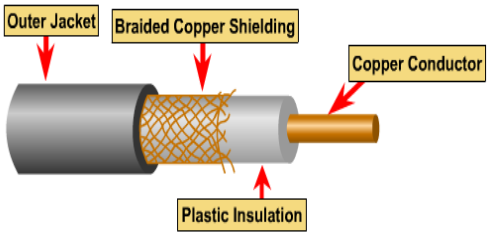
Networking Media

Networking media can be defined simply as the means by which signals, the data, are sent from one computer to another. So it obviously lies in the physical layer of the OSI reference model. There are different types of networking medias, the most common are copper based such as coaxial and twisted-pair cables. Another type uses glass such as fiber-optic cables. The medium can also be the air or the free space such as the case of wireless signals.

➢ Coaxial Cable

Coaxial cable is so named because it contains two conductors; one conductor inside the other. At the center of the cable is the copper core that actually carries the electrical signals. The core can be solid copper or braided strands of copper. Surrounding the core is a layer of insulation, and surrounding that is the second conductor, which is typically made of braided copper mesh. This second conductor functions as the cable's ground. The outer copper or metallic braid in coaxial cable also comprises half the electrical circuit. Finally, the entire assembly is encased in an insulating sheath made of PVC or Teflon.



For LANs, coaxial cable offers several advantages. It can run for longer distances between network nodes than twisted pair cables. Coaxial cable is less expensive than fiber-optic cable, and the technology is well known.

When working with cable, it is important to consider its size. As the thickness or diameter of the cable increases, it becomes more difficult to work with. Coaxial cable comes in a variety of sizes. The most popular which are used in Ethernet networks known as thicknet (also called RG-8) and thinnet (also called RG-58) . These two cables are similar in construction but differ primarily in thickness (0.405 inches for RG-8 versus 0.195 inches for RG-58) and in the types of connectors they use (N connectors for RG-8 and bayonet-Neill-Concelman [BNC] connectors for RG-58).


BNC connector


N-type connector

Special care must be taken to ensure that the outer conductor is properly grounded. Poor or incorrect grounding is one of the biggest problems in the installation of coaxial cable because it results in electrical noise that interferes with signal transmitted on the cable.

➢ Twisted Pair Cable

Twisted-pair is a type of cabling that is used for telephone communications and most modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs. Pairs of copper wires that are encased in color-coded plastic insulation are twisted together. All the twisted-pairs are then protected inside an outer jacket.

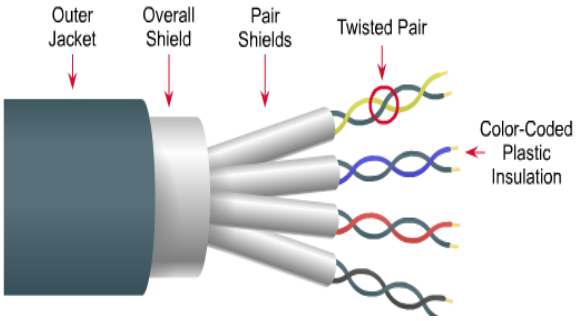
Twisted-pair cable has replaced coaxial cable in the data networking world because it has several distinct advantages. First, because it contains separate wires, the cable is more flexible than the more solidly constructed coaxial cable. This makes it easier to bend, which simplifies installation. The second major advantage is that there are thousands of qualified telephone cable installers who can easily adapt to installing LAN cables as well.

The main disadvantage in twisted pair cables is that the distance between signal boosts (repeaters) is shorter than that for coaxial and fiber optic cables

There are two basic types, Shielded Twisted-Pair (STP) and Unshielded Twisted-Pair (UTP). There are also categories of UTP wiring.

STP

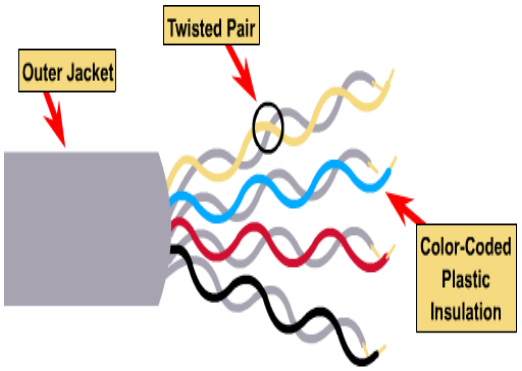
Shielded twisted-pair cable (STP) combines the techniques of shielding, and twisting of wires. Each pair of wires is wrapped in metallic foil. The four pairs of wires are wrapped in an overall metallic braid or foil. STP reduces electrical noise, both within the cable (pair to pair coupling, or cross talk) and from outside the cable, Electromagnetic Interference (EMI), and Radio Frequency Interference (RFI). STP affords greater protection from all types of external interference but more insulation and shielding combine to considerably increase the size, weight, and cost of the cable. The shielding materials also lead to more difficult installation.



The metallic shielding materials in STP need to be grounded at both ends. If improperly grounded, STP become susceptible to major noise problems. Any discontinuities in the entire length of the shielding material will allow the shield to act like an antenna receiving unwanted signals.

