

# [ 2CEIT503 COMPUTER NETWORKS ]

## Practical: 1

**AIM-** Introduction to network software, hardware and transmission media.  
Exercise: Construct a Cable that can connect PC to Switch.



**Ganpat  
University**

॥ विद्यया समाजोत्कर्षः ॥

**U.V. Patel  
College of  
Engineering**

Department of Computer  
Engineering/Information Technology

## Introduction

A network is simply a group of two or more Personal Computers linked together. Many types of networks exist, but the most common types of networks are Local-Area Networks (LANs), and Wide-Area Networks (WANs).

In a LAN, computers are connected together within a "local" area (for example, an office or home). In a WAN, computers are further apart and are connected via telephone/communication lines, radio waves or other means of connection.

## How are Networks Categorized?

A computer network is a system for communication among two or more computers. Computer networks can be categorized by range, functional relationship, network topology and specialized function.

### By range

- personal area network (PAN)
- wireless PAN
- local area network (LAN)
- wireless LAN
- metropolitan area network (MAN)
- wide area network (WAN)

### By functional relationship

- client-server
- multitier architecture
- Peer-to-peer

### By network topology

- bus network
- star network
- ring network
- grid network
- toroidal networks and hypercubes
- tree and hypertree networks

### By specialized function

- Storage area networks
- Server farms
- Process control networks
- Value added network

## Practical: 1

---

- SOHO network
- Wireless community network

### NETWORK TOPOLOGIES

A network topology refers to either the physical or logical layout of a network installation.

**Physical Topology** when in the context of networking refers to the physical layout of the devices connected to the network, including the location and cable installation.

The **Logical Topology** refers to the way it actually operates (transfers data) as opposed to its layout.

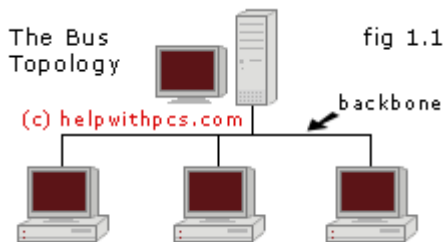
There are four main network topologies (and mixtures of the four) in common use today.

- Bus
- Mesh
- Ring
- Star

The most common types of physical topologies, which we are going to analyze, are: Bus, Hub/Star and Ring.

### The Physical Bus Topology

The Bus topology is one of the simplest of the four network topologies to use, in its most basic form it is simply a case of running one cable (referred to as the **backbone**) from the first device/PC in the network to the last device/PC, and then add any further devices/PCs to the existing cable (backbone) between the first and last machines (see **fig** below).

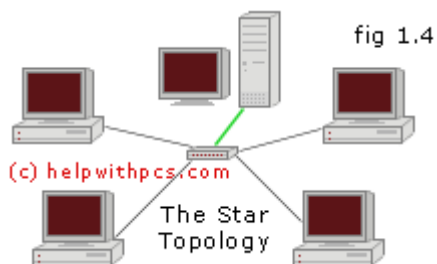


This topology is probably the cheapest network type of all to setup initially; as only one cable is used the installation is fairly simple and economical. The problems can come when trying to add a device to an existing Bus topology network. To add a device requires physically linking it to the existing backbone which can turn out to be a major job.

Another consideration if using a bus topology for a network is fault tolerance, or the lack of it, this type of network transfers data by passing messages through the same cable, so a break in any part of the cable will bring the whole network down.

## The Physical HUB or STAR Topology

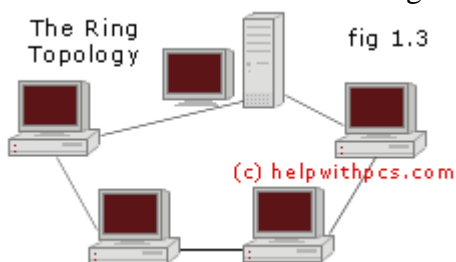
In the computer networking world the most commonly used topology in LAN is the star topology. Star topologies can be implemented in home, offices or even in a building. All the computers in the star topologies are connected to central devices like hub, switch or router. The functionality of all these devices is different. I have covered the detail of each networking devices in the separate portion of my website. Computers in a network are usually connected with the hub, switch or router with the Unshielded Twisted Pair (UTP) or Shielded Twisted Pair Cables.



