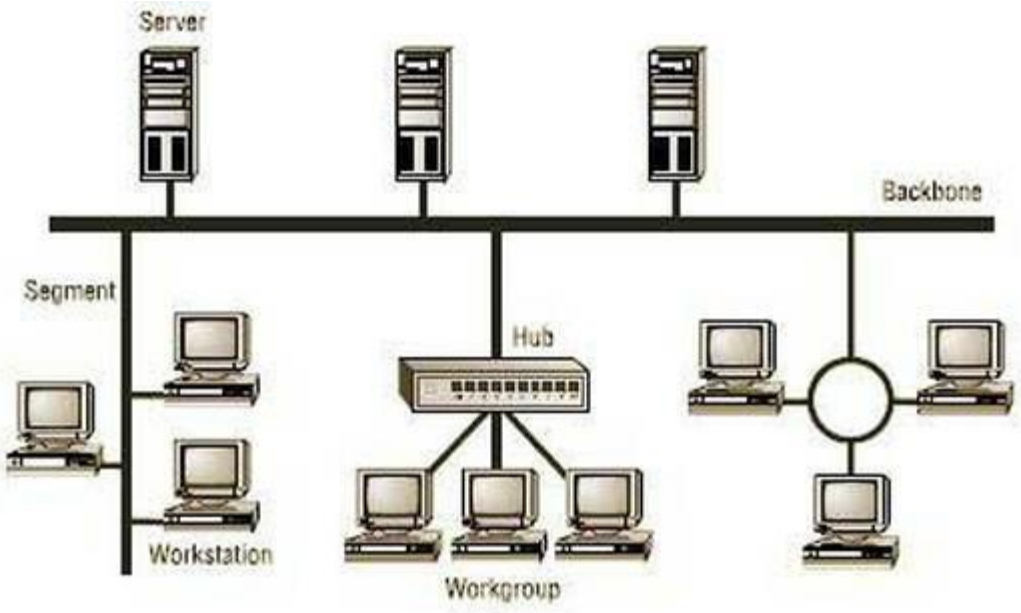
Computer Networks

Computer Network

A network can be defined as a group of computers and other devices connected in some ways so as to be able to exchange data. Each of the devices on the network can be thought of as a node; each node has a unique address. Addresses are numeric quantities that are easy for computers to work with, but not for humans to remember. Example: 204.160.241.98. Some networks also provide names that humans can more easily remember than numbers. Example: www.javasoft.com, corresponding to the above numeric address.

Categories of Networks

Local Area Networks (LAN): Local area networks, generally called **LANs**, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.



Metropolitan Area Network (MAN): Metropolitan Area Network: A metropolitan area network, or MAN, covers a city. The best-known example of a MAN is the cable television network available in many cities. This system grew from earlier community antenna systems used in areas with poor over-the-air television reception. In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses. At first, these were locally-designed, ad hoc systems

Wide Area Network (WAN): Wide Area Network: A wide area network, or WAN, spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user (i.e., application) programs. These machines are called as hosts. The hosts are connected by a communication subnet, or just subnet for short. The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider. The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.

Types of Network Topology

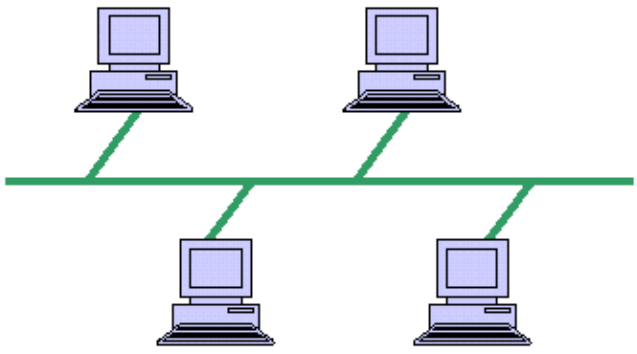
Computer network topology refers to the physical communication schemes used by connected devices on a network. The basic computer network topology types are:

- Bus
- Ring
- Star
- Mesh
- Tree
- Wireless

Networks that are more complex can be built as hybrids using two or more of these basic topologies.

