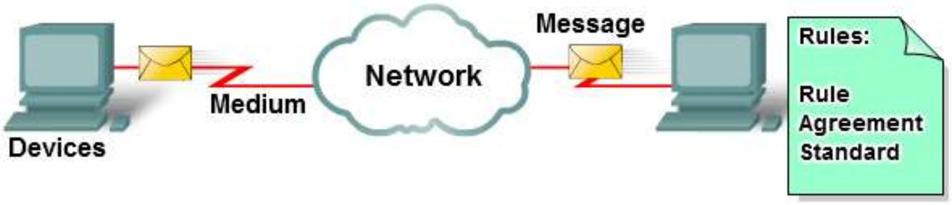
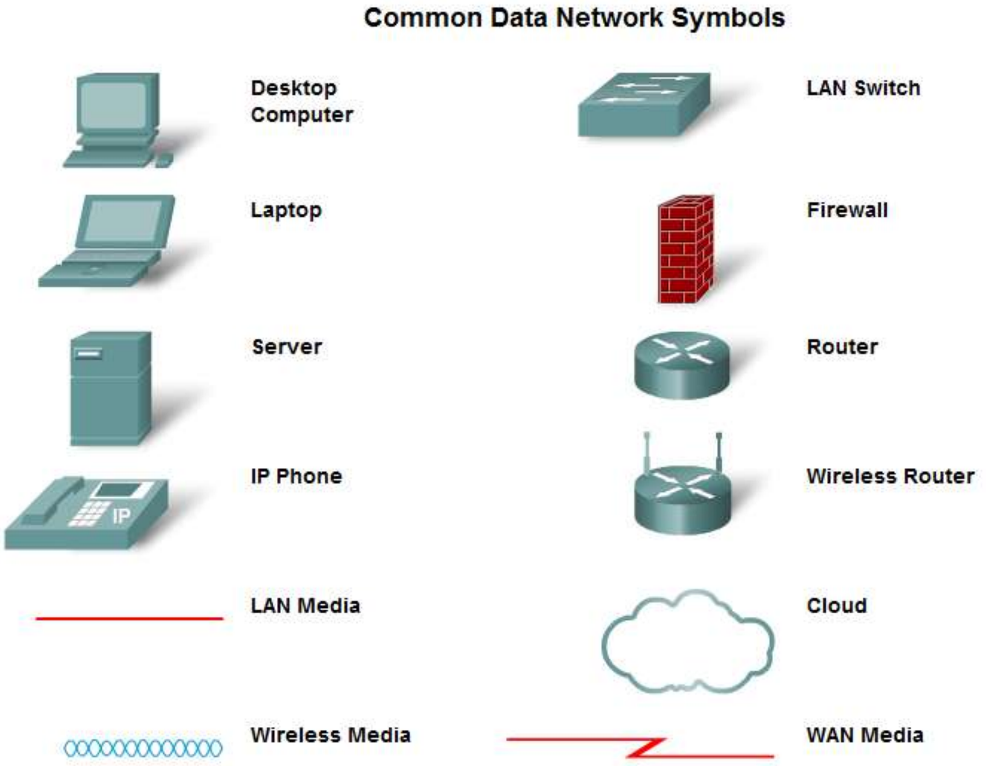
Topic 6: Building a Network

Elements of a Network

The diagram shows elements of a typical network, including devices, media, and services, tied together by rules, that work together to send messages. We use the word messages as a term that encompasses web pages, e-mail, instant messages, telephone calls, and other forms of communication enabled by the Internet. In this course, we will learn about a variety of messages, devices, media, and services that allow the communication of those messages. We will also learn about the rules, or protocols, that tie these network elements together.



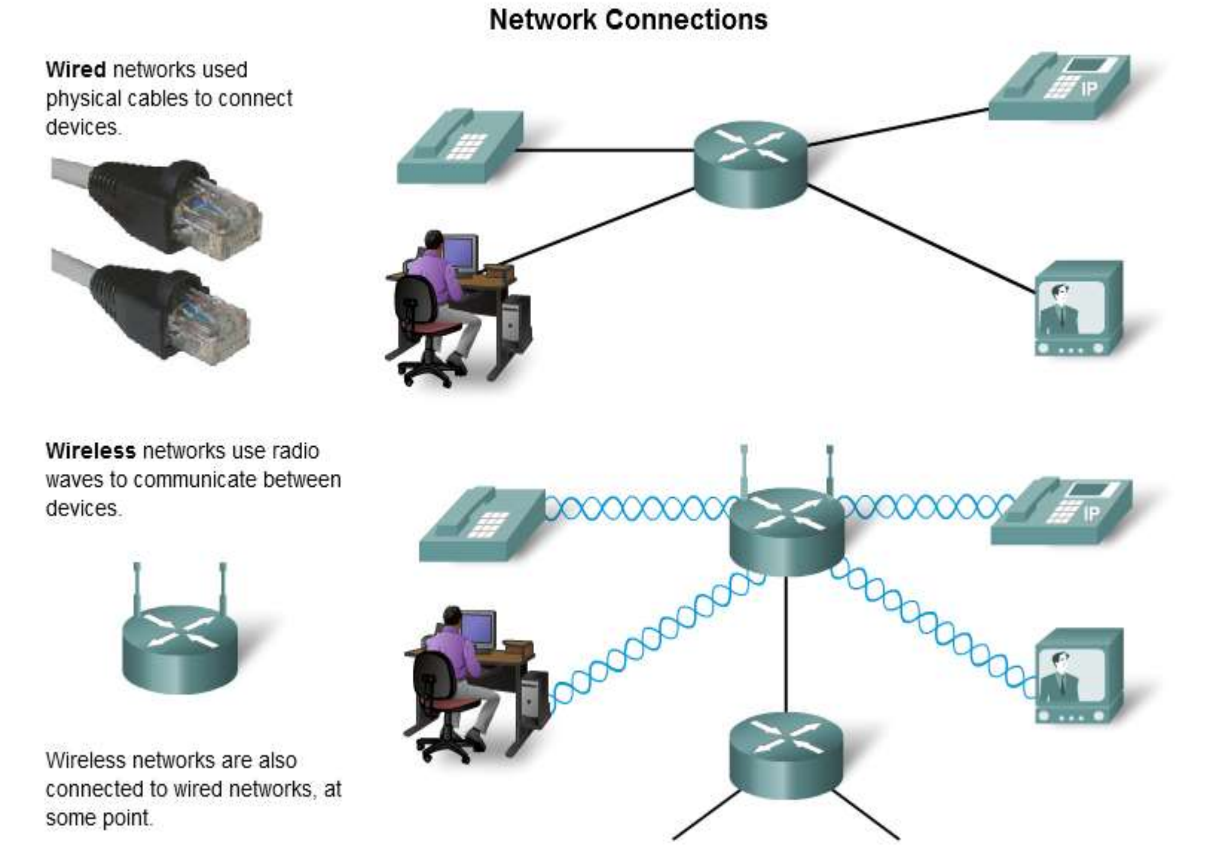
Networking is a very graphically oriented subject, and icons are commonly used to represent networking devices. On the left side of the diagram are shown some common devices which often originate messages that comprise our communication. These include various types of computers (a PC and laptop icon are shown), servers, and IP phones. On local area networks these devices are typically connected by LAN media (wired or wireless).



The right side of the figure shows some of the most common intermediate devices, used to direct and manage messages across the network, as well as other common networking symbols. Generic symbols are shown for:

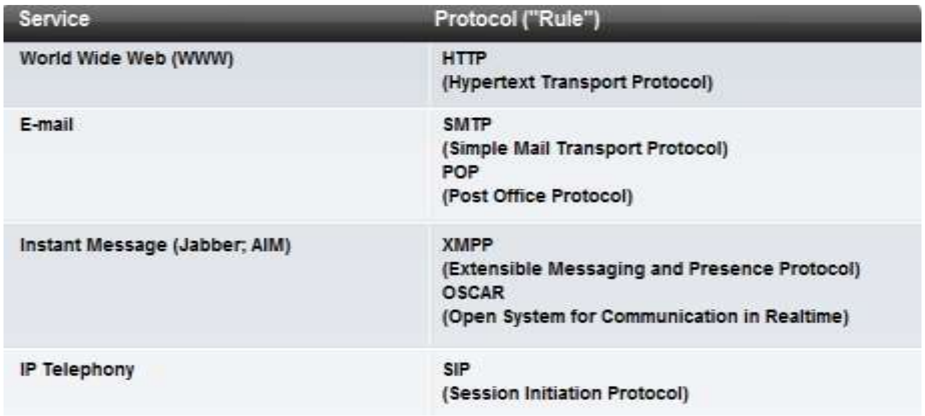
- Switch - the most common device for interconnecting local area networks
- Firewall - provides security to networks
- Router - helps direct messages as they travel across a network
- Wireless Router - a specific type of router often found in home networks
- Cloud - used to summarize a group of networking devices, the details of which may be unimportant to the discussion at hand
- Serial Link - one form of WAN interconnection, represented by the lightning bolt-shaped line

For a network to function, the devices must be interconnected. 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. Copper medium includes cables, such as twisted pair telephone wire, coaxial cable, or most commonly, what is known as Category 5 Unshielded Twisted Pair (UTP) cable. Optical fibers, 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, the terrestrial wireless connection between two ground stations, or the communication between devices on earth and satellites. In a typical journey across the Internet, a message may travel across a variety of media.


Network Connections
Wired networks used physical cables to connect devices.
Wireless networks use radio waves to communicate between devices.
Wireless networks are also connected to wired networks, at some point.
IP
IP

Human beings often seek to send and receive a variety of message using computer applications; these applications require services be provided by the network. Some of these services include the World Wide Web, e-mail, instant messaging, and IP Telephony. Devices interconnected by medium to provide services must be governed by rules, or protocols. In the chart, some common services and a protocol most directly associated with that service are listed.

Protocols are the rules that the networked devices use to communicate with each other. The industry standard in networking today is a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is used in home and business networks,



Service	Protocol ("Rule")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Instant Message (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
IP Telephony	SIP (Session Initiation Protocol)

as well as being the primary protocol of the Internet. It is TCP/IP protocols that specify the formatting, addressing and routing mechanisms that ensure our messages are delivered to the correct recipient.

We close this section with an example to tie together how the elements of networks - devices, media, and services - are connected by rules to deliver a message. People often only picture networks in the abstract sense. We create and send a text message and it almost immediately shows up on the destination device. Although we know that between our sending device and the receiving device there is a network over which our message travels, we rarely think about all the parts and pieces that make up that infrastructure.

The Messages

In the first step of its journey from the computer to its destination, our instant 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.

The Devices

To begin to understand the robustness and complexity of the interconnected networks that make up the Internet, it is necessary to start with the basics. Take the example of sending the text message using an instant messaging program on a computer. When we think of using network services, we usually think of using a computer to access them. But, a computer is only one type of device that can send and receive messages over a network. Many other types of devices can also be connected to the network to participate in network services. Among these devices are telephones, cameras, music systems, printers and game consoles.

In addition to the computer, there are numerous other components that make it possible for our instant message to be directed across the miles of wires, underground cables, airwaves and satellite stations that might exist between the source and destination devices. One of the critical components in any size network is the router. A router joins two or more networks, like a home network and the Internet, and passes information from one network to another. Routers in a network work to ensure that the message gets to its destination in the most efficient and quickest manner.

