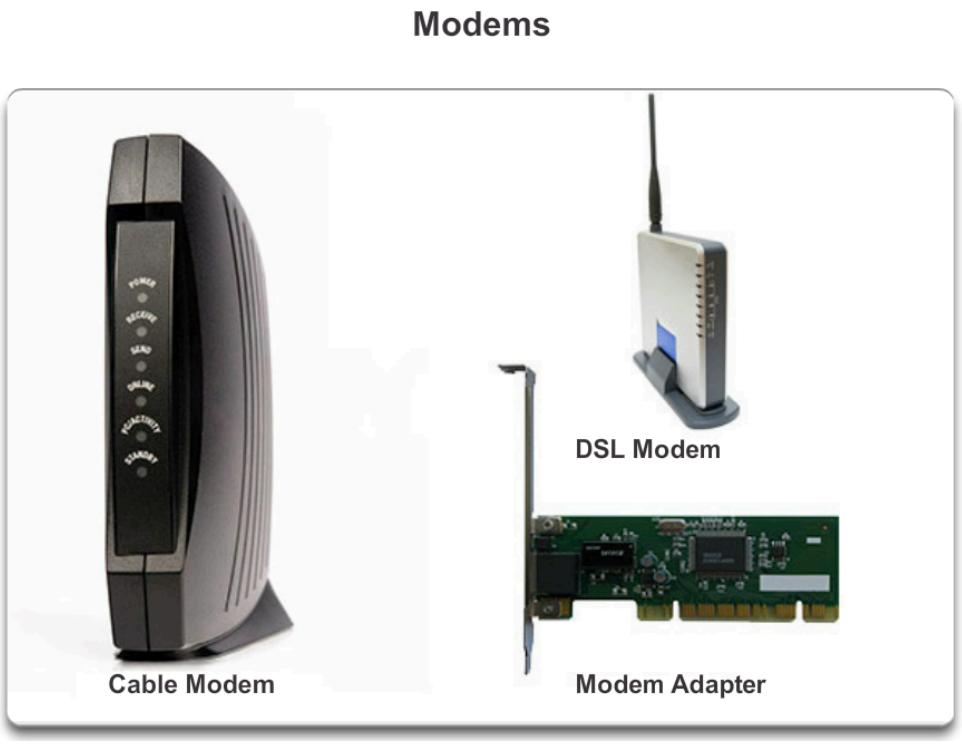
Physical Components of a Network

Network Devices - Modems

To support the immediate delivery of the millions of messages being exchanged between people all over the world, we rely on a web of interconnected networks. The standardization of the various elements of the network enables equipment and devices created by different companies to work together. It is important that IT technicians understand the purpose and function of different network equipment used to support personal and business operations.



A modem is an electronic device that connects to the Internet via an ISP. The modem converts digital data to analog signals for transmission over a phone line. Because the analog signals change gradually and continuously, they can be drawn as waves. In this system, the digital signals are represented as binary bits. The digital signals must be converted to a waveform to travel across telephone lines. They are converted back to bits by the receiving modem so that the receiving computer can process the data.

The modem at the receiving end reconverts the analog signals back to digital data to be interpreted by the computer. The process of converting analog signals to digital and back again is called modulation/demodulation. The accuracy of modem-based transmission has increased with the development of error detection and correction protocols, which has reduced or eliminated the effects of noise and interference on telephone lines.

An internal modem plugs into an expansion slot on the motherboard. External modems connect to a computer through the serial and USB ports. Software drivers must be installed and connection ports configured for the modem to work properly.

When computers use the public telephone system to communicate, it is called Dialup Networking (DUN). Modems communicate with each other using audio tone signals. This means that modems are able to duplicate the dialing characteristics of a telephone. DUN creates a Point-to-Point Protocol (PPP). A PPP is simply a connection between two computers over a phone line.

Hubs, Bridges, and Switches

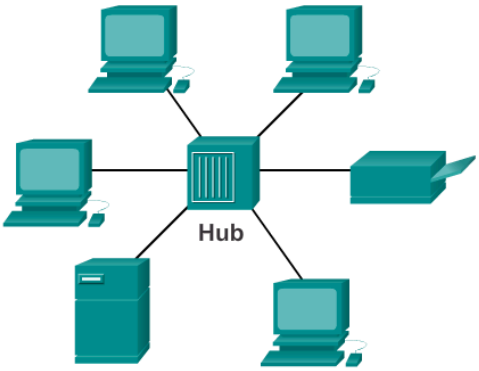
To make data transmission more extensible and efficient than a simple peer-to-peer network, network designers use specialized network devices, such as hubs, bridges and switches, routers, and wireless access points, to send data between devices.

Hubs

Hubs, shown in Figure 1, extend the range of a network by receiving data on one port and then regenerating the data and sending it out to all other ports. A hub can also function as a repeater. A repeater extends the reach of a network because it rebuilds the signal, which overcomes the effects of data degradation over distance. The hub can also connect to another networking device, like a switch or router that connects to other sections of the network.

Hub Front and Back

Connection Through a Hub

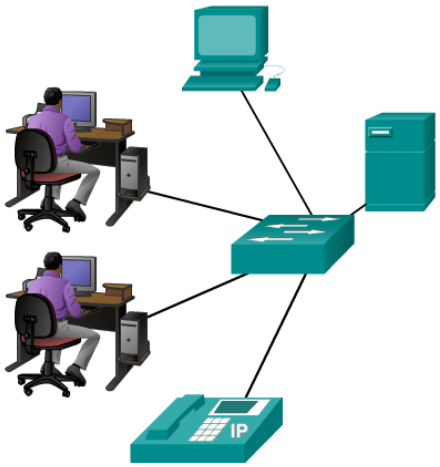


Hubs are used less often today because of the effectiveness and low cost of switches. Hubs do not segment network traffic, so they decrease the amount of available bandwidth for all devices connected to them. In addition, because hubs cannot filter data, a lot of unnecessary network traffic constantly moves between all the devices connected to it.

