Chapter 2

Data Communication and Network Components

Outline

- Communication
- Data Communication
- Modes of Data Communication
- Components of the network Devices
- Network Media

What is Data Communication?

- *Communication* is simply the act of transferring information from one place, person or group to another.
- **Data communication** (also **data transmission** or digital communications) is the transfer of **data** (a digital bitstream or a digitized analog signal) over a point-to-point or point-to-multipoint **communication** channel.

Data Communication

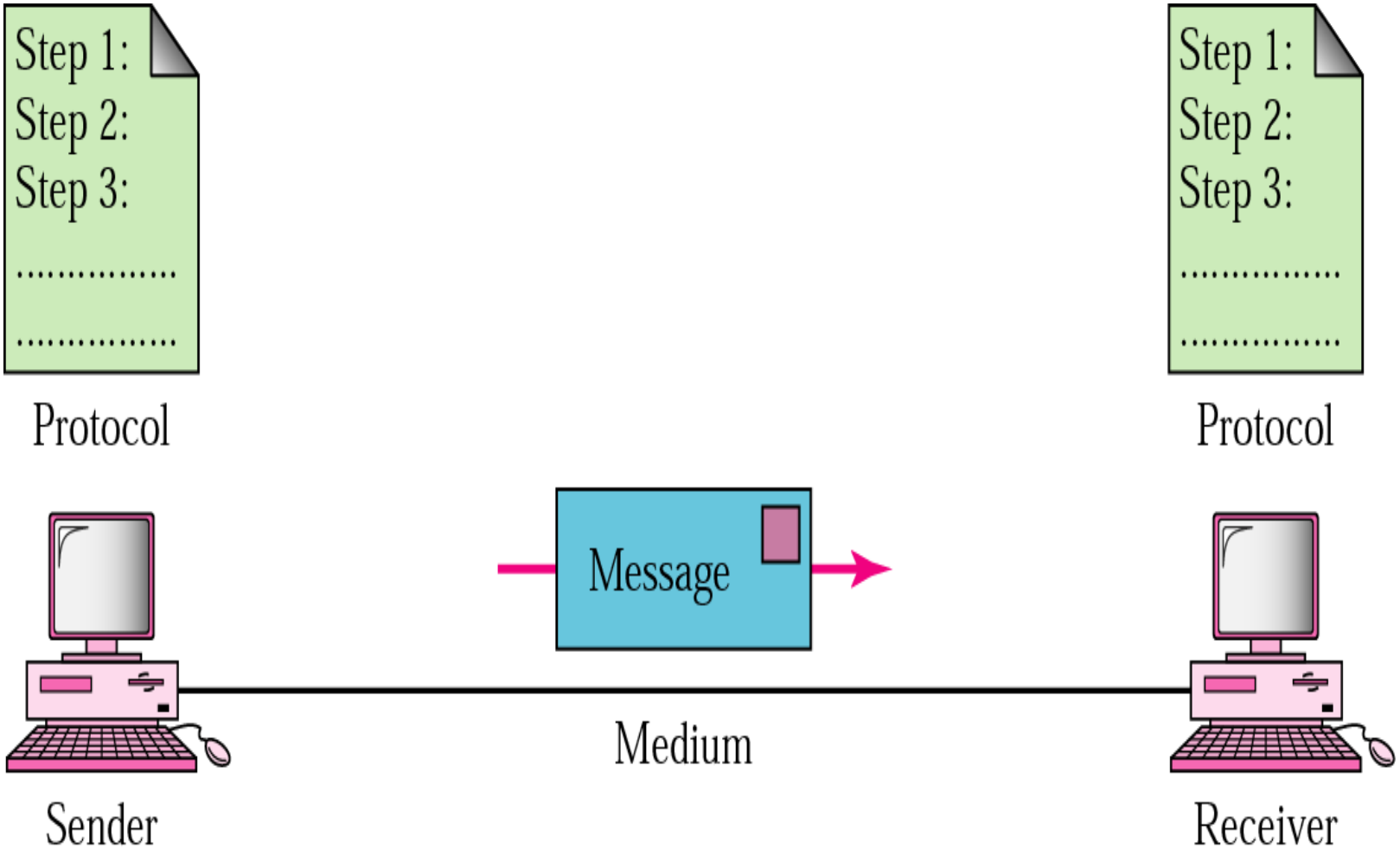
- Data communication involves transporting data from one point to another.
- In data communication, five basic elements can be identified.
  - The source (the sender)
  - The medium (the channel)
  - The destination (receiver)
  - The Information(message)
  - The communication Protocol

Data Communication

There are five components in data communication system.

- **Message**: the information to be communicated
- **Sender**: the device that sends the message
- **Receiver**: the device that receives the message
- **Medium**: the transmission medium is the physical path that communicates the message from sender to receiver.
- **Protocol**: refers to a set of rules that coordinates the exchange of information. Both the sender and the receiver should follow the same protocol to communicate data.