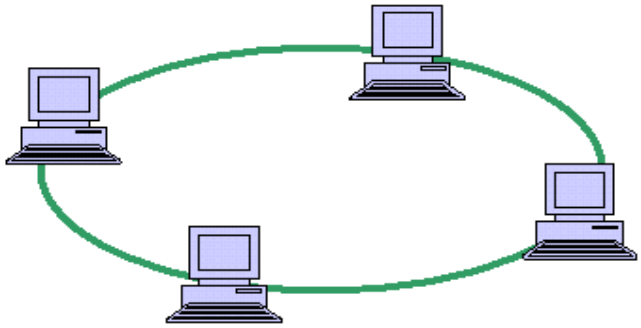
Bus Network Topology

Bus networks share a common connection that extends to all devices. This network topology is used in small networks, and it is simple to understand. Every computer and network device connects to the same cable, so if the cable fails, the whole network is down, but the cost of setting up the network



is reasonable.

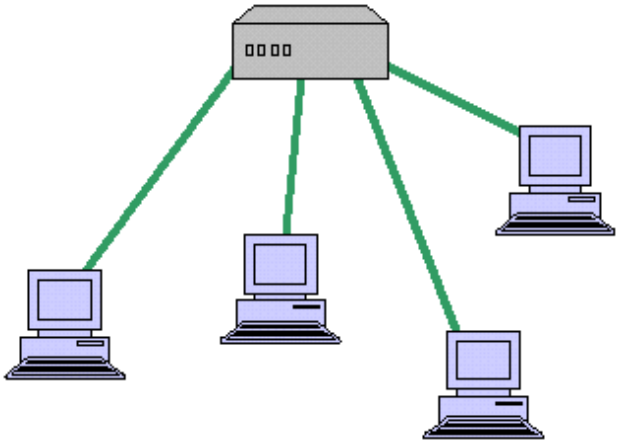
This type of networking is cost effective. However, the connecting cable has a limited length, and the network is slower than a ring network.



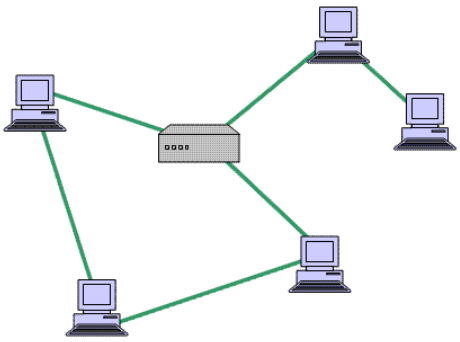
Ring Network Topology

Each device in a ring network is attached to two other devices, and the last device connects to the first to form a circular network. Each message travels through the ring in one direction—clockwise or counterclockwise—through the shared link. Ring topology that involves a large number of connected devices requires repeaters. If the connection cable or one device fails in a ring network, the whole network fails. Although ring networks are faster than bus networks, they are more difficult to troubleshoot.

Star Network Topology



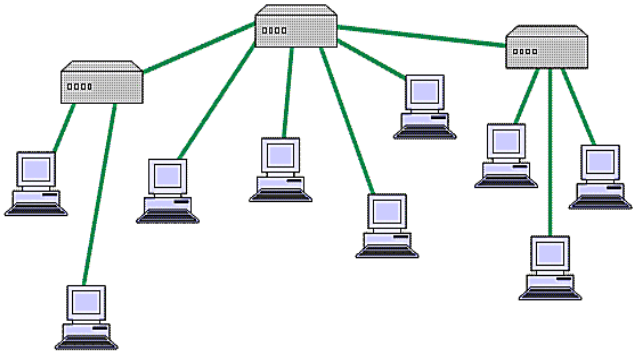
Star Network Topology typically uses a network hub or switch and is common in-home networks. Every device has its own connection to the hub. The performance of a star network depends on the hub. If the hub fails, the network is down for all connected devices. The performance of the attached devices is usually high because there are usually fewer devices connected in star topology that in other types of networks. A star network is easy to set up and easy to troubleshoot. The cost of setup is higher than for bus and ring network topology, but if one attached device fails, the other connected devices are unaffected.