Bridges and Switches

Files are broken up into small pieces of data, called packets, before they are transmitted over a network. This process allows for error checking and easier retransmission if the packet is lost or corrupted. Address information is added to the beginning and end of packets before they are transmitted. The packet, along with the address information, is called a frame.

LANs are often divided into sections called segments, similar to the way a company is divided into departments, or a school is divided into classes. The boundaries of segments can be defined using a bridge. A bridge filters network traffic between LAN segments. Bridges keep a record of all the devices on each segment to which the bridge is connected. When the bridge receives a frame, the bridge examines the destination address to determine if the frame is to be sent to a different segment or dropped. The bridge also helps to improve the flow of data by keeping frames confined to only the segment to which the frame belongs.



Switch

Switches, shown in Figure 2, are sometimes called multiport bridges. A typical bridge has two ports, linking two segments of the same network. A switch has several ports, depending on how many network segments are to be linked. A switch is a more sophisticated device than a bridge.

In modern networks, switches have replaced hubs as the central point of connectivity. Like a hub, the speed of the switch determines the maximum speed of the network. However, switches filter and segment network traffic by sending data only to the device to which it is sent. This provides higher dedicated bandwidth to each device on the network.

Switches maintain a switching table. The switching table contains a list of all MAC addresses on the network, and a list of which switch port can be used to reach a device with a given MAC address. The switching table records MAC addresses by inspecting the source MAC address of every incoming frame, as well as the port on which the frame

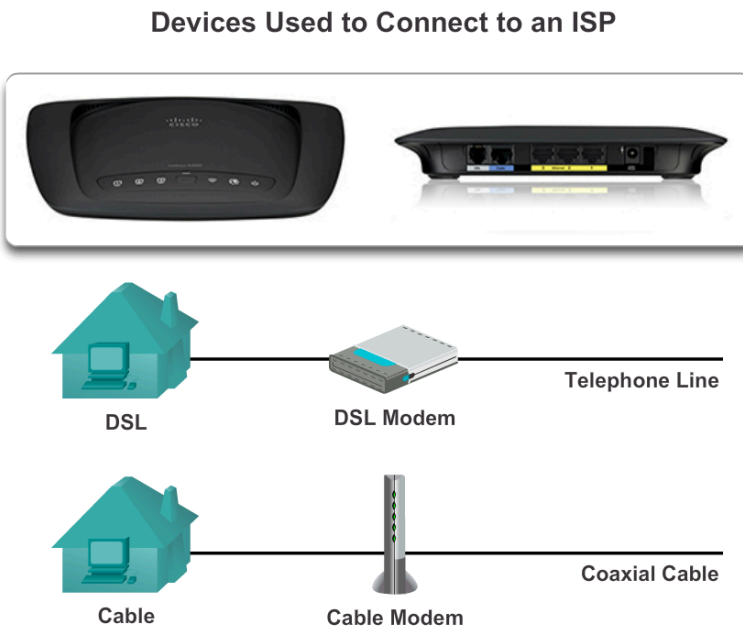
arrives. The switch then creates a switching table that maps MAC addresses to outgoing ports. When a frame arrives that is destined for a particular MAC address, the switch uses the switching table to determine which port to use to reach the MAC address. The frame is forwarded from the port to the destination. By sending frames out of only one port to the destination, other ports are not affected.

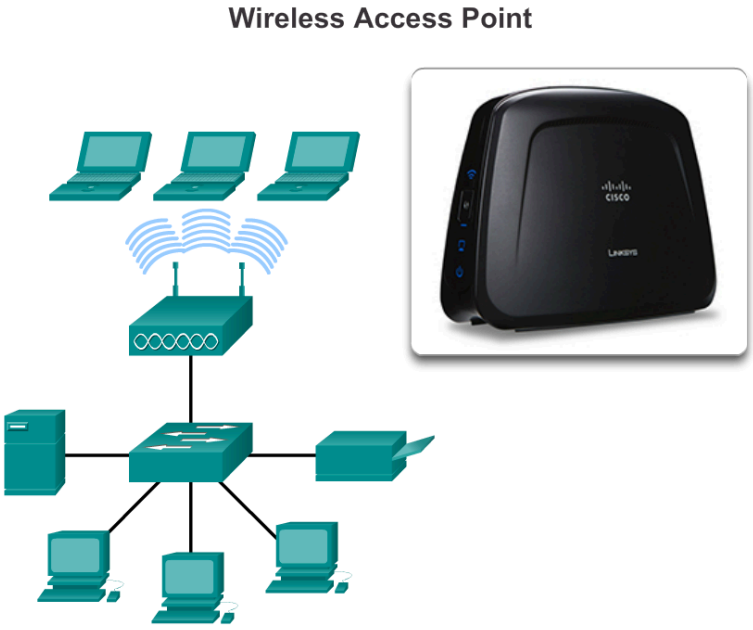
Power over Ethernet (PoE)

A PoE switch transfers small amounts of DC current over Ethernet cable, along with data, to power PoE devices. Low voltage devices that support PoE, such as Wi-Fi access points, surveillance video devices, and NICs, can be powered from remote locations. Devices that support PoE can receive power over an Ethernet connection at distances up to 330 ft (100 m) away.