Data Communication Model



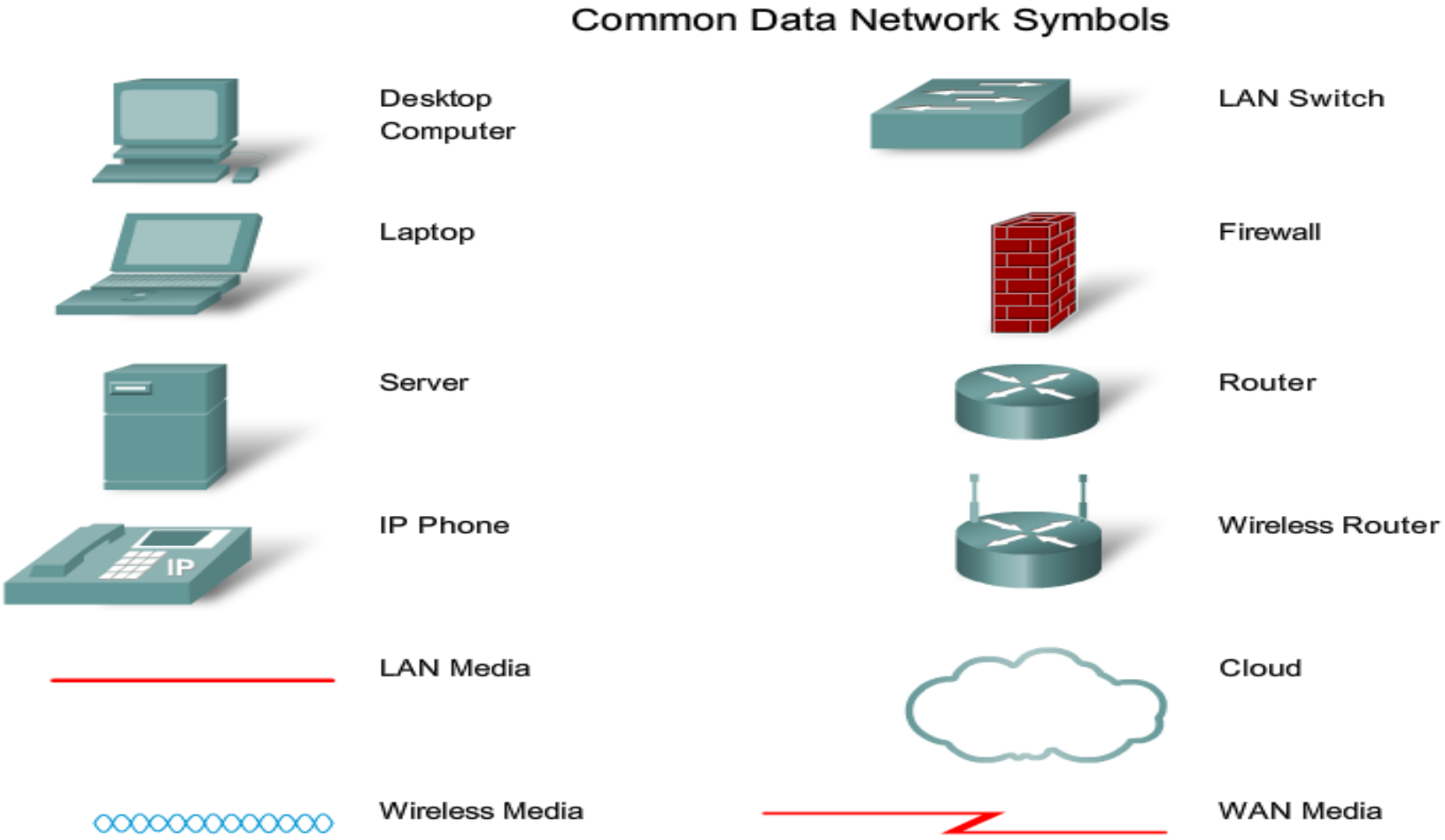
Messages

- The messages or units of information that travel from one device to another
- In the first step of its journey from the computer to its destination, message gets converted into a format that can be transmitted on the network.
- All types of messages must be converted to bits, binary coded digital signals, before being sent to their destinations.
- This is true no matter what the original message format was: text, video, voice, or computer data. Once our instant message is converted to bits, it is ready to be sent onto the network for delivery.

Network Devices Sender/Receiver

- Devices on the network that exchange messages with each other.
- Senders and Receivers are network devices.
  - Switch
  - Firewall-provides security to networks
  - Router- helps direct messages as they travel across a network
  - Wireless Router
  - Serial Link - one form of WAN interconnection, represented by the lightning bolt-shaped line

Network Devices



Rules/Protocols

- Rules or agreements to govern how the messages are sent, directed, received and interpreted.

- Rules are the standards and protocols that specify how the messages are sent, how they are directed through the network, and how they are interpreted at the destination devices

Modes of Data Communication

When data are transmitted from one point to another, three modes of transmission can be identified:

- Simplex
- Half Duplex
- Full Duplex

Simplex Data Communication Mode

- In simplex mode, data is transmitted in only one direction.
- A terminal can only send data and cannot receive it or it can only receive data but cannot send it.
- Simplex mode is usually used for a remote device that is meant only to receive data.
- It is not possible to confirm successful transmission of data in simplex mode.

Simplex Data Communication Mode

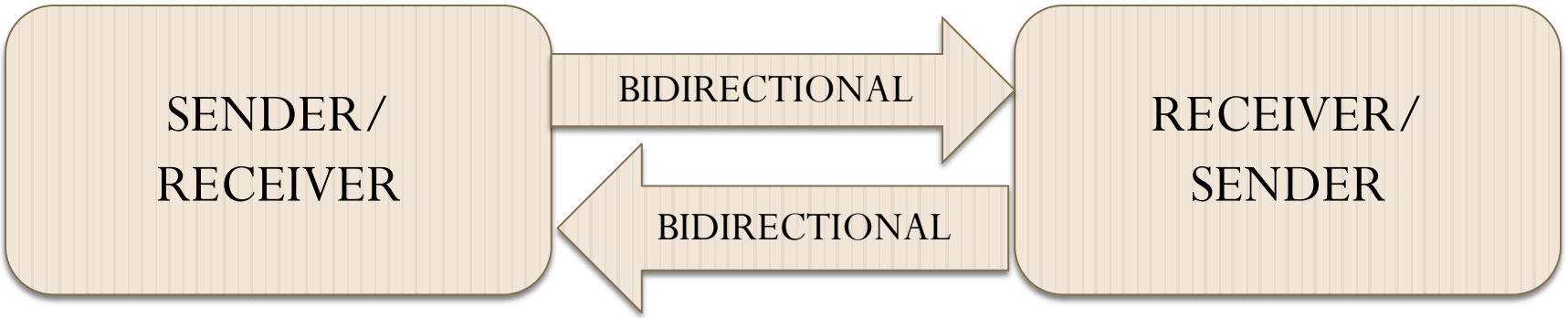
- This mode is not widely used.
  - Examples
    - Speaker, radio and television broadcasting are examples of simplex transmission, on which the signal is send from the transmission to your TV antenna.
- There is no return signal.

Half-Duplex Data Communication Mode

- In half duplex mode, data can be transmitted in both directions but only in one direction at a time.
- During any transmission, one is the transmitter and the other is receiver.
- So each time for sending or receiving data, direction of data communication is reversed, this slows down data transmission rate.

Half-Duplex Data Communication Mode

- In half duplex modes, transmission of data can be confirmed



Full Duplex Data Communication Mode

- In full mode, data can be transmitted in both directions simultaneously.
- It is a faster mode for transmitting data because no time wastes in switching directions.
  - Example of full duplex is a computer network in which both the users can send and receive data at the same time.
  - Telephone conversation, Internet

Full Duplex Mode

Simplex, Half Duplex & Full Duplex

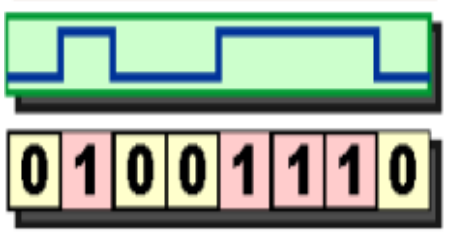
	Simplex	Half Duplex	Full Duplex
Cost	Cheapest communication	Expensive	Most Expensive
Data transmission	One way	Two way one at a time	Simultaneous transmission
Bandwidth	Low	Medium	High

Communication Signals

- There are two types of Communication Signals. These are
  - Digital Signal
  - Analog Signal

Digital signal:

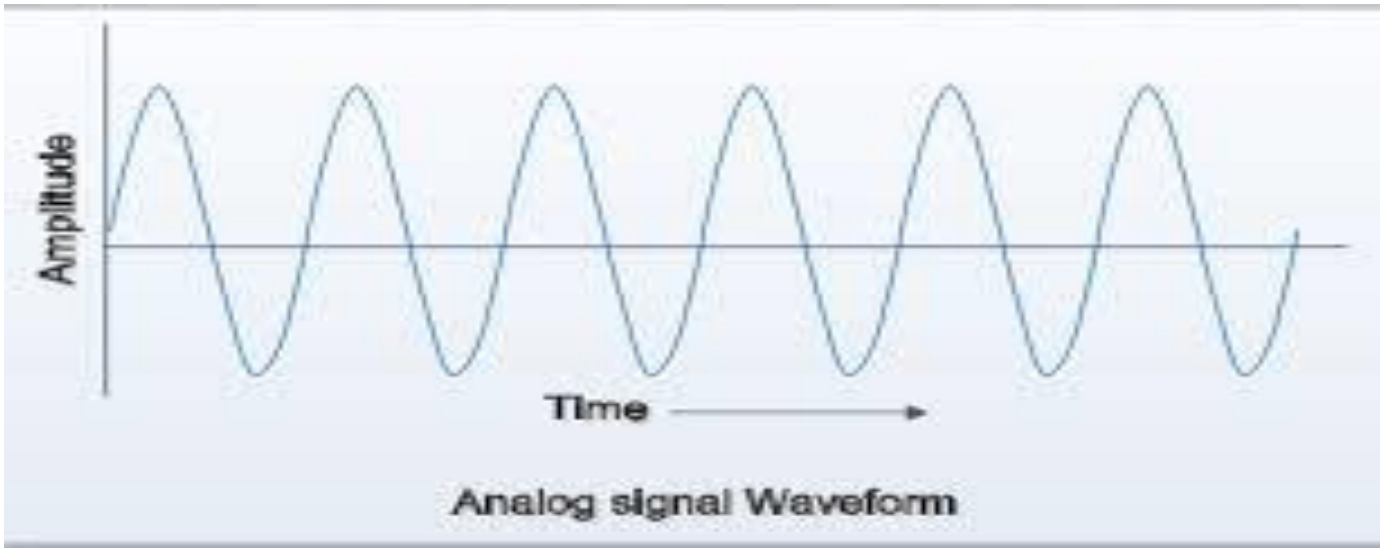
- A signal which is discrete with respect to time is called digital signal.
- Such signal can be modeled using binary number system as shown in the figure below.



