NETWORK TECHNOLOGY WITH ADMINISTRATION AND MAINTENANCE

Name : _______________________ ID Number : ___________________

Cabling and Topology

Every network must provide some method to get data from one system to another. In most cases, this method consists of some type of cabling (usually copper or fiber-optic) running between systems, although many networks skip wires and use wireless methods to move data. Stringing those cables brings up a number of critical issues we need to understand to work on a network.

Several issues to consider:

- How do all these cables connect the computers together?
- Does every computer on the network run a cable to a central point?
- Does a single cable snake through the ceiling, with all the computers on the network connected to it?

Furthermore, some standards should be in place so that manufacturers can make networking equipment that works well together.

Topology

Computer networks employ many different topologies, or ways of connecting computers together.

Bus and Ring

The first generation of wired networks used one of two topologies, both shown in Figure 2.1. A bus topology uses a single bus cable that connects all of the computers in line. A ring topology connects all computers on the network with a central ring of cable.

Note that topologies are diagrams, much like an electrical circuit diagram. Real network cabling doesn't go in perfect circles or perfect straight lines. Figure 2.2 shows a bus topology network that illustrates how the cable might appear in the real world.

Data flows differently between bus and ring networks, creating different problems and solutions. In bus topology networks, data from each computer simply goes out on the whole bus. A network using a bus topology needs termination at each end of the cable to prevent a signal sent from one computer from reflecting at the ends of the cable, creating unnecessary traffic (Figure 2.3). In a ring topology network, in contrast, data traffic moves in a circle from one computer to the next in the same direction (Figure 2.4). With no end of the cable, ring networks require no termination.

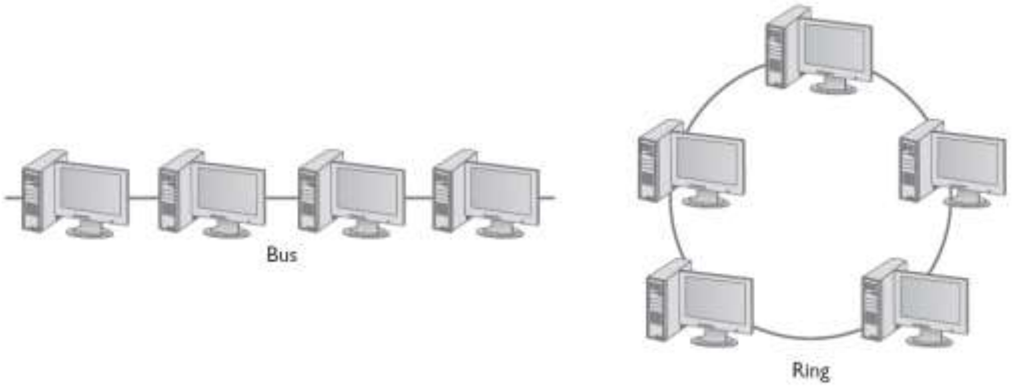


Figure 2.1 - Bus and ring topologies

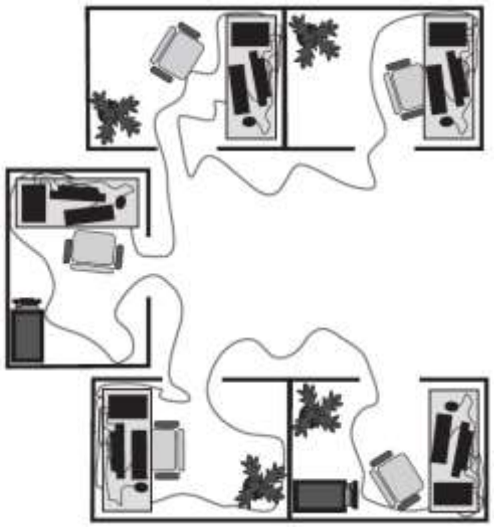


Figure 2.2 - Real-world bus topology

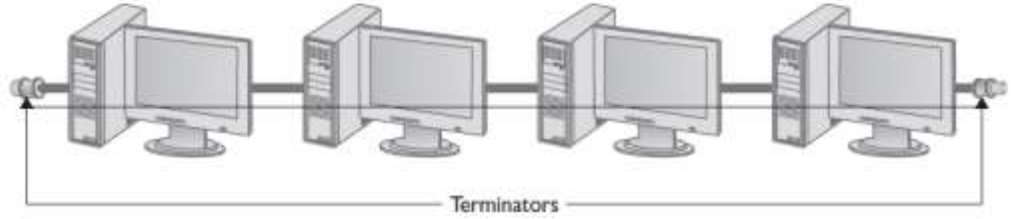


Figure 2.3 - Terminated bus topology

Bus and ring topology networks worked well, but suffered from the same problem: the entire network stopped working if the cable broke at any point. The broken ends on a bus topology aren't terminated, causing reflection between computers still connected. A break in a ring topology network simply breaks the circuit and stops the data flow.

