NOS LAB RECORD

Submitted By -

KUMAR SHUBHAM

39

S7,CS-A

SOE,CUSAT

Cycle-1

Exp-1a

DATE: 09/07/15

**STUDY OF COMPUTER NETWORKS**

**AIM**: To study the basics of a computer networks

**THEORY**:

**COMPUTER NETWORK**:

Computer network is an interconnection of a number of autonomous computing devices governed by a set of common rules. A Computer network consists of two or more autonomous computers that are linked (connected) together in order to:

• Share resources (files, printers, modems, fax machines).

• Share Application software like MS Office.

• Allow Electronic communication.

• Increase productivity (makes it easier to share data amongst users).

Some of the basic goals that a Computer network should satisfy are:

• Cost reduction by sharing hardware and software resources.

• Provide high reliability by having multiple sources of supply.

• Provide an efficient means of transport for large volumes of data among various locations (High throughput).

* Provide inter-process communication among users and processors.

• Reduction in delay driving data transport.

• Increase productivity by making it easier to share data amongst users.

• Standards and protocols should be supported to allow many types of equipment from different vendors to share the network (Interoperatability).

• Provide centralized/distributed management and allocation of network resources like host processors, transmission facilities etc.



Figure 1.1 : A Computer Network

**NETWORK TOPOLOGY**:

Topology refers to the shape of a network, or the network’s layout. How different nodes in a network are connected to each other and how they communicate with each other is determined by the network's topology. Topologies are either physical or logical.

Some of the most common network topologies are:

• Bus topology

• Star topology

• Ring topology

• Mesh topology.

The parameters that are to be considered while selecting a physical topology are:

• Ease of installation.

• Ease of reconfiguration.

• Ease of troubleshooting.

**BUS TOPOLOGY**:

In Bus topology, all devices are connected to a central cable, called the bus or backbone. The bus topology connects workstations using a single cable. Each workstation is connected to the next workstation in a point-to-point fashion. All workstations connect to the same cable

Advantages of Bus Topology

• Installation is easy and cheap when compared to other topologies.

• Connections are simple and this topology is easy to use.

• Less cabling is required.

Disadvantages of Bus Topology

• Used only in comparatively small networks.

• As all computers share the same bus, the performance of the network deteriorates when we increase the number of computers beyond a certain limit.

• Fault identification is difficult.

• A single fault in the cable stops all transmission.

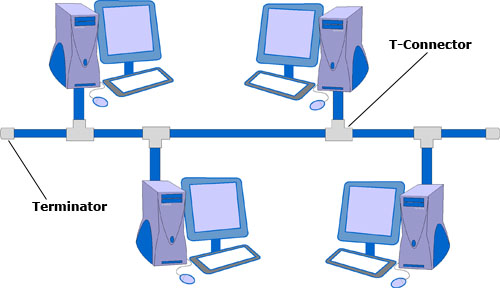


Figure 1.2 : Bus Topology

**STAR TOPOLOGY**:

Star topology uses a central hub through which, all components are connected. In a Star topology, the central hub is the host computer, and at the end of each connection is a terminal

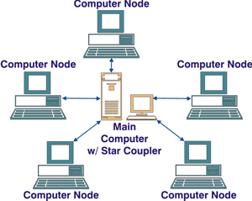


Figure 1.3 : Star topology

Advantages of Star Topology

• Installation and configuration of network is easy.

• Less expensive when compared to mesh topology.

• Faults in the network can be easily traced.

• Expansion and modification of star network is easy.

• Single computer failure does not affect the network.

• Supports multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc.

Disadvantages of Star Topology

• Failure in the central hub brings the entire network to a halt.

• More cabling is required in comparison to tree or bus topology because each node is connected to the central hub.

**RING TOPOLOGY**:

In Ring Topology all devices are connected to one another in the shape of a closed loop, so that each device is connected directly to two other devices, one on either side of it, i.e., the ring topology connects workstations in a closed loop. Each terminal is connected to two other terminals (the next and the previous), with the last terminal being connected to the first. Data is transmitted around the ring in one direction only; each station passing on the data to the next station till it reaches its destination.

Advantages of Ring Topology

• Easy to install and modify the network.

• Fault isolation is simplified.

• Unlike Bus topology, there is no signal loss in Ring topology because the tokens are data packets that are re-generated at each node.

Disadvantages of Ring Topology

• Adding or removing computers disrupts the entire network.

• A break in the ring can stop the transmission in the entire network.

• Finding fault is difficult.

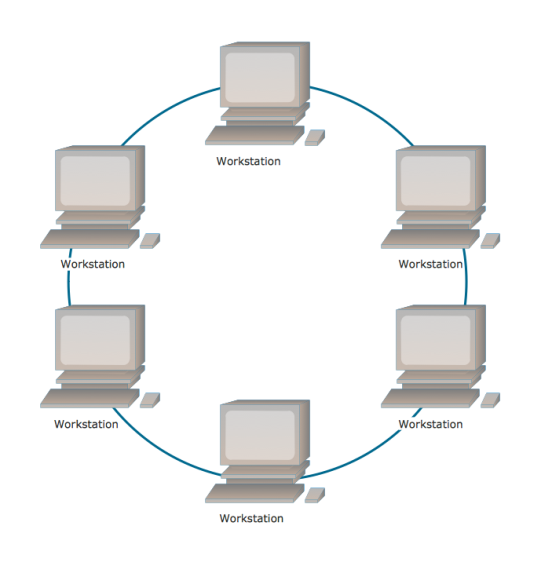


Figure 1.4 : Ring topology

**MESH TOPOLOGY**:

Devices are connected with many redundant interconnections between network nodes. In a well-connected topology, every node has a connection to every other node in the network. The cable requirements are high, but there are redundant paths built in. Failure in one of the computers does not cause the network to break down, as they have alternative paths to other computers. Mesh topologies are used in critical connection of host computers (typically telephone exchanges). Alternate paths allow each computer to balance the load to other computer systems in the network by using more than one of the connection paths available.

Advantages of Mesh Topology

• Use of dedicated links eliminates traffic problems.

• Failure in one of the computers does not affect the entire network.

• Point-to-point link makes fault isolation easy.

• It is robust.

• Privacy between computers is maintained as messages travel along dedicated path.

Disadvantages of Mesh Topology

• The amount of cabling required is high.

• A large number of I/O (input/output) ports are required.

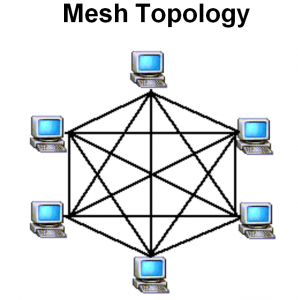


Figure 1.5: mesh topology

**NETWORK ARCHITECTURE**:

Depending on the architecture used Networks can be classified as Client/Server or Peer-to-Peer Networks.

**CLIENT/SERVER ARCHITECTURE**:

Client/Server Architecture is one in which the client (personal computer or workstation) is the requesting machine and the server is the supplying machine, both of which are connected via a local area network (LAN) or wide area network (WAN). Since the early 1990s, client/server has been the buzzword for building applications on LANs in contrast to centralized minis and mainframes with dedicated terminals. A client/server network is called Centralized or Server based network. The client contains the user interface and may perform some or all of the application processing. Servers can be high-speed microcomputers, minicomputers or even mainframes. A database server maintains the databases and processes requests from the client to extract data from or update the database. An application server provides additional business processing for the clients.

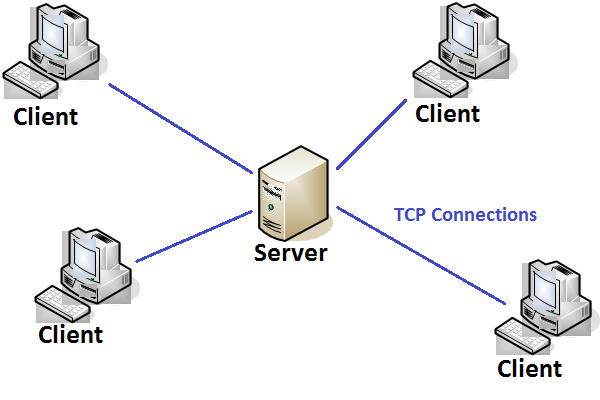


Figure 1.6 : Client-Server architecture

Servers - Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are many different kinds of servers, and one server can provide several functions. For example, there are file servers, print servers, mail servers, communication servers, database servers, print servers, fax servers and web servers, to name a few.