Communication Signals

Analog signal

- is any continuous signal for which the time varying feature of the signal is a representation of some other time varying quantity.



Components Network Devices

- End network Devices
- Intermediary network Devices

End Devices and Their Roles on the Network

End Devices

- The network devices that people are most familiar with are called end devices.
- These devices form the interface between the human network and the underlying communication network.
- A source or destination **device** in an end networked system
- end devices are referred to as hosts.

End Devices

Some examples of end devices are:

- Computers
  - Desktops
  - Laptops
  - Tablet
  - file servers, web servers)
- Network printers
- VoIP phones
- Mobile handheld devices (PDAs)

End Devices

- A host device (end devices) is either the source or destination of a message transmitted over the network.
- In order to distinguish one host from another, each host on a network is identified by an address.
- When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

Intermediary Devices

- In addition to the end devices that people are familiar with, networks rely on intermediary devices to provide connectivity and to work behind the scenes to ensure that data flows across the network.
- These devices connect the individual hosts (end devises) to the network and can connect multiple individual networks to form an internetwork.
- **Internetworking** is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices

Intermediary Devices

Examples of intermediary network devices are:

- Network Access Devices
  - Hubs
  - switches
  - wireless access points
- Internetworking Devices (routers)
- Communication Servers and Modems
- Security Devices (firewalls)

Intermediary Devices

- The management of data as it flows through the network is also a role of the intermediary devices.

- These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Intermediary Devices

Processes running on the intermediary network devices perform these functions:

- Regenerate and retransmit data signals
- Maintain information about what pathways exist through the network and internetwork
- Direct data along alternate pathways when there is a link failure
- Notify other devices of errors and communication failures
- Classify and direct messages according to QoS (quality of services) priorities
- Permit or deny the flow of data, based on security settings

Network Medias

- A means of interconnecting these devices - a medium that can transport the messages from one device to another
- For a network to function, the devices must be inter-connected. Network connections can be wired or wireless.
- In wired connections, the medium is either copper, which carries electrical signals, or optical fiber, which carries light signals.
- In wireless connections, the medium is the Earth's atmosphere, or space, and the signals are microwaves.

Network Medias

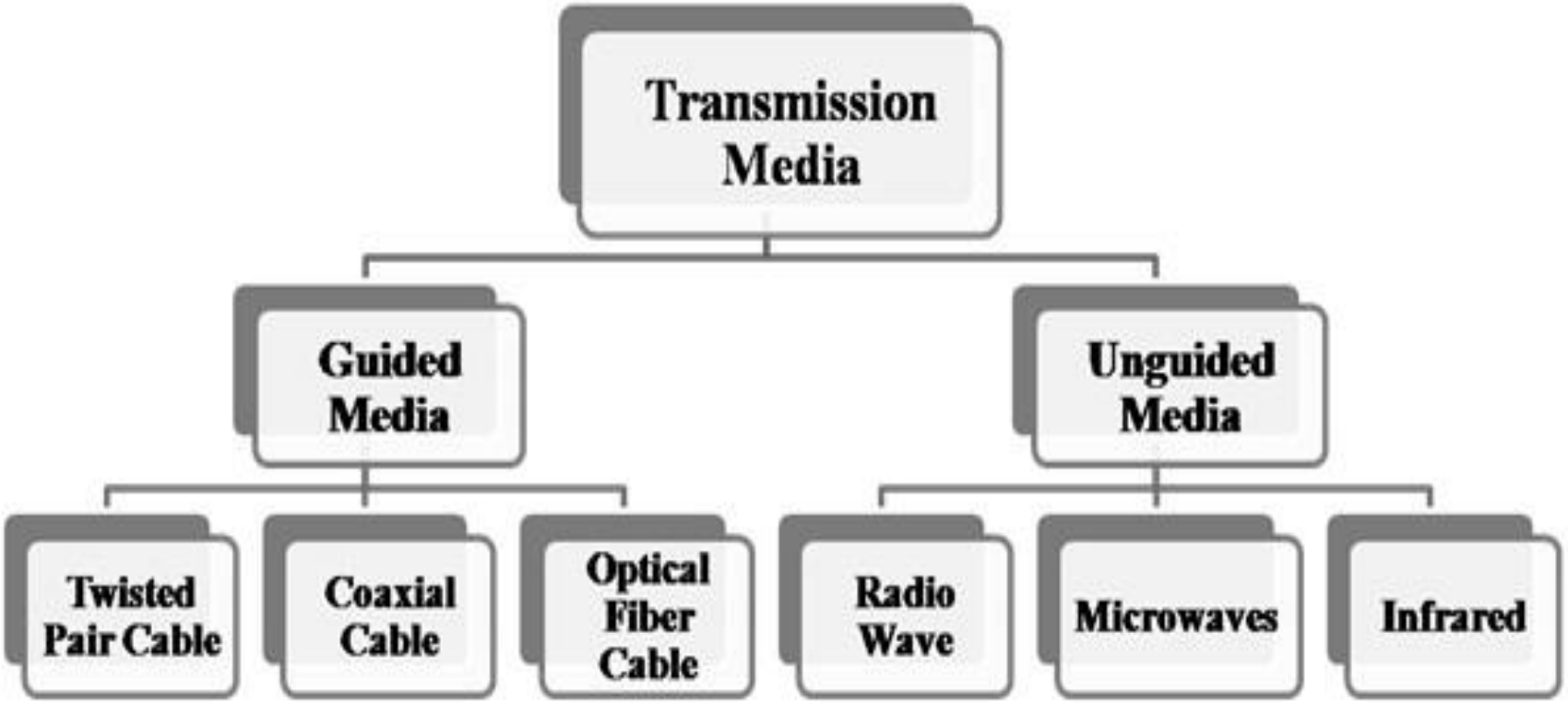
- Copper medium includes cables, such as twisted pair cable and coaxial cable
- Fiber optic cable is a thin strands of glass or plastic that carry light signals, are another form of networking media.
- Wireless media may include the home wireless connection between a wireless router and a computer with a wireless network card, wireless connection between two ground stations, or the communication between devices on earth and satellites.

Network Medias

- The vast majority of networks today are connected by some sort of wiring or cabling that acts as a network transmission medium that carries signals between computers.

- Many cable types are available to meet the varying needs and sizes of networks, from small to large.