The Medium

To send our instant message to its destination, the computer must be connected to a wired or wireless local network. Local networks can be installed in homes or businesses, where they enable computers and other devices to share information with each other and to use a common connection to the Internet.

Wireless networks allow the use of networked devices anywhere in an office or home, even outdoors. Outside the office or home, wireless networking is available in public hotspots, such as coffee shops, businesses, hotel rooms, and airports.

Many installed networks use wires to provide connectivity. Ethernet is the most common wired networking technology found today. The wires, called cables, connect the computers and other devices that make up the networks. Wired networks are best for moving large amounts of data at high speeds, such as are required to support professional-quality multimedia.

The Services

Network services are computer programs that support the human network. Distributed on devices throughout the network, these services facilitate online communication tools such as e-mail, bulletin/discussion boards, chat rooms, and instant messaging. In the case of instant messaging, for example, an instant messaging service, provided by devices in the cloud, must be accessible to both the sender and recipient.

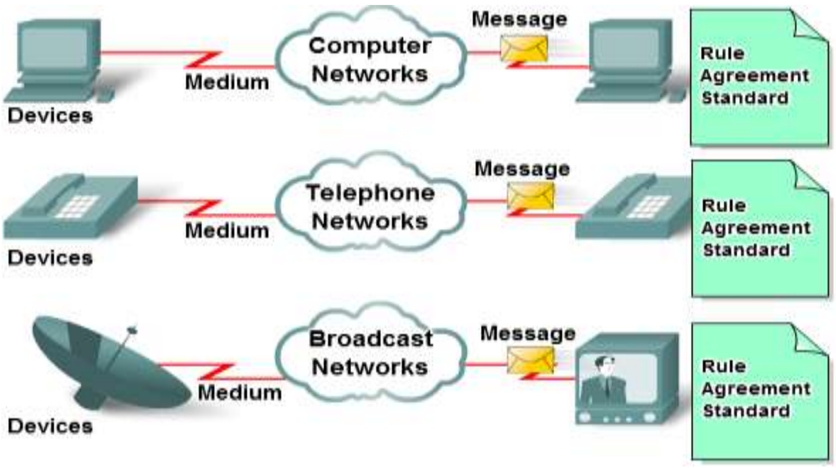
The Rules

Important aspects of networks that are neither devices nor media are rules, or protocols. These 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. For example, in the case of Jabber instant messaging, the XMPP, TCP, and IP protocols are all important sets of rules that enable our communication to occur.

Converged Networks

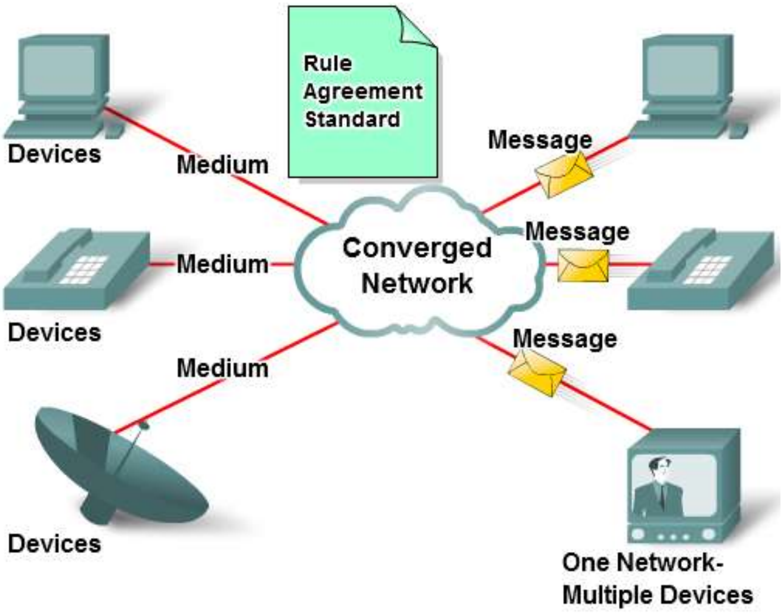
Multiple services-multiple networks

Traditional telephone, radio, television, and computer data networks each have their own individual versions of the four basic network elements. In the past, every one of these services required a different technology to carry its particular communication signal. Additionally, each service had its own set of rules and standards to ensure successful communication of its signal across a specific medium.



Converged networks

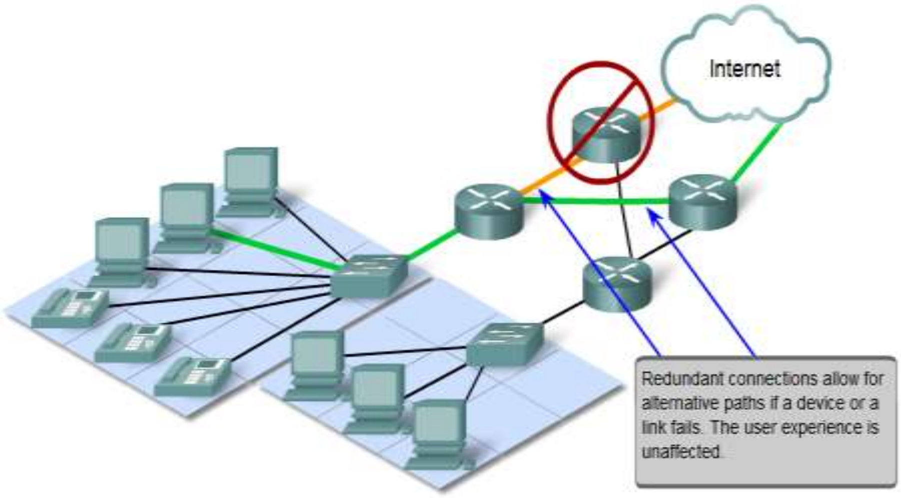
Technology advances are enabling us to consolidate these disparate networks onto one platform - a platform defined as a converged network. The flow of voice, video, and data traveling over the same network eliminates the need to create and maintain separate networks. On a converged network there are still many points of contact and many specialized devices - for example, personal computers, phones, TVs, personal assistants, and retail point-of-sale registers - but only one common network infrastructure.



Network Architecture

Networks must support a wide range of applications and services, as well as operate over many different types of physical infrastructures. The term network architecture, in this context, refers to both the technologies that support the infrastructure and the programmed services and protocols that move the messages across that infrastructure. As the Internet, and networks in general, evolve, we are discovering that there are four basic characteristics that the underlying architectures need to address in order to meet user expectations: fault tolerance, scalability, quality of service, and security.

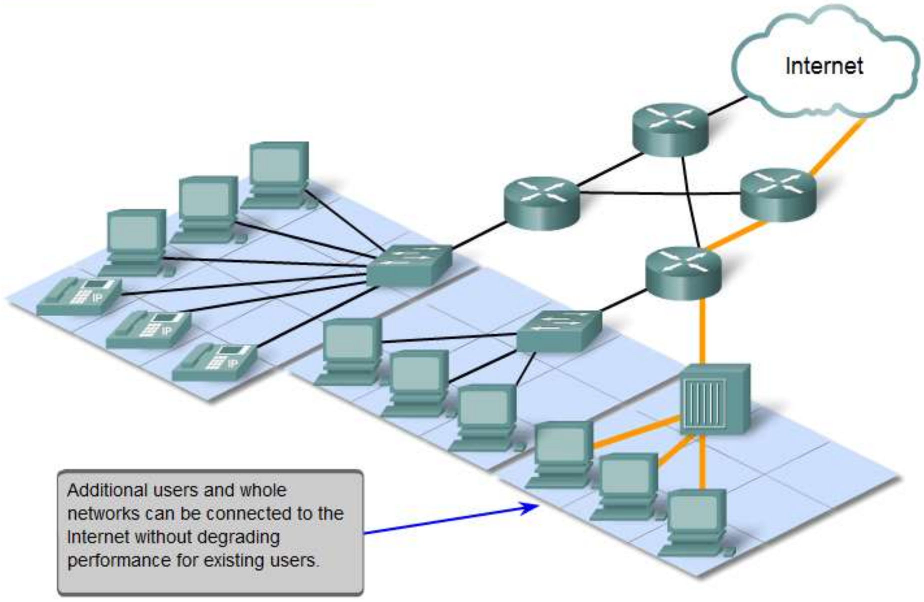
Fault Tolerance



Redundant connections allow for alternative paths if a device or a link fails. The user experience is unaffected.

The expectation that the Internet is always available to the millions of users who rely on it requires a network architecture that is designed and built to be fault tolerant. A fault tolerant network is one that limits the impact of a hardware or software failure and can recover quickly when such a failure occurs. These networks depend on redundant links, or paths, between the source and destination of a message. If one link or path fails, processes ensure that messages can be instantly routed over a different link transparent to the users on either end. Both the physical infrastructures and the logical processes that direct the messages through the network are designed to accommodate this redundancy. This is a basic premise of the architecture of current networks.

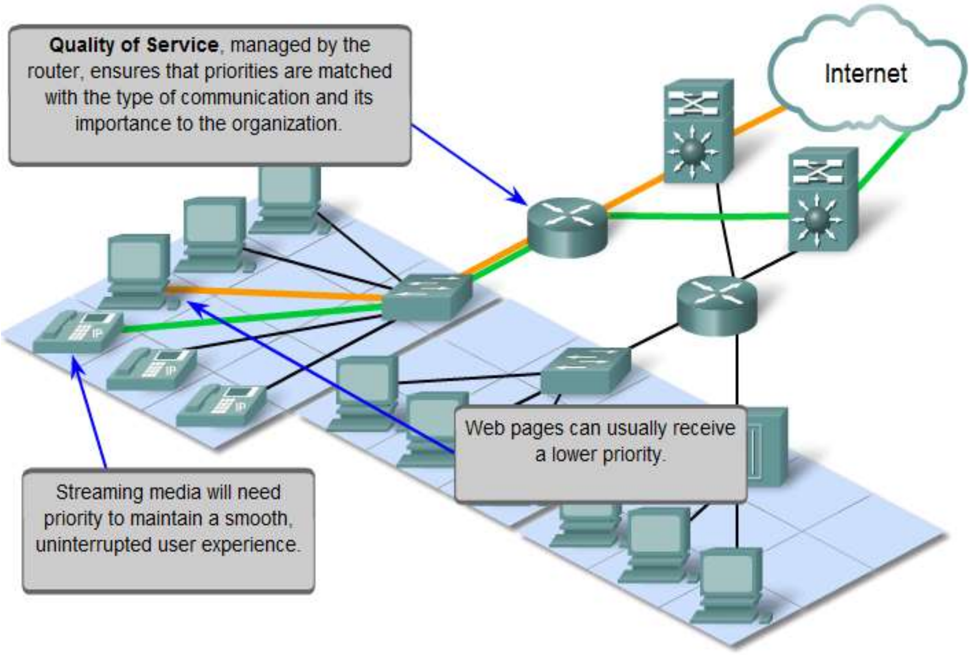
Scalability



Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users. Thousands of new users and service providers connect to the Internet each week. The ability of the network to support these new interconnections depends on a hierarchical layered design for the underlying physical infrastructure and logical architecture. The operation at each layer enables users or service providers to be inserted without causing disruption to the entire network. Technology developments are constantly increasing the message carrying capabilities and performance of the physical infrastructure components at every layer. These developments, along with new methods to identify and locate individual users within an internetwork, are enabling the Internet to keep pace with user demand.