Clients - Clients are computers that access and use the network and shared network resources. Client computers are basically the customers(users) of the network, as they request and receive services from the servers.

Transmission Media - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called channels, links or lines.

Shared data - Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.

Shared printers and other peripherals - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

Local Operating System - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, Unix, Linux, Windows 2000, Windows 98, Windows XP etc.

Network Operating System - The network operating system is a program that runs on computers and servers, and allows the computers to communicate over the network.

Hub - Hub is a device that splits a network connection into multiple computers. It is like a distribution center. When a computer request information from a network or a specific computer, it sends the request to the hub through a cable. The hub will receive the request and transmit it to the entire network. Each computer in the network should then figure out whether the broadcast data is for them or not.

Switch - Switch is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses physical device addresses in each incoming messages so that it can deliver the message to the right destination or port.

Like a hub, switch doesn't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words, switch connects the source and destination directly which increases the speed of the network. Both switch and hub have common features: Multiple RJ-45 ports, power supply and connection lights

|  |  |  |  |
| --- | --- | --- | --- |
| NETWORK | SIZE | TRANSMISSION  MEDIA | MAXIMUM  DISTANCE |
| Local Area Network | Confined to building or campus | Cable used | Covers up to 10 km |
| Metropolitan Area Network | Network confined to city or town | Different hardware & transmission media are used | Covers the area of a city or town. |
| Wide Area Network | Larger than MAN | Telephone lines, radio waves, leased lines or satellites | Covers a number of cities or countries |

Table 1: Comparison between different types of networks.

**PEER TO PEER ARCHITECTURE**:

A type of network in which each workstation has equal capabilities and responsibilities is called peer-to-peer network. . Here each workstation acts as both a client and a server. There is no central repository for information and there is no central server to maintain. Data and resources are distributed throughout the network, and each user is responsible for sharing data and resources connected to their system. This differs from client/server architectures, in which some computers are dedicated to serving the others. Peer-to-peer networks are generally simpler and less expensive, but they usually do not offer the same performance under heavy loads. A peer-to-peer network is also known as a Distributed network.

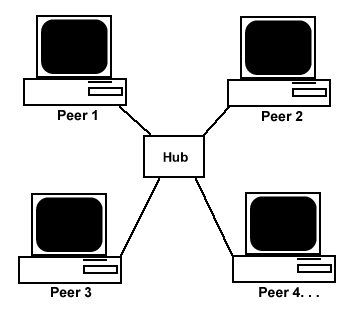


Figure 1.7 : peer to peer architecture

**TYPES OF COMPUTER NETWORK**:

Computer Networks are mostly classified on the basis of the geographical area that the network covers, the topology used, the transmission media used and the computing model used.

Based on the geographical area covered the networks may be LAN, MAN, WAN.

**METROPOLITAN AREA NETWORK (MAN)**:

Metropolitan Area Network is a Computer network designed for a town or city. . In terms of geographic area MAN’s are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MAN’s are usually characterized by very high-speed connections using fiber optical cable or other digital media. It is slower than a LAN but faster than a WAN.

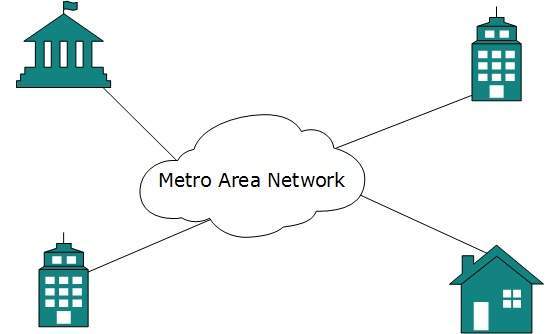


Figure 1.8 : MAN

**WIDE AREA NETWORK (WAN)**:

Wide Area Network is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs). They can connect networks across cities, states or even countries. Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.

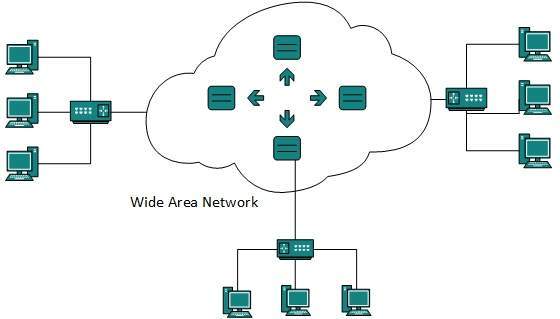


Figure 1.9 : WAN

**LOCAL AREA NETWORK (LAN)**:

The network that spans a relatively small area that is, in the single building or campus is known as LAN. Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it is also able to access data and devices anywhere on the LAN. This means that many users can share data as well as expensive devices, such as laser printers, fax machines etc. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. There are many different types of LANs, Ethernets being the most common for PCs.

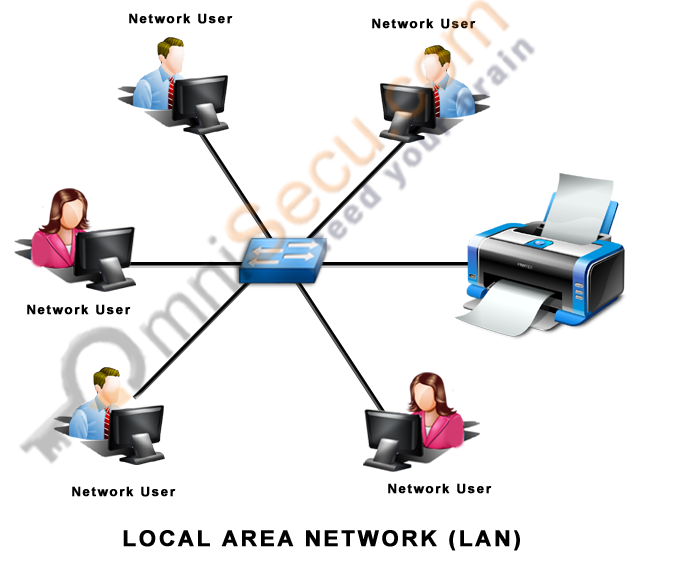


Figure 1.10 : LAN

Types of Connections

**Point-to-point**

A point-to-point link is a dedicated link that connects exactly two communication facilities (e.g., two nodes of a network, an intercom station at an entryway with a single internal intercom station, a radio path between two points, etc.). Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa. If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

**Multipoint**

A multipoint cable is the one in which two or more devices share a single link. Also known as a multidrop link, a multipoint link is a link that connects two or more nodes. Also known as general topology networks, these include ATM and Frame Relay links, as well as X.25 networks when used as links for a network layer protocol like IP.

Unlike broadcast links, there is no mechanism to efficiently send a single message to all other nodes without copying and retransmitting the message.

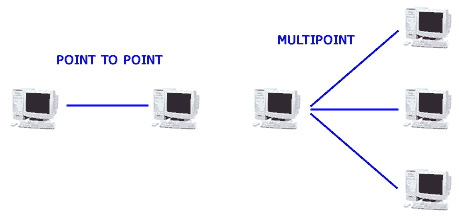


Figure 1.11 : Point-to-point & Multipoint

**Supernetting**

Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. The original Internet Protocol (IP) defines IP addresses in four major classes of address structure, Classes A through D. Each class allocates one portion of the 32-bit Internet address format to a network address and the remaining portion to the specific host machines within the network. Using supernetting, the network address 192.168.2.0/24 and an adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses. Supernetting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.

Supernetting was created as a way to solve the problem of routing tables growing beyond the ability of current software and people to manage and to provide a solution to the exhaustion of Class B network address space. Supernetting allows one routing table entry to represent an aggregation of networks much like one area code represents an aggregation of telephone numbers in an area.

The Border Gateway Protocol (BGP), the prevailing exterior (interdomain) gateway protocol and the Open Shortest Path First (OSPF) router protocol both support supernetting.

**Classful Addressing Scheme**

**Class A Address**  
The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e. Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses. The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27-2) and 16777214 hosts (224-2).  
  
Class A IP address format is  
thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

**Class B Address**  
An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (214) Network addresses and 65534 (216-2) Host addresses.

Class B IP address format  
is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

**Class C Address**  
The first octet of Class C IP address has its first 3 bits set to 110, that is:  
Class C IP addresses range from 192.0.0.x to 192.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives 2097152 (221) Network addresses and 254 (28-2) Host addresses.

Class C IP address format  
is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

**Class D Address**  
Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of: Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.  
  
**Class E Address**  
This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

**RESULT**:

The basic concepts of computer network were studied and understood.