Network Transmission Media



Types of Guided Media

Three major groups of cabling connect the majority of networks:

- Twisted-pair cable
- Coaxial cable
- Fiber-optic cable

Twisted Pair Cables

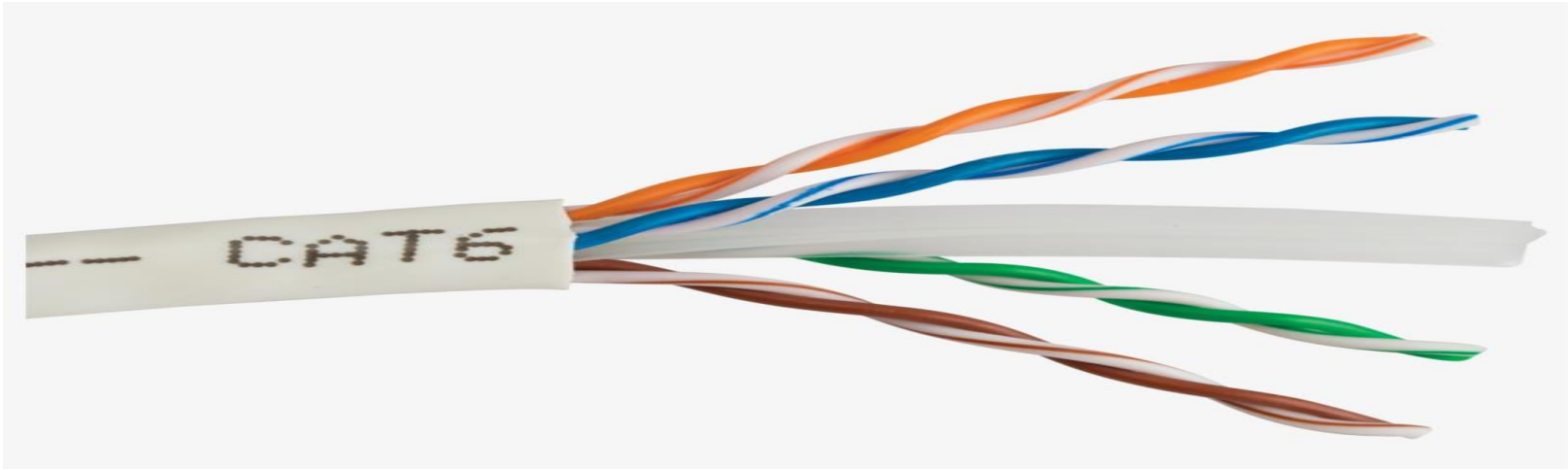
- Twisted-pair cable is a type of cabling that is used for telephone communications and most modern Ethernet networks
- A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable.
- The total number of pairs in a cable varies.
- The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs.

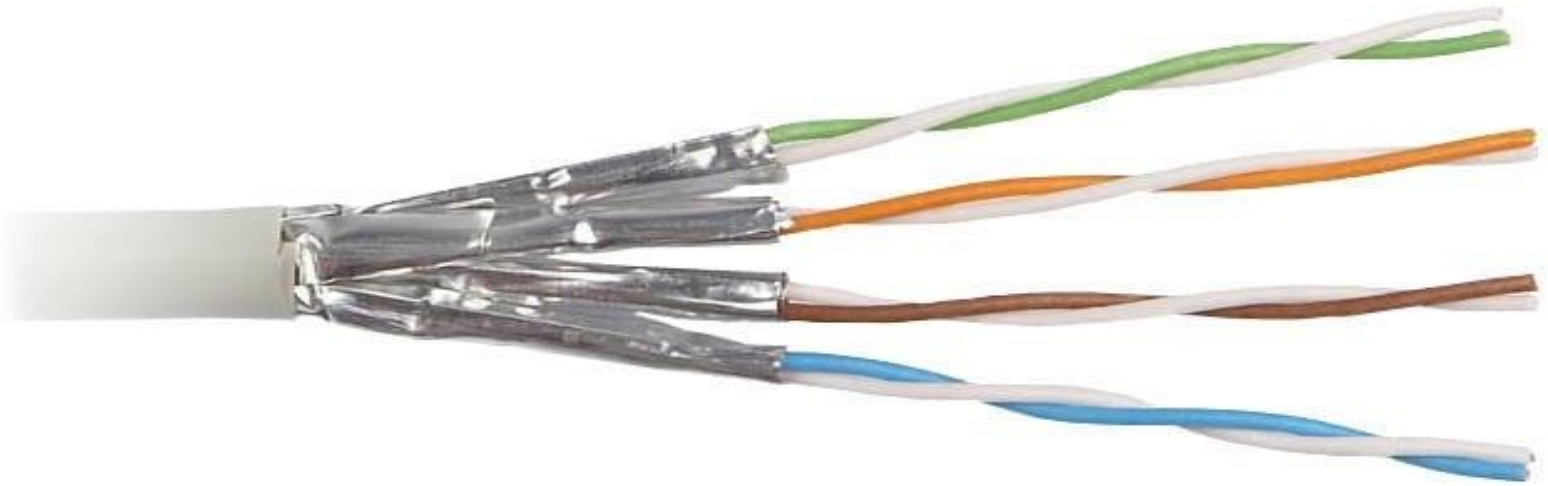
Twisted Pair Cables

Two basic types of twisted-pair cable exist:

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP).

UTP Vs STP

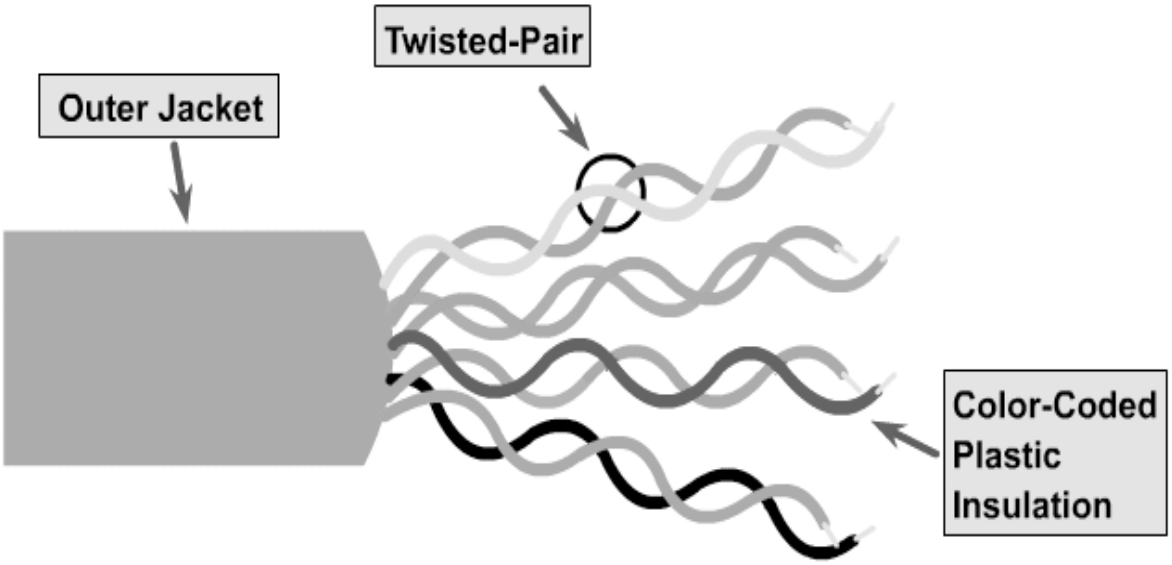


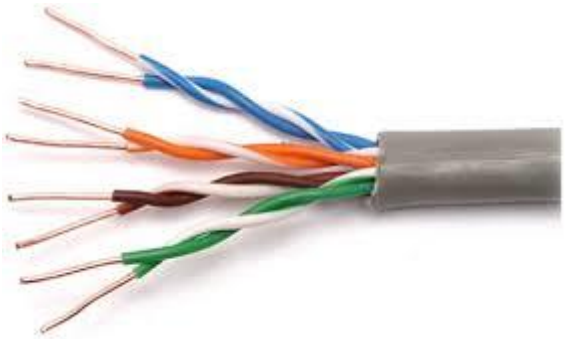


Unshielded Twisted Pair (UTP)

- UTP cable is a medium that is composed of pairs of wires.
- UTP cable is used in a variety of networks.
- Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other.

UTP





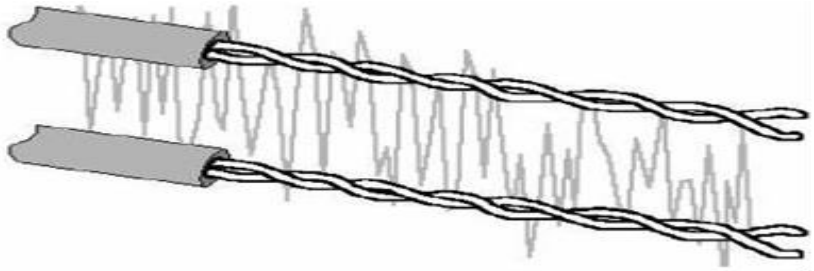
UTP

- UTP cable relies on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by Electromagnetic interference (EMI) or Radio frequency interference (RFI)

- To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies.