As compared to the bus topology, a star network requires more devices & cables to complete a network. The failure of each node or cable in a star network, won't take down the entire network as compared to the Bus topology. However if the central connecting devices such as hub, switch or router fails due to any reason, then ultimately all the network can come down or collapse.

## The Physical Ring Topology

In ring Network, every computer or devices has two adjacent neighbors for communication. In a ring network, all the communication messages travel in the same directory whether clockwise or anti clockwise. Any damage of the cable of any cable or device can result in the breakdown of the whole network. Ring topology now has become almost obsolete.



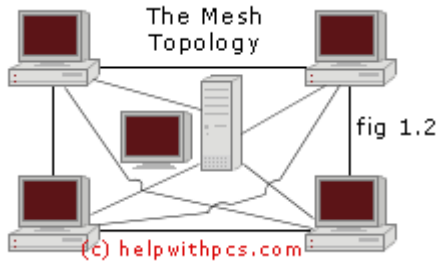
FDDI, SONET or Token Ring Technology can be used to implement Ring Technology. Ring topologies can be found in office, school or small buildings.

## The Physical Mesh Topology

This type of network topology boasts the highest fault tolerance of all of the network topologies; it is also usually the most expensive. In a mesh topology each device/PC is connected to every other device/PC in the network by its own cable (see fig below), which means vast amounts of cables for any sizeable network.

## Practical: 1

---

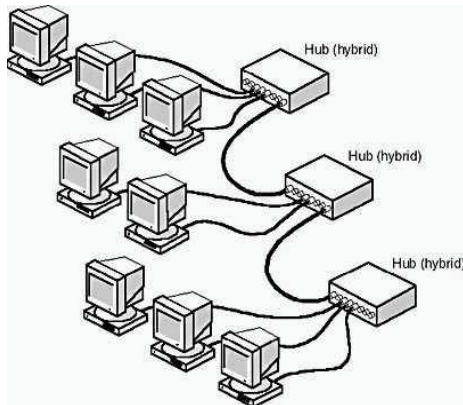


The Mesh topology provides fault tolerance by having separate cables for each connection, allowing any one cable to break without interfering with the rest of the network. Unfortunately because each connection needs its own cable a Mesh topology can get very expensive. Every time you add a client to a mesh network you have to run cables to each of the other devices.

### The Physical Hybrid Topology

With the hybrid topology, two or more topologies are combined to form a complete network. For example, a hybrid topology could be the combination of a star and bus topology. These are also the most common in use.

#### Star-Bus



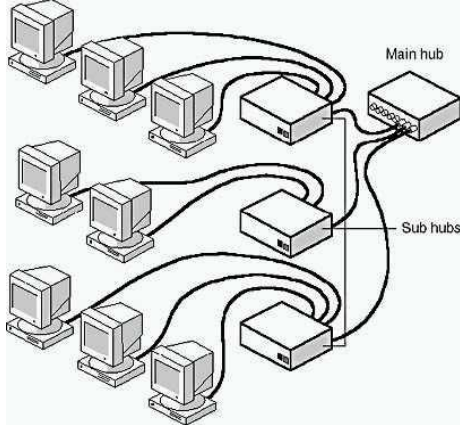
A type of network topology in which the central nodes of one or more individual networks that are based upon the physical star topology are connected together using a common 'bus' network whose physical topology is based upon the physical linear bus topology, the endpoints of the common 'bus' being terminated with the characteristic impedance of the transmission medium where required – e.g., two or more hubs connected to a common backbone with drop cables through the port on the hub that is provided for that purpose (e.g., a properly configured 'uplink' port) would comprise the physical bus portion of the physical star-bus topology, while each of the individual hubs, combined with the individual nodes which are connected to them, would comprise the physical star portion of the physical star-bus topology.

#### Star-Ring

## Practical: 1

---

A type of hybrid physical network topology that is a combination of the physical star topology and the physical ring topology, the physical star portion of the topology consisting of a network in which each of the nodes of which the network is composed are connected to a central node with a point-to-point link in a 'hub' and 'spoke' fashion, the central node being the 'hub' and the nodes that are attached to the central node being the 'spokes' (e.g., a collection of point-to-point links from the peripheral nodes that converge at a central node) in a fashion that is identical to the physical star topology, while the physical ring portion of the topology consists of circuitry within the central node which routes the signals on the network to each of the connected nodes sequentially, in a circular fashion.



