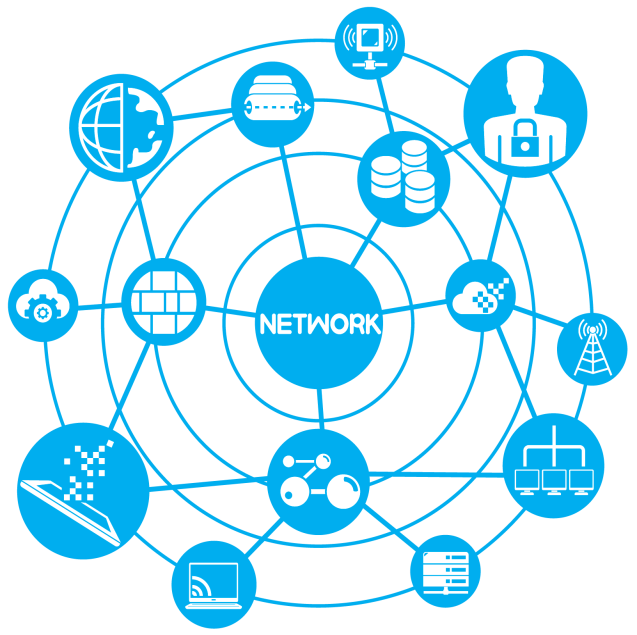
**Chapter-1**

**INTRODUCTION**

**Network**

Networks are everywhere—or so it seems. You can hardly do anything with data that does not involve a network. Like the human networks that we areall part of, computer networks let us share information and resources. In business,the reliance on networks is even more pervasive than in homes or schools



Networks help individuals and businesses alike save money, but they also help Create income. Without a doubt, networking within the home will catch on over the next few years as it has in business. Soon, nearly all individuals in even moderately developed nations will have networked components throughout their Homes. Those that don’t will be etiologically disadvantaged because they will not be able to learn or to function at the same level as those who are networked.

In this chapter, you’ll begin by relating networks to situations and concepts you already know. Once you have a basic understanding of what networks are and what they can do, it helps if you can actually begin working with them. In Fact, it is so helpful to learn the ropes of networking through hands-on guided Practice that that’s what is planned for you here. You will play the role of an Employee in a fictional company and you’ll have to learn on the job. The more youbecomethe person, the more you will learn about the need for and operation of computer Networks.

**Computer Networks**

A computer network is an interconnected collection of autonomous computers that communicate with one another using sets of rules known as protocols. Interconnected means that the computers are capable of exchanging information via wired or wireless connections. Autonomous means that the computers must



Function independently, i.e. there is no master/slave relationship where one computer controls another. Computer networking enables computers to share data, application software and hardware devices. The most basic network consists of two computers connected directly by cable, for example sharing resources, such as printers and modems. Any computer capable of communicating on the network is known as a device or node.

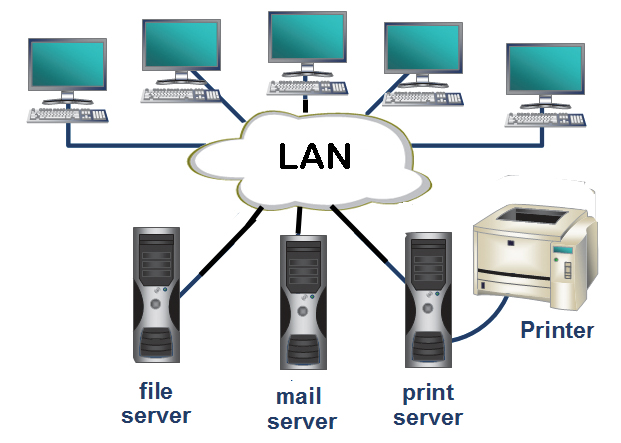
**Chapter 2**

**Categories of Networks**

**Local Area Network**

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually, LAN covers an organization offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

LAN provides a useful way of sharing the resources between end users. The resources such as printers, file servers, scanners, and internet are easily sharable among computers



LANs are composed of inexpensive networking and routing equipment. It may contain local servers serving file storage and other locally shared applications.

It mostly operates on private IP addresses and does not involve heavy routing. LAN works under its own local domain and controlled centrally. LAN uses either Ethernet or Token-ring technology. Ethernet is most widely employed LAN technology and uses Star topology, while Token-ring is rarely seen. LAN can be wired, wireless, or in both forms at once.

**Categories of LAN Networks**

**Personal Area Network**

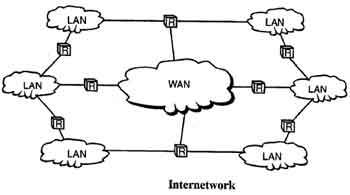
A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers, and TV remotes.



For example, Pico net is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

**Internetwork**

A network of networks is called an internetwork, or simply the internet. It is the largest network in existence on this planet. The internet hugely connects all WANs and it can have connection to LANs and Home networks.



Internet uses TCP/IP protocol suite and uses IP as its addressing protocol. Present day, Internet is widely implemented using IPv4. Because of shortage of address spaces, it is gradually migrating from IPv4 to IPv6.

Internet enables its users to share and access enormous amount of information worldwide. It uses WWW, FTP, email services, audio, and video streaming etc. At huge level, internet works on Client-Server model.

Internet uses very high speed backbone of fiber optics. To inter-connect various continents, fibers are laid under sea known to us as submarine communication cable.

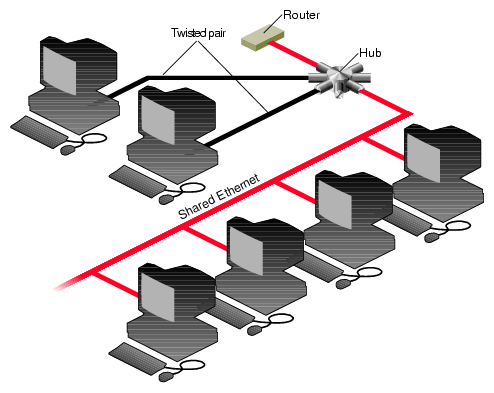
Internet is widely deployed on World Wide Web services using HTML linked pages and is accessible by client software known as Web Browsers. When a user requests a page using some web browser located on some Web Server anywhere in the world, the Web Server responds with the proper HTML page. The communication delay is very low.

Internet is serving many proposes and is involved in many aspects of life. Some of them are:

**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.

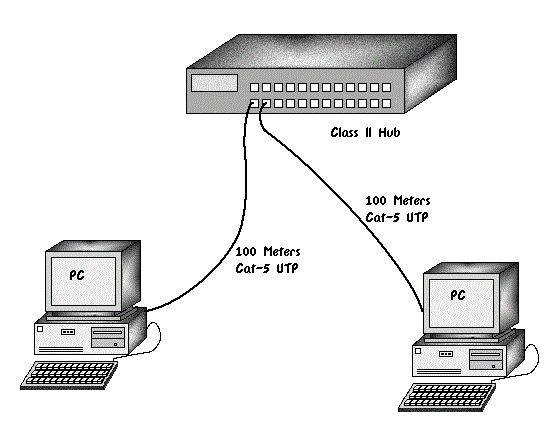


Ethernet connector is network interface card equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet.

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-45 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 100MBPS. 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 100MBPS 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 retained its high speed status only for three years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 mbits/seconds. IEEE802.3ab standardizes Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.