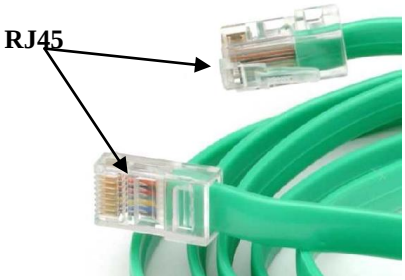
UTP

Unshielded twisted-pair cable (UTP) is a four-pair wire medium composed of pairs of wires. It is used in a variety of networks. Each of the individual copper wires in the UTP cable is covered by insulating material. Each pair of wires are also twisted around each other. This type of cable relies solely on the cancellation effect, produced by the twisted wire pairs, to limit signal degradation caused by EMI and RFI. To further reduce cross talk between the pairs in UTP cable, the number of twists in the wire pairs increased.



Unshielded twisted-pair cable has many advantages. It is easy to install and is less expensive than other types of networking media. This is really due to its small size and weight.

UTP cable is installed using Registered Jack (RJ) connectors called RJ45. These connectors are the same as the RJ11 connectors used on standard telephone cables, except that they have eight electrical contacts instead of four or six.



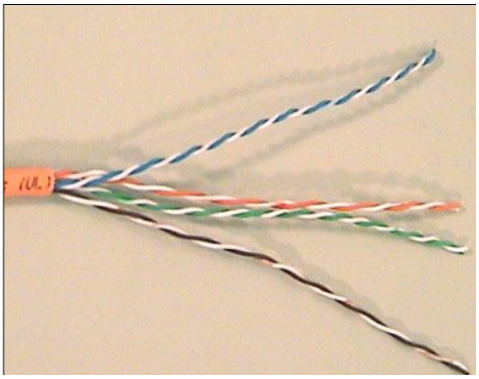
The main disadvantage of using UTP cable is that it is more susceptible to electrical noise and interference than other types of networking media.

Although most Ethernet networks use only two of the four wire pairs in the UTP cable, one for transmitting data and one for receiving it. However, this does not mean that you are free to utilize the other two pairs for another application, such as voice telephone traffic. The presence of signals on the other two wire pairs is almost certain to increase the amount of crosstalk on the cable, which could lead to signal damage and data loss.

UTP Grades

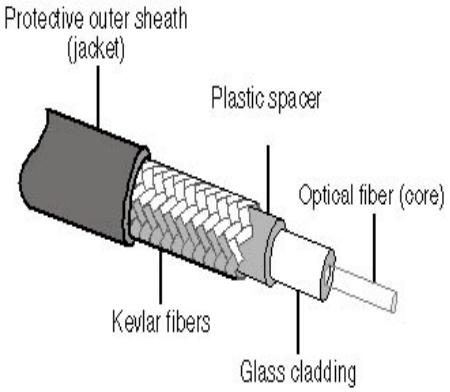
Unshielded twisted pair cable comes in a variety of different grades, called categories by the Electronics Industry Association (EIA) and the Telecommunications Industry Association (TIA), the combination being referred to as EIA/TIA. These categories differs in the number of pairs and number of twists per meter. The most currently used in networking today are cat5, cat5e, and cat6.

CAT 5 Cable



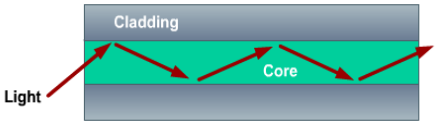
➢ Fiber Optic Cable

Fiber optic cable is a completely different type of network medium than twisted-pair or coaxial cable. Instead of carrying signals over copper conductors in the form of electrical voltages, fiber optic cables transmit pulses of light over a glass or pure plastic filament. A fiber optic cable, consists of a clear glass or a clear plastic core that actually carries the light pulses, surrounded by a reflective layer called the cladding. Surrounding the cladding is a plastic spacer layer, a protective layer of woven Kevlar fibers, and an outer sheath.



The core and the cladding are the light guiding parts of the optical fiber. The core which is usually very pure glass with a high index of refraction. When the core glass is surrounded by a cladding layer of glass or plastic with a low index of refraction, light can be trapped in the fiber core. This process is called total internal reflection, and it allows the optical fiber to act like a light pipe, guiding light for tremendous distances, even around bends.

Total Internal Reflection



Fiber optic cable is completely resistant to the electromagnetic interference that so easily affects copper-based cables. Fiber optic cables are also much less subject to attenuation (the tendency of a signal to weaken as it travels over a cable) than copper cables. On copper cables, signals weaken after 100 to 500 meters (depending on the type of cable). Some fiber optic cables, by contrast, can span distances up to 120 kilometers without excessive signal degradation.

Fiber optic cable is also inherently more secure than copper because it is impossible to tap into a fiber optic link without affecting normal communication over that link.

The connectors for fiber-optic are expensive, as is the labor that is necessary to terminate the ends of the cables. The tools and testing equipment required for installation are different, as are the cabling guidelines. Generally speaking, fiber optic cable is more expensive than twisted-pair or coaxial cable in every way, although prices have come down in recent years.