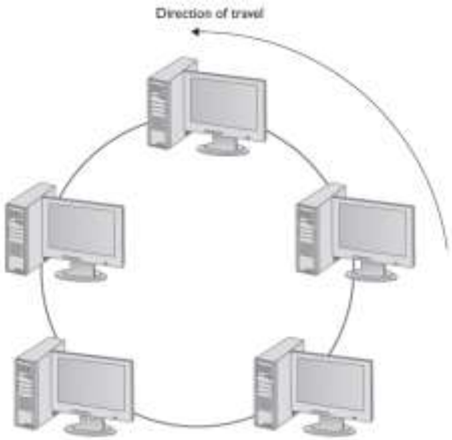


Figure 2.4 - Ring topology moving in a certain direction

Star

The star topology uses a central connection for all the computers on the network (Figure 2.5). Star topology had a huge benefit over ring and bus by offering fault tolerance—if one of the cables broke, all of the other computers could still communicate.

Bus and ring were popular and inexpensive to implement, so the old-style star topology wasn't very successful. Network hardware designers couldn't easily redesign their existing networks to use star topology.

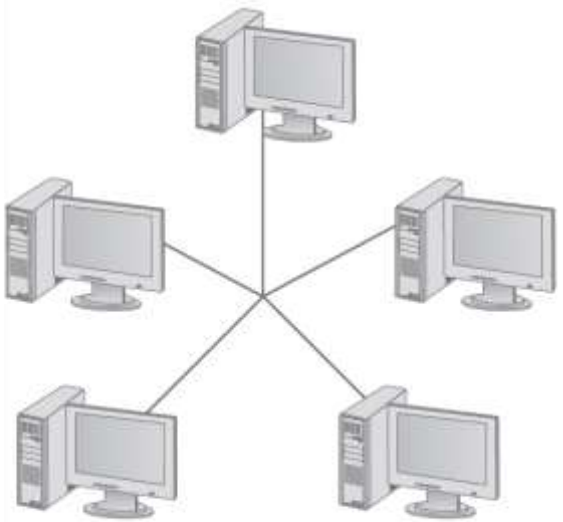


Figure 2.5 - Star topology

Hybrids

Even though network designers couldn't use a star topology, the benefits of star were overwhelming, motivating smart people to come up with a way to use star without a major redesign—and the way they did so was ingenious. The ring topology networks struck first by taking the entire ring and shrinking it into a small box, as shown in Figure 2.6.

This was quickly followed by the bus topology folks, who in turn shrunk their bus (better known as the segment) into their own box (Figure 2.7).

Physically, they looked like a star, but if you looked at it as an electronic schematic, the signals acted like a ring or a bus. Clearly the old definition of topology needed a little clarification. When we talk about topology today, we separate how the cables physically look (the physical topology) from how the signals travel electronically (the signaling topology).

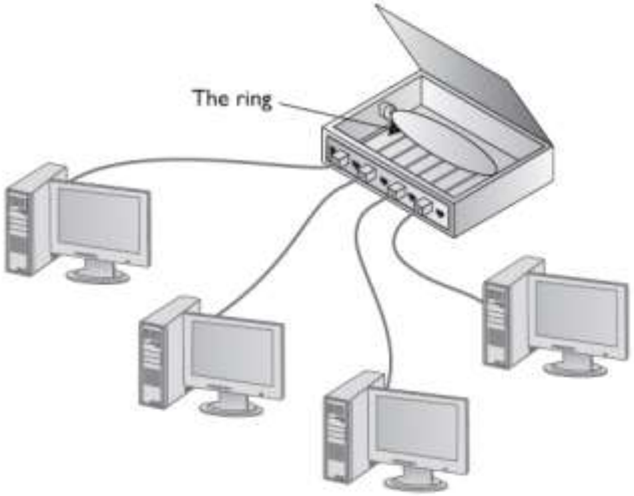


Figure 2.6 - Shrinking the ring

We call any form of networking technology that combines a physical topology with a signaling topology a hybrid topology. Hybrid topologies have come and gone since the earliest days of networking. Only two hybrid topologies, star-ring and star-bus, ever saw any amount of popularity. Eventually star-ring lost market and star-bus reigns as the undisputed king of topologies.