**Virtual LAN**

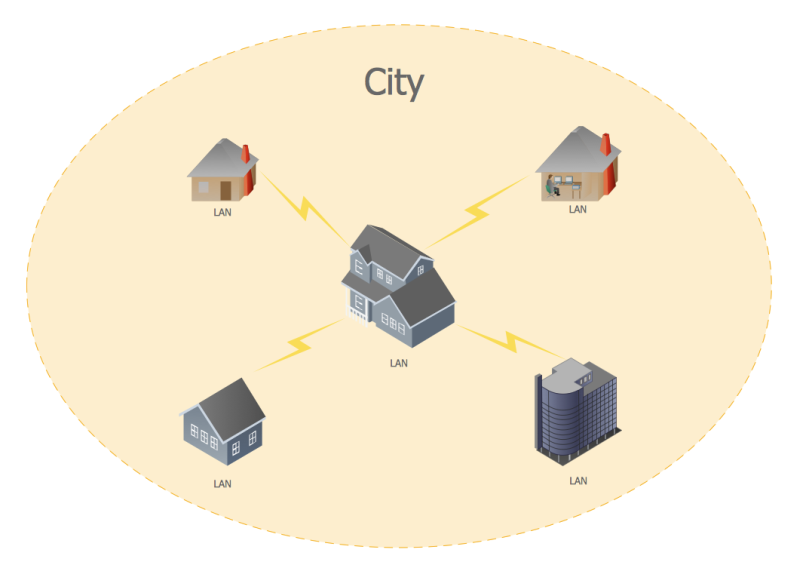
LAN uses Ethernet which in turn works on shared media. Shared media in Ethernet create one single Broadcast domain and one single Collision domain. Introduction of switches to Ethernet has removed single collision domain issue and each device connected to switch works in its separate collision domain. 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. 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.

**Metropolitan Area Network**

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city

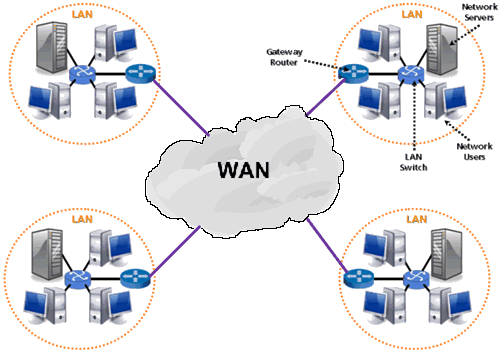


Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet

**Categories of MAN Networks**

**Wide Area Network**

As the name suggests, the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment



WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administrations

**WAN Connection Type**

WANs are generally grouped into three separate connection types:

* Point-to-Point technologies
* Circuit-switched technologies
* Packet-switched technologies

**Point-to-Point technologies**

Point-to-Point technologies (often called dedicated or leased lines) are usually the most expensive form of WAN technology. Point-to-Point technologies are leased from a service provider, and provide guaranteed bandwidth from location to another (hence point-to-point). Cost is determined by the distance of the connection, and the amount of bandwidth allocated. Generally, point-to-point links require no call-setup, and the connection is usually always on. Examples of point-to-point technologies include

* T1 lines
* T3 lines

**Circuit-switched technologies**

Circuit-Switched technologies require call-setup to occur before Information can be transferred. The session is usually torn down once data transfer is complete (this is identified as an On-Demand Circuit). Circuit switched lines are generally low-speed compared to point-to-point lines.

**Examples**: circuit-switched technologies include

* Dial-up
* ISDN

**Packet-switched technologies**

Packet-Switched technologies share a common infrastructure between all the provider’s subscribers. Thus, bandwidth *is* not guaranteed, but is instead allocated on a best effort basis. Packet-switched technologies are ill-suited for applications that require consistent bandwidth, but are considerably less expensive than dedicated point-to-point lines.

**Examples** of packet-switched technologies include

* Frame-Relay
* X25

**Chapter 3**

**NETWORK TOPOLOGY**

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically. Physical Topologyis the placement of the various components of a network, including device location and cable installation,

While logical topologyillustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

An example is a local area network (LAN). Any given node in the LAN has one or more physical links to other devices in the network; Graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines theological topology of the network.

**Topology**

Two basic categories of network topologies exist, physical topologies and logical topologies.

**Physical Topologies**

The cabling layout used to link devices is the physical topology of the network. This refers to the layout of cabling,

The locations of nodes, and the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or Fault Tolerance desired, and the cost associated with cabling or telecommunications circuits.

**OR**

Physical topology is called local area network (LAN) Topology,

LAN Topologies Four LAN topologies exist

• Star (Hub-and-Spoke)

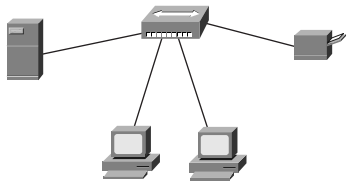
• Ring

• Bus

• Tree

**Star (Hub-and-Spoke) Topology**

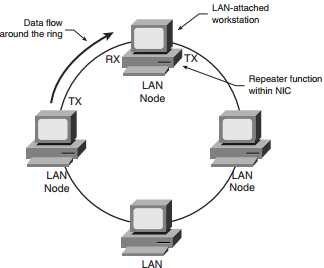
All stations are attached by cable to a central point, usually a wiring hub or other device operating in a similar function. Several different cable types can be used for this point-to-point link, such as shielded twisted-pair (STP), unshielded twisted-pair (UTP), and fiber-optic cabling. Wireless media can also be used for communications links. The advantage of the star topology is that no cable segment is a single point of failure impacting the entire network. This allows for better management of the LAN. If one of the cables develops a problem, only that LAN-attached station is affected; all other stations remain operational. The disadvantage of a star (hub-and-spoke) topology is the central hub device. This central hub is a single point-of-failure in that if it fails, every attached station is out of service. These central hubs, or concentrators, have changed over the years. Today, it is common to deploy hubs with built-in redundancy. Such redundancy is designed to isolate a faulty or failed component, such as the backplane or power supply. Figure is an example of a star (hub-and-spoke) topology.



This example demonstrates a star topology with a file server, printer, and two workstations. If a cable to one of the workstations fails, the rest of the devices are unaffected unless they need to access resources from the “disconnected” device.

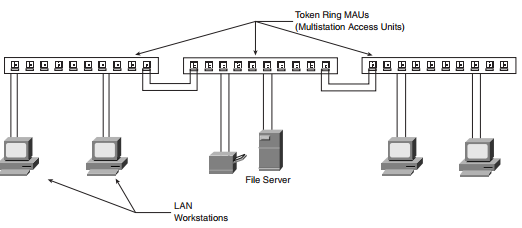
**Ring Topology**

All stations in a ring topology are considered repeaters and are enclosed in a loop. Unlike the star (hub-and-spoke) topology, a ring topology has no end points. The repeater in this case is a function of the LAN-attached station’s network interface card (NIC). Because each NIC in a LAN-attached station is a repeater, each LAN station will repeat any signal that is on the network, regardless of whether it is destined for that particular station. If a LAN-attached station’s NIC fails to perform this repeater function, the entire network could come down. The NIC controller is capable of recognizing and handling the defective repeater and can pull itself off the ring, allowing the ring to stabilize and continue operating. Token Ring (IEEE 802.5) best represents a ring topology. Although the physical cabling is considered to be a star topology, Token Ring is a ring in logical topology, as demonstrated by the following figures. Although physical topology is a physical layer attribute, the media access method used at the data link layer determines the logical topology. Token Ring defines a logical ring and contention, as Ethernet defines a logical bus. Even when attached to a hub, when one Ethernet device transmits, everyone hears the transmission, just as though on a bus. Figures are examples of ring topologies.

****

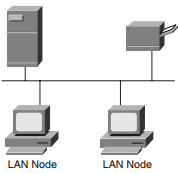
Fiber Data Distributed Interface (FDDI) is another example of a ring topology implementation. Like Token Ring, FDDI rings are physically cabled in a star topology. FDDI stations can be configured either as a single attachment station (SAS) or as a dual attachment station (DAS). SASs is connected to one of the two

FDDI rings, whereas DASs are connected to both rings via an A and B port on the FDDI stations and concentrator. Token Ring and FDDI LANs will be discussed in greater detail in Chapters 6, “Token Ring/ IEEE 802.5,” and 7, “FDDI.”