### Introduction of Network Communication Devices

#### Introduction

Here we will talk about hubs and explain how they work. In the next section we will move to switches and how they differ from hubs, how they work and the types of switching methods that are available; we will also compare them.

Before we start there are a few definitions which I need to speak about so you can understand the terminology we will be using.

**Domain:** Defined as a geographical area or logical area (in our imagination) where anything in it becomes part of the domain. In computer land, this means that when something happens in this domain (area) every computer that's part of it will see or hear everything that happens in it.

**Collision Domain:** Putting it simple, whenever a collision between two computers occurs, every other computer within the domain will hear and know about the collision. These computers are said to be in the same collision domain. As you're going to see later on, when computers connect together using a hub they become part of the same collision domain. This doesn't happen with switches.

**Broadcast Domain:** A domain where every broadcast (a broadcast is a frame or data which is sent to every computer) is seen by all computers within the domain. Hubs and switches do not break up broadcast domains. You need a router to achieve this.

There are different devices which can break-up collision domains and broadcast domains and make the network a lot faster and efficient. Switches create separate collision domains but not broadcast domains. Routers create separate broadcast and collision domains. Hubs are too simple to do either, can't create separate collision or broadcast domain.

#### Hubs and Repeaters

## Practical: 1

---

Hubs are a form of repeater for an Ethernet LAN which has multiple ports (they are sometimes also known as "**multi-port repeaters**" or "active star networks"). Ethernet hubs and repeaters operate at the Physical Layer of the OSI Reference model and are defined by IEEE 802.3c/d. They are used to connect together one or more Ethernet cable segments of any media type. A very important fact about hubs and repeaters is that they allow users to share an Ethernet LAN. A network of repeaters and hubs is therefore called a "**Shared Ethernet**" or a "**Collision Domain**". The various systems sharing the Ethernet all compete for access using the CSMA/CD access protocol. This means that only one system is allowed to proceed with a transmission of a frame within a Collision Domain at any one time. Each system has to share a proportion of the available network bandwidth.



If a repeater sees a collision on a cable segment, the repeater detects this (in the normal way), and then generates a JAM signal to *all* connected output ports. This ensures that every computer connected to the LAN is aware of the collision, and does not try to transmit during the collision period.

### Switches and Bridges:

#### Switching Technology

Ethernet *switch* is a device that gathers the signals from devices that are connected to it, and then regenerates a new copy of each signal. Like a hub, a *switch* is a device that connects individual devices on an Ethernet network so that they can communicate with one another. But a switch also has an additional capability; it momentarily connects the sending and receiving devices so that they can use the entire bandwidth of the network without interference. If you use switches properly, they can improve the performance of your network by reducing network interference.



Switches have two benefits: (1) they provide each pair of communicating devices with a fast connection; and (2) they segregate the communication so that it does not enter other portions of the network. (Hubs, in contrast, broadcast all data on the network to every other device on the network.) These benefits are particularly useful if your network is congested and traffic pools in

## Practical: 1

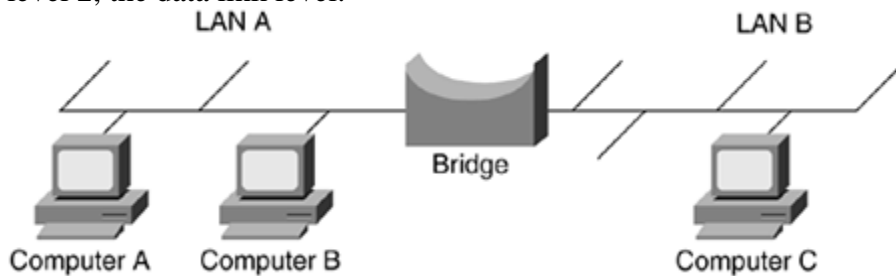
---

particular areas. However, if your network is not congested or if your traffic patterns do not create pools of local traffic, then switches may cause your network performance to deteriorate. This performance degradation occurs because switches examine the information inside each signal on your network (to determine the addresses of the sender and receiver) and therefore process network information more slowly than hubs (which do not examine the signal contents). Most switches operate by examining incoming or outgoing signals for information at OSI level 2, the data link level.

### Bridges

A *bridge* is a device that connects two or more local area networks, or two or more segments of the same network. A bridge connects two or more networks, or segments of the same network. In addition to connecting networks, bridges perform an additional, important function. They filter information so that network traffic intended for one portion of the network does not congest the rest of the network. These networks may use different physical and data link protocols. For example, you can install a bridge to connect a small lab of Macintosh computers using Local Talk to the school's main Ethernet network.