Quality of Service (QoS)

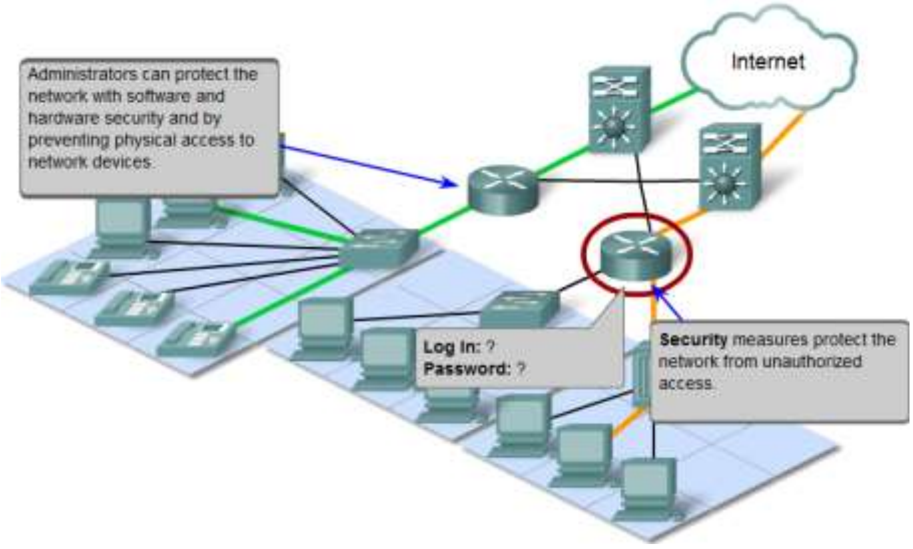

Quality of Service, managed by the router, ensures that priorities are matched with the type of communication and its importance to the organization.

Web pages can usually receive a lower priority.

Streaming media will need priority to maintain a smooth, uninterrupted user experience.

The Internet is currently providing an acceptable level of fault tolerance and scalability for its users. But new applications available to users over internetworks create higher expectations for the quality of the delivered services. Voice and live video transmissions require a level of consistent quality and uninterrupted delivery that was not necessary for traditional computer applications. Quality of these services is measured against the quality of experiencing the same audio or video presentation in person. Traditional voice and video networks are designed to support a single type of transmission, and are therefore able to produce an acceptable level of quality. New requirements to support this quality of service over a converged network are changing the way network architectures are designed and implemented.

Security


Administrators can protect the network with software and hardware security and by preventing physical access to network devices.

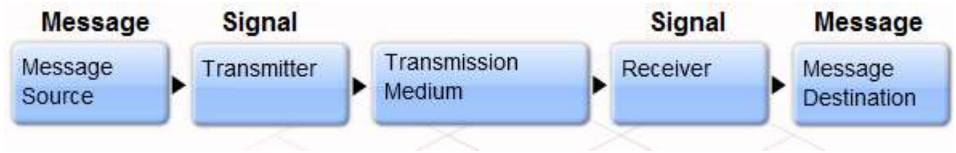
Log In: ?
Password: ?

Security measures protect the network from unauthorized access.

The Internet has evolved from a tightly controlled internetwork of educational and government organizations to a widely accessible means for transmission of business and personal communications. As a result, the security requirements of the network have changed. The security and privacy expectations that result from the use of internetworks to exchange confidential and business critical information exceed what the current architecture can deliver. Rapid expansion in communication areas that were not served by traditional data networks is increasing the need to embed security into the network architecture. As a result, much effort is being devoted to this area of research and development. In the meantime, many tools and procedures are being implemented to combat inherent security flaws in the network architecture.

Principles of Communication

Source, Channel, and Destination



The primary purpose of any network is to provide a method to communicate information. From the very earliest primitive humans to the most advanced scientists of today, sharing information with others is crucial for human advancement.

All communication begins with a message, or information, that must be sent from one individual or device to another. The methods used to send, receive and interpret messages change over time as technology advances.

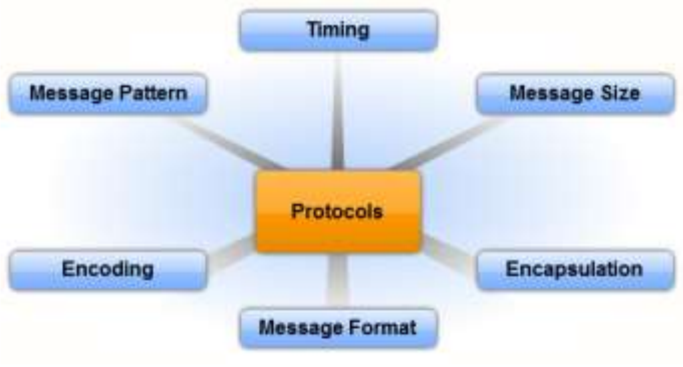
All communication methods have three elements in common. The first of these elements is the message source, or sender. Message sources are people, or electronic devices, that need to communicate a message to other individuals or devices. The second element of communication is the destination, or receiver, of the message. The destination receives the message and interprets it. A third element, called a channel, provides the pathway over which the message can travel from source to destination.

Rules of Communication

In any conversation between two people, there are many rules, or protocols, that the two must follow in order for the message to be successfully delivered and understood. Among the protocols for successful human communication are:

- Identification of sender and receiver
- Agreed-upon medium or channel (face-to-face, telephone, letter, photograph)
- Appropriate communication mode (spoken, written, illustrated, interactive or one-way)
- Common language
- Grammar and sentence structure
- Speed and timing of delivery

Protocols are specific to the characteristics of the source, channel and destination of the message. The rules used to communicate over one medium, like a telephone call, are not necessarily the same as communication using another medium, such as a letter.



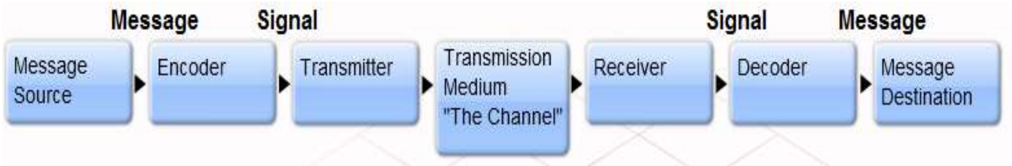
Protocols define the details of how the message is transmitted, and delivered. This includes issues of:

- Message format
- Message size
- Timing
- Encapsulation
- Encoding
- Standard message pattern

Many of the concepts and rules that make human communication reliable and understandable also apply to computer communication.

Message Encoding

One of the first steps to sending a message is encoding it. Written words, pictures, and spoken languages each use a unique set of codes, sounds, gestures, and/or symbols to represent the thoughts being shared. Encoding is the process of converting thoughts into the language, symbols, or sounds, for transmission. Decoding reverses this process in order to interpret the thought.



Imagine a person watching a sunset and then calling someone else to talk about how beautiful the sunset looks. To communicate the message, the sender must first convert, or encode, their thoughts and perceptions about the sunset into words. The words are spoken into the telephone using the sounds and inflections of spoken language that convey the message. On the other end of the telephone line, the person listening to the description, receives and decodes the sounds in order to visualize the image of the sunset described by the sender.

Encoding also occurs in computer communication. Encoding between hosts must be in an appropriate form for the medium. Messages sent across the network are first converted into bits by the sending host. Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media over which the bits are transmitted. The destination host receives and decodes the signals in order to interpret the message.

Message Formatting

When a message is sent from source to destination, it must use a specific format or structure. Message formats depend on the type of message and the channel that is used to deliver the message.

Letter writing is one of the most common forms of written human communication. For centuries, the agreed format for personal letters has not changed. In many cultures, a personal letter contains the following elements:

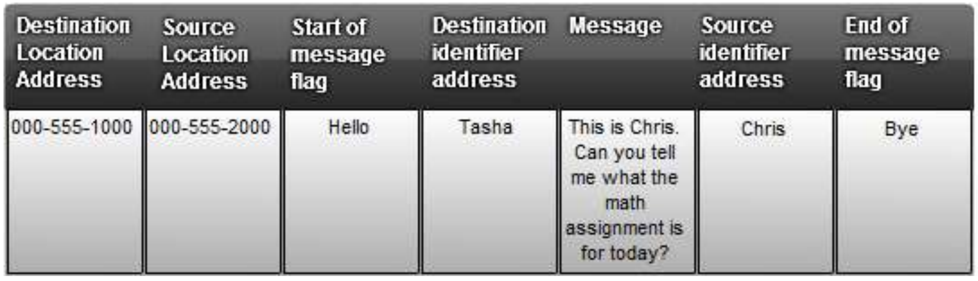
- An identifier of the recipient
- A salutation or greeting
- The message content
- A closing phrase
- An identifier of the sender

In addition to having the correct format, most personal letters must also be enclosed, or encapsulated, in an envelope for delivery. The envelope has the address of the sender and receiver on it, each located at the proper place on the envelope. If the destination address and formatting are not correct, the letter is not delivered.

The process of placing one message format (the letter) inside another message format (the envelope) is called encapsulation. De-encapsulation occurs when the process is reversed by the recipient and the letter is removed from the envelope.

A letter writer uses an accepted format to ensure that the letter is delivered and understood by the recipient. In the same way, a message that is sent over a computer network follows specific format rules for it to be delivered and processed. Just as a letter is encapsulated in an envelope for delivery, so computer messages are encapsulated. Each computer message is encapsulated in a specific format, called a frame, before it is sent over the network. A frame acts like an envelope; it provides the address of the intended destination and the address of the source host.

The format and contents of a frame are determined by the type of message being sent and the channel over which it is communicated. Messages that are not correctly formatted are not successfully delivered to or processed by the destination host.



Destination Location Address	Source Location Address	Start of message flag	Destination identifier address	Message	Source identifier address	End of message flag
000-555-1000	000-555-2000	Hello	Tasha	This is Chris. Can you tell me what the math assignment is for today?	Chris	Bye

Message Size
Imagine what it would be like to read this course if it all appeared as one long sentence; it would not be easy to read and comprehend. When people communicate with each other, the messages that they send are usually broken into smaller parts or sentences. These sentences are limited in size to what the receiving person can process at one time. An individual conversation may be made up of many smaller sentences to ensure that each part of the message is received and understood.

Likewise, when a long message is sent from one host to another over a network, it is necessary to break the message into smaller pieces. The rules that govern the size of the pieces, or frames, communicated across the network are very strict. They can also be different, depending on the channel used. Frames that are too long or too short are not delivered.

The size restrictions of frames require the source host to break a long message into individual pieces that meet both the minimum and maximum size requirements. Each piece is encapsulated in a separate frame with the address information, and is sent over the network. At the receiving host, the messages are de-encapsulated and put back together to be processed and interpreted.

Message Timing
One factor that affects how well a message is received and understood is timing. People use timing to determine when to speak, how fast or slow to talk, and how long to wait for a response. These are the rules of engagement.

> Access Method
> Access Method determines when someone is able to send a message. These timing rules are based on the environment. For example, you may be able to speak whenever you have something to say. In this environment, a person must wait until no one else is talking before speaking. If two people talk at the same time, a collision of information occurs and it is necessary for the two to back off and start again. These rules ensure communication is successful. Likewise, it is necessary for computers to define an access method. Hosts on a network need an access method to know when to begin sending messages and how to respond when errors occur.
>
> Flow Control
> Timing also effects how much information can be sent and the speed that it can be delivered. If one person speaks too quickly, it is difficult for the other person to hear and understand the message. The receiving person must ask the sender

to slow down. In network communication, a sending host can transmit messages at a faster rate than the destination host can receive and process. Source and destination hosts use flow control to negotiate correct timing for successful communication.