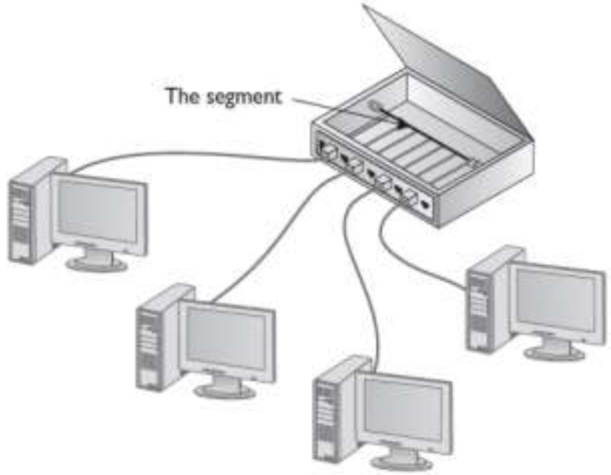


Figure 2.7 - Shrinking the segment

Mesh and Point-to-Multipoint

Topologies aren't just for wired networks. Wireless networks also need a topology to get data from one machine to another, but using radio waves instead of cables makes for somewhat different topologies. Almost all wireless networks use one of two different topologies: mesh topology or point-to-multipoint topology (Figure 2.8).

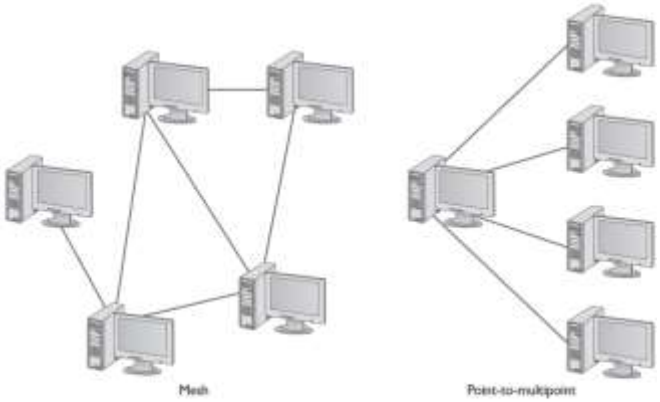


Figure 2.8 - Mesh and point-to-multipoint

Mesh

In a mesh topology network, every computer connects to every other computer via two or more routes. Some of the routes between two computers may require traversing through another member of the mesh network.

There are two types of meshed topologies: partially meshed and fully meshed (Figure 2.9). In a partially meshed topology network, at least two machines have redundant connections. Every machine doesn't have to connect to every other machine. In a fully meshed topology network, every computer connects directly to every other computer.

If you're looking at Figure 2.9 and thinking that a mesh topology looks amazingly resilient and robust at least on paper. Because every computer connects to every other computer on the fully meshed network, even if half the PCs crash, the network still functions as well as ever (for the survivors). In a practical sense, however, implementing a fully meshed topology in a wired network would be an expensive mess. For example, even for a tiny fully meshed network with only 10 PCs, you would need 45 separate and distinct pieces of cable to connect every PC to every other PC.