UTP

- Crosstalk is defined the situation in which, signals from one line interfering with signals from another line.
- UTP is particularly susceptible to crosstalk, but the greater the number of twists per foot of cable, the more effective the protection against crosstalk.



Crosstalk occurs when signals from one line bleed into another line

Twisted-Pair Cabling Components

- Twisted-pair cabling uses RJ-45 connectors to connect to a computer. These are similar to RJ-11 telephone connectors.
- Although RJ-11 and RJ-45 connectors look alike at first glance, there are crucial differences between them:
- **The RJ-45 connector:** is slightly larger and will not fit into the RJ-11 telephone jack.
- The RJ-45 connector houses eight cable connections, while the RJ-11 houses only four.

Twisted-Pair Cabling Components

RJ45

RJ11

UTP advantages

- It has a large installed base and is a familiar technology.
- It is relatively inexpensive and easy to install.
- Most LAN systems are readily capable of running over UTP.
- It does not require bonding and grounding.
- Easy to install.

UTP disadvantages

- UTP is potentially more sensitive to external electromagnetic interference, crosstalk, and attenuation than other media.
- Not suitable for transmitting data over long distances at high speeds.
- The distance between signal boosts is shorter for UTP than it is for coaxial and fiber-optic cables. (100m Max)

Shielded Twisted-Pair (STP) Cable

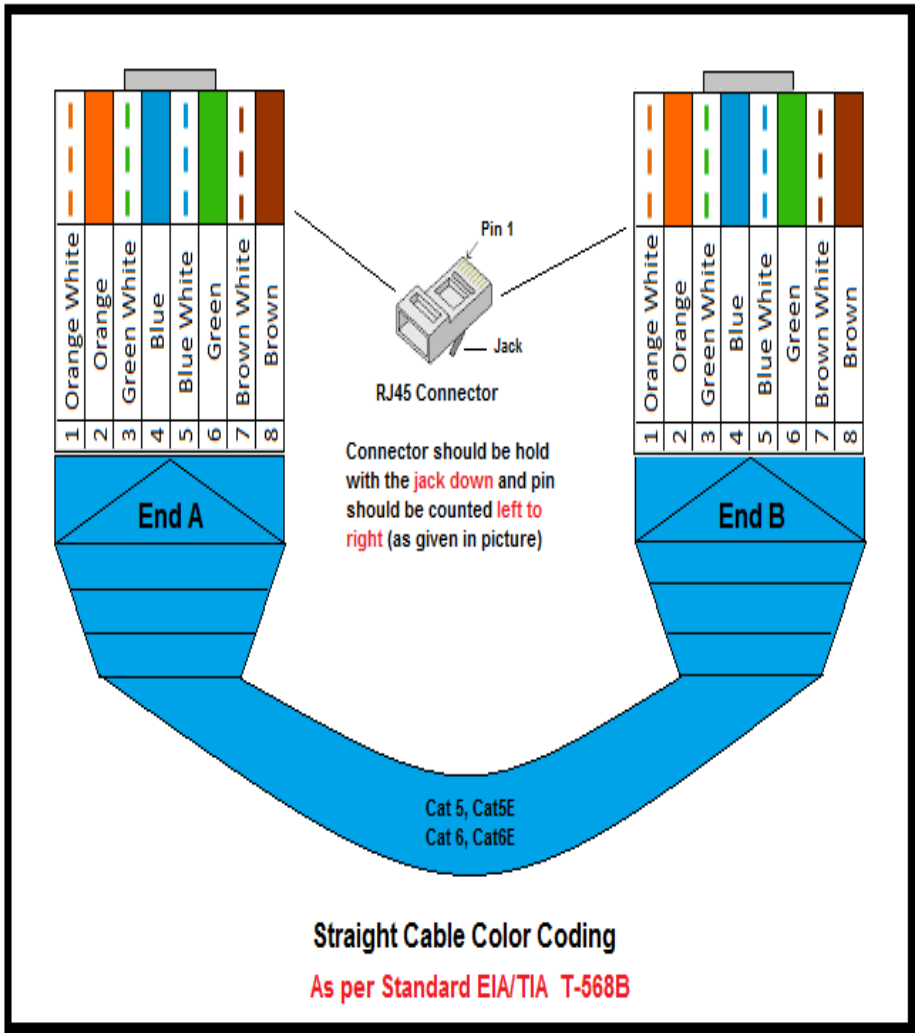
- STP cable uses a *woven/wounded copper-braid jacket* that is more protective and of a higher quality than the jacket used by UTP.
- STP also uses a *foil (very thin sheet of metal)* wrap around each of the wire pairs.
- This gives STP excellent shielding to protect the transmitted data from outside interference.
- STP usually is installed with STP data connector, which is created especially for the STP cable.
- However, STP cabling also can use the same RJ connectors that UTP uses.

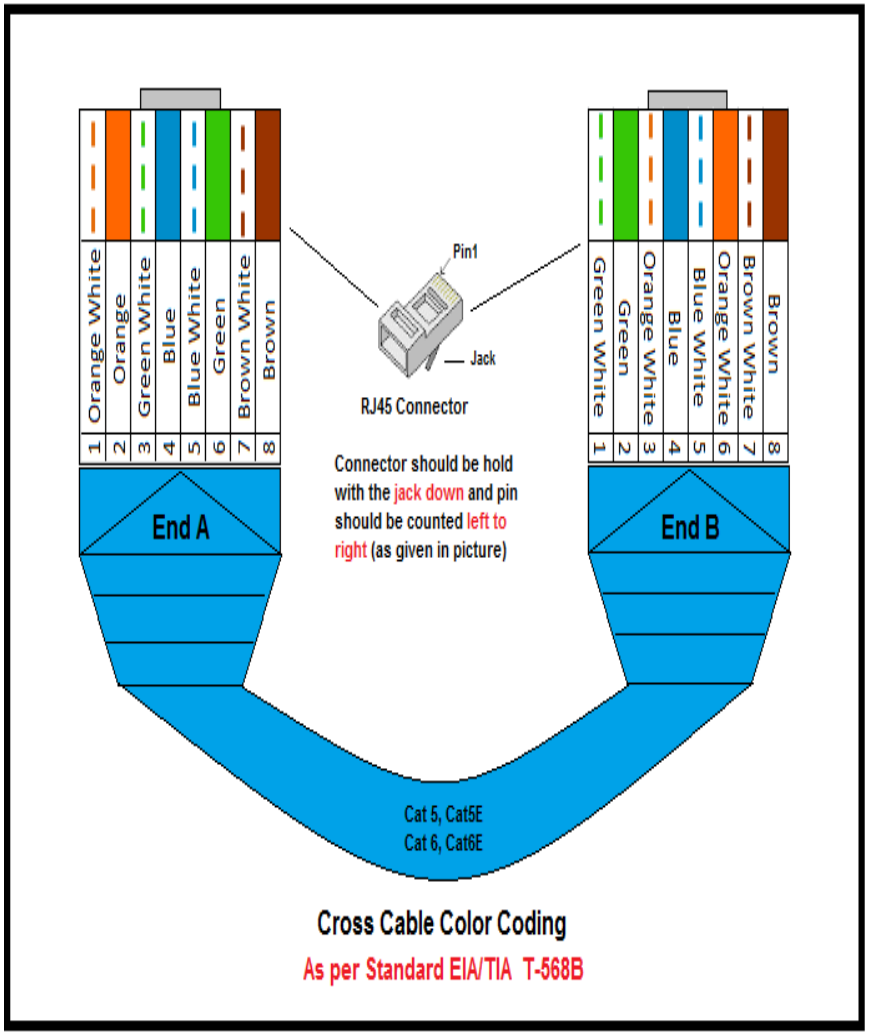
STP

UTP versus STP

- The speed of both types of cable is usually satisfactory for local-area network distances.
- These are the least-expensive media for data communication. UTP is less expensive than STP.
- Because most buildings are already wired with UTP, many transmission standards are adapted to use it, to avoid costly rewiring with an alternative cable type.
- Although STP prevents interference better than UTP, it is more expensive and difficult to install.