Response Timeout

If a person asks a question and does not hear a response within an acceptable amount of time, the person assumes that no answer is coming and reacts accordingly. The person may repeat the question, or may go on with the conversation. Hosts on the network also have rules that specify how long to wait for responses and what action to take if a response timeout occurs.

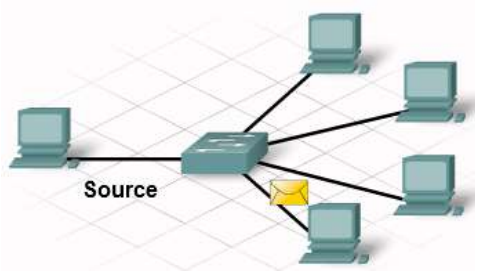
Message Patterns

Sometimes, a person wants to communicate information to a single individual. At other times, the person may need to send information to a group of people at the same time, or even to all people in the same area. A conversation between two people is an example of a one-to-one pattern of communication. When a group of recipients need to receive the same message simultaneously, a one-to-many or one-to-all message pattern is necessary.

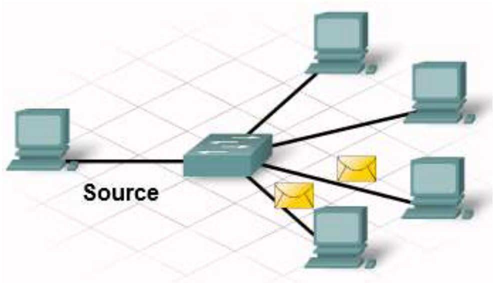
There are also times when the sender of a message needs to be sure that the message is delivered successfully to the destination. In these cases, it is necessary for the recipient to return an acknowledgement to the sender. If no acknowledgement is required, the message pattern is referred to as unacknowledged.

Hosts on a network use similar message patterns to communicate.

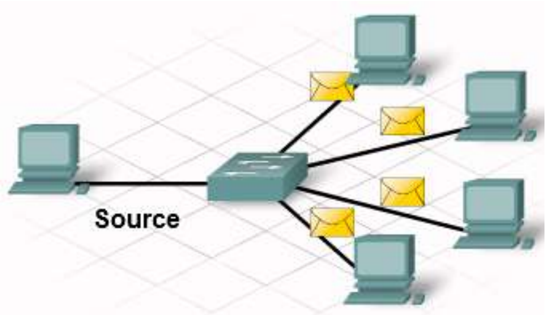
A one-to-one message pattern is referred to as a unicast, meaning that there is only a single destination for the message.



When a host needs to send messages using a one-to-many pattern, it is referred to as a multicast. Multicasting is the delivery of the same message to a group of host destinations simultaneously.



If all hosts on the network need to receive the message at the same time, a broadcast is used. Broadcasting represents a one-to-all message pattern. Additionally, hosts have requirements for acknowledged versus unacknowledged messages.



Rules or the Protocol

All communication, both human and computer, is governed by pre-established rules, or protocols. These protocols are determined by the characteristics of the source, channel and destination. Based on the source, channel and destination, the protocols define the details for the issues of message format, message size, timing, encapsulation, encoding and standard message pattern.

Computers, just like humans, use rules, or protocols, in order to communicate.

Protocols are especially important on a local network. In a wired environment, a local network is defined as an area where all hosts must "speak the same language" or in computer terms "share a common protocol".

If everyone in the same room spoke a different language they would not be able to communicate. Likewise, if devices in a local network did not use the same protocols they would not be able to communicate.

The most common set of protocols used on local wired networks is Ethernet.

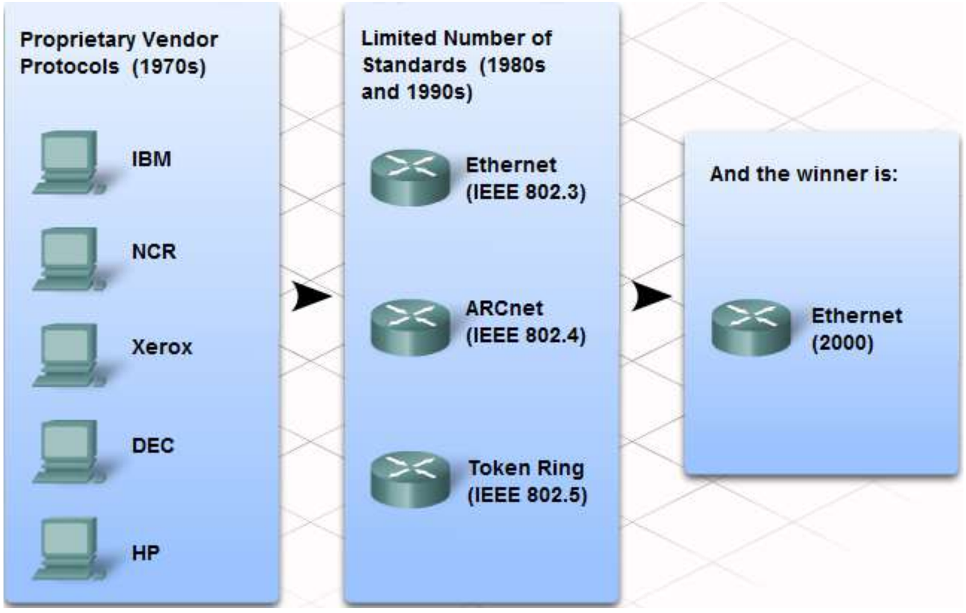
The Ethernet protocol defines many aspects of communication over the local network, including: message format, message size, timing, encoding, and message patterns.

In the early days of networking, each vendor used their own, proprietary methods of interconnecting network devices and networking protocols. Equipment from one vendor could not communicate with equipment from another.

As networks became more widespread, standards were developed that defined rules by which network equipment from different vendors operated. Standards are beneficial to networking in many ways:

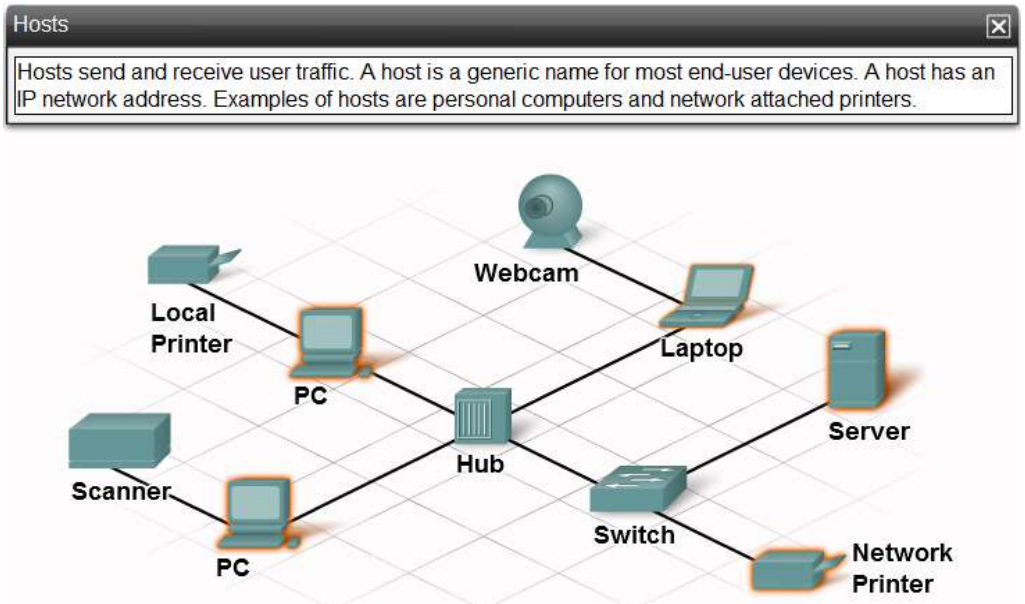
- Facilitate design
- Simplify product development
- Promote competition
- Provide consistent interconnections
- Facilitate training
- Provide more vendor choices for customers

There is no official local networking standard protocol, but over time, one technology, Ethernet, has become more common than the others. It has become a de facto standard.



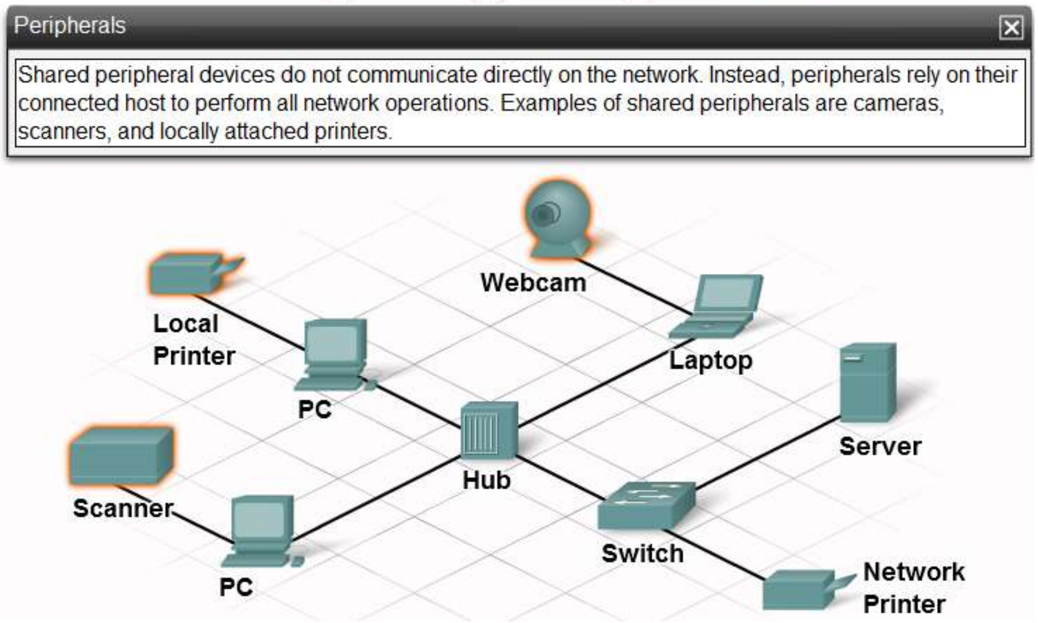
Basic Network Components

There are many components that can be part of a network, for example personal computers, servers, networking devices, and cabling. These components can be grouped into four main categories:



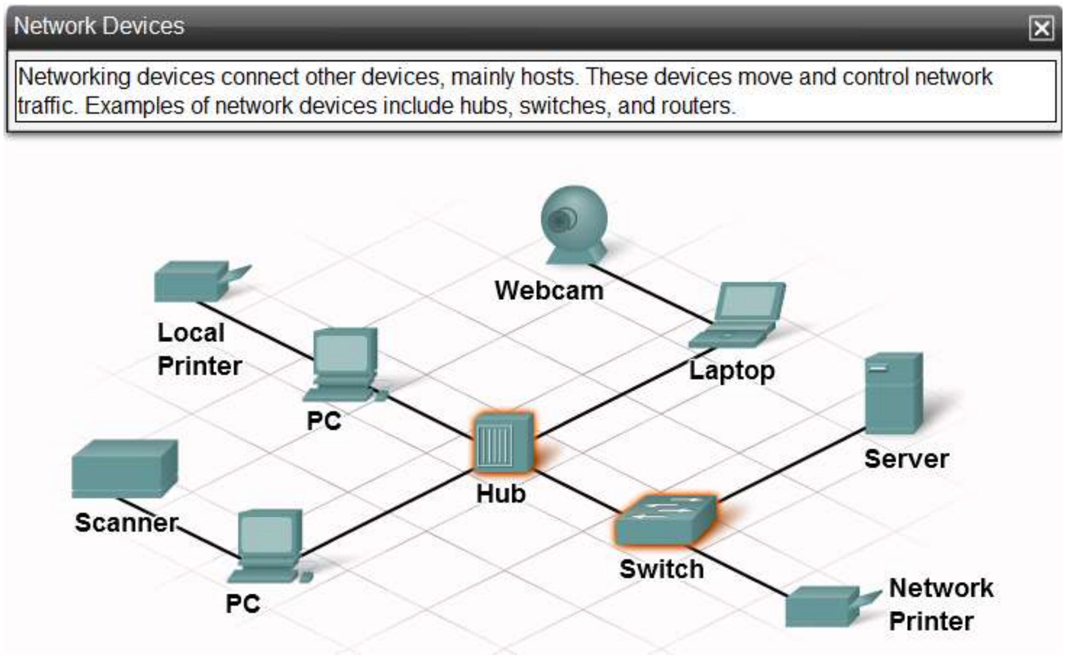
Hosts

Hosts send and receive user traffic. A host is a generic name for most end-user devices. A host has an IP network address. Examples of hosts are personal computers and network attached printers.



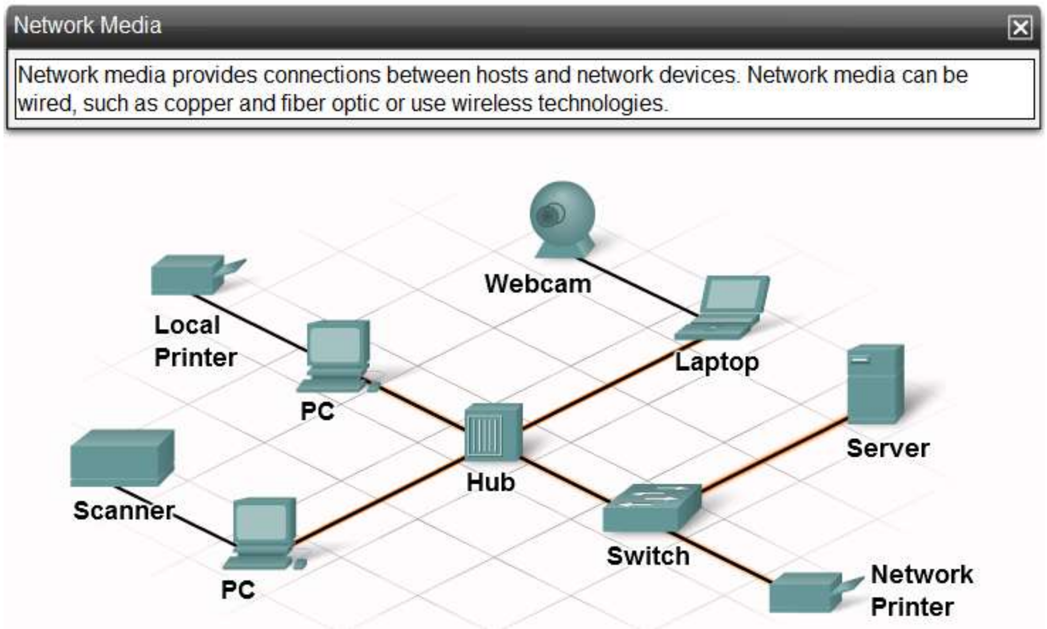
Peripherals

Shared peripheral devices do not communicate directly on the network. Instead, peripherals rely on their connected host to perform all network operations. Examples of shared peripherals are cameras, scanners, and locally attached printers.



Network Devices

Networking devices connect other devices, mainly hosts. These devices move and control network traffic. Examples of network devices include hubs, switches, and routers.



Network Media

Network media provides connections between hosts and network devices. Network media can be wired, such as copper and fiber optic or use wireless technologies.

The network components that people are most familiar with are hosts and shared peripherals. Hosts are devices that send and receive messages directly across the network.

Shared peripherals are not directly connected to the network, but instead are connected to hosts. The host is then responsible for sharing the peripheral across the network. Hosts have computer software configured to enable people on the network to use the attached peripheral devices.

The network devices, as well as networking media, are used to interconnect hosts.

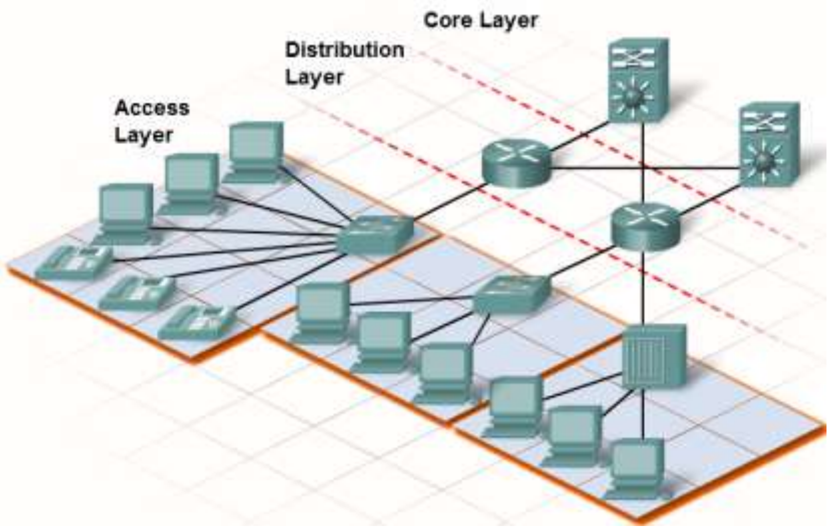
Some devices can play more than one role, depending on how they are connected. For example, a printer directly connected to a host (local printer) is a peripheral. A printer directly connected to a network device and participates directly in network communications is a host.

Building the Access Layer of an Ethernet Network

Access Layer

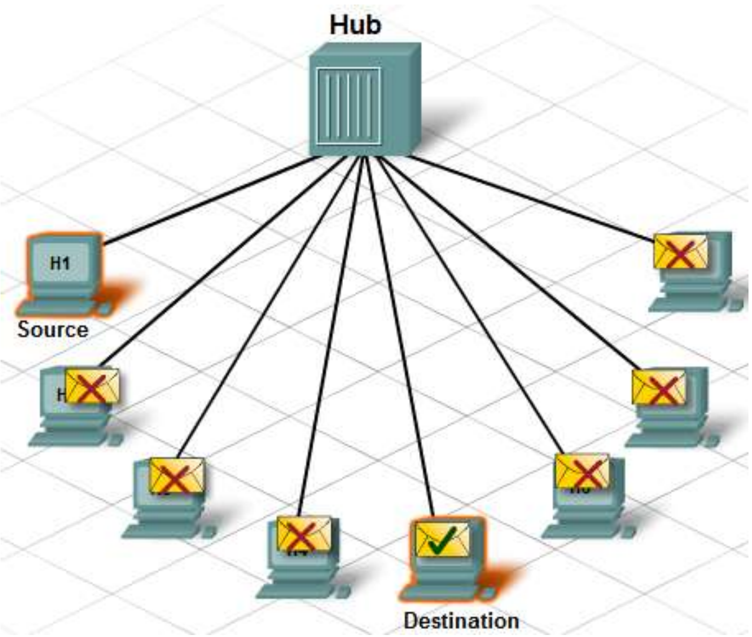
The Access Layer is the most basic level of the network. It is the part of the network in which people gain access to other hosts and to shared files and printers. The Access Layer is composed of host devices, as well as the first line of networking devices to which they are attached.

Networking devices enable us to connect many hosts with each other and also provide those hosts access to services offered over the network. Unlike the simple network consisting of two hosts connected by a single cable, in the Access Layer, each host is connected to a networking device. This type of connectivity is shown in the graphic.



Within an Ethernet network, each host is able to connect directly to an Access Layer networking device using a point-to-point cable. These cables are manufactured to meet specific Ethernet standards. Each cable is plugged into a host NIC and then into a port on the networking device. There are several types of networking devices that can be used to connect hosts at the Access Layer, including Ethernet hubs and switches.

Function of Hubs



A hub is one type of networking device that is installed at the Access Layer of an Ethernet network. Hubs contain multiple ports that are used to connect hosts to the network. Hubs are simple devices that do not have the necessary electronics to decode the messages sent between hosts on the network. Hubs cannot determine which host should get any particular message. A hub simply accepts electronic signals from one port and regenerates (or repeats) the same message out all of the other ports.

Remember that the NIC on a host accepts messages only addressed to the correct MAC address. Hosts ignore messages that are not addressed to them. Only the host specified in the destination address of the message processes the message and responds to the sender.

All of the ports on the Ethernet hub connect to the same channel to send and receive messages. Because all hosts must share the bandwidth available on that channel, a hub is referred to as a shared-bandwidth device.

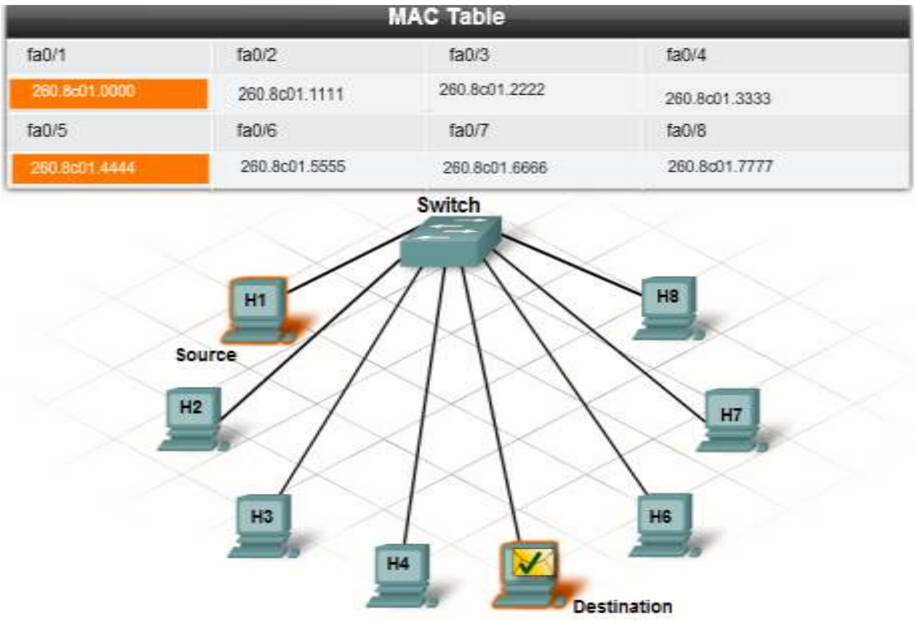
Only one message can be sent through an Ethernet hub at a time. It is possible for two or more hosts connected to a hub to attempt to send a message at the same time. If this happens, the electronic signals that make up the messages collide with each other at the hub.