****

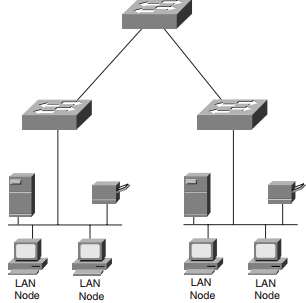
**Bus Topology**

Sometimes referred to as linear-bus topology, Bus is a simple design that utilizes a single length of cable, also known as the medium, with directly attached LAN stations. All stations share this cable segment. Every station on this segment sees transmissions from every other station on the cable segment; this is known as a broadcast medium. The LAN attachment stations are definite endpoints to the cable segment and are known as bus network termination points. This single cable segment lends itself to being a single point of failure. If the cable is broken, no LAN station will have connectivity or the ability to transmit and receive. Ethernet (IEEE 802.3) best represents this topology. Ethernet has the ability to utilize many different cable schemes. Further discussion of Ethernet and these cable schemes will be found in greater detail in Figure is an example of a bus topology



**Tree Topology**

The tree topology is a logical extension of the bus topology and could be described as multiple interconnected bus networks. The physical (cable) plant is known as a branching tree with all stations attached to it. The tree begins at the root, the pinnacle point, and expands to the network endpoints. This topology allows a network to expand dynamically with only one active data path between any two network endpoints. A tree topology network is one that does not employ loops in its topology. An example of a tree topology network is a bridged or switched network running the spanning tree algorithm, usually found with Ethernet (IEEE 802.3) networks. The spanning tree algorithm disables loops in what would otherwise be a looped topology. Spanning tree expands through the network and ensures that only one active path exists between any two LAN-attached stations. Figure is an example of a tree topology



**Chapter 4**

**Network Devices**

The four primary devices used in LANs are as follows:

• Hubs

• Bridges

• Switches

• Routers

Respective to the OSI model, these devices operate at the following layers:

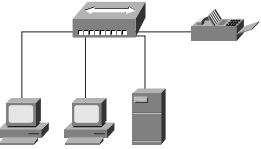
• OSI Layer 1 (physical)—Hubs, repeaters (hubs are considered to be multiport repeaters)

• OSI Layer 2 (data link)—Bridges, switches

• OSI Layer 3 (network)—Routers

**Hubs**

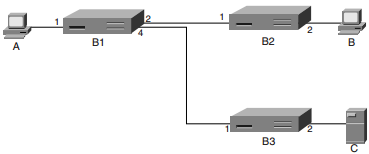
Hubs operate at the physical layer (Layer 1) of the OSI model. A hub is used to connect devices so that they are on one shared LAN, as shown in Figure 2-9. Because only two devices can be directly connected with LAN cables, a hub is needed to interconnect two or more devices on a single LAN. The cable termination points are the hub and the LAN device (host).

****

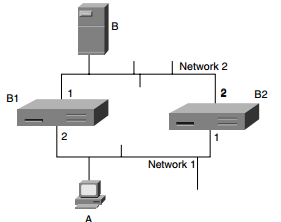
Ethernet hubs are not “smart” devices; hubs send all the data from a network device on one port to all other hub ports. When network devices are connected via a hub, LAN-attached devices will hear all conversations across the LAN. Each station then examines the message header to determine if it is the intended recipient. If more than one LAN station transmits at the same time, a collision occurs and both stations initiate a back off algorithm before attempting retransmission. This type of operation is also known as contention. All devices attached to the hub are said to be in a single collision domain. Backbone hubs are hubs deployed to connect other hubs to a single termination, or root, point. This is known as a multitier design and is illustrated in Figure

**Bridges**

This section focuses on transparent bridges, which can also be referred to as learning or Ethernet bridges. Bridges have a physical layer (Layer 1), but are said to operate at the data link layer (Layer 2) of the OSI model. Bridges forward data frames based on the destination MAC address. Bridges also forward frames based on frame header information. Bridges create multiple collision domains and are generally deployed to provide more useable bandwidth. Bridges don’t stop broadcast traffic; they forward broadcast traffic out every port of each bridge device. Each port on a bridge has a separate bandwidth (collision) domain, but all ports are on the same broadcast domain. Bridges were also deployed in complex environments, which is where broadcast storms became such a problem. Routers were added to the complex bridged environments to control broadcasts. Later, VLANs were devised when switches were deployed in enterprise environments and brought back the old problem of broadcast storms.



The original all-ports broadcast of A’s first frame to B ensures that B3 knows how to send to frames to A. An attempt by C to communicate with B results in B3 broadcasting the frame on all ports (except number 2), so the frame reaches B1 on port 4. While B1 forwards this frame to B2, it also learns what to do with frames destined for C. Unfortunately; this simple and elegant arrangement breaks down disastrously if loops are in the network. Consider the following arrangement. Figure is an example of a looped bridge network.



Suppose host A has just booted up and wants to communicate with B. A’s initial frame will be seen on both Bridge 1’s (B1) port 1 and Bridge 2’s (B2) port 2, so both bridges know that host A is on network 1. The frame is then transmitted onto network 2 by B1 on port 2 and by B2 on port 1. One of the bridges will transmit it first—suppose it is B1—and then B2 will see a frame from A on its network 2 port 1. It will now update its table as to the location of A and retransmit the frame on network 1. B1 sees this frame and does not know that it’s a duplicate, so it retransmits it on network 2. From there, B2 retransmits it on network 1, and so on indefinitely. Adding a third bridge to this two-network scenario makes things exponentially more complicated. This is clearly unsatisfactory. Prohibiting loops is an unrealistic target. Practical bridges use a method known as the spanning tree algorithm to construct an effective non-looping topology by deciding not to use certain links in the network. It is also possible to reconfigure this network dynamically. Bridges interchange special messages known as configuration messages. The spanning tree algorithm (IEEE 802.1) uses BPDUs. The bridge configuration message contains enough information to enable the bridges to do the following:

Elect a single bridge from among all the connected bridges to be the “root” bridge.

• Calculate the least cost path to the “root” bridge from each bridge.

• For each LAN, identify a “designated bridge” on that LAN that will be used for forwarding frames toward the root.

• Choose a port on each bridge that gives the best path toward the root.

• Select ports to be included in the spanning tree.

The effective topology after construction of the spanning tree is loop free; this is achieved by effectively choosing not to use certain links between bridges. The links are still there and might come into use if the network is reconfigured. Configuration messages are sent to a special multicast MAC address, meaning all bridges that use the binary SAP value 01000010. Configuration messages are autonomously originated by bridges, but they are not forwarded by bridges. A configuration message contains four pieces of information:

• The ID of the bridge assumed to be root.

• The ID of the bridge transmitting the message.

• The cost of the least cost-known path from the transmitting bridge to the assumed root.

• The port number on which the message was transmitted.

A bridge initially assumes itself to be the root, with a path cost of zero. For each bridge port, a bridge will receive incoming configuration messages from other bridges on the LAN connected to that same port. For each port, the bridge will remember the lowest cost Topologies configuration message.