There are two primary types of fiber optic cable:

1-Multimode

2-Singlemode

1-Multimode

Where multiple beams can move through the core in different paths. Most multimode fiber typically has a core diameter of 62.5 or 50 microns, and the thickness of the core and cladding together is 125 microns. This is generally referred to as 62.5/125 or 50/125 multimode fiber. Multimode fiber, uses a light-emitting diode (LED) as a light source which can give multiple wavelengths.

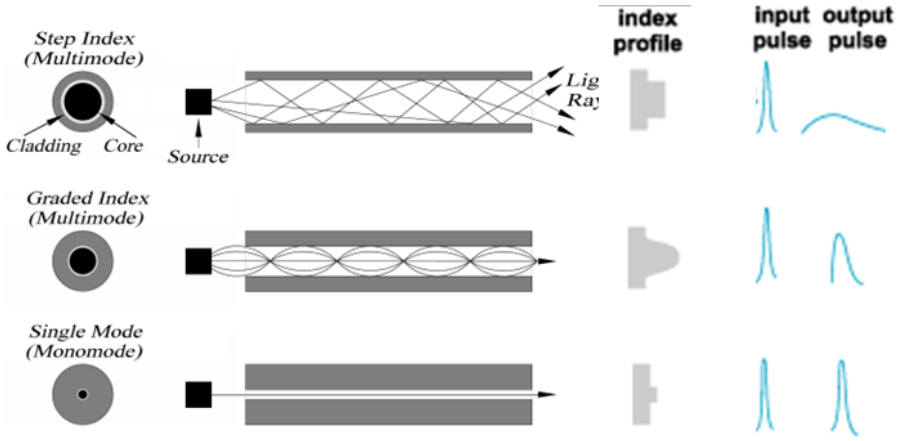
According to the refraction index of the core multimode fibers are fabricated into two ways:-

-Step Index: where the optical density of the core remains constant from the center to the edges of the core. Here a beam of light moves in straight line down the core until reaching the interface with the cladding of the lower optical density. When the incidence angle greater than a specific critical value the beam is totally reflected due to lower refraction index. This suddenness change in the value of refraction indexes led to the name step index.

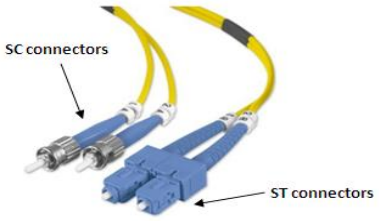
- Graded Index: is one with varying densities. Density is highest at the center of the core and decreases to its lower value at the edges of the core. The graded decrease in the refraction index led to the name graded index.

2- Singlemode

Only one beam (or single wavelength) can move through singlemode fiber. Most singlemode fibers are rated as 8.3/125 and 9/125. Singlemode fiber uses a single-wavelength laser as a light source, and as a result, it can carry signals for extremely long distances. For this reason, singlemode fiber is more commonly found in outdoor installations that span long distances, such as telephone and cable television networks. This type of cable is less suited to LAN installations because it is much more expensive than multimode cable and it has a higher bend radius, meaning that it cannot be bent around corners as tightly. Single mode are step-index; they are fabricated so that the beam is limited inside the core to a small range of angles (close to 90°) which makes the propagation of beam almost horizontal.



Fiber optic cables usually use one of two connectors, the Straight Tip (ST) connector or the Subscriber Connector (SC).



Wireless

Sometimes the cost of running cables is too high or computers need to be movable without being tethered to cables. When this is the case, wireless is an alternative method of connecting a LAN. Wireless signals are electromagnetic waves, which travel through the vacuum of outer space and/or through media such as air. No physical medium is necessary for wireless signals. Wireless siganls are highly subjected to interference and may suffer a poor security. Wireless networks may operate in Radio Frequency (RF), Microwaves or Infrared (IR) frequency regions.

Signals:-

The following paragraphs discuss some of the concepts related to signals, these includes noise, losses, timing, encoding and modulation. All these terms lies in the Physical layer of OSI reference model.

1-Noise

Noise is unwanted random signal added to original signal. No electrical signal is without noise, however, it is important to keep the Signal-to-Noise (S/N) ratio as high as possible. The S/N ratio is an engineering calculation that gives a measure of how easy it will be to decipher the desired, intended signal from the unwanted, but unavoidable, noise. Too much noise can corrupt a bit, turning a binary 1 into a binary 0 (zero), or a 0 (zero) into a 1, thereby destroying the message. Generally there are five sources of noise. Here we briefly offer to kinds of noise that especially affect copper mediums.

A-Cross Talk Noise

When electrical noise on the cable originates from signals on other wires in the cable, this is known as cross talk. When two wires are near each other and untwisted, energy from one wire can wind up in an adjacent wire and vice versa. Twisting is a good solution to reduce the effect of cross talk noise.

B-Thermal Noise

Thermal noise, is due to the random motion of electrons within the media, it is unavoidable but usually relatively small compared to the signals. There is nothing that can be done about thermal noise, other than to give the signals large enough amplitude so that it does not matter.

C-AC Power Noise

AC Power and reference ground noises are crucial problems in networking. Electricity is carried to appliances and machines by wires concealed in walls, floors, and ceilings. Consequently, inside the buildings AC power line noise is all around us. Good grounding is a good solution for the AC power noise.