Routers and Wireless Access Points

When subscribing to an ISP, determine what type of equipment is available to select the most appropriate device. An ISP is a company that provides Internet services to individuals and businesses. An ISP usually provides a connection to the Internet, email accounts, and web pages, for a monthly service fee. Some ISPs rent equipment on a month-to-month basis. This could be more attractive than purchasing the equipment because the ISP supports the equipment if there is a failure, change, or upgrade to the technology. Equipment that can be used to connect to an ISP is shown in Figure 1.





Wireless Access Points

Wireless access points, shown in Figure 2, provide network access to wireless devices, such as laptops and tablets. The wireless access point uses radio waves to communicate with the wireless NIC in the devices and other wireless access points. An access point has a limited range of coverage. Large networks require several access points to provide adequate wireless coverage. A wireless access point provides connectivity only to the network, while a wireless router provides additional features, such as assigning IP addresses.

Routers

Routers connect networks to each other. Switches use MAC addresses to forward a frame within a single network. Routers use IP addresses to forward packets to other networks. A router can be a computer with special network software installed or a device built by network equipment manufacturers.

On a corporate network, one router port connects to the WAN connection and the other ports connect to the corporate LANs. The router becomes the gateway, or path to the outside, for the LAN.

Multipurpose Devices

Multipurpose devices, shown in Figure 3, are network devices that perform more than one function. It is more convenient to purchase and configure one device that serves all your needs than to purchase a separate device for each function. This is especially true for the home user. In a home network, the router connects the computers and network devices in the home to the Internet. The router serves as a home gateway and a switch. The wireless router serves as a home gateway, wireless access point, and a switch. Multipurpose devices may also include a modem.

Multipurpose Device

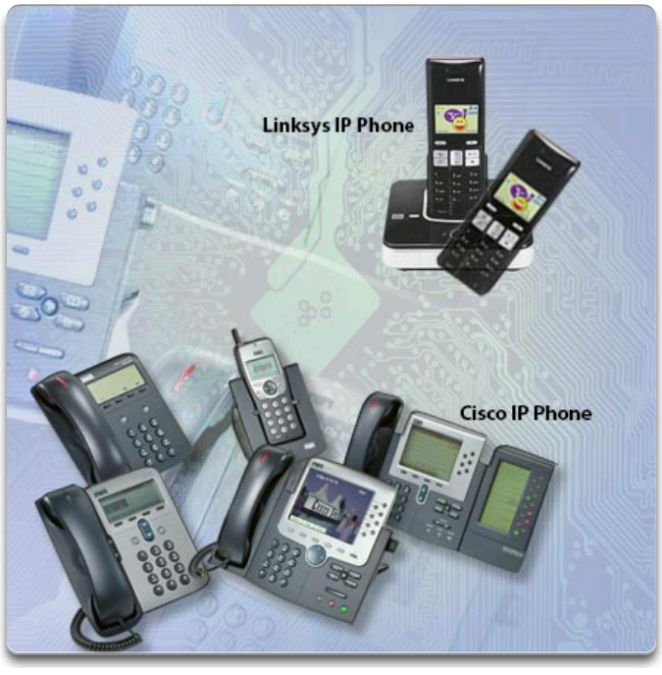
NAS

Network-attached storage (NAS) is a device consisting of one or more hard drives, an Ethernet connection, and an embedded operating system rather than a full-featured network operating system. The NAS device connects to the network, allowing users on the network to access and share files, stream media, and back up data to a central location. NAS devices that support multiple hard drives can provide RAID-level data protection.

NAS is a client/server design. A single hardware device, often called the NAS head, acts as the interface between the NAS and the network clients. Clients always connect to the NAS head, not the individual storage devices. A NAS device requires no monitor, keyboard, or mouse.

NAS systems provide easy administration. They often include built-in features, such as disk space quotas, secure authentication, and automatic sending of email alerts if an error is detected in the equipment.

VoIP Phones



VoIP Phones

Voice over IP (VoIP) is a method to carry telephone calls over the data networks and Internet. VoIP converts the analog signals of voices into digital information that is transported in IP packets. VoIP can also use an existing IP network to provide access to the public switched telephone network (PSTN).

VoIP phones look like normal phones, but instead of using the standard RJ-11 phone connector, they use an RJ-45 Ethernet connector. VoIP phones connect directly to a network and have

all the hardware and software necessary to handle the IP communications.

When using VoIP to connect to the PSTN, you might be dependent on an Internet connection. This can be a disadvantage if the Internet connection experiences an interruption in service. When a service interruption occurs, the user cannot make phone calls.