**Types of Bridging**

Following is a discussion of the four types of bridging:

• Transparent bridging

• Source-route bridging

• Source-route translational, or mixed-media, bridging

• Source-route transparent bridging

**Transparent Bridging**

Transparent bridging is so named because its operation is transparent to the network hosts. When a host on a remote LAN sends data to a specific destination, it does not look to see where on the bridging LAN the data is. The transparent bridge will read the source frames and forward the data, as discussed earlier. The major difference between the tables built by bridges and the tables built by routers (Layer 3 devices) is that bridge tables are based on the MAC addresses, whereas routers build their tables based on the network addresses. Transparent bridges build their tables independently of each other, rather than exchange information like routers. Each bridge learns different MAC addresses by associating the source addresses of transmitted frames with the port on which the frame arrived into the bridge. Each entry in this bridge table has a maximum age associated with it. If this maximum age timer is exceeded—meaning that no traffic has originated from that port within the defined timeframe—the entry is flushed out of the table. A discussion of bridge states can be found later in this chapter, in the section “Spanning Tree Topology

**Source-Route Bridging**

In a source-route bridged (SRB) network, frames are sent with the complete source-to destination path included. Source-route bridges check frames for destination information and store and forward as appropriate. The source will make the forwarding choice based on configurable source-route bridging metrics. 0390.book Page 31 Wednesday, November 14, 2001 3:28 PM 32 Chapter 2: LAN Topologies In an SRB network, end systems, or hosts, send an explorer frame to the network to find a path from source to destination prior to sending data. The source-route bridges are responsible for adding the path information to these explorer frames and making sure they are passed to and from the appropriate end systems. In addition to passing these explorer frames, source-route bridges also store this routing information in what is called a RIF cache. Source-route bridges look into a Token-Ring frame and determine whether routing information exists by checking the routing information indicator (RII) bit. The bridges then add the RII bit ring and bridge information to the routing descriptor (RD) field, also called the routing information field (RIF) or RI field. Unlike transparent bridges, source-route bridges do not build and maintain tables of MAC addresses and associated ports. Instead, source-route bridges examine the contents of each Token-Ring frame as follows

1. Source-route bridges start by examining the first bit of a Token-Ring frame’s source address to see if the value is a zero or a one. This first bit is the RII. The source host of the frame sets the value of the RII.
2. If the RII is set to zero, no source-route information exists in the Token-Ring frame.
3. If the RII is set to one, source-route information exists within the Token-Ring frame and resides in the RIF. Three types of explorer frames are found in a source-route bridged network: local explorers, all-routes explorers, and spanning tree explorers.
4. Local explorers are used with local source-route bridged networks. Local source route bridging directly connects two or more Token-Ring networks. Bridged traffic does not cross non-Token media.
5. All-paths explorers, as the name implies, take all possible paths on their way to the destination. The amount of traffic generated by all-paths explorers could be considerable in a complex network, which is not good.
6. Spanning tree explorers solve the problem of the all-paths explorer by sending packets only to branches in the spanning tree. The network administrator can statically assign which interfaces will forward spanning tree explorer frames and which interfaces will block them. The network administrator can also use the spanning tree algorithm to automatically set a single route explorer.

**Source-Route Translational, or Mixed-Media, Bridging**

Source-route translational bridging (SR/TLB) is used when connecting two networks that are running different types of bridging technologies; the most common are Ethernet and Token-Ring. SR/TLB is implemented to perform several functions:

• Overcome MTU and frame format differences between Ethernet and Token Ring.

• Reconcile differences between Token-Ring frames (which contain RIFs) and Ethernet frames (which never contain RIFs) by using Source-route translational bridging.

• Resolve the formatting differences between Ethernet and Token Ring. Token Ring addresses are in non-canonical format; Ethernet addresses are in canonical format

Source-route translational bridging assures that all these differences are resolved when forwarding frames from Token Ring to Ethernet and Ethernet to Token Ring.

**Switches**

LAN switches are used to connect a common broadcast domain (a hub). They are also used to provide frame-level filtering as well as dedicated port speed to specific end users. Some switches have limited routing capabilities and can provide Layer 3 routing functions at the most basic level. Some of the major benefits of using switches in a network are higher bandwidth to the desktop and ease of configuration. Switches are being deployed more often to replace hubs and bridges as more bandwidth-intensive applications are being implemented at all levels of an organization.

**Switch Operations**

The following discussion focuses on Ethernet switches. The switches transfer data on a network by receiving data frames from a source port and forwarding them out to the destination through a different port on the switch based on the frame information. Like transparent bridges, Layer 2 Ethernet switching works by looking at the MAC addressing information in the data frame’s header and forwarding the data according to the switch, or Content Addressable Memory (CAM), table information. If the switch looks at the MAC addressing information and still doesn’t know from which port to send out the frames, it will broadcast the frames out all of the switch ports. This is known as flooding, and it is used to determine the destination. After the destination address is found, the information is added to the switching table. Switches work by providing dedicated bandwidth per port to an end user or application. Switches allow fewer users in each network segment, and they provide dedicated bandwidth, which is increasingly important with graphics and multimedia applications. Deploying LAN switches in an existing network environment requires minimal configuration and little or no changes to existing wiring closets, hubs, LAN cabling, or NICs. Switches allow network users the ability to transfer data traffic in a network environment free of collisions and bandwidth contention. Several types of switching technologies enable quick and scalable network transmission.

**Routers**

Routers are not usually active in simple LAN environments because routers are WAN devices. Routers are typically found at the edge of a LAN, interfacing with a WAN. Routers operate at the network layer (Layer 3) of the OSI model. Broadcast containment and security are needed in more complex environments.

**Source-Route Transparent Bridging**

Source-route transparent (SRT) bridging is a bridge that wills either source-route Bridge or transparent bridge a Token-Ring frame. The RII value makes this determination to either source-route or transparently bridge the frame.

• If the RII value is zero, the frame will be transparently bridged.

• If the RII value is one, the frame will be source-route bridged.

**Logical Topology**

In contrast, logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the Physical interconnection of the devices, Logical topologies

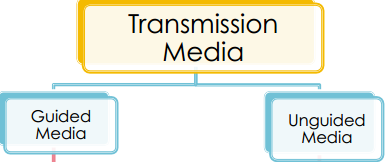
Are often closely associated with media access control methods and protocols. Some networks are able to dynamically change their logical topology through configuration changes to their routers and switches.

**Chapter 5**

**Transmission media**

**Transmission media**

Transmission mediais a pathway that carries the information from sender to receiver. We use different types of cables or waves to transmit data. Data is transmitted normally through electrical or electromagnetic signals. An electrical signal is in the form of current. An electromagnetic signal is series of electromagnetic energy pulses at various frequencies. These signals can be transmitted through copper wires, optical fibers, atmosphere, water and vacuum Different Medias have different properties like bandwidth, delay, cost and ease of installation and maintenance. Transmission media is also called Communicationchannel.



Types of Transmission Media

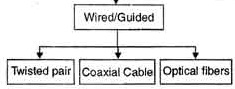
Transmission media is broadly classified into two groups.

**1.** Wired or Guided Media or Bound Transmission Media

2. Wireless or Unguided Media or Unbound Transmission Media

1. Wired or Guided Media or Bound Transmission Media

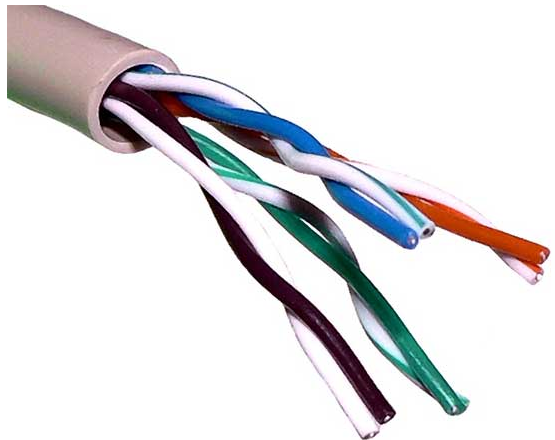
Wired or Guided Media or BoundTransmission Media Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography.



Popular [bound transmission media](http://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-bound-transmission-media-type-of-bound-transmission-media-explain) in use are twisted pair cable, co-axial cable and fiber optical cable. Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

**Twisted pair cable**

A twisted pair cable is made of two plastic insulated copper wires twisted together to form a single media. Out of these two wires, only one carries actual signal and another is used for ground reference. The twists between wires are helpful in reducing noise (electro-magnetic interference) and crosstalk.