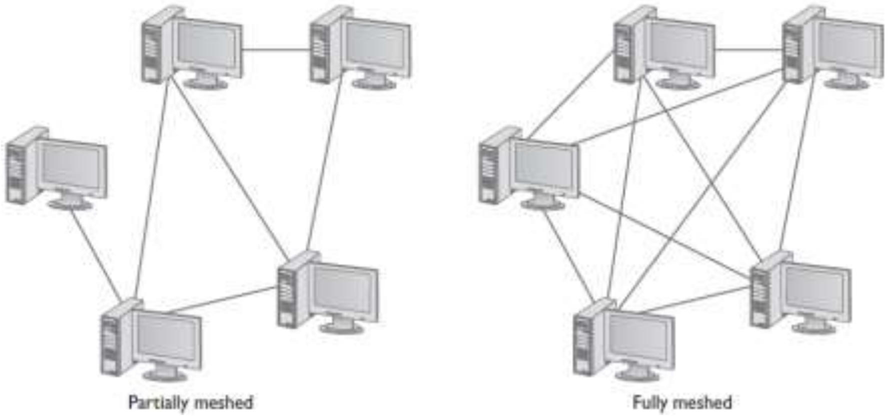


Figure 2.9 - Partially and fully meshed topologies

Point-to-Multipoint

In a point-to-multipoint topology, a single system acts as a common source through which all members of the point-to-multipoint network converse. If you compare a star topology to a slightly rearranged point-to-multipoint topology, you might be tempted to say they're the same thing. Granted, they're similar, but look at Figure 2.10. The important difference is that a point-to-multipoint topology requires an intelligent device in the center, while the device or connection point in the center of a star topology has little more to do than send or provide a path for a signal down all the connections.

Point-to-Point

In a point-to-point topology network, two computers connect directly together with no need for a central hub or box of any kind. You'll find point-to-point topologies implemented in both wired and wireless networks (Figure 2.11).

Parameters of a Topology

While a topology describes the method by which systems in a network connect, the topology alone doesn't describe all of the features necessary to enable those networks. The term bus topology, for example, describes a network that consists of some number of machines connected to the network via a single linear piece of cable. However, several considerations can be noticed:

- What is the cable made of? How long can it be?
- How do the machines decide which machine should send data at a specific moment?

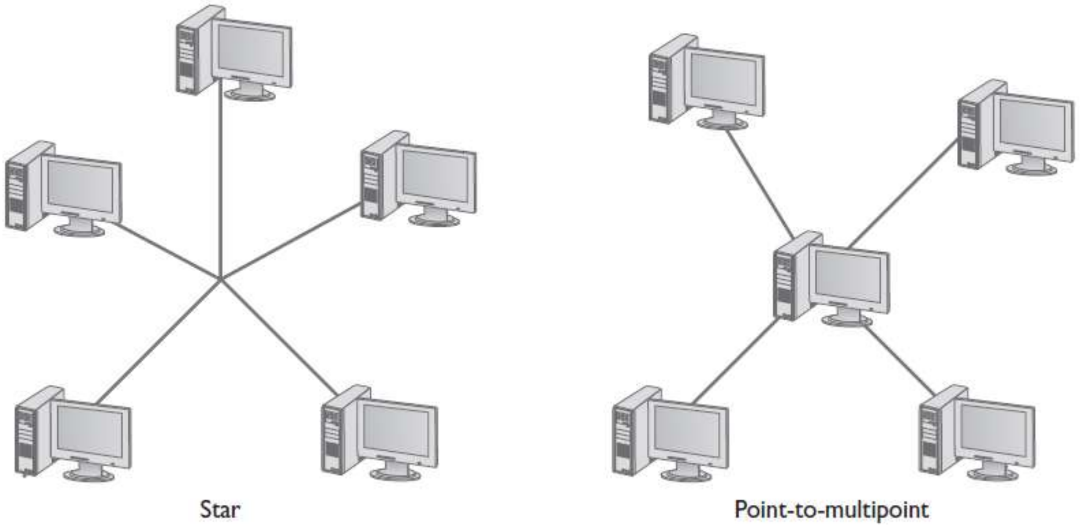


Figure 2.10 - Comparing star and point-to-multipoint

A network based on a bus topology can answer these questions in a number of different ways—but it's not the job of the topology to define issues like these. A functioning network needs a more detailed standard.

Figure 2.11 - Point-to-point

Over the years, particular manufacturers and standards bodies have created several specific network technologies based on different topologies. A network technology is a practical application of a topology and other critical technologies to provide a method to get data from one computer to another on a network. These network technologies have names like 10BaseT, 1000BaseF, and 10GBaseLX.

Cabling

The majority of networked systems link together using some type of cabling. Different types of networks over the years have used a number of different types of cables.

Coaxial Cable

Coaxial cable contains a central conductor wire surrounded by an insulating material, which in turn is surrounded by a braided metal shield. The cable is referred to as coaxial (coax for short) because the center wire and the braided metal shield share a common axis or centerline.