There are several ways to use VoIP:

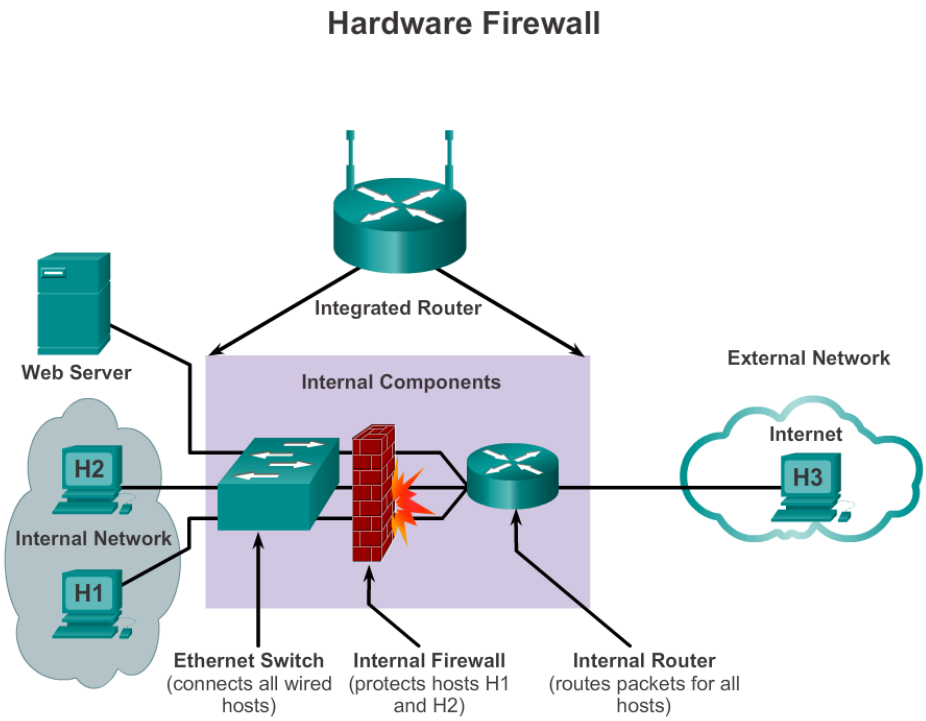
- **IP phone** - A device that connects to an IP network using an RJ-45 Ethernet connector or a wireless connection.
- **Analog Telephone Adapter (ATA)** - A device that connects standard analog devices, such as telephones, facsimile machines, or answering machines, to an IP network.
- **IP phone software** - This application connects by using a microphone, speakers, and a sound card to emulate the IP phone functionality.

Hardware Firewalls

Hardware firewalls, such as integrated routers, protect data and equipment on a network from unauthorized access. A hardware firewall is a free-standing unit that resides between two or more networks, as shown in the figure. It does not use the resources of the computers it is protecting, so there is no impact on processing performance.

A firewall should be used in addition to security software. A firewall resides between two or more networks and controls the traffic between them as well as helps prevent unauthorized access. Firewalls use various techniques for determining what is permitted or denied access to a network segment.

Considerations when selecting a hardware firewall include:



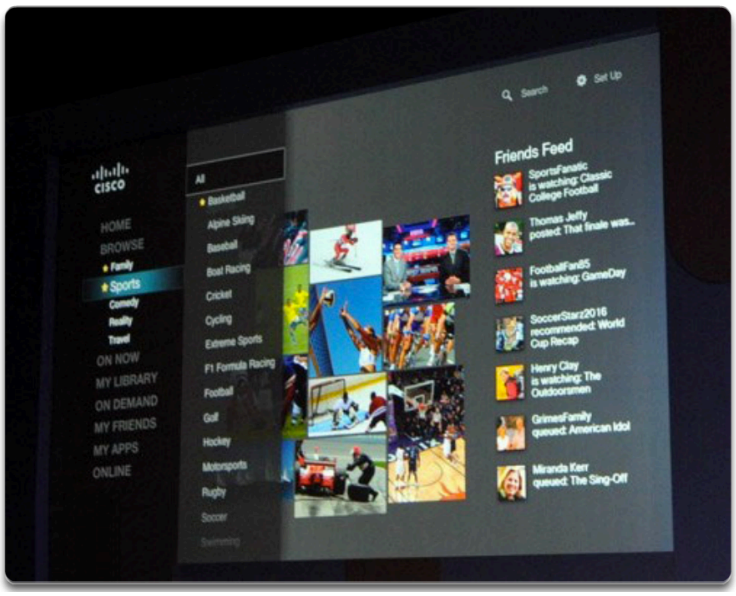
- **Space** - Free standing and uses dedicated hardware
- **Cost** - Initial cost of hardware and software updates can be costly
- **Number of computers** - Multiple computers can be protected
- **Performance requirements** - Little impact on computer performance

NOTE: On a secure network, if computer performance is not an issue, enable the internal operating system firewall for additional security. Some applications might not operate properly unless the firewall is configured correctly for them.

Internet Applications

An Internet appliance is also called a Net appliance, a smart appliance, or an information appliance. Examples of Internet appliance devices include televisions, game consoles, Blu-ray players, and streaming media players. The device is designed for the specific function and has built-in hardware for Internet connectivity. The Internet connection is either wired or wireless. Internet appliances include a CPU and RAM that support email, web surfing, gaming, as well as video streaming and social networking, as shown in the figure.

Web TV



Purchasing Authentic Network Devices

Computer and network problems can be related to counterfeit components. The cosmetic differences between an authentic product and a counterfeit one can be subtle. There are also performance differentiators between authentic products and counterfeits. Many manufacturers have teams that are staffed with engineers well-versed in these differentiators.

Counterfeit products pose network as well as personal health and safety risks. The trafficking of counterfeit computer and networking equipment is a crime that carries serious penalties. In 2008, a former owner of a computer company was sentenced to 30 months in prison and ordered to pay a large sum in restitution as a result of his conviction for trafficking in counterfeit computer components. This type of case serves as an important reminder to customers about the risk of purchasing outside the manufacturer's authorized sales and distribution channels.

The cosmetic differences between an authentic product and a counterfeit can be extremely subtle or non existent.