D-Reference Ground Noise

Ideally, the signal reference ground should be completely isolated from the electrical ground. Isolation would keep AC power leakage and voltage spikes off the signal reference ground. Long ground wires also should be avoided because these wires can act as an antenna for electrical noise. Short and separate signal reference ground cables can decrease the effects of reference ground noise.

E- EMI/RFI

External sources of electrical impulses that can attack the quality of electrical signals on the media referred to as electromagnetic interference (EMI) like lightning, electrical motors , and radio frequency interference (RFI) like radio systems. Shielding and good grounding are good solutions to reduce the effect of EMI/RFI noise.

2- Losses:

Mediums and connectors are the source of different types of losses. Here we divide losses according to the type of transmission medium into:

A- Copper losses:-

The main reasons for losses in copper mediums are:-

1- Conductor losses: This is due to the resistance of the copper medium.
2- Radiation losses: Portion of signal energy is lost as electromagnetic radiation due to the flow of current in the copper conductor.
3- Coupling losses: Connectors are discontinuities which are locations on which dissimilar materials meet. Discontinuities tend to heat up, radiate energy and dissipate power.

B-Fiber optic losses:

1- Absorption losses: Impurities in fiber optic tend to absorb light in the fiber and convert it to heat.
2- Scattering losses: microscopic irregularities and impurities along the fiber causes the light to be diffracted and spread and out in different directions.
3- Radiation losses: portion of the light can be radiated out of the core due to bends and kinks in the fiber.
4- Coupling losses: these losses occurs at the junctions in fiber optics. Junctions are either source-to-fiber, fiber-to-fiber, or fiber-to-photodetector.

3-Timing

Dispersion, jitter, and latency are actually three different things that can happen to a bit. They are grouped together because each affects the timing of a bit. Since millions and billions of bits travel on a medium in one second, timing is extremely important.

A-Dispersion

Dispersion occurs when the signal broadens in time. It is caused by the type of media involved. If serious enough, one bit can start to interfere with the next bit and confuse it with the bits before and after it.

B- Jitter

Packets may arrive a little earlier and later than expected. This is known as jitter. Jitter is a problem especially in real time audio or video applications.

C-Latency

Latency, also known as delay is the time it takes for the entire packet to completely arrive the destination. Latency is made of four components.

1- Propagation time: signals in different mediums have different propagations speeds. So the propagation time differs according to:

Propagation time = Distance / Propagation Speed

2- Transfer time: The transfer time depends on the throughput. Where

Transfer time = Packet Size / Throughput

3- Queuing time: the time needed by each intermediate or device to hold the message before it pass it or process it.
4- Processing time: the time needed to process the packet.

4- Encoding:-

Encoding means converting 1s and 0s (data) into something real and physical, such as electrical signals and light pulses. On the other hand encoding methods goal to get one or more of the followings:-

1- Self synchronization techniques.
2- Built in error Detection.
3- Immunity to noise.
4- Better channel usage by maximizing bit rates.
5- Reducing or eliminating low freq components.

Generally coding methods are divided into:-

- Line coding.
- Block coding.

- **Line Coding**

Converting data bits sequentially into signals. There are different types of line coding but the most important in computer networks are:-

A- Non Return to Zero Level (NRZL):-

NRZL encoding is polar; NRZL uses positive voltage to represent a binary 1 and negative voltage to represent a binary 0. Non return to zero means that the voltage never returns to a value of zero in the bit interval. While and the value of the voltage during a bit time is level.

B- Non Return to Zero Inverted (NRZI):-

In NRZI is NRZ polar encoding scheme. It is encoding is similar to NRZL in that the voltage never returns to a value of zero through the bit time but the main difference here is that a transition at the beginning of the bit time is used to represent a 1 while a 0 is represented by no transition or no change. NRZI offers better power balancing, and immunity to noise than NRZL.

C- Manchester Encoding:-

Manchester encoding is RZ (Return to Zero) biphase encoding scheme. RZ means that that voltage returns to zero in the middle of the bit interval. And the term biphase referred to the two phases used to represent a 1 or 0 bit. Manchester encoding results in 1 being encoded as a low-to-high transition and 0 being encoded as a high-to-low transition. Because both 0s (zeros) and 1s result in a transition to the signal, the clock can be effectively recovered at the receiver. Manchester encoding is more complex than NRZL and NRZI, but is more immune to noise , it is better at remaining synchronized and it results in better elimination of low freq components.