There are two types of twisted pair cables:

* Shielded Twisted Pair (STP) Cable
* Unshielded Twisted Pair (UTP) Cable

**Shielded Twisted Pair (STP) Cable**

STP cables comes with twisted wire pair covered in metal foil. This makes it more indifferent to noise and crosstalk.

**Unshielded Twisted Pair (UTP) Cable**

UTP has seven categories, each suitable for specific use. In computer networks, Cat-5, Cat-5e, and Cat-6 cables are mostly used. UTP cables are connected by RJ45 connectors.

**Unshielded Twisted Pair** (UTP) cable is most certainly by far the most popularcable around the world. UTP cable is used not only for networking but also for the traditional telephone (UTP-Cat 1**).** There are seven different types of UTPcategories**a**nd, depending on what you want to achieve, you would need the appropriate type of cable. UTP-CAT5e is the most popular UTP cable which came to replace the old coaxial cable that was not able to keep up with the constant growing need for faster and more reliable networks.

**CHARACTERISTICS OF UTP**

The characteristics of UTP are very good and make it easy to work with, install, expand and troubleshoot and we are going to look at the different wiring schemes available for UTP, how to create a straight through UTP cable, rules for safe operation and a lot of other cool stuff! So let's have a quick look at each of the UTP categories available today along with their specifications.

**Category 1/2/3/4/5/6/7** – 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). In Datacenters for backbone connections between servers, network switches and storage devices

**Electronic Industries Association** (EIA), **Telecommunications Industries Association** (TIA) and **American National Standards Institute** (ANSI) are the organizations which have defined standards for Unshielded Twisted Pair Cables (UTP) cabling. The ANSI/EIA/ The 568 commercial Building Wiring Standards define various types of cables to be used for various purposes. The cables are divided into different categories namely.

**Category 1** - Defines a traditional UTP cable. It is designed to carry only voice and not data. This type of cable is not recommended for networking purposes and is used in telephony services.

**Category 2** - Defines a cable that can carry data up to 4 Mbps. It consists of 4 pairs of wires.

**Category 3** - Defines a cable that can carry data up to 10 Mbps. It consists of 4 pairs of wires. It is 1000 feet in length with marks of length at every 2 Feet. The frequency of this cable is 16 MHz it’s used for 10Base T network.

**Category 4** - Defines a cable that can carry data up to 16 Mbps. It cable consists of 4 pairs of wires. The signaling frequency of this cable is up to 20 MHz

**Category 5**-Defines a cable that can carry data up to 100 Mbps. The signaling frequency of this cable is up to 100 MHz this type of cable is primarily used in today's networking environment. The cable is used in 100baseX. Ethernet architecture and Asynchronous Transfer Mode (ATM) architectures.

**Category 5e** - Defines a cable that can carry data up to 1000 Mbps with a signaling frequency of 100 MHz it is used to connect computers, hubs, switches and print servers.

**Category 6**- Defines a 4-pair cable that provides an improved performance as compared to Cat 5e. Data is transferred at the rate of 1000Mbps with a signaling frequency of 250 MHz

**Category 7** - Defines a fully shielded twisted pair cable that operates at the signal frequency of 600 MHz Fully shielded means all the four pairs of a cable have additional shield over them. MBps stands for Mega Bytes per second and Mbps stands for Mega Bits per second. Both terms are different as 1 Byte = 8 Bits.

**Advantages of Unshielded Twisted Pair Cables (UTP)**

• Cheapest form of cable available for networking purposes.

• Easy to handle and install.

**Disadvantages of Unshielded Twisted Pair Cables (UTP)**

• Highly prone to external interference like EMI and RFI.

• Highly prone to crosstalk.

• Unable to provide secured transmission of data

**Coaxial Cable**

Coaxial cable has two wires of copper. The core wire lies in the center and it is made of solid conductor. The core is enclosed in an insulating sheath. The second wire is wrapped around over the sheath and that too in turn encased by insulator sheath. This all is covered by plastic cover.



Because of its structure, the coax cable is capable of carrying high frequency signals than that of twisted pair cable. The wrapped structure provides it a good shield against noise and cross talk. Coaxial cables provide high bandwidth rates of up to 450 mbps.

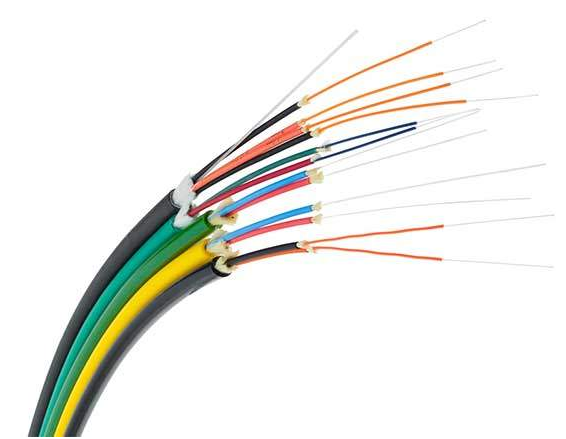
There are three categories of coax cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), RG-11 (Thick Ethernet). RG stands for Radio Government.

Cables are connected using BNC connector and BNC-T. BNC terminator is used to terminate the wire at the far ends

**Optical fiber**

Fiber Optic works on the properties of light. When light ray hits at critical angle it tends to refracts at 90 degree. This property has been used in fiber optic. The core of fiber optic cable is made of high quality glass or plastic. From one end of it light is emitted, it travels through it and at the other end light detector detects light stream and converts it to electric data.

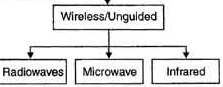
Fiber Optic provides the highest mode of speed. It comes in two modes; one is single mode fiber and second is multimode fiber. Single mode fiber can carry a single ray of light whereas multimode is capable of carrying multiple beams of light.



Fiber Optic also comes in unidirectional and bidirectional capabilities. To connect and access fiber optic special type of connectors are used. These can be Subscriber Channel (SC), Straight Tip (ST), or MT-RJ.

**Wireless or Unguided Media or** **Unbound Transmission Media:**

Unbound transmission media are the ways of transmitting data without using any cables. These media are not bounded by physical geography. This type of transmission is called Wireless communication. Nowadays wireless communication is becoming popular.



Wireless LANs are being installed in office and college campuses. This transmission uses Microwave, Radio wave, Infra-red are some of popular unbound transmission media.

**Radio waves,**

Radio waves also called radio waves as they were discovered by German physicist Heinrich Hertz in 1888 are electromagnetic waves, that is to say the combined oscillation of an electric field and a magnetic field. Radio waves, infrared, visible light, ultraviolet, X-rays or gamma rays are all examples of electromagnetic waves. It is a technique where data is transmitted using radio waves and therefore energy travels through the air rather than copper or glass. Conceptually, radio, TV, cellular phones etc. uses radio transmission in one form or another. The radio waves can travel through walls and through an entire building. Depending upon the frequency, they can travel long distance or short distance. Satellite relay is the one example of long distance communication.

Therefore, each frequency range is divided into different bands, which has a specific range of frequencies in the radio frequency, (RF) spectrum. The RF is divided in different ranges starting from very low frequencies (VLF) to extremely high frequencies (EHF). Two transmitters cannot share the same frequency band because of mutual interference and therefore band usage is regulated. International use of the radio spectrum is regulated by the International Telecommunication Union (ITU). Domestic use of the radio spectrum is regulated by national agencies such as Wireless Planning and Coordination (WPC) in India. WPC assigns each transmission source a band of operation, a transmitter radiation pattern, and a maximum transmitter power.