To help ensure that you are getting authentic products, consider these points when placing orders or requesting quotes:

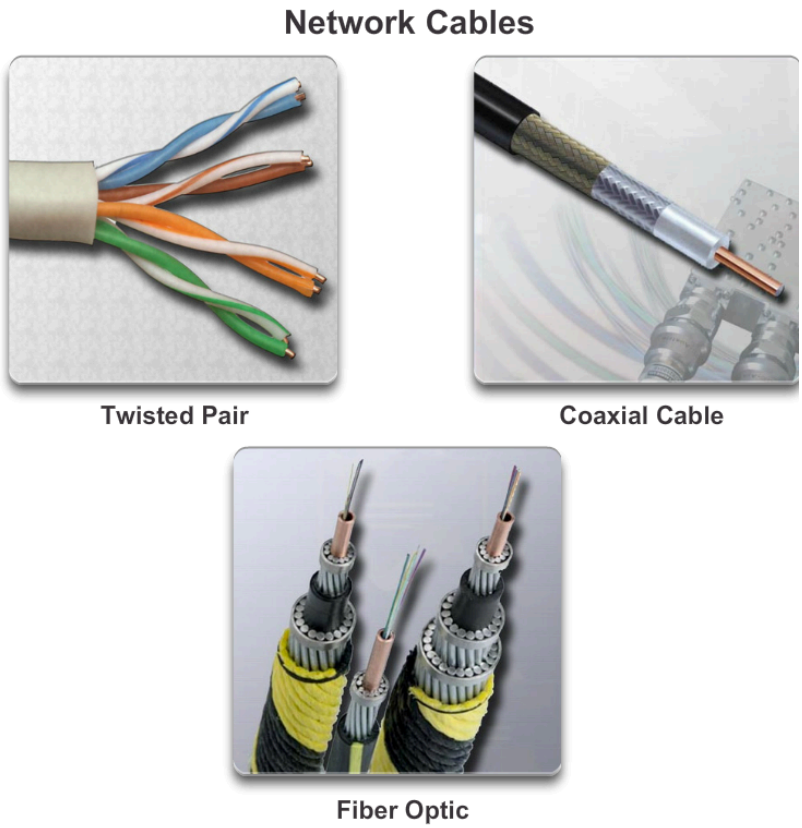
- Always purchase your equipment directly from authorized channels.
- Confirm that the equipment is a new, authentic product and not previously owned.
- Be suspicious when prices seem too good to be true.
- The product is offered at a much higher discount than authentic products. These discounts could be as high as 70 to 90 percent off.

- Check that the equipment comes with a valid software license.
- Check that the equipment has a full warranty enclosed.
- Ask whether the equipment includes service support.
- The product appears to have proper labeling, logos, and trademarks, but the performance or appearance is substandard as compared to authentic products.
- Be suspicious of packaging that appears to be substandard, not original, tampered with, or previously used.

Do not do business with any supplier who insists that you:

- Order immediately to beat a price increase.
- Take advantage of a special offer that is about to expire.
- Reserve the last few remaining products in stock.
- Purchase OEM specials.
- Take advantage of Internet, email, or telemarketing offers that send representatives to pick up your payment in person or demand cash on delivery.

Cables and Connectors



A wide variety of networking cables are available, as shown in the figure. Coaxial and twisted-pair cables use copper to transmit data. Fiber-optic cables use glass or plastic to transmit data. These cables differ in bandwidth, size, and cost. You need to know what type of cable to use in different situations to install the correct cables for the job. You also need to be able to troubleshoot and repair problems that you encounter. Select the cable type that is the most beneficial and cost effective for the users and services that will connect to the network.

Cost

When designing a network, cost is a consideration. Installing cables is expensive, but after a one-time expense, a wired network is normally inexpensive to maintain.

Security

A wired network is usually more secure than a wireless network. The cables in a wired network are usually installed in walls and ceilings and are therefore not easily accessible. It is easier to gain unauthorized access to the signals on a wireless network than a wired network. Radio signals are available to anyone who has a receiver. To make a wireless network as secure as a wired network requires using authentication and encryption.

Design for the Future

Many organizations install the highest grade of cable that is available. This ensures that the networks are prepared for additional bandwidth requirements in the future. To avoid expensive cable installations later, you and your customer must decide if the cost of installing a higher grade cable is necessary.

Wireless

A wireless solution might be needed in places where cables cannot be installed, such as an older, historic building where local building codes do not permit structural modifications.

Coaxial Cables

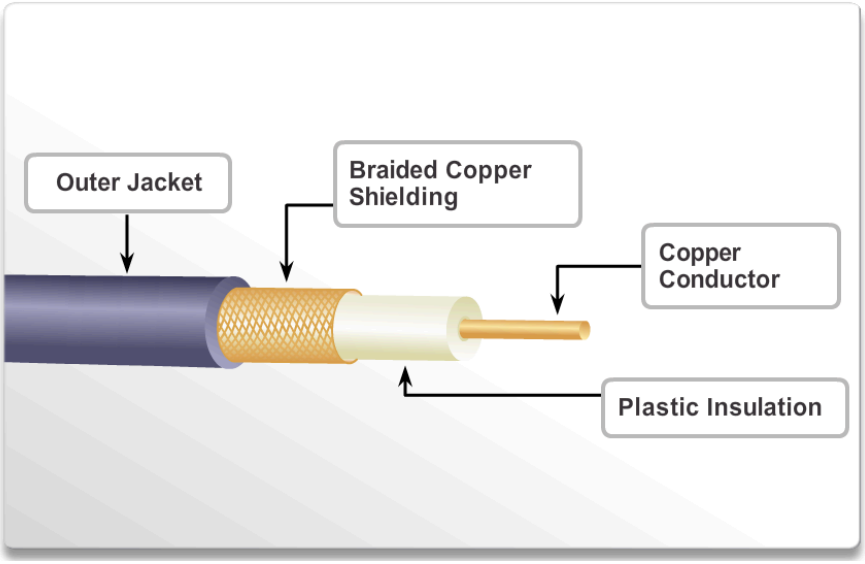
Coaxial cable, shown in Figure 1, is usually constructed of either copper or aluminum. It is used by cable television companies to provide service and for connecting the various components that make up satellite communication systems.