Bridges filter network traffic. They examine each set of data, transmitting only appropriate data to each connected segment. (Hubs, by contrast, broadcast all information to each connected computer, whether or not that computer is the intended recipient.) In this manner, bridges help reduce overall network traffic. Bridges are relatively simple and efficient traffic regulators. However, in most networks they have been replaced by their less expensive or more powerful cousins—hubs, switches, and routers. Most bridges operate by examining incoming or outgoing signals for information at OSI level 2, the data link level.



### Introduction of Routers

A router essentially performs two functions. Firstly it identifies a suitable link between the source system or source network and the destination system or destination network, and secondly

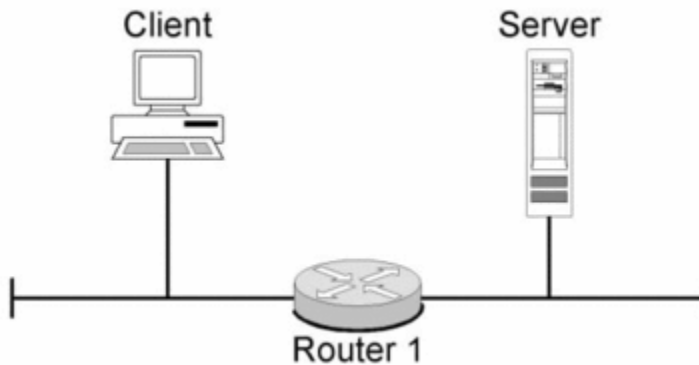


## Practical: 1

---

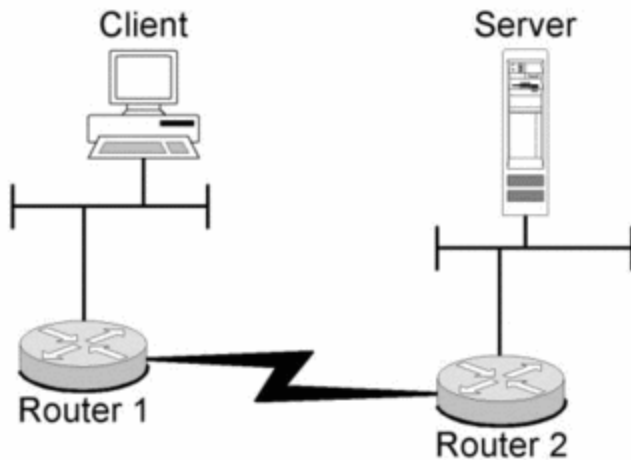
it transports data packets along this link. If the destination system (destination network) is directly connected to the router, i.e. router and destination systems are on the same subnet, the data packet sent by the source system goes directly to the destination system.

*Figure 1: routing*



If the destination system (destination network) is not directly connected to the router, then the router transmits the data packet to a neighboring router that is closer to the destination system (or destination network), and is known as the *next hop*. The last router in this chain is always directly connected to the destination network and transmits the data packet to the destination system.

*Figure 2: routing*



The function of a router is either to pass incoming data packets directly to the specified recipient or else to forward them to the next network. The *routing metric* determines the network to which the data packet should be forwarded if it cannot be delivered directly. The metric is a measure of the quality of the link between the originator and the router or destination of the packet. The router uses the metric to decide to which next hop it should forward the packet. Routing metrics are not just concerned with the length of the path between sender and recipient, but other features, such as the quality of the lines, the bandwidth or loading, can also be taken into account in the decision. Which criteria are used depends on the routing protocol used.



The routing information is managed in *routing tables*. Routing tables contain information about which neighboring routers can serve as the next hop for particular destination networks. The decision as to the next hop to which an incoming data packet will be forwarded is made solely on the basis of these routing tables. Hence it is particularly important to protect these tables from tampering. A number of attacks are known to exploit the vulnerability of routing tables to tampering. The table below illustrates the possible content of a routing table.