Color Codes in UTP/STP





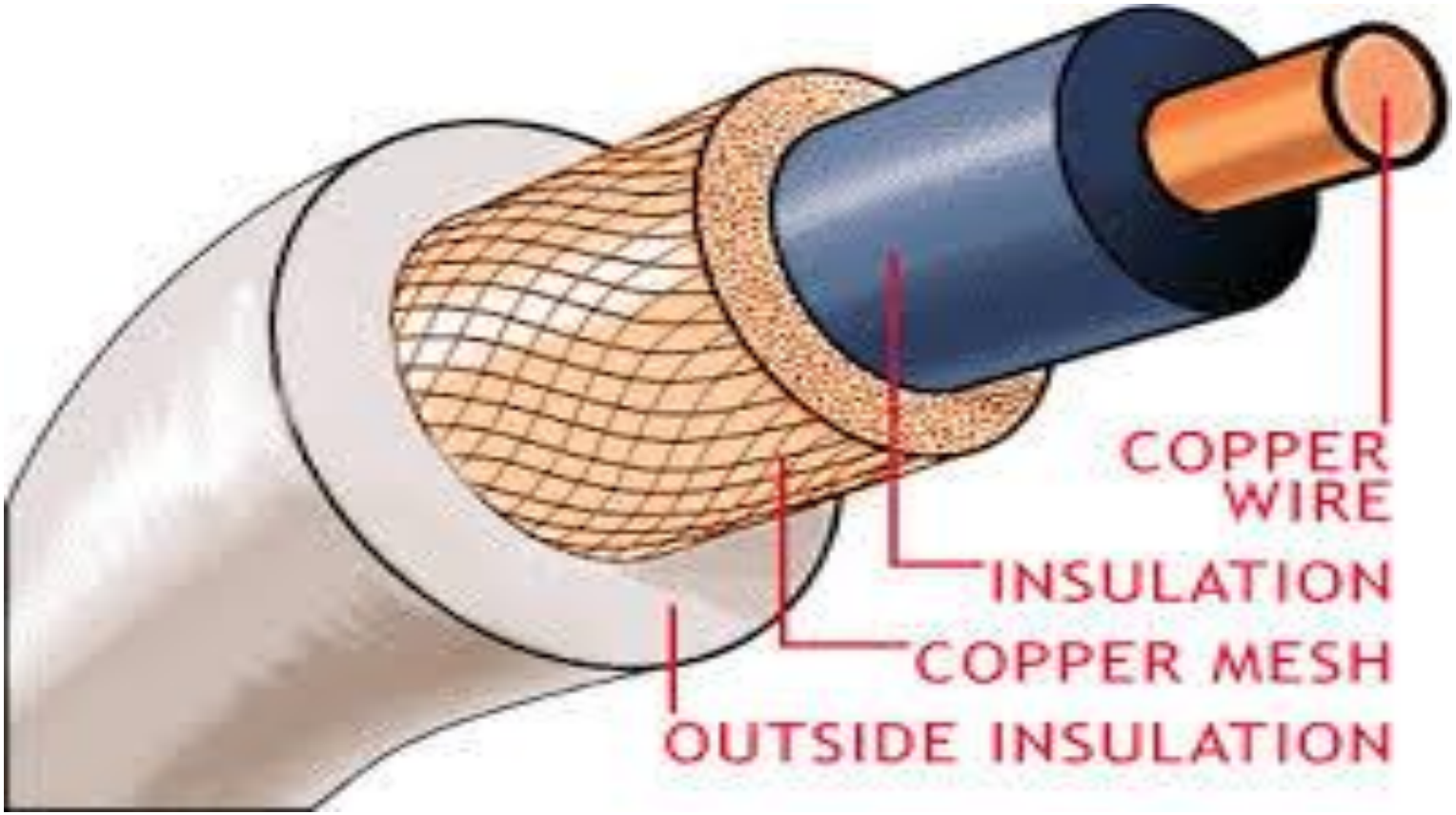
There are 7 standards categories of UTP:

- **Category 1:** This refers to traditional UTP telephone cable that can carry voice but not data transmissions.
- **Category 2:** This category certifies UTP cable for data transmissions up to 4 megabits per second (4 Mbps). It consists of four twisted pairs of copper wire.
- **Category 3:** This category certifies UTP cable for data transmissions up to 10 Mbps. It consists of four twisted pairs of copper wire with three twists per foot.
- **Category 4:** This category certifies UTP cable for data transmissions up to 16 Mbps. It consists of four twisted pairs of copper wire.
- **Category 5:** This category certifies UTP cable for data transmissions up to 100 Mbps. It consists of four twisted pairs of copper wire.
- **Category 5e:** Improved version of cat 5 category. The bandwidth is 1000MBPS
- **Category 6:** Similar to CAT5 wire, but contains a physical separator between the 4 pairs to further reduce electromagnetic interference.
- Category 7or 7e
- Category 8: is currently the fastest standard for UTP/STP. (30m)