A collision causes the messages to become garbled and unreadable by the hosts. A hub does not decode the messages; therefore it does not detect that the message is garbled and repeats it out all the ports. The area of the network where a host can receive a garbled message resulting from a collision is known as a collision domain.

Inside a collision domain, when a host receives a garbled message, it detects that a collision has occurred. Each sending host waits a short amount of time and then attempts to send, or retransmit, the message again. As the number of hosts connected to the hub increases, so does the chance of collisions. More collisions cause more retransmissions. Excessive retransmissions can clog up the network and slow down network traffic. For this reason, it is necessary to limit the size of a collision domain.

Function of Switches

An Ethernet switch is a device that is used at the Access Layer. Like a hub, a switch connects multiple hosts to the network. Unlike a hub, a switch can forward a message to a specific host. When a host sends a message to another host on the switch, the switch accepts and decodes the frames to read the physical (MAC) address portion of the message.



MAC Table

fa0/1	fa0/2	fa0/3	fa0/4
260.8c01.0000	260.8c01.1111	260.8c01.2222	260.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
260.8c01.4444	260.8c01.5555	260.8c01.6666	260.8c01.7777

A table on the switch, called a MAC address table, contains a list of all of the active ports and the host MAC addresses that are attached to them. When a message is sent between hosts, the switch checks to see if the destination MAC address is in the table. If it is, the switch builds a temporary connection, called a circuit, between the source and destination ports. This new circuit provides a dedicated channel over which the two hosts can communicate. Other hosts attached to the switch do not share bandwidth on this channel and do not receive messages that are not addressed to them. A new circuit is built for every new conversation between hosts. These separate circuits allow many conversations to take place at the same time, without collisions occurring.

What happens when the switch receives a frame addressed to a new host that is not yet in the MAC address table? If the destination MAC address is not in the table, the switch does not have the necessary information to create an individual circuit. When the switch cannot determine where the destination host is located, it uses a process called flooding to forward the message out to all attached hosts. Each host compares the destination MAC address in the message to its own MAC address, but only the host with the correct destination address processes the message and responds to the sender.
f
How does the MAC address of a new host get into the MAC address table? A switch builds the MAC address table by examining the source MAC address of each frame that is sent between hosts. When a new host sends a message or responds to a flooded message, the switch immediately learns its MAC address and the port to which it is connected. The table is dynamically updated each time a new source MAC address is read by the switch. In this way, a switch quickly learns the MAC addresses of all attached hosts.

Sometimes, it is necessary to connect another networking device, like a hub, to a switch port. This is done to increase the number of hosts that can be connected to the network. When a hub is connected to a switch port, the switch associates the MAC addresses of all hosts connected to that hub with the single port on the switch. Occasionally, one host on the attached hub sends a message to another host attached to the same hub. In this case, the switch receives the frame and checks the table to see where the destination host is located. If both the source and destination hosts are located on the same port, the switch discards the message.

When a hub is connected to a switch port, collisions can occur on the hub. The hub forwards to all ports the damaged messages resulting from a collision. The switch receives the garbled message, but, unlike a hub, a switch does not forward the damaged messages caused by collisions. As a result, every switch port creates a separate collision domain. This is a good thing. The fewer hosts contained in a collision domain, the less likely it is that a collision will occur.

MAC and IP

On a local Ethernet network, a NIC only accepts a frame if the destination address is either the broadcast MAC address, or else corresponds to the MAC address of the NIC.

Most network applications, however, rely on the logical destination IP address to identify the location of the servers and clients.

What if a sending host only has the logical IP address of the destination host? How does the sending host determine what destination MAC address to place within the frame?

The sending host can use an IP protocol called address resolution protocol (ARP) to discover the MAC address of any host on the same local network.

Address Resolution Protocol

ARP uses a three step process to discover and store the MAC address of a host on the local network when only the IP address of the host is known.

1. The sending host creates and sends a frame addressed to a broadcast MAC address. Contained in the frame is a message with the IP address of the intended destination host.

2. Each host on the network receives the broadcast frame and compares the IP address inside the message with its configured IP address. The host with the matching IP address sends its MAC address back to the original sending host.

3. The sending host receives the message and stores the MAC address and IP address information in a table called an ARP table.

Once the sending host has the MAC address of the destination host in its ARP table, it can send frames directly to the destination without doing an ARP request.

Function of Routers

A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation. Routers, like switches, are able to decode and read the messages that are sent to them. Unlike switches, which only decode (unencapsulate) the frame containing the MAC address information, routers decode the packet that is encapsulated within the frame.

The packet format contains the IP addresses of the destination and source hosts, as well as the message data being sent between them. The router reads the network portion of the destination IP address and uses it to find which one of the attached networks is the best way to forward the message to the destination.

Anytime the network portion of the IP addresses of the source and destination hosts do not match, a router must be used to forward the message. If a host located on network 1.1.1.0 needs to send a message to a host on network 5.5.5.0, the host will forward the message to the router. The router receives the message and unencapsulates it to read the destination IP address. It then determines where to forward the message. It re-encapsulates the packet back into a frame, and forwards the frame on to its destination.

Default Gateway

The method that a host uses to send messages to a destination on a remote network differs from the way a host sends messages on the same local network. When a host needs to send a message to another host located on the same network, it will forward the message directly. A host will use ARP to discover the MAC address of the destination host. It includes the destination IP address within the packet and encapsulates the packet into a frame containing the MAC address of the destination and forwards it out.

On the other hand, when a host needs to send a message to a remote network, it must use the router. The host includes the IP address of the destination host within the packet just like before. However, when it encapsulates the packet into a frame, it uses the MAC address of the router as the destination for the frame. In this way, the router will receive and accept the frame based on the MAC address.

How does the source host determine the MAC address of the router? A host is given the IP address of the router through the default gateway address configured in its TCP/IP settings. The default gateway address is the address of the router interface connected to the same local network as the source host. All hosts on the local network use the default gateway address to send messages to the router. Once the host knows the default gateway IP address, it can use ARP to determine the MAC address. The MAC address of the router is then placed in the frame, destined for another network.

It is important that the correct default gateway be configured on each host on the local network. If no default gateway is configured in the host TCP/IP settings, or if the wrong default gateway is specified, messages addressed to hosts on remote networks cannot be delivered.

OSI Physical Layer

Physical Layer-Purpose

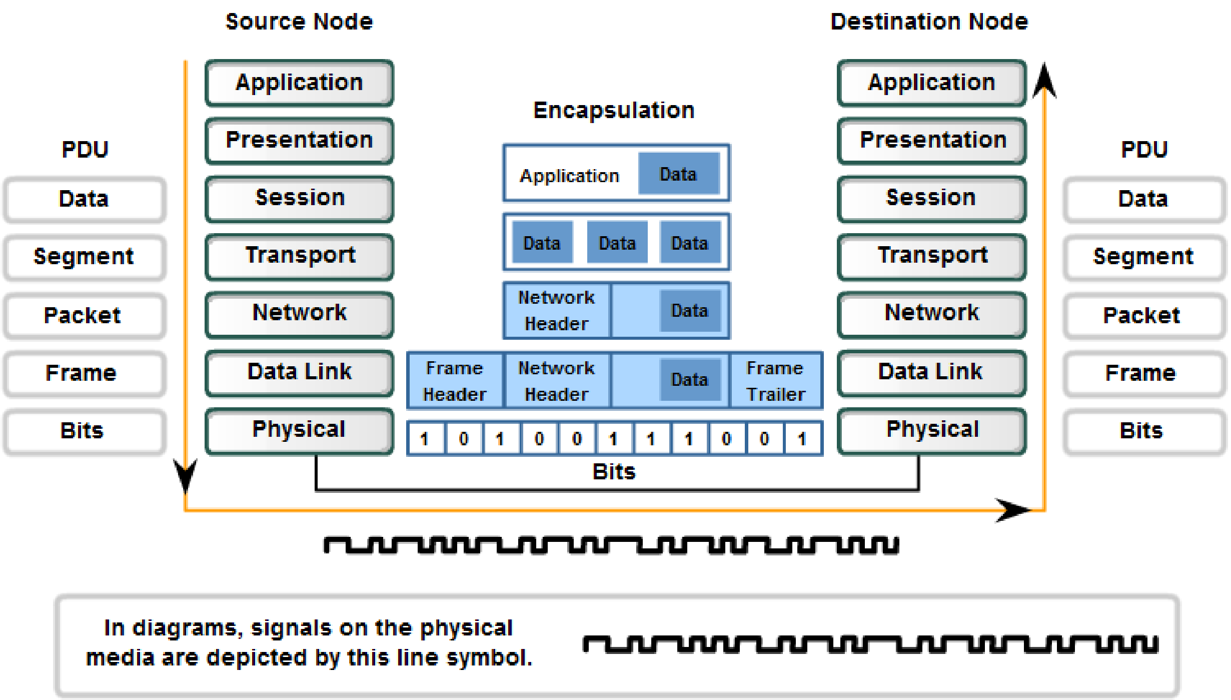
The OSI Physical layer provides the means to transport across the network media the bits that make up a Data Link layer frame. This layer accepts a complete frame from the Data Link layer and encodes it as a series of signals that are transmitted onto the local media. The encoded bits that comprise a frame are received by either an end device or an intermediate device.

- The delivery of frames across the local media requires the following Physical layer elements:
- The physical media and associated connectors
- A representation of bits on the media
- Encoding of data and control information
- Transmitter and receiver circuitry on the network devices

At this stage of the communication process, the user data has been segmented by the Transport layer, placed into packets by the Network layer, and further encapsulated as frames by the Data Link layer. The purpose of the Physical layer is to create the electrical, optical, or microwave signal that represents the bits in each frame. These signals are then sent on the media one at a time.

It is also the job of the Physical layer to retrieve these individual signals from the media, restore them to their bit representations, and pass the bits up to the Data Link layer as a complete frame.

Transforming Human Network Communications to Bits



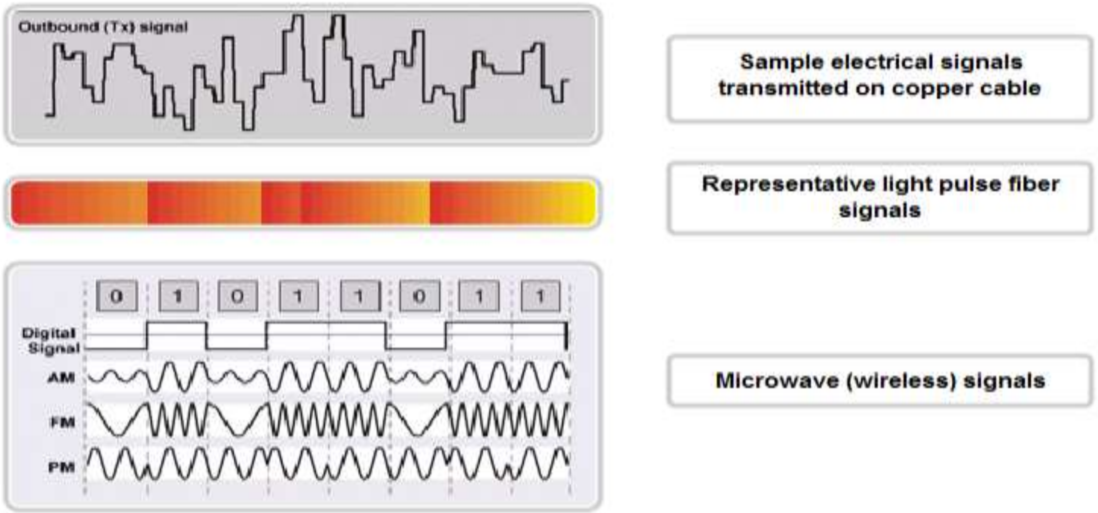
Operation

The media does not carry the frame as a single entity. The media carries signals, one at a time, to represent the bits that make up the frame.