CYCLE-1

EXP-1b

DATE: 09/07/15

**FAMILIARIZE COMPUTER NETWORK COMPONENTS**

**AIM**: To familiarize with computer network components

1. Cables
2. Connectors
3. Switches/hubs
4. Router
5. Network cards and Other Network parts

**THEORY**

**CABLES**:

**COAXIAL CABLE**:

Coaxial cable is braided-grounded strands of wire that can provide some shielding and noise immunity; however, the installation and the termination of the cable itself can be costly. Coaxial cabling, which uses connectors called BNC (Bayonet Nut Connector) is known as, in forms of Ethernet, thick net and thin net, in the older LAN technology, ARC net, and cable TV. Coaxial cable conducts electrical signal using an inner conductor (usually a solid copper, stranded copper or copper plated steel wire) surrounded by an insulating layer and all enclosed by a shield, typically one to four layers of woven metallic braid and metallic tape. The cable is protected by an outer insulating jacket. Normally, the shield is kept at ground potential and a voltage is applied to the center conductor to carry electrical signals. The advantage of coaxial design is that electric and magnetic fields are confined to the dielectric with little leakage outside the shield. Conversely, electric and magnetic fields outside the cable are largely kept from causing interference to signals inside the cable. Larger diameter cables and cables with multiple shields have less leakage. This property makes coaxial cable a good choice for carrying weak signals that cannot tolerate interference from the environment or for stronger electrical signals that must not be allowed to radiate or couple into adjacent structures or circuits.

Common applications of coaxial cable include video and CATV distribution, RF and microwave transmission, and computer and instrumentation data connections.

The characteristic impedance of the cable (Z_0) is determined by the dielectric constant of the inner insulator and the radii of the inner and outer conductors. Controlled cable characteristic impedance is important because the source and load impedance should be matched to ensure maximum power transfer and minimum standing wave ratio. Other important properties of coaxial cable include attenuation as a function of frequency, voltage handling capability, and shield quality.

Coaxial cable is used as a transmission line for radio frequency signals. Its applications include feed lines connecting radio transmitters and receivers with their antennas, computer network (Internet) connections, digital audio (S/PDIF), and distributing cable television signals. One advantage of coaxial over other types of radio transmission line is that in an ideal coaxial cable the electromagnetic field carrying the signal exists only in the space between the inner and outer conductors. This allows coaxial cable runs to be installed next to metal objects such as gutters without the power losses that occur in other types of transmission lines. Coaxial cable also provides protection of the signal from external electromagnetic interference.

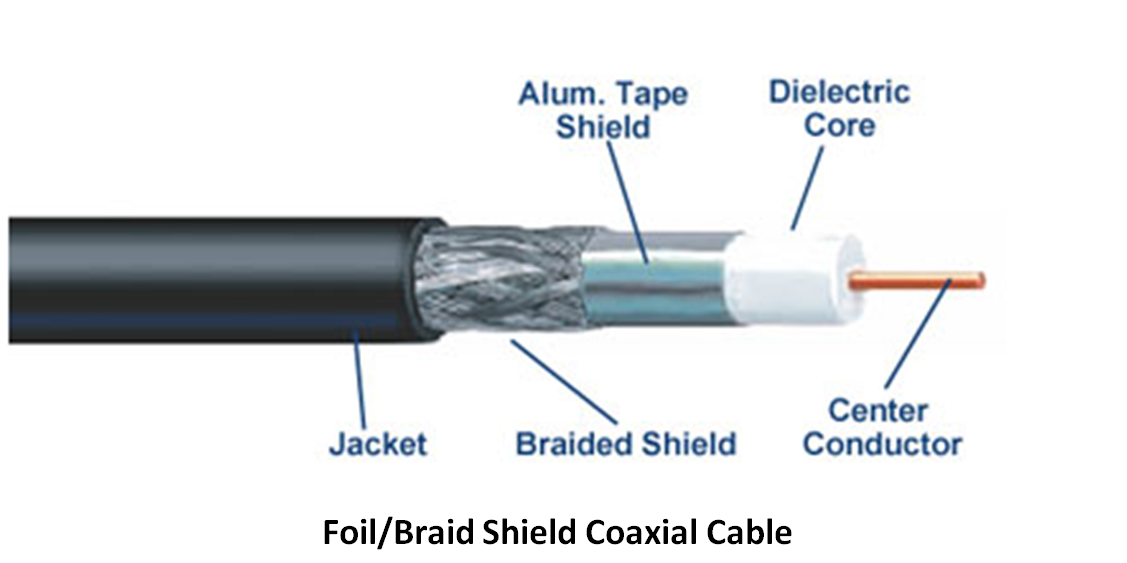


Figure 1.12 : Coaxial cable

**FIBER OPTIC**

Fiber optic cabling carries signals, which have been converted from electrical to optical (pulses of light) form. It consists of the core, either an extremely thin cylinder of glass or optical quality plastic, which is surrounded by a second glass or plastic layer called the cladding. The interface between the core and cladding can trap light signals by a process called Total Internal Reflection (TIR), resulting in the optical fiber acting as a light pipe. Protective buffer and jackets materials are used to cover the cladding layer. This type of cabling is less frequently used because it is somewhat more expensive; however, it is rapidly decreasing in both raw cost and installed cost. Fiber optic cables are not susceptible to interference, such as radio waves, fluorescent lighting, or any other source of electrical noise. It is the common cable used for network backbones and can support up to 1000 stations; carrying signals beyond 25 km. Fiber terminations include SC, ST, and a variety of proprietary connectors.

Optical fiber consists of a core and a cladding layer, selected for total internal reflection due to the difference in the refractive index between the two. In practical fibers, the cladding is usually coated with a layer of acryl ate polymer or polyimide. This coating protects the fiber from damage but does not contribute to its optical waveguide properties. Individual coated fibers (or fibers formed into ribbons or bundles) then have a tough resin buffer layer and/or core tube(s) extruded around them to form the cable core. Several layers of protective sheathing, depending on the application, are added to form the cable. Rigid fiber assemblies sometimes put light-absorbing ("dark") glass between the fibers, to prevent light that leaks out of one fiber from entering another. This reduces cross-talk between the fibers, or reduces flare in fiber bundle imaging applications.

An important aspect of a fiber optic communication is that of extension of the fiber optic cables such that the losses brought about by joining two different cables is kept to a minimum. Joining lengths of optical fiber often proves to be more complex than joining electrical wire or cable and involves careful cleaving of the fibers, perfect alignment of the fiber cores, and the splicing of these aligned fiber cores. For applications that demand a permanent connection a mechanical splice which holds the ends of the fibers together mechanically could be used or a fusion splice that uses heat to fuse the ends of the fibers together could be used. Temporary or semi-permanent connections are made by means of specialized optical fiber connectors.

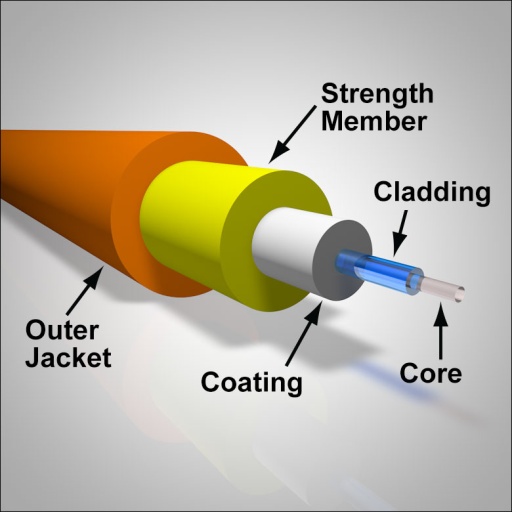


Figure 1.13 : Fiber-optic Cable

**UNSHIELDED TWISTED PAIR (UTP)**

Unshielded Twisted Pair (UTP) is a set of three or four pairs of wires with each wire in each pair twisted around the other to prevent electromagnetic interference. UTP cabling uses RJ-45, RJ-11, RS232, and RS-449 connectors. Because it is less expensive and easier to install, UTP is more popular than Shielded Twisted Pair (STP) or Coaxial Cabling. An example of UTP application is telephone networks, which use RJ-11 connectors, and 10BASE-T networks, which use RJ-45 connectors. UTP comes in the form of Cat 2, 3, 4, and 5 grades; however, only Cat 5 is now recommended for any data applications. The maximum length is 100 meters, without using any kind of signal regeneration device, and a maximum data transfer rate of 1000 Mbps for Gigabit Ethernet.