Coaxial cable shields data transmissions from electro-magnetic interference (EMI). Many devices in the typical office environment generate magnetic fields, including lights, fans, copy machines, and refrigerators. When a metal wire encounters these magnetic fields, electrical current is generated along the wire. This extra current—EMI—can shut down a network because it is easily misinterpreted as a signal by devices like NICs. To prevent EMI from affecting the network, the outer mesh layer of a coaxial cable shields the center wire (on which the data is transmitted) from interference.

Early bus topology networks used coaxial cable to connect computers together. The most popular back in the day used special bayonet-style connectors called BNC connectors. Even earlier bus networks used thick cable that required vampire connections—sometimes called vampire taps— that literally pierced the cable.

Coaxial cable is used today primarily to enable a cable modem to connect to an Internet service provider (ISP). Connecting a computer to the cable modem enables that computer to access the Internet. This is the same type of cable used to connect televisions to cable boxes or to satellite receivers. These cables use an F-type connector that screws on, making for a secure connection .

Cable modems connect using either RG-6 or, rarely, RG-59. RG-59 was used primarily for cable television rather than networking. Its thinness and the introduction of digital cable motivated the move to the more robust RG-6, the predominant cabling used today.

All coax cables have an RG rating; the U.S. military developed these ratings to provide a quick reference for the different types of coax. The only important measure of coax cabling is its Ohm rating, a relative measure of the resistance (or more precisely, characteristic impedance) on the cable. You may run across other coax cables that don't have acceptable Ohm ratings, although they look just like network-rated coax. Fortunately, most coax cable types display their Ohm ratings on the cables themselves. Both RG-6 and RG-59 cables are rated at 75 Ohms.

This isn't simple resistance. Impedance also factors in things like how the wire to get a full charge— the wire's capacitance—and other things.

Given the popularity of cable for television and Internet in homes today, you'll run into situations where people need to take a single coaxial cable and split it. Coaxial handles this quite nicely with coaxial splitters like the one shown in Figure 2.12. It's also easy to connect two coaxial cables together using a barrel connector when you need to add some distance to a connection (Figure 2.13).

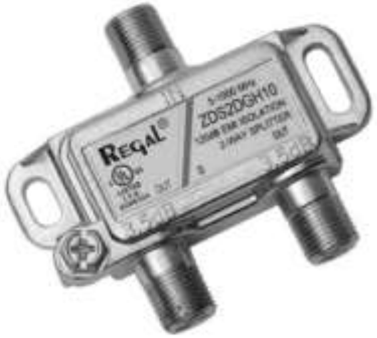


Figure 2.12 - Coaxial splitter

Twisted Pair

The most overwhelmingly common type of cabling used in networks consists of twisted pairs of cables, bundled together into a common jacket. Networks use two types of twisted-pair cabling: shielded twisted pair and unshielded twisted pair. Twisted-pair cabling for networks is composed of multiple pairs of wires, twisted around each other at specific intervals. The twists serve to reduce interference, called crosstalk: the more twists, the less crosstalk.

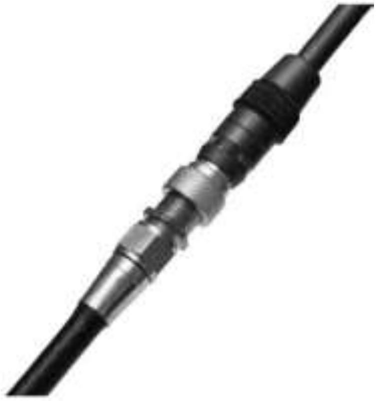


Figure 2.13 - Barrel connector

Shielded Twisted Pair

Shielded twisted pair (STP), as its name implies, consists of twisted pairs of wires surrounded by shielding to protect them from EMI. STP is pretty rare, primarily because there's so little need for STP's shielding; it only really matters in locations with excessive electronic noise, such as a shop floor with lots of lights, electric motors, or other machinery that could cause problems for other cables. Figure 3-21 shows the most common STP type: the venerable IBM Type 1 cable used in Token Ring network technology.

Unshielded Twisted Pair

Unshielded twisted pair (UTP) is by far the most common type of network cabling used today. UTP consists of twisted pairs of wires surrounded by a plastic jacket. This jacket does not provide any protection from EMI, so when installing UTP cabling, you must be careful to avoid interference from light, motors, and so forth. UTP is much cheaper than, and in most cases does just as good a job as, STP.