Coaxial cable (or coax) carries data in the form of electrical signals. It provides improved shielding compared to unshielded twisted-pair (UTP), so it has a higher signal-to-noise ratio and can therefore carry more data. However, twisted-pair cabling has replaced coax in LANs because, when compared to UTP, coax is physically harder to install, more expensive, and harder to troubleshoot.

Coaxial cable is enclosed in a sheath or jacket, as shown in Figure 2. There are several types of coaxial cable:

Coaxial Cabling

Coaxial Cable Design



- **Thicknet or 10BASE5** - Used in networks and operated at 10 Mb/s with a maximum length of 1640.4 ft. (500 m.)

- **Thinnet 10BASE2** - Used in networks and operated at 10 Mb/s with a maximum length of 607 ft. (185 m.)

- **RG-59** - Most commonly used for cable television in the United States

- **RG-6** - Higher quality cable than RG-59, with more bandwidth and less susceptibility to interference

Coaxial Connections

Cable service provider wiring inside a customer's premises is coax. Several connecting methods are used to connect coaxial cable together. Two common connection types, shown in Figure 3, include:

- **F series** - Primarily used in television cable and antenna applications up to 1 GHz

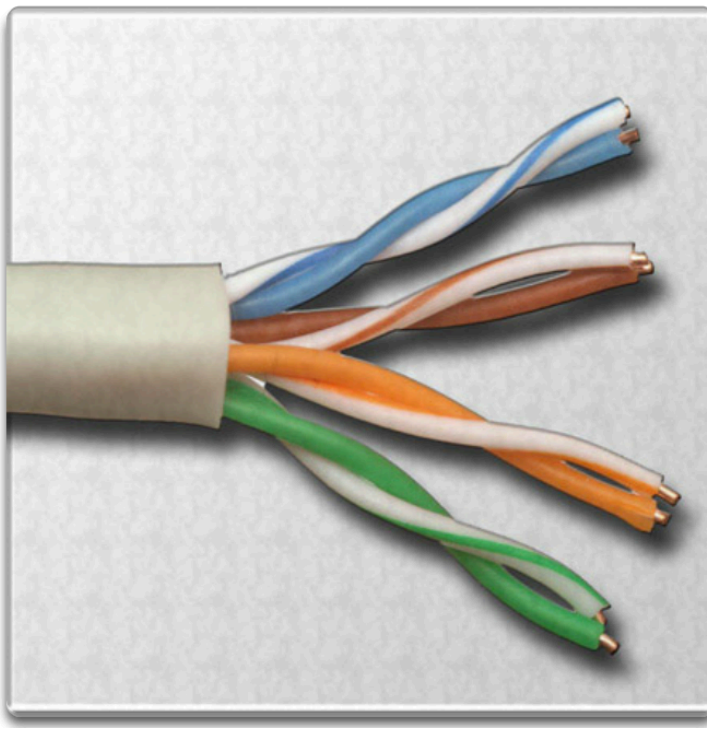
- **BNC** - Designed for military use and also used in video and RF applications to 2 GHz

The F series connector has a standard thread pattern, but push-on designs are also available. The BNC uses a push, twist, and lock connector. Coaxial cable has no specific maximum bandwidth, and the type of signaling technology used determines the speed and limiting factors.

Twisted-Pair Cables

Twisted-pair is a type of copper cabling used for telephone communications and most Ethernet networks. A pair of wires forms a circuit that can transmit data. The pair is twisted to provide protection against crosstalk, which is the noise generated by adjacent pairs of wires in the cable. Pairs of copper wires are encased in color-coded plastic insulation and twisted together. An outer jacket protects the bundles of twisted pairs. A twisted-pair cable is shown in Figure 1.

Twisted-Pair Cabling



When electricity flows through a copper wire, a magnetic field is created around the wire. A circuit has two wires. The two wires in that circuit have oppositely charged magnetic fields. When the two wires of the circuit are next to each other, the magnetic fields cancel each other out. This is called the cancellation effect. Without the cancellation effect, network communications become slow due to the interference caused by the magnetic fields.

There are two basic types of twisted-pair cables:

- **Unshielded twisted-pair (UTP)** - Cable that has two or four pairs of wires. This type of cable relies solely on the cancellation effect produced by the twisted-wire pairs that limits signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). UTP is the most commonly used cabling in networks. UTP cables have a length up to 330 ft. (100 m.).

- **Shielded twisted-pair (STP)** - Each pair of wires is wrapped in metallic foil to better shield the wires from noise. Four pairs of wires are then wrapped in an overall metallic braid or foil. STP reduces electrical noise from within the cable. It also reduces EMI and RFI from outside the cable.

Both UTP and STP have the same analog bandwidth performance characteristics. While digital bandwidth is measured in bits per second, analog bandwidth is measured in Hertz. Analog bandwidth is the range of frequency over which a

cable has been tested to operate. For example, Cat 7 cable is tested up to 600MHz to ensure it meets the specifications of the Cat 7 standard.