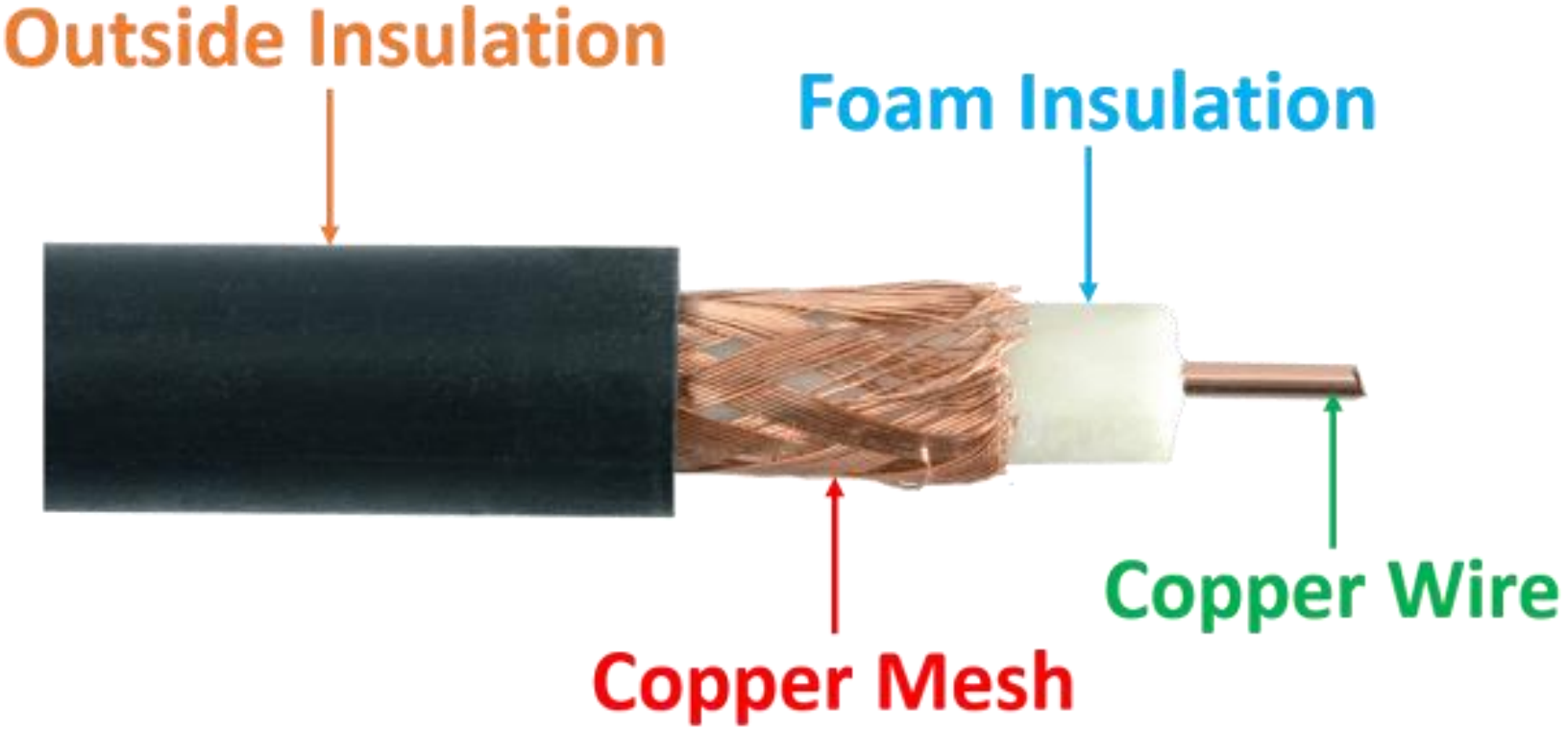
Coaxial Cable

- Coaxial cable consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover.
- The term shielding refers to the woven or stranded metal mesh (or other material) that surrounds some types of cabling.
- Shielding protects transmitted data by absorbing stray electronic signals, called noise, so that they do not get onto the cable and distort the data.
- Cable that contains one layer of foil insulation and one layer of braided metal shielding is referred to as dual shielded.

Coaxial Cable



Coaxial Cable Networks



Coaxial Cable

- The core of a coaxial cable carries the electric signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper.
- Surrounding the core is an insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk.
- The conducting core and the wire mesh must always be kept separate from each other. If they touch, the cable will experience a short, and noise or stray signals on the mesh will flow onto the copper wire.

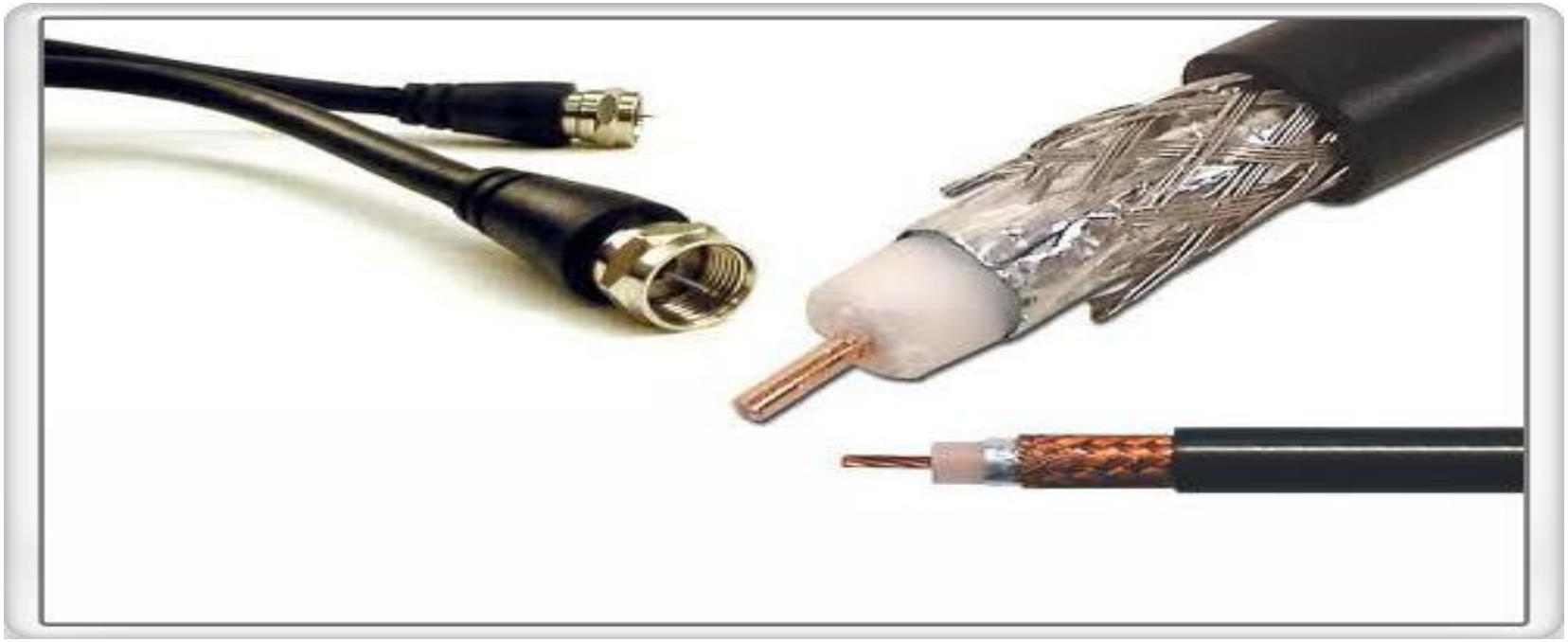
Coaxial Cable

- A non-conducting outer shield—usually made of rubber, Teflon, or plastic surrounds the entire cable.
- Coaxial cable is more resistant to interference and attenuation than twisted pair cabling.
- Attenuation is the loss of signal strength that begins to occur as the signal travels farther along a copper cable.

Types of Coaxial Cable

There are two types of coaxial cable:

- Thinnet Coaxial cable
- Thicknet Coaxial cable



Thinnet

- Thinnet cable is a flexible coaxial cable about 0.64 centimeters (0.25 inches) thick.
- This type of coaxial cable is flexible and easy to work with.
- Thinnet coaxial cable can carry a signal for a distance of up to approximately 185 meters (about 607 feet) before the signal starts to suffer from attenuation.

Thicknet

- Thicknet cable is a relatively rigid coaxial cable about 1.27 centimeters (0.5 inches) in diameter.
- Thicknet cable's copper core is thicker than a thinnet cable core.
- The thicker the copper core, the farther the cable can carry signals.
- This means that thicknet can carry signals farther than thinnet cable.

Thicknet

- Thicknet cable can carry a signal for 500 meters (about 1640 feet).
- Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

Coaxial-Cable Connection Hardware

- Both thinnet and thicknet cable use a connection component, known as a BNC connector, to make the connections between the cable and the computers.
- **The BNC T connector:** This connector joins the network interface card (NIC) in the computer to the network cable.

BNC Connector

Coaxial Cable

Advantage of Coaxial Cable

- It is less susceptible to interference than twisted-pair cable.
- Transmit data for greater distances than is possible with less expensive cabling.