The characteristics of UTP are very good and make it easy to work with, install, expand and troubleshoot

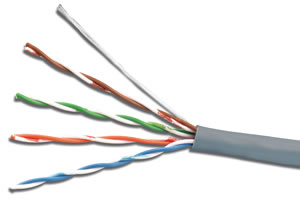


Figure 1.14 : UTP Cable

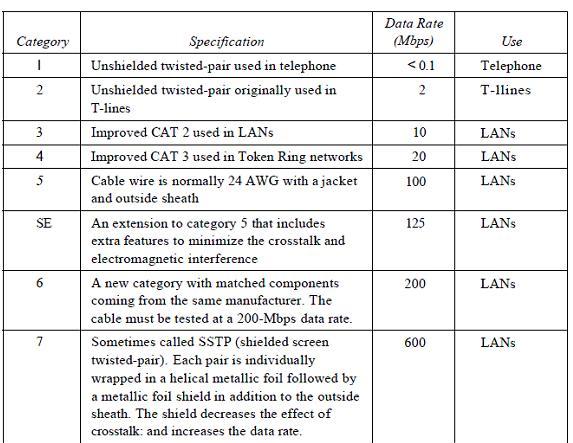


TABLE 1.2: categories of UTP

Category 1/2/3/4/5/6 – a specification for the type of copper wire (most telephone and network wire is copper) and jacks. The number (1, 3, 5, etc) refers to the revision of the specification and in practical terms refers to the number of twists inside the wire (or the quality of connection in a jack).

CAT1 is typically telephone wire. This type of wire is not capable of supporting computer network traffic and is not twisted. It is also used by phone companies who provide ISDN, where the wiring between the customer's site and the phone company's network uses CAT 1 cable.

CAT2, CAT3, CAT4, CAT5 and CAT6 are network wire specifications. This type of wire can support computer network and telephone traffic. CAT2 is used mostly for token ring networks, supporting speeds up to 4 Mbps. For higher network speeds (100Mbps plus) you must use CAT5 wire, but for 10Mbps CAT3 will suffice. CAT3, CAT4 and CAT5 cable are actually 4 pairs of twisted copper wires and CAT5 has more twists per inch than CAT3 therefore can run at higher speeds and greater lengths. The "twist" effect of each pair in the cables will cause any interference presented/picked up on one cable to be cancelled out by the cable's partner which twists around the initial cable. CAT3 and CAT4 are both used for Token Ring and have a maximum length of 100 meters.

CAT6 wire was originally designed to support gigabit Ethernet (although there are standards that will allow gigabit transmission over CAT5 wire, that's CAT 5e). It is similar to CAT5 wire, but contains a physical separator between the 4 pairs to further reduce electromagnetic interference.

**SHIELDED TWISTED PAIR (STP)**

Shielded Twisted Pair (STP), like UTP, also has four pairs of wires with each wire in each pair twisted together. However, the difference is that STP is surrounded with a foil shield and copper braided around the wires that allows more protection from any external electromagnetic interference. Because of the shielding, the cable is physically larger, more difficult to install and terminate, and more expensive than UTP. For applications in electrically noisy environments, STP uses RJ-45, RJ-11, RS-232, and RS-449 connectors. Like UTP, STP also comes in Cat 2, 3, 4, or 5 grades; however, only Cat5 is recommended for any data applications. The maximum cable length with no signal regenerating device is 100 meters; with a maximum data transfer rate is 500 Mbps. STP cables have additional shielding material that is used to reduce external interference. The shield also reduces the emission at any point in the path of the cable. UTP cables provide much less protection against such interference and the performance is often degraded when interferences or disturbances are present. Both types of cables, however, have some protection to interference due to the twisted pair design of the conductors.

The drawback of STP cables is that they will increase the total cost of an installation. STP cables are more expensive due to the shielding, which is an additional material that goes into every meter of the cable. The shielding also makes the cable heavier and stiffer. Thus, it is more difficult to handle.

Differentiated physically by little more than a conducting shield, shielded twisted pair cables and unshielded twisted pair cables nonetheless have different advantages, disadvantages, and best applications.



Figure 1.15 : STP Cable

Both shielded twisted pair (STP) and unshielded twisted pair (UTP) have interference canceling capacities, however the way that each one is designed to cancel the interference is different. Interference caused by power lines, radar systems or other high power electromagnetic signals, called noise, can cause an imbalance in the current flowing through the shield or conductors of the cables which interferes with the signal. STP cables have a conducting shield made of metallic foil encasing the twisted wire pairs, which blocks out electromagnetic interference, allowing it to carry data at a faster rate of speed.

However, they have several disadvantages. STP cables work by attracting interference to the shield, then running it off into a grounded cable. If the cable is improperly grounded, then its noise-canceling capabilities are severely compromised. Additionally, STP cables are bigger than UTP cables, and are more expensive. Finally, they are more fragile than UTP cables, as the shield must be kept intact in order for them to work properly. The best use for STP cables is in industrial settings with high amounts of electromagnetic interference, such as a factory with large electronic equipment, where they can be properly installed and maintained.

UTP cables are the most commonly used cables for Ethernet connections, and have a number of advantages. They rely on the cancellation affect caused by the twisting of the wire pairs to handle noise, which is more than enough for most domestic uses. They are also smaller than STP cables, which makes them easier to install, particularly in bulk or in narrow spaces. They are easier to install than STPs, and do not require the presence of a grounding cable. UTP cables are also cheaper than STP cables, and do not require as much maintenance, since they do not rely on an outer shield, and can transmit data as fast as STP cables. However, they are more prone to noise than properly installed and maintained STP cables. They are best used for domestic and office Ethernet connections, and in any area where there is not a high degree of electromagnetic interference.

While both STP and UTP cables have their pros and cons, when installed and maintained properly in a situation appropriate to their uses, both work perfectly fine.

**CONNECTORS:**

An **electrical connector** is an electro-mechanical device for joining electrical circuits as an interface using a mechanical assembly. Connectors consist of plugs (male-ended) and jacks (female-ended). The connection may be temporary, as for portable equipment, require a tool for assembly and removal, or serve as a permanent electrical joint between two wires or devices. An adapter can be used to effectively bring together dissimilar connectors.

There are hundreds of types of electrical connectors. Connectors may join two lengths of flexible copper wire or cable, or connect a wire or cable to an electrical terminal.

In computing, an electrical connector can also be known as a **physical interface** (compare physical layer in OSI model of networking). Cable glands, known as *cable connectors* in the US, connect wires to devices mechanically rather than electrically and are distinct from quick-disconnects performing the latter.

Electrical connectors are characterized by their pin out and physical construction, size, contact resistance, insulation between pins, ruggedness and resistance to vibration, resistance to entry of water

or other contaminants, resistance to pressure, reliability, lifetime (number of connect/disconnect operations before failure), and ease of connecting and disconnecting.

They may be keyed to prevent insertion in the wrong orientation, connecting the wrong pins to each other, and have locking mechanisms to ensure that they are fully inserted and cannot work loose or fall out. Some connectors are designed such that certain pins make contact before others when inserted, and break first on disconnection; this protects circuits typically in connectors that apply power, e.g. connecting safety ground first, and sequencing connections properly in hot swapping applications.

It is usually desirable for a connector to be easy to identify visually, rapid to assemble, require only simple tooling, and be inexpensive. In some cases an equipment manufacturer might choose a connector specifically because it is *not* compatible with those from other sources, allowing control of what may be connected. No single connector has all the ideal properties; the proliferation of types is a reflection of differing requirements.

Fretting is a common failure mode in electrical connectors that have not been specifically designed to prevent it.

**TYPES OF CONNECTORS**:

A *terminal* is a simple type of electrical connector that connects two or more wires to a single connection point. Wire nuts are another type of single point connector

**Terminal blocks**

Terminal blocks (also called terminal *boards* or *strips*) provide a convenient means of connecting individual electrical wires without a splice or physically joining the ends. They are usually used to connect wiring among various items of equipment within an enclosure or to make connections among individually enclosed items. Since terminal blocks are readily available for a wide range of wire sizes and terminal quantity, they are one of the most flexible types of electrical connector available. Some disadvantages are that connecting wires is more difficult than simply plugging in a cable and the terminals are generally not very well protected from contact with persons or foreign conducting materials.