There are three basic forms of network media on which data is represented:

- Copper cable
- Fiber
- Wireless

Representations of Signals on the Physical Media


Outbound (Tx) signal
Sample electrical signals transmitted on copper cable
Representative light pulse fiber signals
0
1
0
1
1
0
1
1
Digital Signal
AM
FM
PM
Microwave (wireless) signals

The representation of the bits - that is, the type of signal - depends on the type of media. For copper cable media, the signals are patterns of electrical pulses. For fiber, the signals are patterns of light. For wireless media, the signals are patterns of radio transmissions.

Identifying a Frame

When the Physical layer encodes the bits into the signals for a particular medium, it must also distinguish where one frame ends and the next frame begins. Otherwise, the devices on the media would not recognize when a frame has been fully received. In that case, the destination device would only receive a string of signals and would not be able to properly reconstruct the frame. As described in the previous chapter, indicating the beginning of frame is often a function of the Data Link layer. However, in many technologies, the Physical layer may add its own signals to indicate the beginning and end of the frame.

To enable a receiving device to clearly recognize a frame boundary, the transmitting device adds signals to designate the start and end of a frame. These signals represent particular bit patterns that are only used to denote the start or end of a frame.

Standards

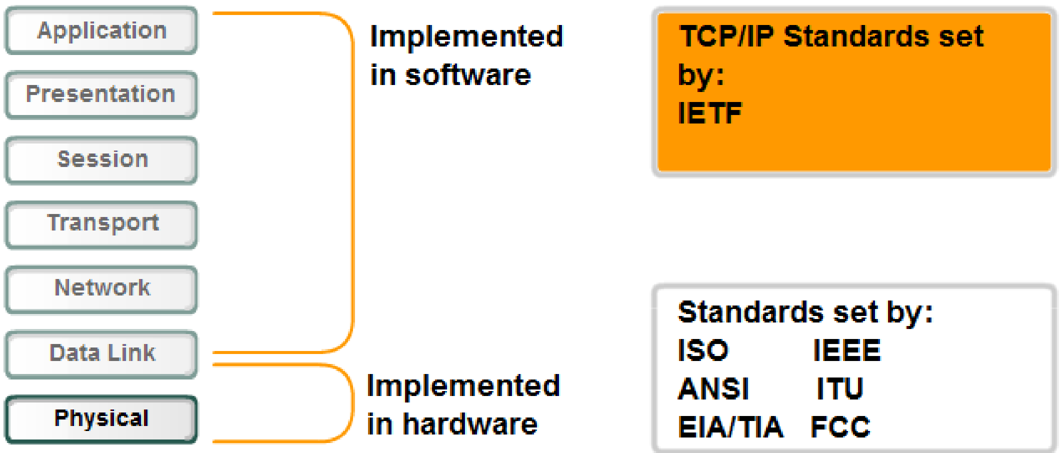
The Physical layer consists of hardware, developed by engineers, in the form of electronic circuitry, media, and connectors. Therefore, it is appropriate that the standards governing this hardware are defined by the relevant electrical and communications engineering organizations.

By comparison, the protocols and operations of the upper OSI layers are performed by software and are designed by software engineers and computer scientists. As we saw in a previous chapter, the services and protocols in the TCP/IP suite are defined by the Internet Engineering Task Force (IETF) in RFCs.

Similar to technologies associated with the Data Link layer, the Physical layer technologies are defined by organizations such as:

- The International Organization for Standardization (ISO)
- The Institute of Electrical and Electronics Engineers (IEEE)
- The American National Standards Institute (ANSI)
- The International Telecommunication Union (ITU)
- The Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA)
- National telecommunications authorities such as the Federal Communication Commission (FCC) in the USA.

Comparison of Physical Layer Standards and Upper Layer Standards



Physical Layer Technologies and Hardware

The technologies defined by these organizations include four areas of the Physical layer standards:

- Physical and electrical properties of the media
- Mechanical properties (materials, dimensions, pinouts) of the connectors
- Bit representation by the signals (encoding)
- Definition of control information signals

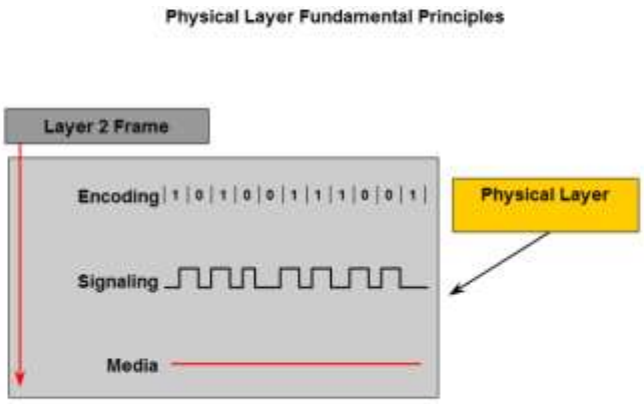
Hardware components such as network adapters (NICs), interfaces and connectors, cable materials, and cable designs are all specified in standards associated with the Physical layer.

Fundamental Principles

The three fundamental functions of the Physical layer are:

- The physical components
- Data encoding
- Signaling

The physical elements are the electronic hardware devices, media and connectors other that transmit and carry the signals to represent the bits.


Physical Layer Fundamental Principles

Encoding

Encoding is a method of converting a stream of data bits into a predefined "code. Codes are groupings of bits used to provide a predictable pattern that can be recognized by both the sender and the received. Using predictable patterns helps to distinguish data bits from control bits and provide better media error detection.

In addition to creating codes for data, encoding methods at the Physical layer may also provide codes for control purposes such as identifying the beginning and end of a frame. The transmitting host will transmit the specific pattern of bits or a code to identify the beginning and end of the frame.

Signaling

The Physical layer must generate the electrical, optical, or wireless signals that represent the "1" and "0" on the media. The method of representing the bits is called the signaling method. The Physical layer standards must define what type of signal represents a "1" and a "0". This can be as simple as a change in the level of an electrical signal or optical pulse or a more complex signaling method.

Data Carrying Capacity

Different physical media support the transfer of bits at different speeds. Data transfer can be measured in three ways:

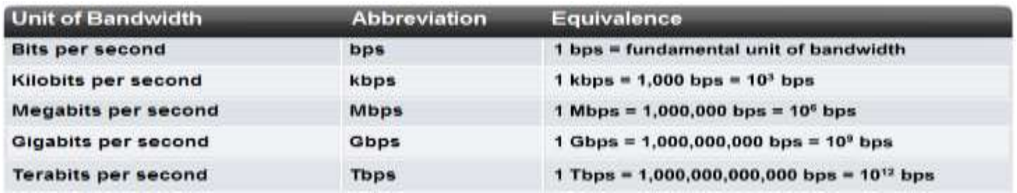
Bandwidth

The capacity of a medium to carry data is described as the raw data bandwidth of the media. Digital bandwidth measures the amount of information that can flow from one place to another in a given amount of time. Bandwidth is typically measured in kilobits per second (kbps) or megabits per second (Mbps).

The practical bandwidth of a network is determined by a combination of factors: the properties of the physical media and the technologies chosen for signaling and detecting network signals.

Physical media properties, current technologies, and the laws of physics all play a role in determining available bandwidth.

The figure shows the commonly used units of bandwidth.



Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps

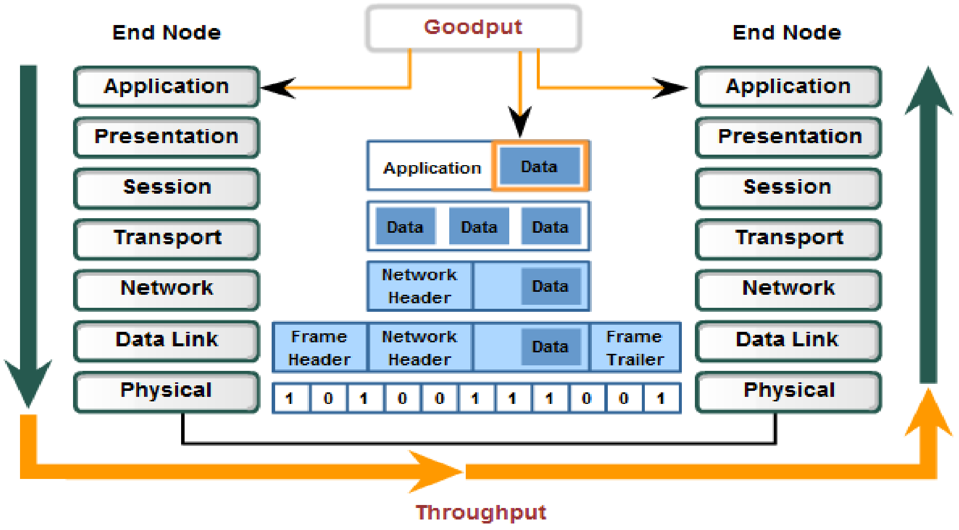
Throughput

Throughput is the measure of the transfer of bits across the media over a given period of time. Due to a number of factors, throughput usually does not match the specified bandwidth in Physical layer implementations such as Ethernet.

Many factors influence throughput. Among these factors are the amount of traffic, the type of traffic, and the number of network devices encountered on the network being measured. In a multi-access topology such as Ethernet, nodes are competing for media access and its use. Therefore, the throughput of each node is degraded as usage of the media increases.

In an internetwork or network with multiple segments, throughput cannot be faster than the slowest link of the path from source to destination. Even if all or most of the segments have high bandwidth, it will only take one segment in the path with low throughput to create a bottleneck to the throughput of the entire network.

Data Throughput and Goodput



Data throughput is actual network performance. Goodput is a measure of the transfer of usable data after protocol overhead traffic has been removed.

Goodput

A third measurement has been created to measure the transfer of usable data. That measure is known as goodput. Goodput is the measure of usable data transferred over a given period of time, and is therefore the measure that is of most interest to network users. As shown in the figure, goodput measures the effective transfer of user data between Application layer entities, such as between a source web server process and a destination web browser device.

Unlike throughput, which measures the transfer of bits and not the transfer of usable data, goodput accounts for bits devoted to protocol overhead. Goodput is throughput minus traffic overhead for establishing sessions, acknowledgements, and encapsulation.

As an example, consider two hosts on a LAN transferring a file. The bandwidth of the LAN is 100 Mbps. Due to the sharing and media overhead the through put between the computers is only 60 Mbps. With the overhead of the encapsulation process of the TCP/IP stack, the actual rate of the data received by the destination computer, goodput, is only 40Mbps.

Types of Physical Media

The Physical layer is concerned with network media and signaling. This layer produces the representation and groupings of bits as voltages, radio frequencies, or light pulses. Various standards organizations have contributed to the definition of the physical, electrical, and mechanical properties of the media available for different data communications. These specifications guarantee that cables and connectors will function as anticipated with different Data Link layer implementations.