Mesh Network Topology

Mesh network topology provides redundant communication paths between some or all devices in a partial or full mesh. In full mesh topology, every device is connected to all the other devices. In a partial mesh topology, some of the connected devices or systems are connected to all the others, but some of the devices only connect to a few other devices. Mesh is robust and troubleshooting is relatively easy. However, installation

and configuration are more complicated than with the star, ring and bus topologies.



Tree Network Topology

Tree topology integrates the star and bus topologies in a hybrid approach to improve network scalability. The network is setup as a hierarchy, usually with at least three levels. The devices on the bottom level all connect to one of the devices on the level above it. Eventually, all devices lead to the main hub that controls the network.

This type of network works well in companies that have various grouped workstations. The system is easy to manage and troubleshoot. However, it is relatively costly to set up. If the central hub fails, then the network fails.

Wireless Network Topology

Wireless networking is the new kid on the block. In general, wireless networks are slower than wired networks, but that is changing quickly. With the proliferation of laptops and mobile devices, the need for networks to accommodate wireless remote access has increased vastly.

It has become common for wired networks to include a hardware access point that is available to all the wireless devices that need access to the network. With this expansion of capabilities comes a potential security issue that must be addressed.

What is Network Cabling?

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs

Unshielded Twisted Pair (UTP) Cable

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).

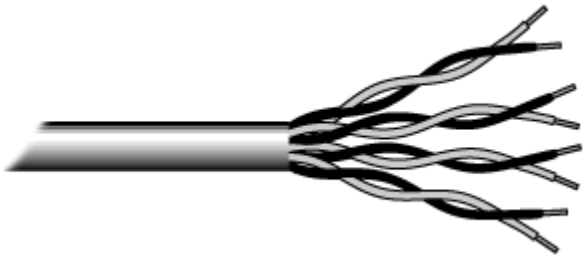


Fig.1. Unshielded twisted pair

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 six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	Local Talk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair)	100BaseT Ethernet
	1000 Mbps (4 pair)	Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

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.

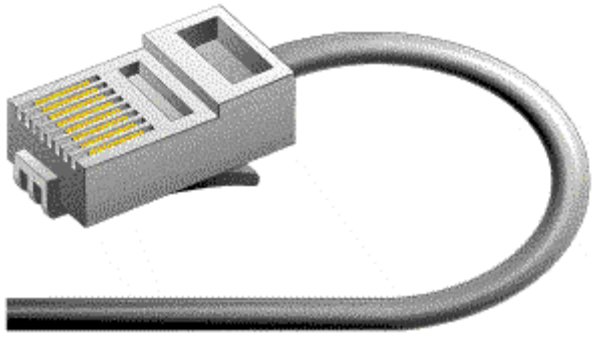


Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

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 (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

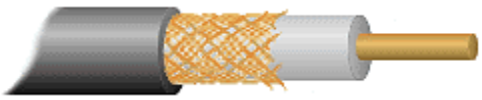


Fig. 3. Coaxial cable

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 Bayone-Neill-Concelman (BNC) connector (See fig. 4). 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 screw, onto the cable.

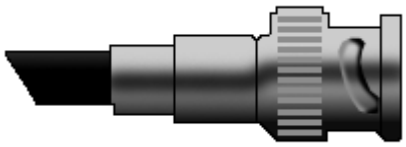


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). 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.

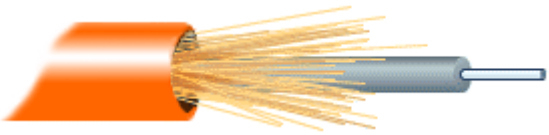


Fig. 5. Fiber optic cable

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.