### **Network Cabling**

#### **Unshielded Twisted Pair**

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1). The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

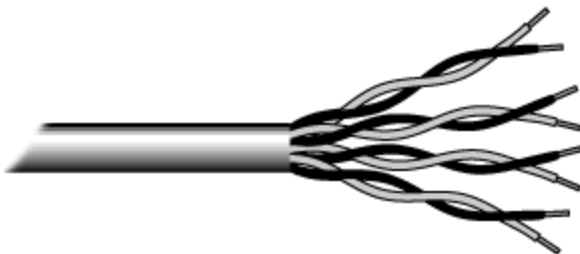


Fig.1. Unshielded twisted pair

Categories of Unshielded Twisted Pair

## Practical: 1

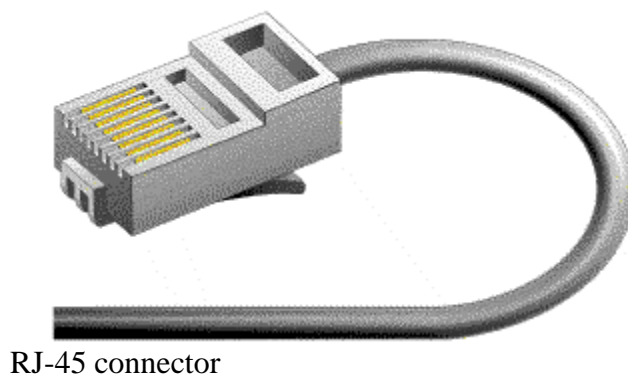
---

Type	Use
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

Buy the best cable you can afford; most schools purchase Category 3 or Category 5. If you are designing a 10 Mbps Ethernet network and are considering the cost savings of buying Category 3 wire instead of Category 5, remember that the Category 5 cable will provide more "room to grow" as transmission technologies increase. Both Category 3 and Category 5 UTP have a maximum segment length of 100 meters. In Florida, Category 5 cable is required for retrofit grants. 10BaseT refers to the specifications for unshielded twisted pair cable (Category 3, 4, or 5) carrying Ethernet signals. Category 6 is relatively new and is used for gigabit connections.

### **Unshielded Twisted Pair Connector**

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.



### **Unshielded and shielded twisted pair cabling standards**

- **Cat 1:** Previously used for POTS telephone communications, ISDN and doorbell wiring.

## Practical: 1

- **Cat 2:** Previously was frequently used on 4 Mbit/s token ring networks.
- **Cat 3:** Currently defined in TIA/EIA-568-B, used for data networks using frequencies up to 16 MHz Historically popular for 10 Mbit/s Ethernet networks.
- **Cat 4:** Provided performance of up to 20 MHz, and was frequently used on 16 Mbit/s token ring networks.
- **Cat 5:** Provided performance of up to 100 MHz, and was frequently used on 100 Mbit/s Ethernet networks. May be unsuitable for 1000BASE-T gigabit ethernet.
- **Cat 5e:** Currently defined in TIA/EIA-568-B. Provides performance of up to 100 MHz, and is frequently used for both 100 Mbit/s and Gigabit Ethernet networks.
- **Cat 6:** Currently defined in TIA/EIA-568-B. Provides performance of up to 250 MHz, more than double category 5 and 5e.
- **Cat 6a:** Currently defined in ANSI/TIA/EIA-568-B.2-10. Provides performance of up to 500 MHz, double that of category 6. Suitable for 10GBase-T.
- **Cat 7:** An informal name applied to ISO/IEC 11801 Class F cabling. This standard specifies four individually-shielded pairs (STP) inside an overall shield. Designed for transmission at frequencies up to 600 MHz

**Category 5 cable**, commonly known as **Cat 5** or "Cable and Telephone", is a twisted pair cable type designed for high signal integrity. Many such cables are unshielded but some are shielded. Category 5 has been superseded by the **Category 5e** specification. This type of cable is often used in structured cabling for computer networks such as Ethernet, and is also used to carry many other signals such as basic voice services, token ring, and ATM (at up to 155 Mbit/s, over short distances).

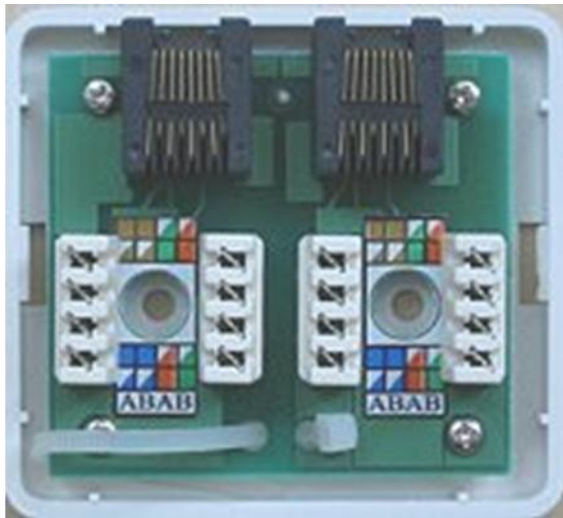









Image of a Cat 5E Wall outlet showing the two wiring schemes: A for T568A, B for T568B.