Omni-directional or directional antennas are used to broadcast radio waves depending upon band. The transceiver unit, which comprises transmitter and receiver along with the antenna, determines the power of RF signal. Other characteristics of radio waves is that in vacuum all electromagnetic waves or radio waves travel at the same speed, i.e. at the speed of light which is equal to 3 x l08·meter per second. In any medium this speed gets reduced and also becomes frequency dependent. In case of copper the speed of light becomes approximately two-thirds of the speed of light.

**The basic features of the radio waves are that:**

 • They are easy to generate

• They have same velocity in vacuum

• They may traverse long distances

• They are Omni-directional

• They can penetrate building easily so they find extensive use in communication both indoor and outdoor

• They are frequency dependent. At low frequency they can pass through obstacles well but the power falls off sharply with distance from the source, as power is inversely proportional to cube of the distance from the source. At HF they travel in straight lines and bounce off obstacles.

**Microwave Transmission**

Microwave transmission also requires line of sight in order to work properly. In order to allow two way communications two frequencies are used. However, this does not mean that there has to be two antennas because the frequencies can be dealt with by one antenna at both ends.The distance covered by microwave signals is based upon the height of the antenna. In order to increase this coverage each antenna has a built-in repeater that regenerates the signal before passing it on to the next antenna in line. The placement of the antenna to do this is approximately 25 miles. The main drawback of microwave signals is that they can be affected by weather, especially rain.



**Microwave transmission relies on three key elements:**

* Use of radio frequency to achieve the transmissions (operating between 1Ghz to 170Ghz)
* Clear line-of-sight with no obstacles in the way
* Regular relay stations required due to line of site and cost considerations

**Advantages:**

* No cables needed
* Multiple channels available
* Wide bandwidth

**Disadvantages:**

* Line-of-sight will be disrupted if any obstacle, such as new buildings, are in the way
* Signal absorption by the atmosphere. Microwaves suffer from attenuation due to atmospheric conditions.
* Towers are expensive to build

**Infra-red**

Infrared light transmissions have existed for many years and their use having been limited to TV remote controls and wireless slide projector remote controls. However, they now are assuming a position of some, if still limited, importance. Infrared systems use the infrared light spectrum to send a focused light beam to a receiver, much, as would a microwave system, although no reflective dish is used. Rather, pair of lenses is used, with a focused lens employed in the transmitting device and a collective lens in the receiving device as shown in Figure. Infrared is an airwave, rather than a conducted transmission system. Although generally used in short-haul transmission, they do offer substantial bandwidth, but with risks of interference.

**Advantages**

Infrared waves are very helpful in medical treatments like some chronic health problems, such as high blood pressure, congestive heart failure and rheumatoid arthritis it is also used in most cameras for night vision

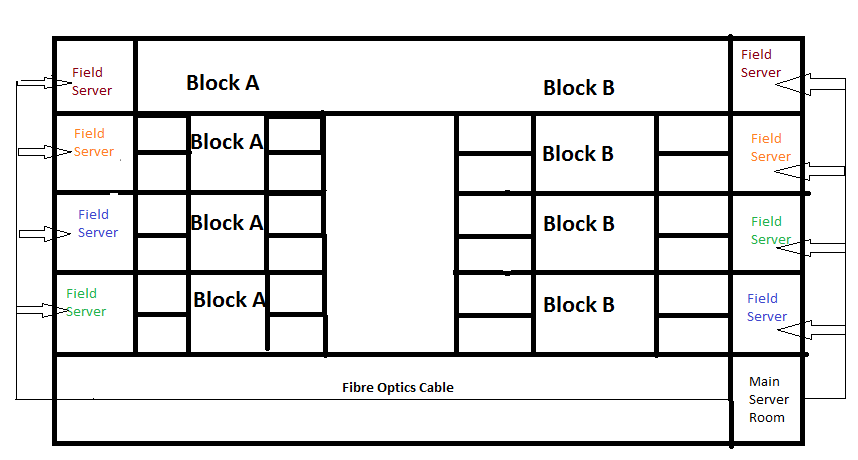
**Disadvantages**

The transmitters and receivers must be closely aligned to communicate by being directly in sight of Each other Plus; the Performance will drop off if the distance to the receiver is out of range for the infrared device and with large areas it require multiple emitter panels

**CHAPTER -6**

**NETWORK ESTBLISHMENT**

The Network was established in Academic Block -3 of **Central UNIVERSITY HARYANA.** This block is divided in four floors, all floors dived two (A & B) parts, my project work is LAN networking establishment in Block- 3. My work is properly LAN establishment. I establish LAN network properly completed in this building all floors .In this building mostly all departments are professionally worked. All student and faculty needs LAN network for prepration.In this building establishment eight server, Figure according are as follows as,



And all server is connected is main server by physically. This building is divided two type server.

* **Main server**
* **Field server**

**Main server**

Main server is main. All building networks is center is main server so it is called server main server is proper working/sending data in field server and field server transfer to department and class . Most point is hear server Room all components deferent and High speed compared field server like switch 32 port (P.O.E- Power over Ethernet )type use in server room. This server room design use component is as follows.

* Switch
* Module
* Fiber patch code
* liu
* Duck cable
* Power supply

**Switch**

On a [network](http://www.computerhope.com/jargon/n/network.htm), a switch is a [hardware](http://www.computerhope.com/jargon/h/hardware.htm) device that [filters](http://www.computerhope.com/jargon/f/filter.htm) and forwards network [packets](http://www.computerhope.com/jargon/p/packet.htm), but often not capable of much more. The first network device that was added to the Internet was a switch called the IMP, which helped send the first message on October 29, [1969](http://www.computerhope.com/history/1969.htm). A network switch is more advanced than a [hub](http://www.computerhope.com/jargon/h/hub.htm) but not as advanced as a [router](http://www.computerhope.com/jargon/r/router.htm). Here my project use 32 & 24 port switch use but main server uses 32 ports (POE- power over Ethernet) type switch use.

And felid server use 24 port (POE- power over Ethernet) type switch use.

**Module**

* In software, a module is a part of a program. Programs are composed of one or more independently developed modules that are not combined until the program is linked. A single module can contain one or several routines
* In hardware, a module is a self-contained component

**Fiber patch code**

A technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber opticcable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves. ... Fiber optic cables have a much greater bandwidth than metal cables.

**l i u**

Fiber Patch Panel (**LIU**) Light interface units are extensively used for wired communication networks. The LIUs are used for routing, terminating and managing optical cable terminations. These light interface units can be wall mounted or rack mounted for ease of use.

**Duck cable**

A technology that use to transmit data two switch or simple words we can say that switch looping.

**Power supply**

Also called a power supply unit or PSU, the component that supplies power to a computer. Most personal computers can be plugged into standard electrical outlets. The power supply then pulls the required amount of electricity and converts the AC current to DC current.

**Field server**

This type server is small server .and this server mostly use department and class. This server and main server difference are as:

This server room is cat-6 patch code use and severs room this type cable is not use (cat-6 use transmission Ethernet switch to jack panel) here use component are as follows

* Switch
* Patch code male connecter (cat-6)
* LIU (light interface unit )
* Jack panel
* IO( female type)
* Duck cable
* Fiber patch code
* Module

**Patch code (cat-6)**

A patch cable or patch cord or patch lead is an [electrical](https://en.wikipedia.org/wiki/Electric) or [optical](https://en.wikipedia.org/wiki/Optical) [cable](https://en.wikipedia.org/wiki/Cable) used to connect ("patch-in") one electronic or optical device to another for [signal](https://en.wiktionary.org/wiki/signal) routing. Devices of different types (e.g., a switch connected to a computer, or a switch to a router) are connected with patch cords.

**Jack panel**

A patch panel in a local area network (LAN) is a mounted hardware assembly that contains ports used to connect and manage incoming and outgoing LAN cables.Patch panels are also referred to as patch bays, patch fields or jack fields and are also commonly used in radio and television.