Although more sensitive to interference than coaxial or STP cable, UTP cabling provides an inexpensive and flexible means to cable networks. UTP cable isn't exclusive to networks; many other technologies (such as telephone systems) employ the same cabling. This makes working with UTP a bit of a challenge. Imagine going up into a ceiling and seeing two sets of UTP cables: how would you determine which is for the telephones and which is for the network? A number of installation standards and tools exist to help those who work with UTP get the answer to these types of questions.

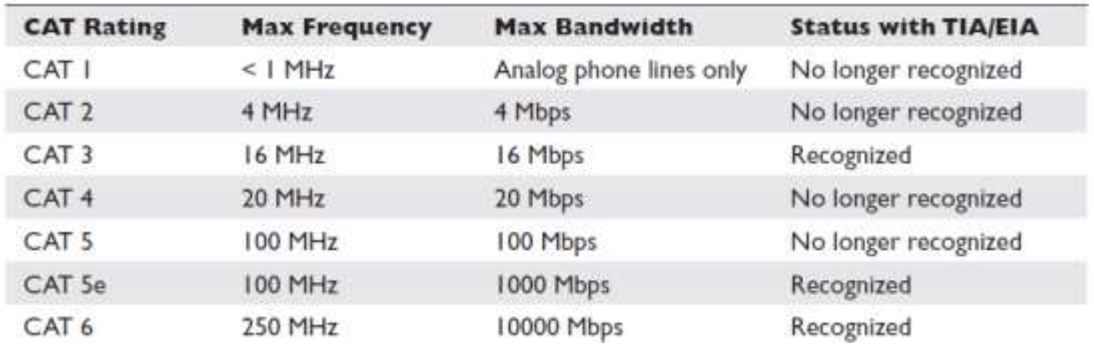
Not all UTP cables are the same. UTP cabling has a number of variations, such as the number of twists per foot, which determine how quickly data can propagate on the cable. To help network installers get the right cable for the right network technology, the cabling industry has developed a variety of grades called category (CAT) ratings. CAT ratings are officially rated in megahertz (MHz), indicating the highest frequency the cable can handle. Table 2.1 shows the most common categories.

UTP cables are rated to handle a certain frequency, such as 100 MHz or 1000 MHz, which originally translated as the maximum throughput for a cable. Each cycle, each hertz basically, accounts for one bit of data. For example, a 10 million cycle per second (10 MHz) cable could accommodate 10 million bits per second (10 Mbps)—1 bit per cycle. The maximum amount of data that goes through the cable per second is called the bandwidth. Through the use of bandwidth-efficient encoding schemes, however, manufacturers squeeze more bits into the same signal, as long as the cable can handle it. Thus, the CAT 5e cable can handle throughput of up to 1000 Mbps, even though it's rated to handle a bandwidth of only up to 100 MHz.

Because most networks can run at speeds of up to 1000 MHz, most new cabling installations use Category 5e (CAT 5e) cabling, although a large number of installations use CAT 6 to future-proof the network.

Make sure you can look at UTP and know its CAT rating. There are two places to look. First, UTP is typically sold in boxed reels, and the manufacturer will clearly mark the CAT level on the. Second, look on the cable itself. The category level of a piece of cable is usually printed on the cable.

Table 2.1 - CAT Ratings for UTP



CAT Rating	Max Frequency	Max Bandwidth	Status with TIA/EIA
CAT 1	< 1 MHz	Analog phone lines only	No longer recognized
CAT 2	4 MHz	4 Mbps	No longer recognized
CAT 3	16 MHz	16 Mbps	Recognized
CAT 4	20 MHz	20 Mbps	No longer recognized
CAT 5	100 MHz	100 Mbps	No longer recognized
CAT 5e	100 MHz	1000 Mbps	Recognized
CAT 6	250 MHz	10000 Mbps	Recognized

Anyone who's plugged in a telephone has probably already dealt with the registered jack (RJ) connectors used with UTP cable. Telephones use RJ-11 connectors, designed to support up to two pairs of wires. Networks use the four-pair RJ-45 connectors.

Fiber-Optic

Fiber-optic cable transmits light rather than electricity, making it attractive for both high- EMI areas and long-distance transmissions. While a single copper cable cannot carry data more than a few hundred meters at best, a single piece of fiber-optic cabling will operate, depending on the implementation, for distances of up to tens of kilometers.

