wired network, to those in rural areas needing fast access where wired solutions may not be viable because of the distances and costs involved - effectively providing WiMAX broadband. Additionally it is being used for mobile applications, providing high speed data to users on the move.

WiMAX is

- Acronym for **Worldwide Interoperability for Microwave Access**.
- Based on Wireless MAN technology.
- A wireless technology optimized for the delivery of IP centric services over a wide area.
- A scalable wireless platform for constructing alternative and complementary broadband networks.
- IEEE 802.16 standard defines the protocols that enable communications

WiMAX uses the two technology

- ***OFDM (Orthogonal Frequency Division Multiplex)***
- ***MIMO (Multiple Input Multiple Output)***

What is Li-Fi

Li-Fi stands for Light Fidelity and is a Visible Light Communications (VLC) system which runs wireless communications that travel at very high speeds.

With Li-Fi, your light blub is essentially your router. It uses common household LED light bulbs to enable data transfer, boasting speeds of up to 224 gigabits per second.

Li-Fi and Wi-Fi are quite similar as both transmit data electromagnetically. However, Wi-Fi uses radio waves, while Li-Fi runs on visible light waves.

Differences between Li-Fi & Wi-Fi

COMPARISON	LI-FI	WI-FI
Full form	stand for light fidelity	stands for wireless fidelity
Invented/Coined	Coined by Prof. Harald Haas in 2011	By NCR corporation on 1991
Operation	it transmits data using light by the help of LED bulbs	it transmits data using radio waves using wifi router
Technology	Present IrDA compliant devices	WLAN 802.11/b/g/n/ac/d standard compliant devices
Data Transfer Speed	About 1 Gbps	Ranges from 150Mbps to maximum of 2Gbps
Privacy	light is blocked by the walls hence provide more secure data transfer	walls cannot block radio waves so we need to employ more techniques to achieve secure data transfer
Frequency of operation	10, 000 times frequency spectrum of the radio	2.4Ghz, 4.9Ghz and 5Ghz
Coverage Distance	about 10 meters	about 32 meters(vary based on transmit power and antenna type)
Data density	work with high dense environment	work in less dense environment due to interference related issues
Bare minimum Components used	LED bulb, LED driver and photo detector	Routers, Modems and access points
Applications	Used in airlines, undersea exploration etc	Used for internet browsing with the help of wifi hotspot