One type of terminal block accepts wires that are prepared only by removing (*stripping*) a short length of insulation from the end. Another type accepts wires that have ring or spade terminal *lugs* crimped onto the wires. Printed circuit board (PCB) mounted terminal blocks allow individual wires to be connected to the circuit board. PCB mounted terminal blocks are soldered to the board, but they are available in a pull-apart version that allows the wire-connecting half of the block to be unplugged from the part that is soldered to the PCB.

**Posts**

A general type of connector that simply screws or clamps bare wire to a post; such connectors are frequently used in electronic test equipment and audio. Many, but not all binding posts will also accept a banana connector plug.

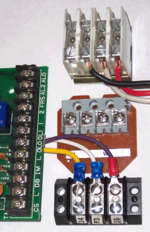
**[](https://en.wikipedia.org/wiki/File:Terminal_Blocks_01CJC.png)**

Figure 1.16 : Terminal Blocks

[](https://en.wikipedia.org/wiki/File:Binding_post_adapter.JPG)

Figure 1.17 : A binding post(red & black) adaptor

**Crimp-on connectors**

A type of solder less connection.

**Insulation displacement connectors**

Since stripping the insulation from wires is time-consuming, many connectors intended for rapid assembly use insulation-displacement connectors so that insulation need not be removed from the wire. These generally take the form of a fork-shaped opening in the terminal, into which the insulated wire is pressed and which cut through the insulation to contact the conductor within. To make these connections reliably on a production line, special tools are used which accurately control the forces applied during assembly. If properly assembled, the resulting terminations are gas-tight and will last the life of the product. A common example is the multi-conductor flat ribbon cable used in computer disk drives; to terminate each of the many (approximately 40) wires individually would be slow and error-prone, but an insulation displacement connector can terminate all the wires in (literally) one stroke. Another very common use is so-called punch-down blocks used for terminating telephone wiring.

Insulation displacement connectors are usually used with small conductors for signal purposes and at low voltage. Power conductors carrying more than a few amperes are more reliably terminated with other means, though "hot tap" press-on connectors find some use in automotive applications for additions to existing wiring.

**Plug and socket connectors**

Plug and socket connectors are usually made up of a male plug (typically pin contacts) and a female receptacle (typically socket contacts), although *hermaphroditic* connectors exist, such as the original IBM token ring LAN connector. Plugs generally have one or more pins or prongs that are inserted into openings in the mating socket. The connection between the mating metal parts must be sufficiently tight to make a good electrical connection and complete the circuit. When working with multi-pin connectors, it is helpful to have a pin out diagram to identify the wire or circuit node connected to each pin.



Figure 1.18 : Plug & Socket Connector

**COMMONLY USED CONNECTORS**

**8P8C connector**

**8P8C** is short for "eight positions, eight conductors", and so an 8P8C modular connector (plug or jack) is a modular connector with eight positions, all containing conductors. The connector is probably most famous for its use in Ethernet and widely used on CAT5 cables.

The 8P8C modular plugs and jacks look very similar to the plugs and jacks used for FCC's registered jack RJ45 variants, although the specified RJ45 socket is not compatible with 8P8C modular plug connectors. It neither uses all eight conductors (but only two of them for wires plus two for connecting a programming resistor) nor does it fit into 8P8C because the true RJ45 is "keyed".

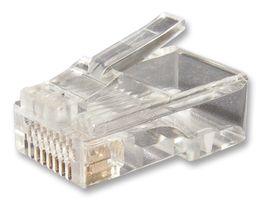


Figure 1.19 : 8P8C Connector

**D-subminiature connectors**

The D-subminiature electrical connector is commonly used for the RS-232 serial port on modems and IBM compatible computers. The D-subminiature connector is used in many different applications, for computers, telecommunications, and test and measurement instruments. A few examples are monitors (MGA, CGA, and EGA), the Commodore 64, MSX, Apple II, Amiga, and Atari joysticks and mice, and game consoles such as Atari and Sega.

Another variants of D-subminiature are the Positron D-subminiature connector which have PosiBand closed entry contact option, solid machined contacts, thermocouple contact options, crimp and PCB mount.; and the Positronic Combo D-subminiature which have Large Surface Area (LSA) contact system that is for low contact resistance and saves energy, and sequential mating option.



Figure 1.20 : Male DE-9 plug

**USB connectors**

The **Universal Serial Bus** is a serial bus standard to interface devices, founded in 1996. It is currently widely used among PCs, Apple Macintosh and many other devices. There are several types of USB connectors, and some have been added as the specification has progressed. The most commonly used is the (male) series "A" plug on peripherals, when the cable is fixed to the peripheral. If there is no cable fixed to the peripheral, the peripheral always needs to have a USB "B" socket. In this case a USB "A" plug to a USB "B" plug cable would be needed. USB "A" sockets are always used on the host PC and the USB "B" sockets on the peripherals. It is a 4-pin connector, surrounded by a shield. There are several other connectors in use, the mini-A, mini- B and mini-AB plug and socket (added in the On-The-Go Supplement to the USB 2.0 Specification).



Figure 1.21 : USB Connector

**SWITCHES/HUBS:**

**SWITCHES:**

A switch is a device that incorporates bridge functions as well as point-to-point ‘dedicated connections’. They connect devices or networks, filter, forward and flood frames based on the MAC destination address of each frame. Switch operates at data link layer of the OSI model. They are technically called bridges. They move data without contention. Ethernet switches provide a combinations of shared/dedicated 10/100/1000 Mbps connections. Some E-net switches support cut-through switching: frame forwarded immediately to destination without awaiting for assembly of the entire frame in the switch buffer. They significantly increases throughput. They provide express lane for traffic.

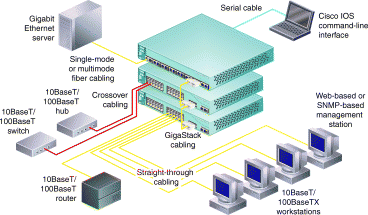


Figure 1.22 : Switch

**HUBS**

If multiple incoming connections need to be connected with multiple outgoing connections, then a hub is required. In data communications, a hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more other directions. Hubs are multi-port repeaters, and as such they obey the same rules as repeaters. They operate at the OSI Model Physical Layer. Hubs are used to provide a Physical Star Topology. At the center of the star is the Hub, with the network nodes located on the tips of the star.

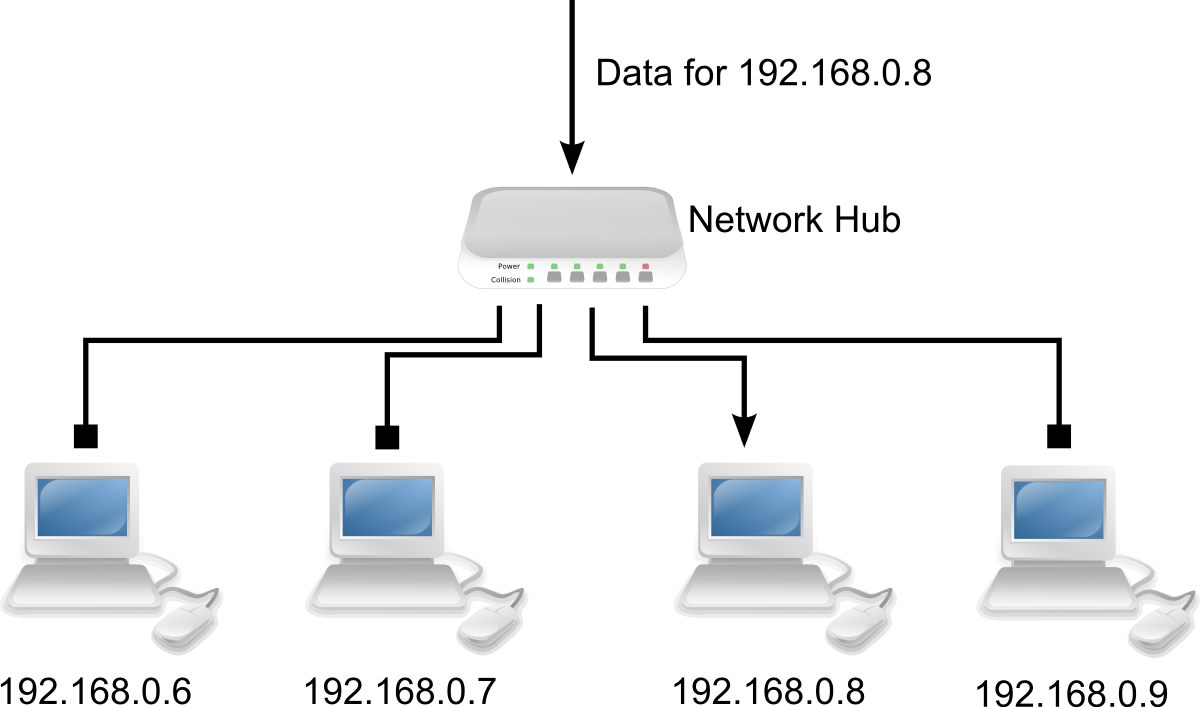


Figure 1.23 : A Hub

|  |  |
| --- | --- |
| HUBS | SWITCHES |
| Collision Domain | Broadcast Domain |
| All of the parts on a hub are part of the same Ethernet | Each part on a switches may be regarded as a separate Ethernet (but all are part of the same local area network) |
| All parts on a hub share the same 10Mb (100 Mb) bandwidth | Each part on a switch has its own 10Mb (100 Mb) bandwidth |
| Any frame appearing on one port of a hub is repeated to all other ports on the hub | A directed frame appearing on one part of a switch is forwarded only to the destination port. |