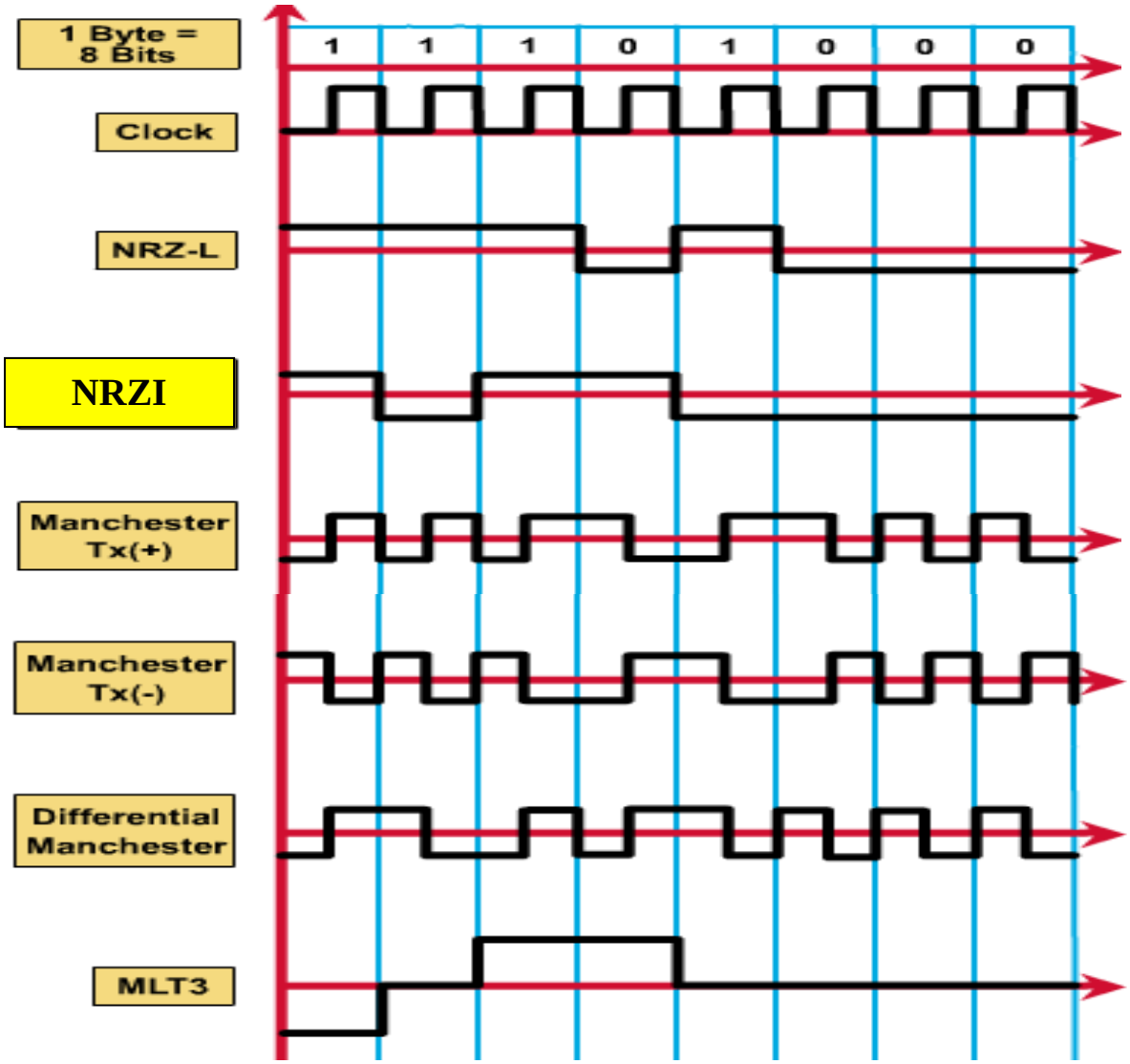
Note:- The type of Manchester encoding described above is known as Tx(+) Manchester Encoding. Another popular type is Tx(-) Manchester Encoding which is similar to Tx(+) but in an opposite procedure.

D- Differential Manchester Encoding:-

Differential Manchester is similar to Manchester in that it is a RZ biphase encoding scheme. In Differential Manchester each bit 1 or 0 has a transition at the middle of the bit time but the main difference here is that a 0 is represented by a transition at the beginning of the bit interval while no change (or transition) is used to represent a 1.

E- Multi-Level Threshold 3 (MLT3):-

In this method three levels are used to represent the signal (-1 volt, 0 volt, +1 volt). These levels changes in cycle (-1,0,1,0,-1....). A 1 is represented by a transition to the next level in the cycle while no transition occurs in the case of zero.



- **Block coding**

In block coding a block of (m bits) is converted into a block of (n bits) where n usually greater than m. Block coding results in better error detection due to redundant codes. Specific codes can be used to start and end communication which helps in better synchronization than line coding. Block coding normally involves three stages :-

1- Division (dividing the stream of data into m-bit blocks)
2- Substitution (substitute the m-bit into appropriate n-bit block)
3- Combination (n- bit blocks are combined together to form a stream)

4 Binary/5 Binary (4B/5B) :-

In this method every four bits of data are encoded in a five-bit code. The selection of the five-bit code is done so that each code does not contain more than one leading zero and ends with no more than two trailing zeros. Therefore when these 5-bit codes are sent in sequence, no more than three consecutive zeros are encountered. 4B/5B block encoder always followed by line encoder (NRZI or MLT3) to maximize bit rate and eliminate low freq components. The following table illustrates the 4B/5B encoding.