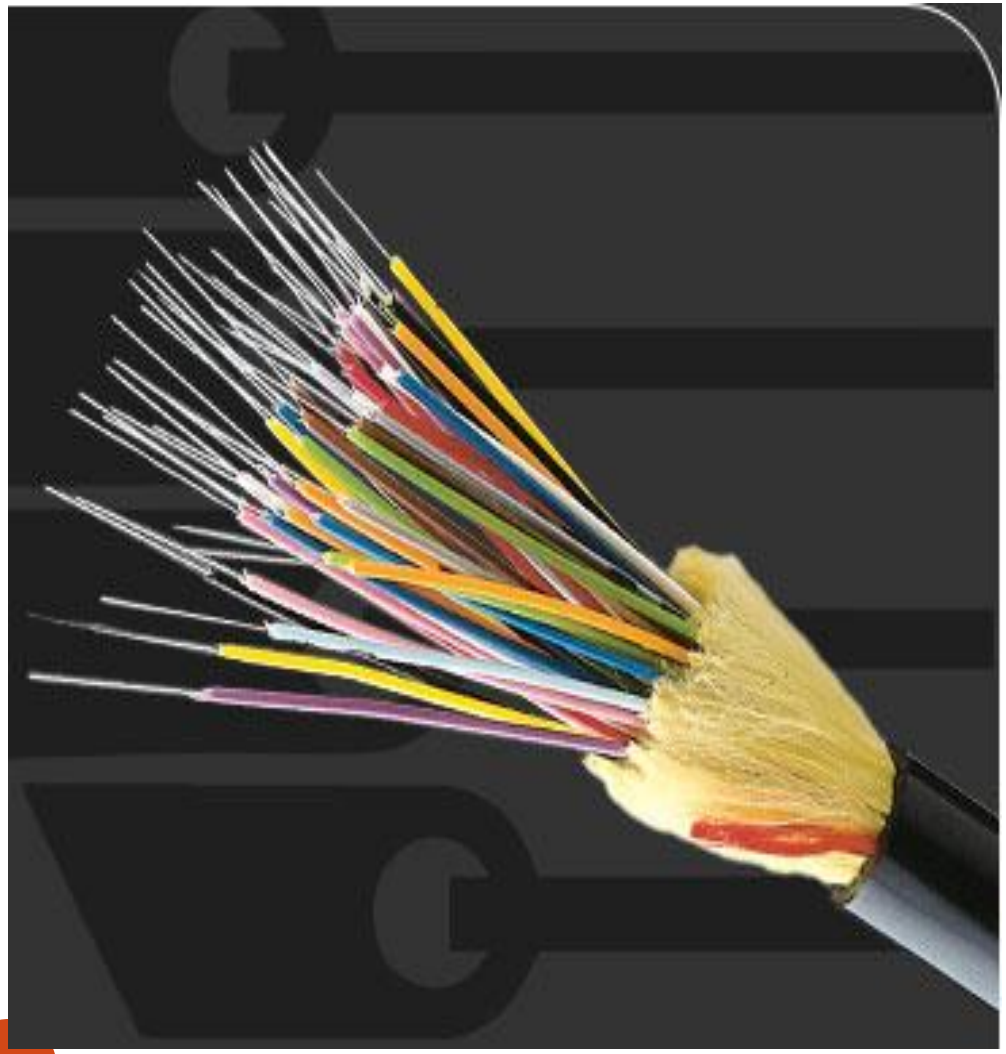
Disadvantages of Coaxial Cable

- Due to its high metallic content, coaxial cable is usually more expensive than other cable types.
- Hard to install

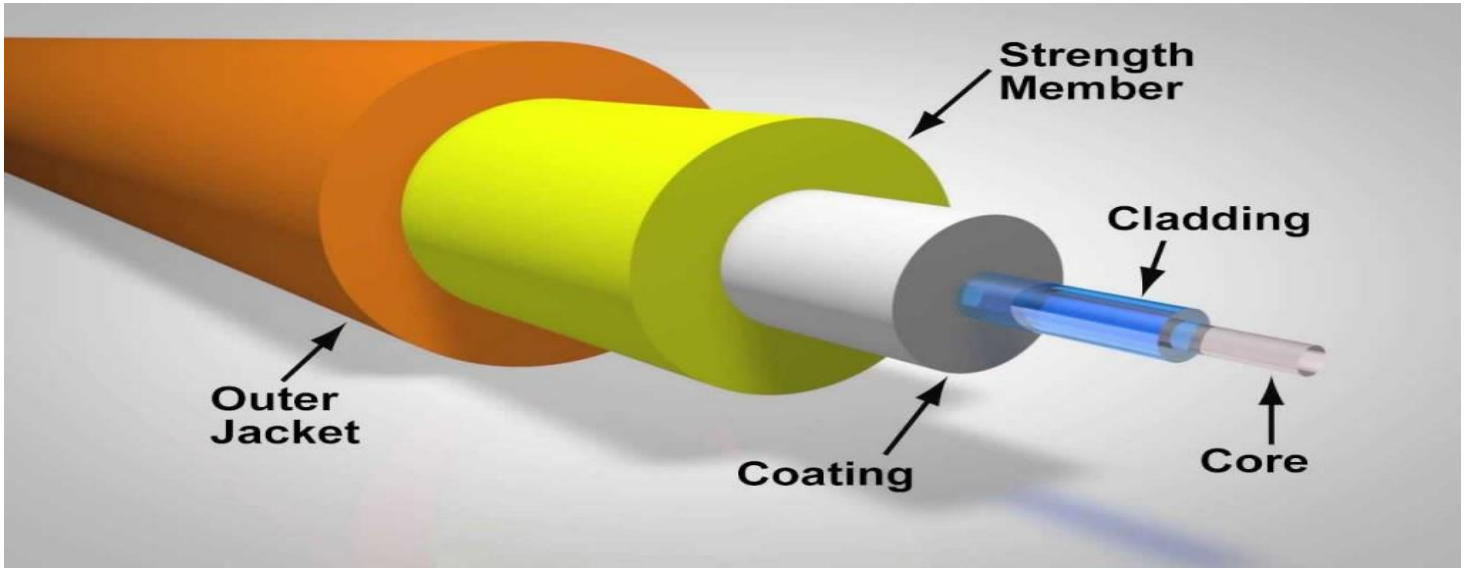
Fiber-Optic Cable

- Fiber optic cable contains glass (or in some cases, plastic) fibers rather than copper wire.
- Signals are transmitted across these fibers in the form of light pulses rather than electrical pulses.
- Optical signals through glass encounter less loss than electrical signals through copper.

Fiber Optic Cable



Structure of Fiber Optic Cable



Types of Fiber optic cable

- There are two primary types of fiber optic cable
  - **Multimode fiber**
    - Multimode fiber can carry multiple light rays (modes) at the same time by having varying optical properties at the core; essentially light travelling the shortest path (down the middle) travels the slowest.
  - **Singlemode fiber**
    - has a much smaller core size of 9 microns and has a single light path and can travel much longer distances of up to 100km.

Optical fiber advantages

- Lower attenuation and higher bandwidth than copper
- Allows transmission to occur over longer distances and/or at greater speeds.
- High level of immunity to electromagnetic interference since signal is sent as light and not as electricity.

Optical Fiber Disadvantage

- Due to the required conversions between light and electricity, more expensive electronics are required than with copper-based systems.
- Requires specialized installation procedures.
- Expensive

Type	Distance	Speed	Cost	Advantages	Disadvantages
UTP	100 m	10 Mbps to 1000 Mbps	Least expensive	Easy to install; widely available and widely used	Susceptible to interference; can cover only a limited distance
STP	100 m	10 Mbps to 100 Mbps	More expensive than UTP	Reduced crosstalk; more resistant to EMI than Thinnet or UTP	Difficult to work with; can cover only a limited distance
Coaxial	500 m (Thicknet) 185 m (Thinnet)	10 Mbps to 100 Mbps	Relatively inexpensive, but more costly than UTP	Less susceptible to EMI interference than other types of copper media	Difficult to work with (Thicknet); limited bandwidth; limited application (Thinnet); damage to cable can bring down entire network
Fiber-Optic	10 km and above single 2 km and farther multi	100 Mb to 100 Gb single mode 100 Mbps to 9.92 Gb multi	Expensive	Cannot be tapped, so security is better; can be used over great distances; is not susceptible to EMI; has a higher data rate than coaxial and twisted-pair cable	Difficult to terminate

Wireless Media

- Wireless Transmission Media is a form of unguided media.
- Wireless communication involves no physical link established between two or more devices, communicating wirelessly.
- Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.