**IO (female type)**

Short for input/output (pronounced "eye-oh"). The term I/O is used to describe any program, operation or device that transfers data to or from a computer and to or from a peripheral device. ... Devices such as keyboards and mouse are input-only devices while devices such as printers are output-only.

**Module**

His guide explains how to install the 16- and 36-port Ethernet switch network modules. The Ethernet switch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The 16-port Ethernet switch network module has 16 10/100BASE-TX ports and an optional 10/100/1000BASE-T Gigabit Ethernet port. The 36-port Ethernet switch network module has 36 10/100BASE-TX ports and 2 optional 10/100/1000BASE-T Gigabit Ethernet ports. The 36-port Ethernet switch network module requires a double-wide slot. An optional power module can also be added to provide inline power for IP telephones.

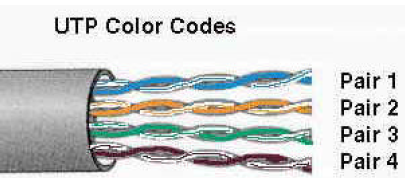
The10/100BASE-TX ports and Gigabit Ethernet ports on the Ethernet switch network module are connected to the network using RJ-45 connectors on the front panel. The power module is connected to an external power supply using a power connection cable

**Component Establishment**

Here this building LAN establishment starts fiber optics cable measurements. In this building LAN network establishment fast process. Then next step is cable tasting and all building cable measurements ‘and any errors detected process is as follows.

**Io punching**

This process is cat- 6 cable punching. This process is used to cat- 6 cables data transmission and produces. Here main process is color coding process color coding is must and main process. Color coding own set of rules of are as figure are as follows



**The cable pairs are color coded as**

Pair 1 - is white-blue/blue,

Pair 2- white-orange/orange,

Pair 3 - is white-green/green

Pair 4- is white-brown/brown.

**COLOR CODING**

**COLOR CODING IS TWO TYPE**

**A** & **B**

1. A color is furan country use
2. Use in Asian country

So my project is working in B types color coding. And am living in India

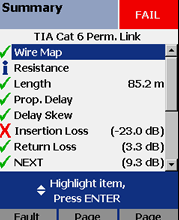
Do data center operators use color-coded cables? If so, what colors?

Represent which functions?   
Although many agreed that color coding could help administrators identify a cable, few agreed on what color should represent which function. Generally, it depended on what kind of facility it was. A telecommunications center would have different distinctions than say, a collocation facility.   
Here was one simple suggestion.

* Red cables ' to external connections.
* Yellow cables ' in the DMZ separating internal from external networks.
* Blue or green cables ' only for internal networks.

**Penta scanning**

Penta scanning process cable measurements and error testing throws are Problems/ error is detected its figure are shows as.



**Insertion loss**

In [telecommunications](https://en.wikipedia.org/wiki/Telecommunications), insertion loss is the loss of [signal](https://en.wikipedia.org/wiki/Signalling_(telecommunication)) [power](https://en.wikipedia.org/wiki/Power_(physics)) resulting from the insertion of a device in a [transmission line](https://en.wikipedia.org/wiki/Transmission_line) or [optical fiber](https://en.wikipedia.org/wiki/Optical_fiber) and is usually expressed in [decibels](https://en.wikipedia.org/wiki/Decibel) (dB).

**Return loss**

In telecommunications, return loss is the loss of power in the signal returned/reflected by a discontinuity in a transmission line or optical fiber. This discontinuity can be a mismatch with the terminating load or with a device inserted in the line. It is usually expressed as a ratio in decibels (dB);

**Write map**

Network mapping/write map is the study of the physical connectivity of networks e.g. the [Internet](https://en.wikipedia.org/wiki/Internet). Network mapping discovers the devices on the network and their connectivity. It is not to be confused with network discovery or [network enumerating](https://en.wikipedia.org/wiki/Network_enumeration) which discovers devices on the network and their characteristics such as ([operating system](https://en.wikipedia.org/wiki/Operating_system), open [ports](https://en.wikipedia.org/wiki/Computer_port_(software)), listening [network services](https://en.wikipedia.org/wiki/Network_service), etc.). The field of automated network mapping has taken on greater importance as networks become more dynamic and complex in nature.

**Resistance**

Resistance is the opposition that a substance offers to the flow of electric [current](http://searchcio-midmarket.techtarget.com/definition/current).  It is represented by the uppercase letter R.  The standard unit of resistance is the [ohm](http://whatis.techtarget.com/definition/ohm), sometimes written out as a word, and sometimes symbolized by the uppercase Greek letter omega.

**Length**

In transport terminology, network length (or, less often, system length) refers to the total length of a transport network, and commonly also refers to the length of any fixed infrastructure associated with the network.

**Prop. Delay**

In computer networks, propagation delay is the amount of time it takes for the head of the signal to travel from the sender to the receiver. It can be computed as the ratio between the link length and the propagation speed over the specific medium.

**Delay skew**

Delay skew is the difference in propagation delay between any two pairs within the same cable sheath

**Measurement**

All cable error and measurement and all data related information store in this process. All process is called penta scanning.

**Splicing**

Splicing is a process in which two items are joined together. Generally, one end of each of the two items is connected in order to achieve the joining

Here main joining fiber to picktal. Here main process fiber to picktal transmission.

All fiber-optic cables and connectors will be tested,

**CHAPTER 7**

**NETWORK** **TESTING**

Networking establishment is process of sequence of all process. But all sequence we testing network management .These process are as sequence follows .Splicing, penta scanning, cable measurement calculates than all cable + picktal test. Here all process like (splicing, penta scanning, and cable measurement) discusses previous chapter. But here only discusses testing. So all testing are as discusses in sequences.

**Cable measurement testing**

This process use main toll laser light. This light throw we see maximum 40km. so this process light testing or linking testing. All node clear than final switch and LIU arrangement (light interface unit) arrangement. Here link fiber patch code.

**Cable tester**

**Cable tester**

**Cable tester**

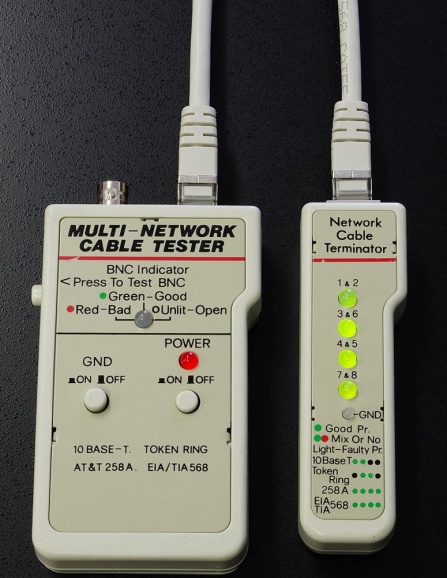
**Signal tester**

**Fiber optic tester**

**Basic cable tester**

**Basic cable tester**

Generally a basic cable tester is a battery operated portable instrument with a source of [electric current](https://en.wikipedia.org/wiki/Electric_current), one or more voltage indicators, and possibly a switching or scanning arrangement to check each of several conductors sequentially.



A cable tester may also have a microcontroller and a display to automate the testing process and show the testing results, especially for multiple-conductor cables. A cable tester may be connected to both ends of the cable at once, or the indication and current source portions may be separated to allow injection of a test current at one an of a cable and detection of the results at the distant end. Both portions of such a tester will have connectors compatible with the application, for example, [modular connectors](https://en.wikipedia.org/wiki/Modular_connector) for [Ethernet](https://en.wikipedia.org/wiki/Ethernet) [local area network](https://en.wikipedia.org/wiki/Local_area_network) cables.