A fiber-optic cable has four components: the glass fiber itself (the core); the cladding, which is the part that makes the light reflect down the fiber; buffer material to give strength, and the insulating jacket (See figure 2.14).

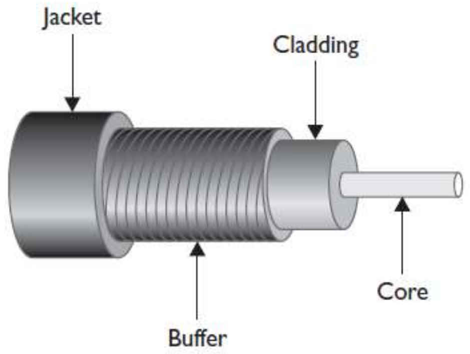


Figure 2.14 - Cross section of fiber-optic cabling

Fiber-optic cabling is manufactured with many different diameters of core and cladding. In a convenient bit of standardization, cable manufacturers use a two-number designator to define fiber-optic cables according to their core and cladding measurements. The most common fiber-optic cable size is 62.5/125 pm. Almost all network technologies that use fiber-optic cable require pairs of fibers. One fiber is used for sending, the other for receiving. In response to the demand for two-pair cabling, manufacturers often connect two fibers together like a lamp cord to create the popular duplex fiber-optic cabling.

Light can be sent down a fiber-optic cable as regular light or as laser light. The two types of light require totally different fiber-optic cables. Most network technologies that use fiber optics use LEDs (light emitting diodes) to send light signals. Fiber-optic cables that use LEDs are known as multimode. Fiber-optic cables that use lasers are known as single-mode. Using laser light and single-mode fiber-optic cables prevents a problem unique to multimode fiber optics called modal distortion and enables a network to achieve phenomenally high transfer rates over incredibly long distances.

Fiber optics also define the wavelength of light used, measured in nanometers (nm). Almost all multimode cables transmit 850-nm wavelength, while single-mode transmit either 1310 or 1550 nm, depending on the laser.

Other Cables

Fiber-optic and UTP make up almost all network cabling, but there are a few other types of cabling that may come up from time to time as alternatives to these two: the ancient serial and parallel cables from the earliest days of PCs and the modern high-speed serial connection, better known as FireWire.

Classic Serial

Serial cabling not only predates networking, it also predates the personal computer. RS-232, the recommended standard (RS) upon which all serial communication takes places on your PC, dates from 1969 and hasn't substantially changed in around 40 years. When IBM invented the PC way back in 1980, serial connections were just about the only standard input/output technology available and IBM added two serial ports to every PC. The most common serial port is a 9-pin, male D-subminiature connector.

Serial ports offer at best a poor option for networking, with very slow data rates— only about 56,000 bps—and only point-to-point connections. In all probability it's faster to copy something on a flash drive and just walk over to the other system, but serial networking does work if needed. Serial ports are quickly fading away and you rarely see them on newer PCs.

Parallel

Parallel connections are almost as old as serial. Parallel can run up to around 2 Mbps, although when used for networking it tends to be much slower. Parallel is also limited to point-to-point topology, but uses a 25-pin female—rather than male—DB type connector. The IEEE 1284 committee sets the standards for parallel communication.

FireWire

FireWire (based on the IEEE 1394 standard) is the only viable alternative cabling option to fiber-optic or UTP. FireWire is also restricted to point-to-point connections, but it's very fast (currently the standard is up to 800 Mbps). FireWire has its own unique connector.

Fire Ratings

To reduce the risk of your network cables burning and creating noxious fumes and smoke, Underwriters Laboratories and the National Electrical Code (NEC) joined forces to develop cabling fire ratings. The two most common fire ratings are PVC and plenum. Cable with a polyvinyl chloride (PVC) rating has no significant fire protection. If you burn a PVC cable, it creates lots of smoke and noxious fumes. Burning plenum-rated cable creates much less smoke and fumes, but plenum-rated cable—often referred to simply as "plenum"—costs about three to five times as much as PVC-rated cable.

The space between the acoustical tile ceiling in an office building and the actual concrete ceiling above is called the plenum—hence the name for the proper fire rating of cabling to use in that space. A third type of fire rating, known as riser, designates the proper cabling to use for vertical runs between floors of a building. Riser-rated cable provides less protection than plenum cable, though, so most installations today use plenum for runs between floors.