Although STP prevents interference better than UTP, STP is more expensive because of extra shielding, and more difficult to install because of the thickness. In addition, the metallic shielding must be grounded at one end. If improperly grounded, the shield acts like an antenna picking up unwanted signals. STP is primarily used outside of North America.

Category Rating

Twisted-pair cables come in several categories (Cat). These categories are based on the number of wires in the cable and the number of twists in those wires.

The size of the network determines the type of network cable that will be used. Most networks today are wired using twisted-pair copper cable. The characteristics of twisted-pair cable are shown in Figure 2.

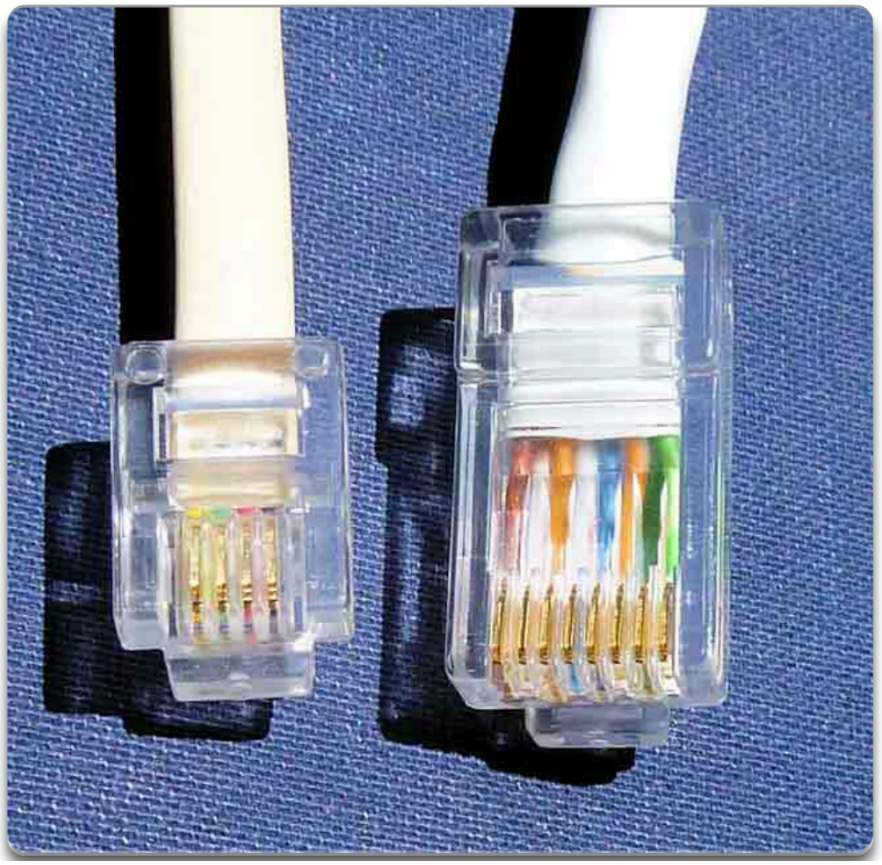
New or renovated office buildings often have some type of UTP cabling that connects every office to a central point called the Main Distribution Facility (MDF). The distance limitation of UTP cabling used for data is 330 ft. (100 m.). Cable runs in excess of this distance limitation need a switch, repeater, or hub to extend the connection to the MDF.

Cables that are installed inside the walls and ceilings of buildings must be plenum rated. A plenum cable is one that is safe for installation between a dropped ceiling and the structural ceiling of a building where air circulation takes place. Plenum-rated cables are made from a special plastic that retards fire and produces less smoke than other cable types.

Twisted-Pair Cable Features

	Speed	Features
Cat 3 UTP	10 Mb/s at 16 MHz	• Suitable for Ethernet LAN. • Most often used for phone lines.
Cat 5 UTP	100 Mb/s at 100 MHz	Manufactured with higher standard than Cat 3 to allow for higher data transfer rates.
Cat 5e UTP	1000 Mb/s at 100 MHz	• Manufactured with higher standard than Cat 5 to allow for higher data transfer rates. • More twists per foot than Cat 5 to better prevent EMI and RFI from outside sources.
Cat 6 UTP	1000 Mb/s at 250 MHz	• Manufactured with higher standard than Cat 5e. • More twists per foot than Cat 5e to better prevent EMI and RFI from outside sources. • Cat 6a has better insulation and performance than Cat 6. • May have a plastic divider to separate pairs of wires inside the cable to better prevent EMI and RFI. • Good choice for customers using applications that require large amounts of bandwidth, such as videoconferencing or gaming. • ScTP (Screened Twisted-Pair) is very expensive and not as flexible as UTP.
Cat 6a UTP	1000 Mb/s at 500 MHz	
Cat 7 ScTP	10 Gb/s at 600 MHz	

RJ-11 and RJ-45 Connectors



NOTE: Cat 3 cables use a 6-pin RJ-11 connector, whereas all other twisted-pair cables use an 8-pin RJ-45 connector, as shown in Figure 3.

Wire Schemes

There are two different patterns, or wiring schemes, called T568A and T568B. Each wiring scheme defines the pinout, or order of wire connections, on the end of the cable. The two schemes are similar except that two of the four pairs are reversed in the termination order.