Data code		Definition
4-bits	5-bits	
0000	11110	Dada0
0001	01001	Data1
0010	10100	Data2
0011	10101	Data3
0100	01010	Data4
0101	01011	Data5
0110	01110	Data6
0111	01111	Data7
1000	10010	Data8
1001	10011	Data9
1010	10110	DataA
1011	10111	DataB
1100	11010	DataC
1101	11011	DataD
1110	11100	DataE
1111	11101	DataF
	00000	Line is dead
	11111	Line is idle
	00100	Halt, transmission error
	11000	Delimiter for part 1 start of data stream
	10001	Delimiter for part 2 start of data stream
	01101	Delimiter for part 1 end of data stream
	00111	Delimiter for part 1 end of data stream

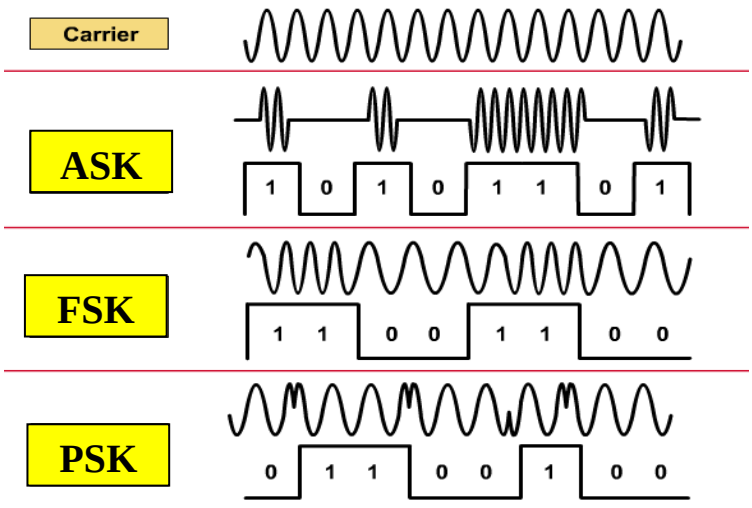
5- Modulation:-

Closely related to encoding is modulation, which specifically means taking a wave and changing, or modulating it so that it carries information. The three main types of modulation are:-

- AM (amplitude modulation) - the amplitude, or height, of a carrier sine wave is varied to carry the message
- FM (frequency modulation) - the frequency of the carrier wave is varied to carry the message
- PM (phase modulation) - the phase, or beginning and ending points of a given cycle, of the wave is varied to carry the message

And digitally when we have a wave modulating 1s and 0s, we are actually talking about the digital counter parts of the previous mentioned methods, these are

- Amplitude Shift Keying (ASK) :- here the amplitude of the carrier varies between two levels, one for 1's and the other for zeros.
- Frequency Shift Keying (FSK) :- here we have two carriers frequencies, one for 1's and the other for zeros
- Phase Shift keying (PSK):- the phase of the carrier changes between two phases according to the message (1's and 0's).



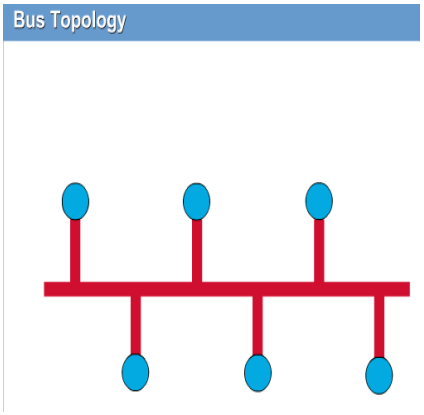
Networking Topologies

The topology of a network is the pattern used to connect the computers and other devices with the cable or other network medium. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions. Thus network topology can be considered as one of the major components of the physical layer. The most popular networking topologies include

- Bus
- Ring
- Star
- Extended star
- Mesh
- Wireless

➢ Bus Topology

A network that uses the bus topology is one in which the computers are connected in a single line. Early Ethernet systems known as thicknet and thinnet used the bus topology with coaxial cable, a type of network that is rarely seen today.



When any one of the computers on the network transmits data, the signals travel down the cable in both directions, reaching all of the other systems. A bus network always has two open ends, which must be terminated. Termination is the process of installing a resistor pack at each end of the bus to negate the signals that arrive there. Without terminators, the signals reaching the end of the bus would reflect back in the other direction and interfere with the newer signals being transmitted.

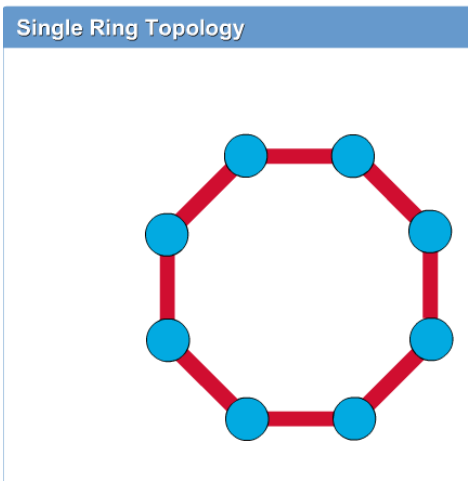
The main problem with the bus topology is that a single faulty connector, faulty terminator, or break in the cable affects the functionality of the entire network. Signals that cannot pass beyond a certain point on the cable cannot reach all of the computers beyond that point. In addition, when a component failure splits the network into two segments, each half of the cable is also unterminated.