Networking Industry Standards—IEEE

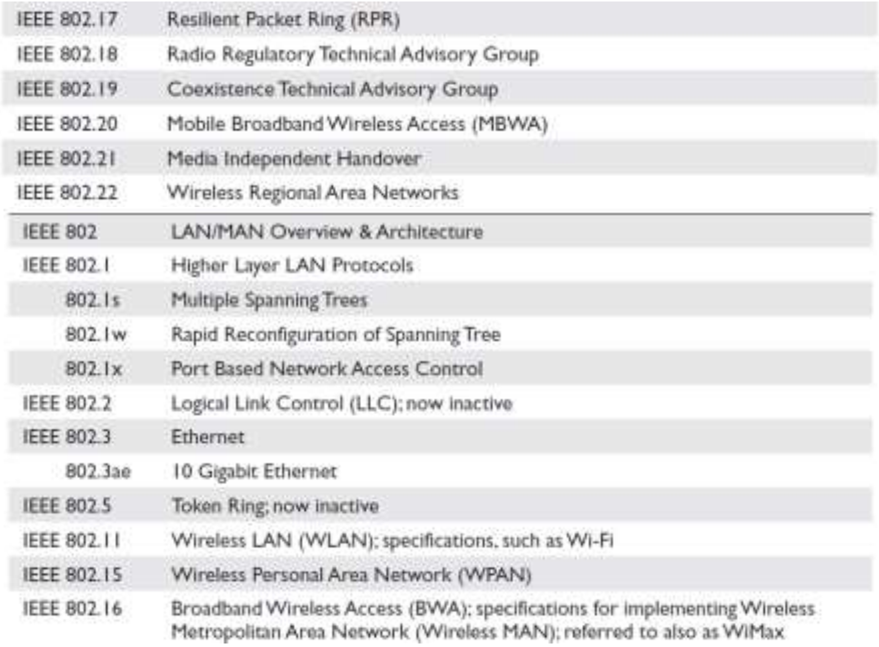
The Institute of Electrical and Electronics Engineers (IEEE) defines industry-wide standards that promote the use and implementation of technology. In February of 1980, a new committee called the

802 Working Group took over from the private sector the job of defining network standards. The IEEE 802 committee defines frames, speed, distances, and types of cabling to use in a network environment. Concentrating on cables, the IEEE recognizes that no single cabling solution can work in all situations, and thus provides a variety of cabling standards.

The IEEE 802 committee sets the standards for networking. Although the original plan was to define a single, universal standard for networking, it quickly became apparent that no single solution would work for all needs. The 802 committee split into smaller subcommittees, with names such as IEEE 802.3 and IEEE 802.5. Table 2.2 shows the currently recognized IEEE 802 subcommittees and their areas of jurisdiction. I've included the inactive subcommittees for reference. The missing numbers, such as 802.4 and 802.12, were used for committees long ago disbanded. Each subcommittee is officially called a Working Group, except the few listed as a Technical Advisory Group (TAG) in the table.

Some of these committees deal with technologies that didn't quite make it, and the committees associated with those standards, such as IEEE 802.4 Token Bus, have become dormant.

Table 2.2 - IEEE 802 Subcommittees



IEEE 802.17	Resilient Packet Ring (RPR)
IEEE 802.18	Radio Regulatory Technical Advisory Group
IEEE 802.19	Coexistence Technical Advisory Group
IEEE 802.20	Mobile Broadband Wireless Access (MBWA)
IEEE 802.21	Media Independent Handover
IEEE 802.22	Wireless Regional Area Networks
IEEE 802	LAN/MAN Overview & Architecture
IEEE 802.1	Higher Layer LAN Protocols
802.1s	Multiple Spanning Trees
802.1w	Rapid Reconfiguration of Spanning Tree
802.1x	Port Based Network Access Control
IEEE 802.2	Logical Link Control (LLC); now inactive
IEEE 802.3	Ethernet
802.3ae	10 Gigabit Ethernet
IEEE 802.5	Token Ring; now inactive
IEEE 802.11	Wireless LAN (WLAN); specifications, such as Wi-Fi
IEEE 802.15	Wireless Personal Area Network (WPAN)
IEEE 802.16	Broadband Wireless Access (BWA); specifications for implementing Wireless Metropolitan Area Network (Wireless MAN); referred to also as WiMax