### TIA/EIA-568-A T568A Wiring

Pin	Pair	Wire	Color
1	3	1	 white/green
2	3	2	 green

## Practical: 1

3	2	1	 white/orange
4	1	2	 blue
5	1	1	 white/blue
6	2	2	 orange
7	4	1	 white/brown
8	4	2	 brown

### TIA/EIA-568-B T568B Wiring

Pin	Pair	Wire	Color
1	2	1	 white/orange
2	2	2	 orange
3	3	1	 white/green
4	1	2	 blue
5	1	1	 white/blue
6	3	2	 green
7	4	1	 white/brown
8	4	2	 brown

The specification for category 5 cable was defined in ANSI/TIA/EIA-568-A, with clarification in TSB-95. These documents specified performance characteristics and test requirements for frequencies of up to 100 MHz

Category 5 cable includes four twisted pairs in a single cable jacket. This use of balanced lines helps preserve a high signal-to-noise ratio despite interference from both external sources and other pairs (this latter form of interference is called crosstalk). It is most commonly used for 100 Mbit/s networks, such as 100BASE-TX Ethernet, although IEEE 802.3ab defines standards for 1000BASE-T - Gigabit Ethernet over category 5 cable. Cat 5 cable typically has three twists per inch of each twisted pair of 24 gauge copper wires within the cable.

### Category 5e

A **cat 5 e cable** is an enhanced version of Cat 5 that adds specifications for far end crosstalk. It was formally defined in 2001 as the TIA/EIA-568-B standard, which no longer recognizes the original Cat 5 specification. Although 1000BASE-T was designed for use with Cat 5 cable, the tighter specifications associated with Cat 5e cable and connectors make it an excellent choice for use with 1000BASE-T. Despite the stricter performance specifications, Cat 5e cable does not enable longer cable distances for Ethernet networks: cables are still limited to a maximum of

## Practical: 1

---

100 m (328 ft) in length (normal practice is to limit fixed ("horizontal") cables to 90 m to allow for up to 5 m of patch cable at each end). Cat 5e cable performance characteristics and test methods are defined in TIA/EIA-568-B.2-2001.

### Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.



Coaxial cable

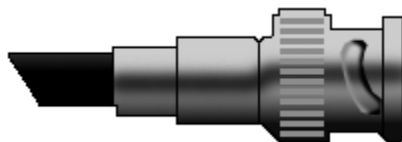
Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

### Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayonet-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.



BNC connector

### Fiber Optic Cable

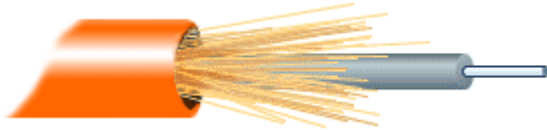
## Practical: 1

---

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and Kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of Teflon or PVC.



*Fiber optic cable*

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Specification	Cable Type
<b>10BaseT</b>	Unshielded Twisted Pair
<b>10Base2</b>	Thin Coaxial
<b>10Base5</b>	Thick Coaxial
<b>100BaseT</b>	Unshielded Twisted Pair
<b>100BaseFX</b>	Fiber Optic
<b>100BaseBX</b>	Single mode Fiber
<b>100BaseSX</b>	Multimode Fiber

## Practical: 1

---

<b>1000BaseT</b>	Unshielded Twisted Pair
<b>1000BaseFX</b>	Fiber Optic
<b>1000BaseBX</b>	Single mode Fiber
<b>1000BaseSX</b>	Multimode Fiber

### Student Experiment

Construct a Cable that can connect PC to Switch.

Reference Simulation link: [http://vlabs.iitb.ac.in/vlabs-dev/labs\\_local/computer-networks/labs/exp1/exp1.html](http://vlabs.iitb.ac.in/vlabs-dev/labs_local/computer-networks/labs/exp1/exp1.html)