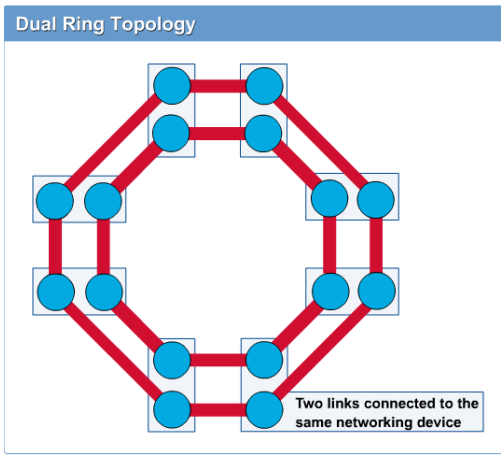
➢ Ring Topology

Ring topology network is like a bus topology network but the two ends are connected instead of being terminated, thus forming an endless loop. This enables a signal originating on one computer to travel around the ring to all of the other

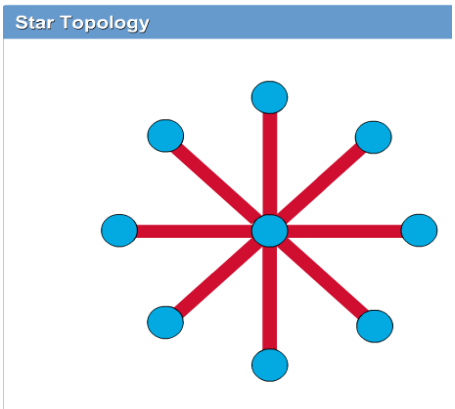
computers and eventually back to its point of origin. There two types of ring topologies:

1. Single ring – All the devices on the network share a single cable, and the data travels in one direction only. An example is the Token Ring network.
2. Dual ring – A dual ring topology is the same as single ring topology, except that there is a second, redundant ring that connects the same devices. This topology allows data to be sent in both directions although only one ring is used at a time. This topology creates redundancy, or fault tolerance, meaning that in the event of a failure of one ring, data will be able to be transmitted on the other ring. An example of a dual ring is Fiber Distributed Data Interface (FDDI).





➢ Star Topology

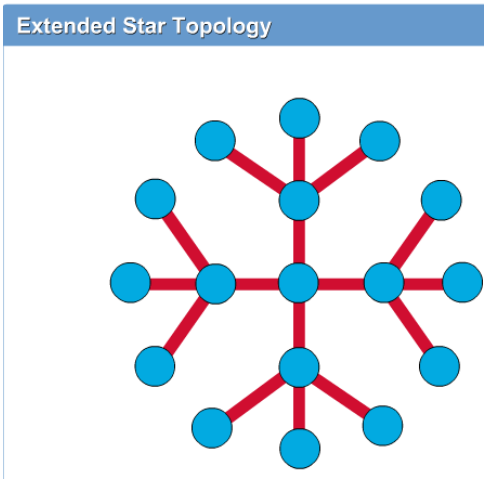


The star topology is the most commonly used architecture in LANs. it is the most widely implemented topology especially in Ethernet LANs. Star topology is made up of a central connection point that is a device such as a hub, switch, or router. All of the cabling segments actually meet at this central connection point. Each node in the network is connected to the central device with its own cable.

The main advantage of the star topology is that each computer has its own dedicated connection to the hub, providing the network with a measure of fault tolerance. If a single cable or connector should fail, only the computer connected to the hub by that cable is affected. The main drawback in star topology networks that if the central device should fail, the entire network goes down. Another disadvantage of the star topology is that an additional piece of hardware (the central device such

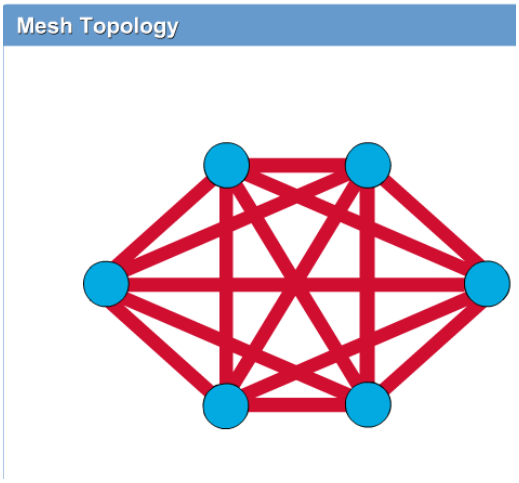
as the hub, switch or router) is required to implement it which results in additional cost. A star topology also costs more to implement than the bus topology. This is because more cables are used in a star topology.

➢ Extended Star Topology



An extended star topology has a core star topology, with each of the end nodes of the core topology acting as the center of its own star topology. The main purpose of using this topology is to expand the network especially when it is wanted to exceed the number of devices that are permitted to be connected to the central device in star topology network. Another advantage with extended star topology is to reduce the traffic in the central device.