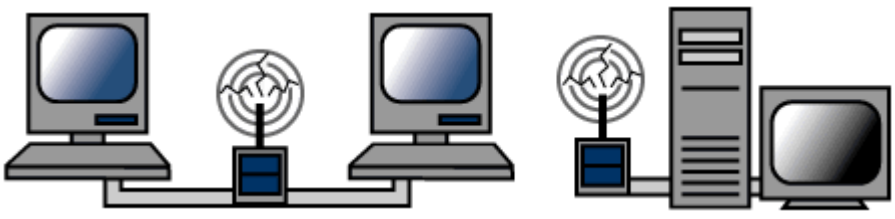
Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

Wireless LANs



More and more networks are operating without cables, in the wireless mode. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to

communicate between the workstations, servers, or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

Wireless networks are great for allowing laptop computers, portable devices, or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walks within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network. Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless standards and speeds

The Wi-Fi Alliance is a global, non-profit organization that helps to ensure standards and interoperability for wireless networks, and wireless networks are often referred to as WiFi (Wireless Fidelity). The original Wi-Fi standard (IEEE 802.11) was adopted in 1997. Since then many variations have emerged (and will continue to emerge). Wi-Fi networks use the Ethernet protocol.

Standard	Max Speed	Typical Range
802.11a	54 Mbps	150 feet
802.11b	11 Mbps	300 feet
802.11g	54 Mbps	300 feet
802.11n	100 Mbps	300+ feet

Wireless Security

Wireless networks are much more susceptible to unauthorized use than cabled networks. Wireless network devices use radio waves to communicate with each other. The greatest vulnerability to the network is that rogue machines can "eves-drop" on

the radio wave communications. Unencrypted information transmitted can be monitored by a third-party, which, with the right tools (free to download), could quickly gain access to your entire network, steal valuable passwords to local servers and online services, alter or destroy data, and/or access personal and confidential information stored in your network servers. To minimize the possibility of this, all modern access points and devices have configuration options to encrypt transmissions. These encryption methodologies are still evolving, as are the tools used by malicious hackers, so always use the strongest encryption available in your access point and connecting devices.

A NOTE ON ENCRYPTION: As of this writing WEP (Wired Equivalent Privacy) encryption can be easily hacked with readily-available free tools which circulate the internet. WPA and WPA2 (WiFi Protected Access versions 1 and 2) are much better at protecting information, but using weak passwords or passphrases when enabling these encryptions may allow them to be easily hacked. If your network is running WEP, you must be very careful about your use of sensitive passwords or other data.

Three basic techniques are used to protect networks from unauthorized wireless use. Use any and all of these techniques when setting up your wireless access points:

Encryption.

Enable the strongest encryption supported by the devices you will be connecting to the network. Use strong passwords (strong passwords are generally defined as passwords containing symbols, numbers, and mixed case letters, at least 14 characters long).

Isolation.

Use a wireless router that places all wireless connections on a subnet independent of the primary private network. This protects your private network data from pass-through internet traffic.

Hidden SSID.

Every access point has a Service Set IDentifier (SSID) that by default is broadcast to client devices so that the access point can be found. By disabling this feature, standard client connection software won't be able to "see" the access point. However, the eves-dropping programs discussed previously can easily find these access points, so this alone does little more than keep the access point name out of sight for casual wireless users.

Advantages of wireless networks:

- Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free WiFi access ("Hot spots").
- Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
- Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.
- Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

Disadvantages of wireless networks:

- Security - Be careful. Be vigilant. Protect your sensitive data with backups, isolated private networks, strong encryption and passwords, and monitor network access traffic to and from your wireless network.
- Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
- Inconsistent connections - How many times have you hears "Wait a minute, I just lost my connection?" Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables. If you are only using wireless for internet access, the actual internet connection for your home or school is generally slower than the wireless network devices, so that connection is the bottleneck. If you are also moving large amounts of data around a private network, a cabled connection will enable that work to proceed much faster.