TABLE 1.3: comparision between switches and hubs

**Hub’s Segment-to-Segment Characteristics** :

To understand the Ethernet segment-to-segment characteristics of a hub, let us first determine how the Ethernet Hubs operate. Logically, they appear as a Bus Topology, and physically as a Star Topology. Looking inside an Ethernet Hub, we can see that it consists of a electronic printed circuit board. Understanding that inside the Hub is only more repeaters, we can draw the conclusion that all connections attached to a Hub are on the same Segment (and have the same Segment Number). A single repeater is said to exist from any port to any port, even though it is indicated as a path of 2 repeaters.

**Cascaded Hub Network**:

Connecting Hubs together through ports creates Cascading Hubs. One Master Hub (Level 1) is connected to many Level 2 (Slave) Hubs, who are masters to Level 3 (Slave) Hubs in a hierarchical tree (or clustered star). The maximum number of stations in a Cascaded Hub Network is limited to 128.

**Hub’s Addressing:**

Because a Hub is just many repeaters in the same box, any network traffic between nodes is heard over the complete network. As far as the stations are concerned, they are connected on one long logical bus (wire).

**Half-Duplex and Full-Duplex Ethernet Hubs**:

Normal Ethernet operation is Half-Duplex: only 1 station or node is talking at a time. The stations take turns talking on the bus (CSMA/CD -bus arbitration).

Full-Duplex Ethernet Hubs are Hubs which allow two-way communication, thus doubling the available bandwidth from 10 Mbps to 20 Mbps. Full duplex Hubs are proprietary products, and normally only work within their own manufacturer’s line.

For example, if A wanted to talk to C, a direct 10 Mbps line would be connected through the 2 switching hubs. Simultaneously, if D wanted to talk to B, another direct 10 Mbps line (in the opposite direction) would be connected through the two switching Hubs (doubling the available bandwidth to 20 Mbps).

There are no official standards for Full-Duplex Ethernet although proprietary standards do exist.

**Switching Hubs**:

Switching hubs are hubs that will directly switch ports to each other. They are similar to full duplex hubs, except that they allow dedicated 10 Mbps channels between ports.

If A wanted to communicate with B, a dedicated 10 Mbps connection would be established between the two. If C wanted to communicate with D, another dedicated 10 Mbps connection would be established.

**ROUTER**:

In an environment consisting of several network segments with different protocols and architecture, a bridge may not be adequate for ensuring fast communication among all of the segments. A complex network needs a device which not only knows the address of each segment, but also can determine the best path for sending data and filtering broadcast traffic to the local segment. Such a device is called a Router.

Routers are both hardware and software devices. They can be cards that plug into a collapsed backbone, stand-alone devices or software that would run on a file server.



Figure 1.24 : A Router

**Purpose of Routers**:

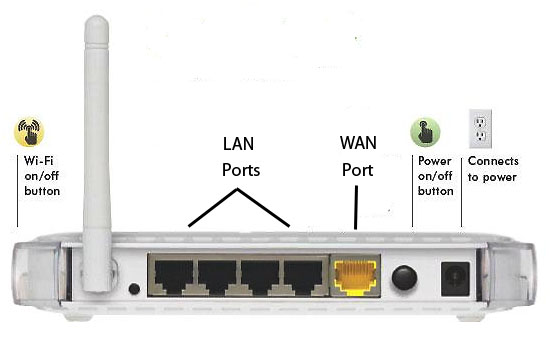
The purpose of a router is to connect nodes across an Internetwork, regardless of the Physical Layer and Data Link Layer protocol that is used. Routers are hardware and topology-independent. Routers are not aware of the type of medium or frame that is being used (Ethernet, Token Ring, FDDI, etc.). Routers are aware of the Network Layer protocol that’s used (e.g., Novell’s IPX, Unix’s IP, XNS, Apple’s DDP, and so on).

Router OSI Operating Layer Routers operate on the OSI Model’s Network Layer. The Internetwork must use the same Network Layer protocol. Routers allow the transport of the Network Layer PDU through the Internetwork, even though the Physical and Data Link Frame size and addressing scheme may change.

Routers that only know Novell IPX (Internetwork Packet Exchange) will not forward Unix’s IP (Internetwork Packet) PDUs, and vice versa. Routers only see the Network Layer protocol that they have been configured for. This means that a network can have multiple protocols running on it (e.g., SPX/IPX, TCP/IP, Appletalk, XNS, etc.).

For example a Novell SPX/IPX router; only sees the Network Layer protocol IPX. This means that any TCP/IP PDUs will not pass through: the router does not recognise the PDUs, and doesn’t know what to do with them. Therefore, Routers allow network traffic to be isolated - or segmented - based on the Network Layer Protocol. This provides a functional segmentation of the network.

Routers that only can see one protocol are called Protocol Dependent Routers. Routers that can see many different protocols (two or more) are called Multi protocol Routers.



Fiure 1.25 : Router(rearview)

**Router Addressing**:

Routers combine the Network Number and the Node Address to make Source and Destination addresses (in routing Network Layer PDUs across a network). Routers have to know the name of the segment that they are on, and the segment name or number where the PDU is going. They also have to know the Node Address: MAC Address for Novell, and the IP address for TCP/IP.

For Novell’s SPX/IPX (Sequential Packet exchange/Internetwork Packet exchange), the Network Layer PDU’s address is composed of the Network Address (32 bit number) and the Host address (48 bit - MAC address).

**Routing Protocols**:

Routing Protocols are a “sub-protocol” of the Network Layer Protocol. They deal specifically with the routing of packets from the source to the destination (across an Internetwork). Examples of Routing Protocols are: RIP, IGRP and OSPF.

**NETWORK CARDS**:

A **Network interface card**, **NIC**, or **Network card** is an electronic device that connects a computer to a computer network, usually a LAN. It is considered a piece of computer hardware. Today, most computers have network cards. Network cards enable a computer to exchange data with the network. To achieve the connection, network cards use a suitable protocol, for example CSMA/CD. Network cards usually implement the first two layers of the OSI model, that is the physical layer, and the data link layer. Today, most network cards use Ethernet. Other network types are ARCNET, introduced in 1977, Local Talk or Token Ring.

A network card usually has two indicator lights (LEDs):

* The green LED shows that the card is receiving electricity;
* The orange (10 Mb/s) or red (100 Mb/s) LED indicates network activity (sending or receiving data). To prepare data to be sent the network card uses a **transceiver**, which transforms parallel data into serial data. Each cart has a unique address, called a **MAC address**, assigned by the card's manufacturer, which lets it be uniquely identified among all the network cards in the world.

A network card is the physical interface between the computer and cable. It converts the data sent by the computer into a form which can be used by the network cable, transfers that data to another computer and controls the dataflow between the computer and cable. It also translates the data coming from the cable into bytes so that the computer's CPU can read it. This is why a network card is an expansion card inserted into an expansion slot.

The computer and the card must communicate so that data can travel between them. For this reason, the computer assigns part of its memory to cards that include DMA (Direct Access Memory).

The interface card indicates that another computer is requesting data from that computer.   
The computer's bus transfers the data from the computer memory to the network card.

If the data is moving too fast for the adapter to process, they are placed in the card's buffer memory (RAM), where they are temporarily stored while the data is being sent and received.