On a network installation, one of the two wiring schemes (T568A or T568B) should be chosen and followed. It is important that the same wiring scheme is used for every termination in that project. If working on an existing network, use the wiring scheme that already exists.

Using the T568A and T568B wiring schemes, two types of cables can be created: a straight-through cable and a crossover cable. These two types of cable are found in data installations.

Straight-through Cables

A straight-through cable is the most common cable type. It maps a wire to the same pins on both ends of the cable. In other words, if T568A is on one end of the cable, T568A is also on the other. If T568B is on one end of the cable, T568B is on the other. This means that the order of connections (the pinout) for each color is the exact same on both ends.

Two devices directly connected and using different pins for transmit and receive are known as unlike devices. They require a straight-through cable to exchange data. There are two unlike devices that require a straight-through cable, a switch port to router port and a hub port to PC.

Crossover Cable

A crossover cable uses both wiring schemes. T568A on one end of the cable and T568B on the other end of the same cable. This means that the order of connection on one end of the cable does not match the order of connections on the other.

Devices that are directly connected and use the same pins for transmit and receive, are known as like devices. They require the use of a crossover cable to exchange data. Like devices that require a crossover cable include:

- Switch port to switch port
- Switch port to hub port
- Hub port to hub port

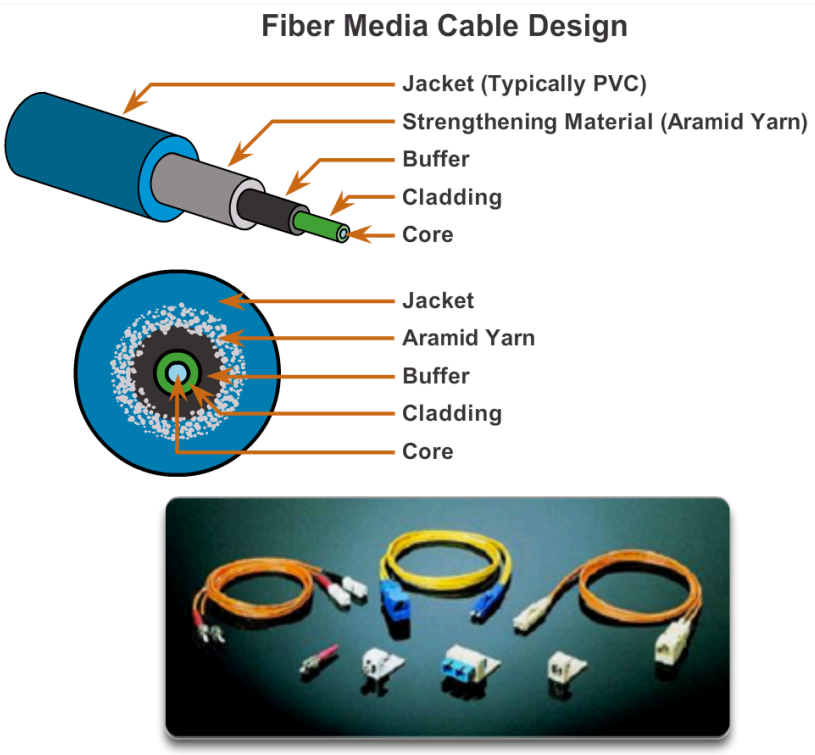
- Router port to router port
- PC to router port
- PC to PC

If the incorrect cable type is used, the connection between network devices will not function.

Some devices can automatically sense which pins are used for transmit and receive and will adjust their internal connections accordingly.

Fiber-Optic Cables

An optical fiber is a glass or plastic medium that transmits information using light. Fiber-optic cable has one or more optical fibers enclosed in a sheath or jacket, as shown in the figure. Because it uses light to transmit signals, fiber-optic cable is not affected by EMI or RFI. All signals are converted to light pulses as they enter the cable, and converted back into electrical signals when they leave it. This means that fiber-optic cable can deliver signals that are clearer, can go farther, and have greater bandwidth than cable made of copper or other metals.



Fiber-optic cables can reach distances of several miles or kilometers before the signal needs to be regenerated. Either lasers or light emitting diodes (LEDs) generate the light pulses that are used to represent the transmitted data as bits on the media. Bandwidth reaches speeds of 100 Gb/s and increases as standards are developed and adopted.

The speed of data transmitted over fiber-optic cable is limited by the devices connected to the cable, as well as impurities within the fiber cable. Electronic semiconductor devices called photodiodes detect the light pulses and convert them to voltages that can then be reconstructed into data frames.

Fiber-optic cable is usually more expensive to use than copper cable, and the connectors are more costly and harder to assemble. Common connectors for fiber-optic networks are:

- **SC** - 2.5 mm ferrule that uses a snap-in connector that latches with a simple push-pull motion
- **ST** - 2.5 mm ferrule that uses a bayonet mount connector that is spring loaded
- **LC** - 1.25 mm ferrule that uses a snap-in connector that latches with a simple push-pull motion

These three types of fiber-optic connectors are simplex, which allows data to flow in only one direction. Therefore, two cables are needed to provide data flow in both directions.

These are the two types of glass fiber-optic cable:

- **Multimode** - Cable that has a thicker core than single-mode cable. It is easier to make, can use simpler light sources (LEDs), and works well over distances up to 6,560 ft (2 km). It often uses LEDs as the light source within LANs or distances of 200 meters within a campus network.

- **Single-mode** - Cable that has a very thin core. It is harder to make, uses lasers as a light source, and can transmit signals up to 62.14 mi (100 km). It often uses lasers as the light source within campus backbones for distances of several thousand meters.