**Cable tester**

A cable tester is used to verify that all of the intended connections exist and that there are no unintended connections in the cable being tested. When an intended connection is missing it is said to be "open". When an unintended connection exists it is said to be a "short" (a [short circuit](https://en.wikipedia.org/wiki/Short_circuit)). If a connection "goes to the wrong place" it is said to be "misfired" (the connection has two faults: it is open to the correct contact and shorted to an incorrect contact).



Generally, the testing is done in two phases. The first phase, called the "opens test" makes sure each of the intended connections is good. The second phase, called the "shorts test" makes sure there are no unintended connections.

There are two common ways to test a connection:

1. A [**continuity test**](https://en.wikipedia.org/wiki/Continuity_test). Current is passed down the connection. If there is current the connection is assumed to be good. This type of test can be done with a series combination of a battery (to provide the current) and a light bulb (that lights when there is a current).
2. A [**resistance**](https://en.wikipedia.org/wiki/Electrical_resistance)**test**. A known current is passed down the connection and the voltage that develops is measured. From the voltage and current the resistance of the connection can be calculated and compared to the expected value.

There are two common ways to test for a short:

1. A [low voltage](https://en.wikipedia.org/wiki/Low_voltage) test. A low power, low voltage source is connected between two conductors that should not be connected and the amount of current is measured. If there is no current the conductors are assumed to be well isolated.

A [high voltage](https://en.wikipedia.org/wiki/High_voltage) test. Again a voltage source is connected but this time the voltage is of several hundred volts. The increased voltage will make the test more likely to find connections that are nearly shorted since the higher voltage will cause the insulation of nearly shorted wires to break down.

**Signal tester**

More powerful cable testers can measure the properties of the cable relevant to signal transmission. These include the DC resistance of the cable, the loss of signal strength (attenuation) of a signal at one or more frequencies, and a measure of the isolation between multiple pairs of a multi-pair cable or [crosstalk](https://en.wikipedia.org/wiki/Crosstalk). While these instruments are several times the cost and complexity of basic continuity testers, these measurements may be required to [certify that](https://en.wikipedia.org/wiki/Copper_cable_certification) a cable installation meets the technical standards required for its use, for example, in local area network cabling.

**Splicing testing**

Fiber-optic cables might have to be spliced together for a number of reasons—for example, to realize a link of a particular length. Another reason might involve *backhoe fade*, in which case a fiber-optic cable might have been ripped apart due to trenching work. The network installer might have in his inventory several fiber-optic cables, but none long enough to satisfy the required link length. Situations such as this often arise because cable manufacturers offer cables in limited lengths—usually 1 to 6 km. A link of 10 km can be installed by splicing several fiber-optic cables together. The installer can then satisfy the distance requirement and avoid buying a new fiber-optic cable. Splices might be required at building entrances, wiring closets, couplers, and literally any intermediate point between a transmitter and receiver.

Connecting two fiber-optic cables requires precise alignment of the mated fiber cores or spots in a single-mode fiber-optic cable. This is required so that nearly all the light is coupled from one fiber-optic cable across a junction to the other fiber-optic cable. Actual contact between the fiber-optic cables is not even mandatory.

There are two principal types of splices:

* Fusion
* Mechanical

**Fusion**

In fusion splicing a machine is used to precisely align the two fiber ends then the glass ends are "fused" or "welded" together using some type of heat or electric arc. This produces a continuous connection between the fibers enabling very low loss light transmission.

**Mechanical**

Mechanical splices are simply alignment devices, designed to  
hold the two fiber ends in a precisely aligned position thus enabling light to pass from one fiber into the other.

Both splices use in optic fiber to picktal connecting process. Here main problem is break splicing .so carefully establish in cover box. Splicing here testing is lazar light using. Testing process.

**Connecter**

Here making two type connecter

* **Male (RJ45 connecter )**
* **Female (IO female connecter**)

**COLOR CODING**

**COLOR CODING IS TWO TYPE**

**A and B**

1. A type color coding is furan country use
2. B type color coding Use in Indian country

So my project is working in B types color coding. And am living in India

Do data center operators use color-coded cables? If so, what colors represent which functions?

Although many agreed that color coding could help administrators identify a cable, few agreed on what color should represent which function. Generally, it depended on what kind of facility it was. A telecommunications center would have different distinctions than say, a collocation facility.   
Here was one simple suggestion:

* Red cables ' to external connections.
* Yellow cables ' in the DMZ separating internal from external networks.
* Blue or green cables ' only for internal networks.

He is fix color coding and right color code define these diagram are show as

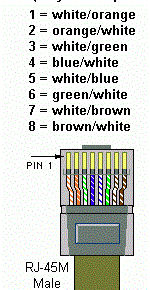
Here is use two type patch code male (Rj45) and female connecter

**RJ45 connecter (male connecter)**

RJ-45 at USOC (**Universal Service Ordering Code**) code identifying an 8-pin modular plug or jack used with unshielded twisted pair cable. Officially, an RJ-45 connector is a telephone connector designed for voice grade circuits only. RJ-45 type connectors with better signal handling characteristics are called 8-pin connectors in most standards documents, though most people continue to use the RJ-45 name for all 8-pin connectors.

**Rj45 color coding are as follows**

Another way of remembering the color coding is to simply switch the Green set of wires in place with the Orange set of wires. Specifically, switch the solid Green (G) with the solid Orange, and switch the green/white with the orange/white.

****

**RJ45 color coding**

**Pin Color Pair Description**

1 White/orange 2 TX Data +

2 Orange 2 TX Data–

3 white/green 3 RecvData +

4 Blue 1 Unused

5 white/blue 1 Unused

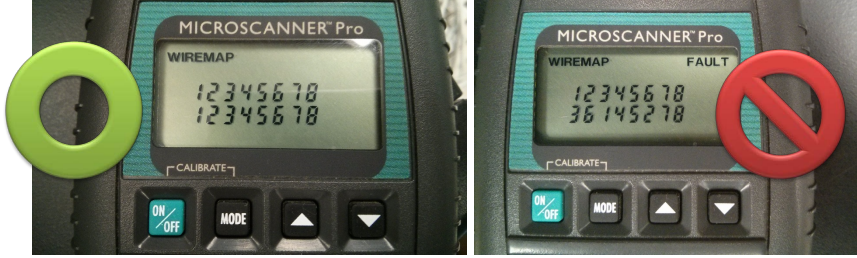
6 Green 3 RecvData –

7 white/brown 4 Unused

8 brown 4 Unused

Here color coding female connecter and Rj45 are same wiring color coding.

Testing is your connecter Micro Scanner pro Cable Verifier throw. Like image are as follows.



Here testing with pair combination related error displayed Micro Scanner is show like pair related and cut and losing related any information are show and both image show wrong and right testing image

**CHAPTER -8**

**Futher scope**

My project is depend future invent technology is supported fulfil. So this project used in future and present technology. My project used in present time is this sequences.

Like - After the installation of LAN in all individual buildings Academic Block 1 to 4, finally the Main server of all buildings will connected to central server.

**CHAPTER -9**

**conculison**

All the network devices are installed configured and connected to provide internet facility in the all floors of Academic Block-3 through LAN.

**CHAPTER 10**

**References**

**Reference Books:**

1.Tanenbaum , A.S. (2002) Computer Networks, Prentice Hall.

2. Spurgeon, Charles E. (2000) Ethernet: The Definitive Guide, O'Reilly Media, Inc.

3. Goleniewski, L. (2006) Telecommunications Essentials, Addison Wesley Professional.

**Reference Sites:**

**1.** **http://www.cisco.com/**

**2.** [**https://en.wikipedia.org/wiki/Computer\_network**](https://en.wikipedia.org/wiki/Computer_network)

**3.** **http://www.techsoup.org/support/articles-and-how-tos/networking-101-concepts-and-definitions**