Network adapters have configuration options: Among others:

* Interruption (IRQ): In most cases, network cards use IRQ 3 and 5. IRQ 5 is recommended (whenever available) and most cards use it as the default setting.
* Input/output (I/O) base address: Each device must have a different address for the corresponding port.
* Memory address: This designates a RAM location in the computer. The network card uses this slot as a buffer for data entering and leaving. This setting is sometimes called the RAM Start Address. In general, a network card's memory address is D8000. The last 0 is left out on some network cards. You have to be careful not to select an address already being used by another device. It should, however, be noted that some network cards have no configurable memory address because they don't use the machine's RAM addresses.

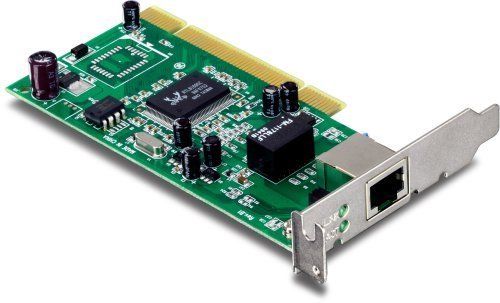


Figure 1.26 : Network Card

**Other Network Parts**

**Ethernet**

* Ethernet is a widely deployed LAN technology.This technology was invented by Bob Metcalfe and D.R. Boggs in the year 1970. It was standardized in IEEE 802.3 in 1980.
* Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data.
* Ethernet connector is,network interface card equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet.
* Traditional Ethernet uses 10BASE-T specifications.The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-5 connector. Ethernet follows star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion.
* Fast-Ethernet
* To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100 MBPS. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 twisted pair cable. It uses CSMA/CD technique for wired media sharing among the Ethernet hosts and CSMA/CA (CA stands for Collision Avoidance) technique for wireless Ethernet LAN.
* Fast Ethernet on fiber is defined under 100BASE-FX standard which provides speed up to 100 MBPS on fiber. Ethernet over fiber can be extended up to 100 meters in half-duplex mode and can reach maximum of 2000 meters in full-duplex over multimode fibers.
* Giga-Ethernet
* After being introduced in 1995, Fast-Ethernet could enjoy its high speed status only for 3 years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.
* Protocol Cable Speed
* Ethernet Twisted Pair, Coaxial, Fiber 10 Mbps
* Fast Ethernet Twisted Pair, Fiber 100 Mbps
* Gigabit Ethernet Twisted Pair, Fiber 1000 Mbps
* Virtual LAN
* LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. But even Switches cannot divide a network into separate Broadcast domains.
* Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains. Host in one VLAN cannot speak to a host in another. By default, all hosts are placed into the same VLAN.

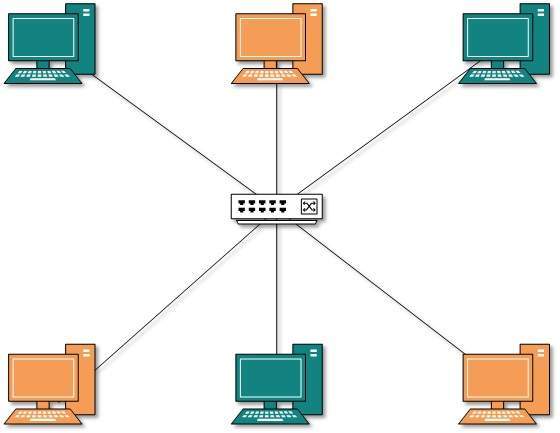


Figure 1.27 : Ethernet

* In this diagram, different VLANs are depicted in different color codes. Hosts in one VLAN, even if connected on the same Switch cannot see or speak to other hosts in different VLANs. VLAN is Layer-2 technology which works closely on Ethernet. To route packets between two different VLANs a Layer-3 device such as Router is required.

**RESULT:**

The components of computer networks were studied and familiarized .

CYCLE-1

EXP-2

DATE: 16/07/15

**CRIMPING UTP CABLES**

**AIM**: To crimp UTP cables to make a direct connection cable

**THEORY :**

UTP has 4 twisted pairs of wires as shown in FIGURE: 2.1. Pairs 2 & 3 are used for normal 10/100Mbit networks, while pairs 1 & 4 are reserved. In Gigabit Ethernet, all 4 pairs are used.

There are 2 popular wiring schemes: T-568A and T-568B, which differ only in which color coded pairs, are connected - pair 2 and 3 is reversed.

UTP cables are terminated with standard connectors, jacks and punch downs. The jack/plug is often referred to as “RJ-45", but that is really a Telco designation for the "modular 8 pin connector" terminated with a USOC pin out used for telephones. The male connector on the end of a patch cord is called a "plug" and the receptacle on the wall outlet is a "jack."

Ethernet is generally carried in 8-conductor cables with 8-pin modular plugs and jacks. The connector standard is called "RJ-45".The eight-conductor data cable contains 4 pairs of wires. Each pair consists of a solid colored wire and a white wire with a stripe of the same color. The pairs are twisted together. To maintain reliability on Ethernet, you should not untwist them any more than necessary (like about 1 cm). The pairs designated for 10 and 100 Mbit Ethernet are Orange and Green. The other two pairs, Brown and Blue, can be used for a second Ethernet line or for phone connections.

The most common application for a straight through cable is a connection between a PC and a hub/switch. In this case the PC is connected directly to the hub/switch which will automatically cross over the cable internally, using special circuits. In the case of a CAT1 cable, which is usually found in telephone lines, only 2 wires are used, these do not require any special cross over since the phones connect directly to the phone socket.

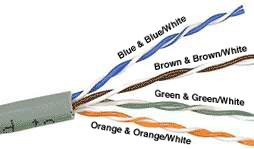


Figure 2.1 : UTP Color Coding

**PROCEDURE**:

1. **Unroll the required length of network cable and add a little extra wire, just in case.** If a boot is to be fitted, do so before stripping away the sleeve and ensure the boot faces the correct way.
2. **Carefully remove the outer jacket of the cable.** Be careful when stripping the jacket as to not nick or cut the internal wiring (13mm). Cut lengthwise with snips or a knife along the side of the cable, away from yourself, about an inch toward the open end. Locate the string inside with the wires, or if no string is found, use the wires themselves to unzip the sheath of the cable by holding the sheath in one hand and pulling sideways with the string or wire. 8 wires twisted in 4 pairs are present. Each pair will have one wire of a certain color and another wire that is white with a colored stripe matching its partner (this wire is called a tracer).
3. **Inspect the newly revealed wires for any cuts or scrapes that expose the copper wire inside.** Exposed copper wire will lead to cross-talk, poor performance or no connectivity at all. It is important that the jacket for all network cables remains intact.
4. **Untwist the pairs so they will lay flat between your fingers.**
5. **Arrange the wires based on the wiring specifications:** white/orange, orange, white/green, blue, white/blue, green, white/brown, brown.
6. **Press all the wires flat and parallel between your thumb and forefinger.** Cut the top of the wires even with one another so that they are 1/2" (12.5 mm) long from the base of the jacket. Ensure that the cut leaves the wires even and clean; failure to do so may cause the wire not to make contact inside the jack and could lead to wrongly guided cores inside the plug.
7. **Keep the wires flat and in order as you push them into the RJ-45 plug with the flat surface of the plug on top.** The white/orange wire should be on the left. The cabling jacket should also enter the rear of the jack about 1/4" (6 mm) to help secure the cable once the plug is crimped. Verify that the sequence is still correct before crimping. A wire should be located in each hole, as seen at the bottom right.
8. **Place the wired plug into the crimping tool.** Give the handle a firm squeeze.
9. **Repeat all of the above steps with the other end of the cable.**
10. **Test the completed cable by connecting it to the computer’s RJ-45 female socket.**
11. **Use the “ping” command to ping the IP address of the connection**; if successful the time taken will be displayed otherwise an error message will be displayed.

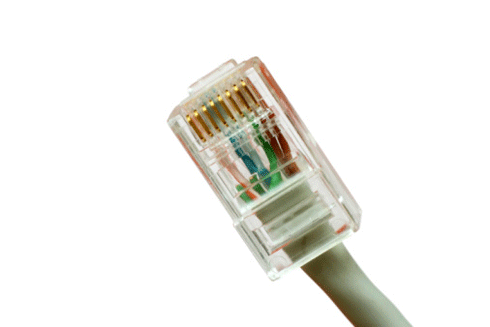


Figure 2.2 : RJ-45 Connector

**RESULT**:

The UTP cable was crimped to make a direct connection cable.