➢ Mesh Topology



On a mesh topology networks, each computer has a dedicated connection to every other computer, A mesh LAN provides excellent fault tolerance, however, as there is no single point of failure that can affect more than one computer.

Mesh topology is usually used in WANs to interconnect LANs. A mesh internetwork has multiple paths between two destinations, made possible by the use of redundant routes. However implementing the mesh topology is expensive and difficult especially when the number of interconnected nodes increased.

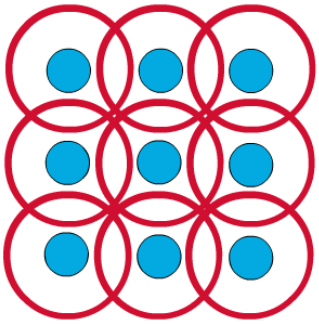
➢ Wireless Topologies

The term topology usually refers to the arrangement of cables that forms a network, but it doesn't have to. Although wireless networks use what are called unbounded media, the computers still have specific patterns they use to communicate with each other. Wireless LANs have two basic topologies, the ad-hoc topology and the infrastructure topology.

In the ad-hoc topology, a group of computers are all equipped with wireless network interface adapters and are able to communicate freely with each other. This topology is useful for a home, office or small business networks.

An infrastructure network consists of wireless-equipped computers that communicate with a network using wireless transceivers usually connected to the LAN by standard cables. These transceivers are called network Access Points. In this arrangement, the wireless computers do not communicate directly with each other. Instead, they communicate only with the cabled network via the network access points. This topology is better suited to larger networks. The infrastructure topology some times referred to as cellular topology because it divides the network coverage area into small cells.

Cellular Topology



The main advantages of wireless topologies comes from the fact that they overcome all the limitations regarded to cables installation, they also provide the best way to connect mobile devices. The main disadvantage in wireless communication is that it is very susceptible to interference.

Physical and logical topology

It is important when studying networking topologies to remember that that they are mainly classified into:-

1. Physical topology – Refers to the layout of the devices and media.
2. Logical topology – Refers to the paths that signals travel from one node on the network to another. That is, the way in which data accesses media and transmits packets across it.

The physical and logical topologies of a network can be the same. For instance, in a network physically shaped as a linear bus, the data travels in a straight line from one computer to the next. Therefore, it has both a bus physical topology and a bus logical topology.

A network can also have physical and logical topologies that are quite different. For example, a physical topology in the shape of a star can in fact have a logical ring topology. Remember that in a ring, the data travels from one computer to the next. That is because inside the hub, the wiring connections are such that the signal actually travels around in a circle from one port to the next, creating a logical ring. The way data travels in a network cannot always be predicted by simply observing its physical layout.

Layer1 (Physical Layer) Devices

Here we present to some examples on layer1 devices, we will focus on devices deals with the Ethernet which is the most popular data link layer protocol. The following items will discuss repeaters and hubs which are the most common layer1 devices.

1-Repeater

Repeaters are internetworking devices that exist at the physical layer (Layer 1) of the OSI model. Repeaters usually two port devices (one input port and one output port).They can increase the distance over which the network can extend. Thus the number of nodes that can be connected to a network can also be increased. Repeaters reshape, regenerate, and retime signals before sending them on along the network.

To understand the purpose of repeater, consider when the signal first leaves a transmitting station, it is clean and easily recognizable. After a while, however, it begins to weaken, and deteriorate. The longer the cable (media) length, the weaker and more deteriorated the signal becomes. To keep the signal from becoming unrecognizable to the receiver, the repeater takes in the weakened signal, cleans it up, amplifies it, and sends it on its way.

Repeaters cannot filter network traffic. This means that data (bits) that arrive at one port of a repeater are sent out on the other port. The data gets passed along to all other LAN segment of a network regardless of the destination address.

2-Hubs

A hub is a physical layer device used to connect all of the computers on a star or ring network. Ethernet hubs are the most common because Ethernet is the most popular data-link layer protocol.

Hub Types

Hubs can be classified according to signal amplification or repetition into two classes

1. Passive hubs: they don't do any amplification, but just distributing the signal coming on one port on to the other ports. So, passive hubs cannot extend the range of the network.
2. Active Hubs: in addition to distribute the incoming signal on one port of the hub on the other ports, active hub takes in the weakened signal, cleans it up, and amplifies it before sending it out. For this reason and due the fact that hubs have multiple ports, active hubs are also called multiport repeaters. Active hubs can extend the range of the network and they are more expensive than passive hubs.

Hubs can also classified according to the way they deal the data into two types

1. Dumb Hubs: The hubs used on most Ethernet networks are purely physical-layer devices. This means that the hub works with the signals native to the network medium, such as electrical voltages, but does not interpret the signals, read the data inside packets, or even recognize that there is data there. This type of hub is relatively inexpensive.
2. Intelligent Hubs: they are Ethernet hubs with more intelligence that can process the data they receive in more elaborate ways. Some intelligent hubs include management features that enable them to monitor the operation of each of the hub's ports. In most cases, an intelligent hub uses the Simple Network Management Protocol (SNMP) to transmit periodic reports to a centralized network management console.