CYCLE-1

EXP-3a

DATE: 16/07/15

**SUBNETTING & SUPERNETTING**

**AIM**: Study the basic concept of subnetting and supernetting.

**THEORY**

**SUBNETTING:**

**Some basic definitions**:

* IP Address: A logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network
* Subnet: A separate and identifiable portion of an organization's network, typically arranged on one floor, building or geographical location
* Subnet Mask: A 32-bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address
* Network Interface Card (NIC): A computer hardware component that allows a computer to connect to a network

To subnet a network is to create logical divisions of the network. Subnetting, therefore, involves dividing the network into smaller portions called subnets. Subnetting applies to IP addresses because this is done by borrowing bits from the host portion of the IP address. In a sense, the IP address then has three components - the network part, the subnet part and, finally, the host part.

We create a subnet by logically grabbing the last bit from the network component of the address and using it to determine the number of subnets required. In the following example, a Class C address normally has 24 bits for the network address and eight for the host, but we are going to borrow the left-most bit of the host address and declare it as identifying the subnet. If the bit is a 0, then that will be one subnet; if the bit is a 1, that would be the second subnet. Of course, with only one borrowed bit we can only have two possible subnets. By the same token, that also reduces the number of hosts we can have on the network to 127 (but actually 125 useable addresses given all zeros and all ones are not recommended addresses), down from 255. A subnet mask is used to indicate how many bits are being “borrowed” from the host component of an IP address.

**Subnet mask**

Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address. Subnet mask is always used with IP address. Subnet mask has only one purpose, to identify which part of an IP address is network address and which part is host address.

**SUPERNETTING:**

Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. The original Internet Protocol (IP) defines IP addresses in four major classes of address structure, Classes A through D. Each class allocates one portion of the 32-bit Internet address format to a network address and the remaining portion to the specific host machines within the network. Using supernetting, the network address 192.168.2.0/24 and an adjacent address 192.168.3.0/24 can be merged into 192.168.2.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses. Supernetting is most often used to combine Class C network addresses and is the basis for most routing protocols currently used on the Internet.

Supernetting was created as a way to solve the problem of routing tables growing beyond the ability of current software and people to manage and to provide a solution to the exhaustion of Class B network address space. Supernetting allows one routing table entry to represent an aggregation of networks much like one area code represents an aggregation of telephone numbers in an area.

The benefits of supernetting are conservation of address space and efficiencies gained in routers in terms of memory storage of route information and processing overhead when matching routes.

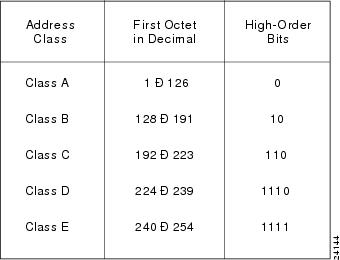


Table 3.1 : Class-full addressing

**RESULT**

The basic concept of subnetting and supernetting were understood.

CYCLE-1

EXP-3b

DATE:30/07/15

**SUBNETTING PROGRAM**

**AIM**: Write a program in python to find out the number of networks, number of hosts ,the first address and the last address of the subnet.

**ALGORITHM**:

1. Start
2. ip = raw\_input(‘Enter the IP Address’)
3. for i in range(0,3)

addr[i] = ip.split( . )

endfor

1. cidr = raw\_input(‘Enter the CIDR number’)
2. quo = cidr/8
3. rem = cidr%8
4. power = 8\*quo
5. no\_of\_networks = pow(2,power)
6. no\_of\_subnets = pow(2,rem)-2
7. no\_of\_hosts = pow(2,32-cidr)
8. inc = pow(2,8-rem)
9. addr[quo] = inc
10. copy = addr
11. tmp=quo
12. while(quo<4) :

add[tmp]=0

endwhile

1. indicated=3
2. snt=0
3. while(snt < no\_of\_subnets):

print(‘ Subnet Address : ’)

for I in range(0,2)

print(addr[i]+’.’)

endfor

print(addr[3])

for i in range(0 , 8-rem)

addr[tmp]=addr[tmp]+pow(2,i)

while(indicated > tmp) :

for j in range(0,254) :

addr[indicated] = j

for k in range(0 , 2)

print(addr[i]+’.’)

endfor

print(addr[3])

endfor

addr[indicated]=254

indicated - -

endwhile

endfor

snt++

endwhile

1. print( ‘No. of networks : ’ + no\_of\_networks)
2. print( ‘No. of hosts : ’ + no\_of\_hosts)
3. print( ‘No. of Subnets : ’ + no\_of\_subnets)
4. Stop

**RESULT**:

The python program to find out the number of networks, number of hosts ,the first address and the last address of the subnet , has been executed successfully.

CYCLE: 01

EXPERIMENT: 04

DATE: 17/08/15

**VLAN**

**AIM**: To create a VLAN using Switches and Routers

**THEORY**:

Virtual Local Area Networks are used to divide a physical network into several broadcast domains. The reason to use VLANs is to divide a network and separate hosts that shouldn't be able to access each other. There are two types of packets on a VLAN, these are tagged and untagged packets. The untagged packet is a regular packet and looks just like a packet that exists on a regular network. Untagged packets are the most common type on a VLAN. The decision of which VLAN an untagged packet belongs to is made by the switch. A switch can be configured to assign specific ports to specific VLANs. The switch can also be configured to receive tagged packets.

If the switch receives a tagged packet and the port which it receives the packet with is configured to allow tagged packets, it knows which ports it can send the packet to.

A switch can also be configured to transmit tagged packets, this could be used to make a VLAN span more than one switch or to make use of a VLAN aware NIC (Network Interface Card) on a router, firewall, server or even a workstation.

A VLAN is assigned a specific id. This id can be anything between 1 and 4094. VLAN 1 is most commonly used for management so this should not be used.

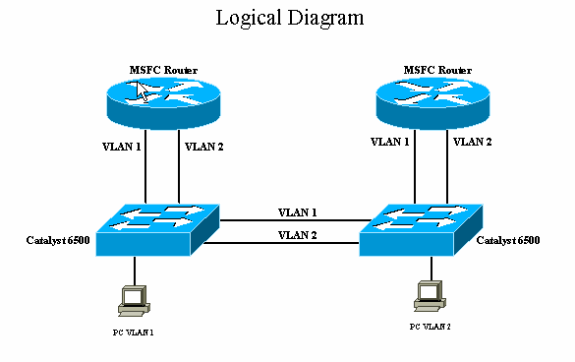


Figure 4.1 : Logical diagram of a VLAN

**Procedure**:

1. Start
2. Select Three Machines
3. Assign IP addresses to the machines so that they belong to same network

sudo ifconfig eth0 192.168.10.112

3.1 Verify if IP has been set command 0: ifconfig

1. Create a gateway for accessing the interface of the HP switch at 172.16.12.24 by executing the command sudo route add default gw 192.168.10.1erify the default gateway is set to 192.168.0.1 by executing the command route
2. Open the browser to get the web interface of the HP switch at 172.16.12.24
3. Login using the required credentials
4. Under the network tab select the VLAN

7.1 Edit the existing VLAN to free upthe ports for creating a new VLAN

7.2 Assign a new VLAN id and allot the ports for the new VLAN created

7.3 Create another VLAN in a similar way and assign other free ports for conformation of working of VLAN

1. Connect the PC1 to the corresponding port allotted to the VLAN
2. Connect PC2 and PC3 to the other ports of VLAN2
3. Ping from PC1 toPC2 to check that no communication occurs between the PCs in VLAN1 and VLAN2 though they are in the same network

Command : ping 192.168.10.122

It shows unreachable host

1. Now check the PC’s in VLAN i.e. PC2 and PC are reachable by sending the ping command to PC2 to PC3 using command : ping 192.168.10.126 . Its shows reply from 192.168.10.126

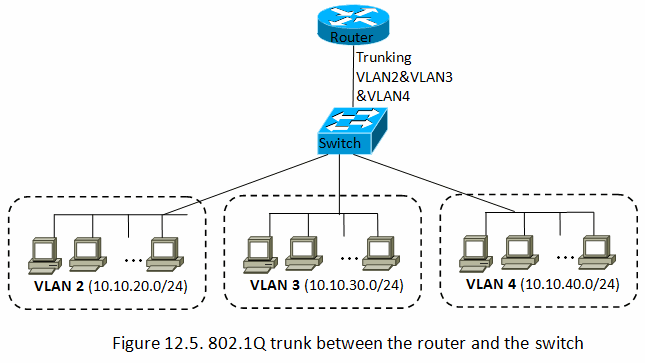


Figure 4.2 : Trunking between Router and Switch

**RESULT**:

Two VLANs have been setup using Switch and its working has been verified.