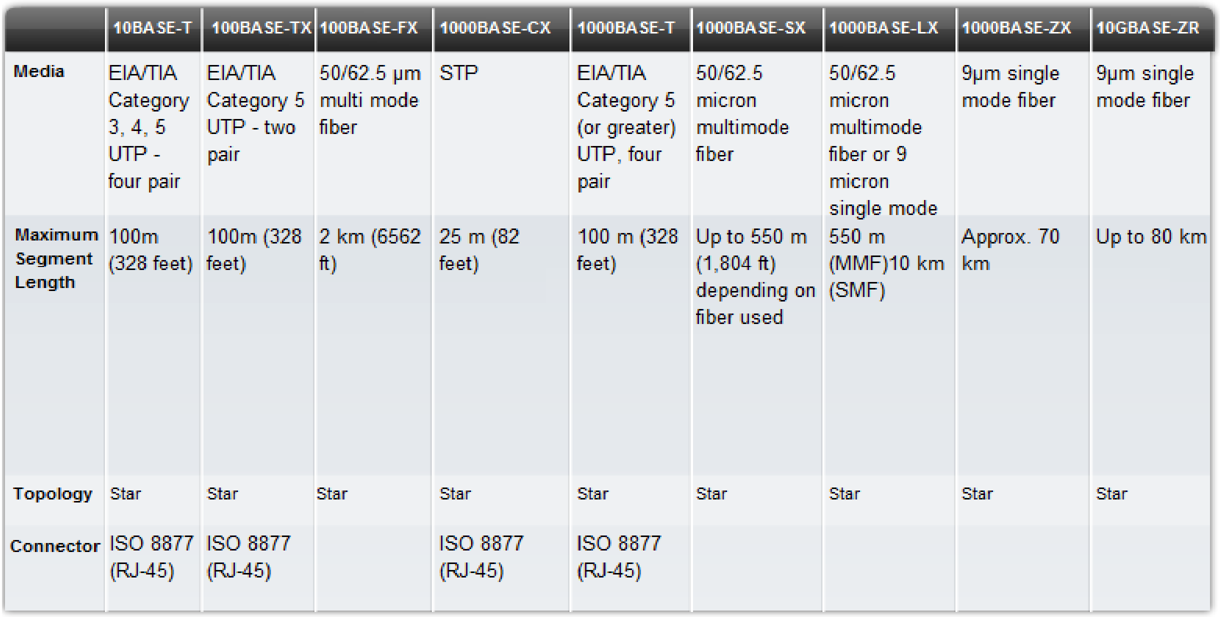
As an example, standards for copper media are defined for the:

- Type of copper cabling used
- Bandwidth of the communication
- Type of connectors used
- Pinout and color codes of connections to the media
- Maximum distance of the media

The figure shows some of the characteristics of networking media.

Physical Media - Characteristics

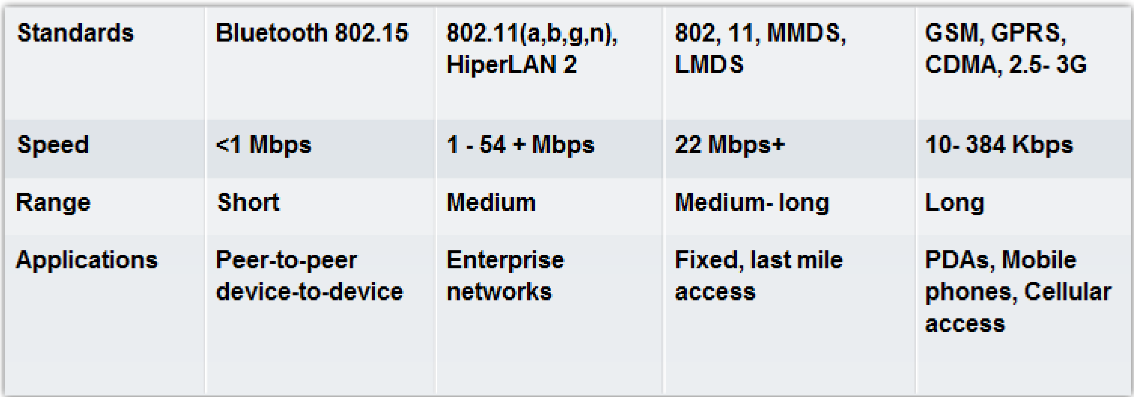
Ethernet Media



	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX	1000BASE-ZX	10GBASE-ZR
Media	EIA/TIA Category 3, 4, 5 UTP - four pair	EIA/TIA Category 5 UTP - two pair	50/62.5 µm multi mode fiber	STP	EIA/TIA Category 5 (or greater) UTP, four pair	50/62.5 micron multimode fiber	50/62.5 micron multimode fiber or 9 micron single mode	9µm single mode fiber	9µm single mode fiber
Maximum Segment Length	100m (328 feet)	100m (328 feet)	2 km (6562 ft)	25 m (82 feet)	100 m (328 feet)	Up to 550 m (1,804 ft) depending on fiber used	550 m (MMF)10 km (SMF)	Approx. 70 km	Up to 80 km
Topology	Star	Star	Star	Star	Star	Star	Star	Star	Star
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)				

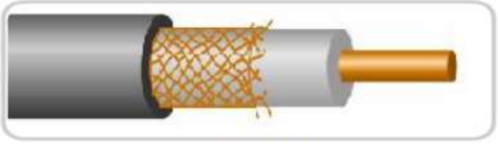
Physical Media - Characteristics

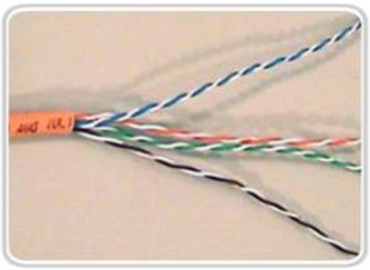
Wireless Media



Standards	Bluetooth 802.15	802.11(a,b,g,n), HiperLAN 2	802, 11, MMDS, LMDS	GSM, GPRS, CDMA, 2.5- 3G
Speed	<1 Mbps	1 - 54 + Mbps	22 Mbps+	10- 384 Kbps
Range	Short	Medium	Medium- long	Long
Applications	Peer-to-peer device-to-device	Enterprise networks	Fixed, last mile access	PDAs, Mobile phones, Cellular access

Copper Media


Coaxial cable


Unshielded twisted-pair cable

RJ-45 connections

The most commonly used media for data communications is cabling that uses copper wires to signal data and control bits between network devices. Cabling used for data communications usually consists of a series of individual copper wires that form circuits dedicated to specific signaling purposes.

Other types of copper cabling, known as coaxial cable, have a single conductor that runs through the center of the cable that is encased by, but insulated from, the other shield. The copper media type chosen is specified by the Physical layer standard required to link the Data Link layers of two or more network devices.

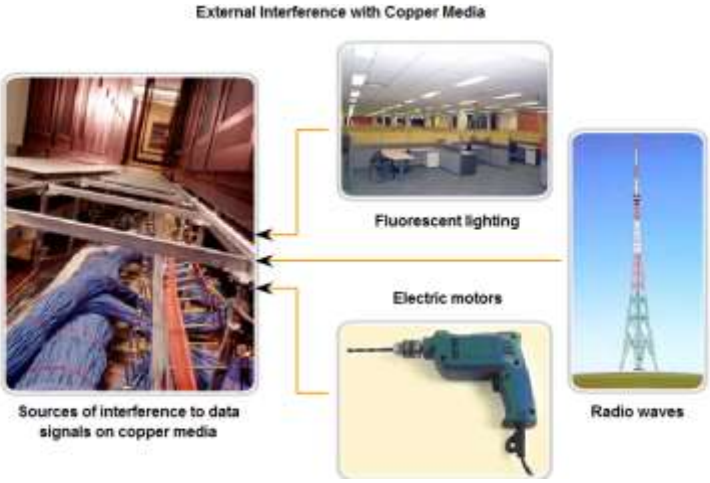
These cables can be used to connect nodes on a LAN to intermediate devices, such as routers and switches. Cables are also used to connect WAN devices to a data services provider such as a telephone company. Each type of connection and the accompanying devices have cabling requirements stipulated by Physical layer standards.

Networking media generally make use of modular jacks and plugs, which provide easy connection and disconnection. Also, a single type of physical connector may be used for multiple types of connections. For example, the RJ-45 connector is used widely in LANs with one type of media and in some WANs with another media type.

External Signal Interference

Data is transmitted on copper cables as electrical pulses. A detector in the network interface of a destination device must receive a signal that can be successfully decoded to match the signal sent.

The timing and voltage values of these signals are susceptible to interference or "noise" from outside the communications system. These unwanted signals can distort and corrupt the data signals being carried by copper media. Radio waves and electromagnetic devices such as fluorescent lights, electric motors, and other devices are potential sources of noise.


External Interference with Copper Media
Fluorescent lighting
Electric motors
Radio waves
Sources of interference to data signals on copper media

Cable types with shielding or twisting of the pairs of wires are designed to minimize signal degradation due to electronic noise.

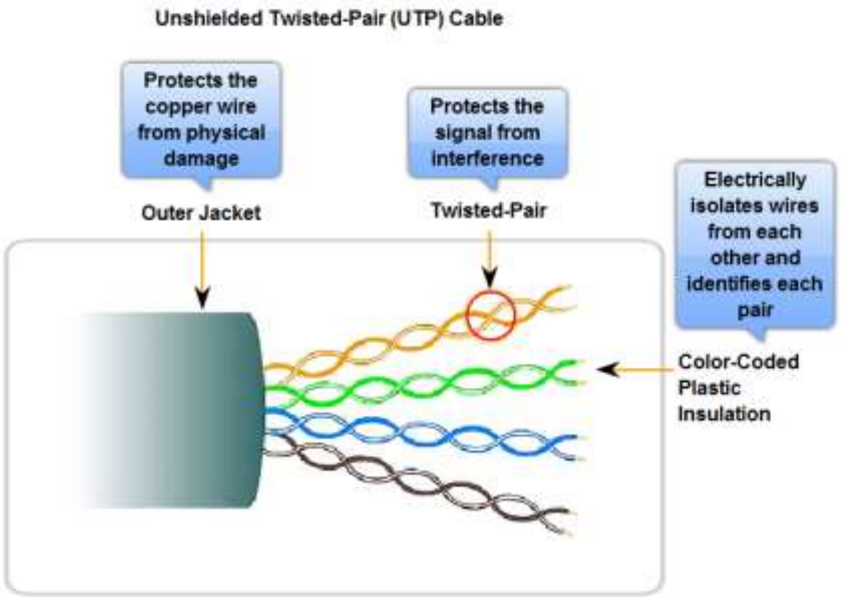
The susceptibility of copper cables to electronic noise can also be limited by:

- Selecting the cable type or category most suited to protect the data signals in a given networking environment

- Designing a cable infrastructure to avoid known and potential sources of interference in the building structure
- Using cabling techniques that include the proper handling and termination of the cables

There are three types of twisted pair cable: unshielded twisted pair, shielded twisted pair, and screened twisted pair.

Unshielded Twisted Pair (UTP)
Unshielded twisted-pair (UTP) cabling, as it is used in Ethernet LANs, consists of four pairs of color-coded wires that have been twisted together and then encased in a flexible plastic sheath. As seen in the figure, the color codes identify the individual pairs and wires in the pairs and aid in cable termination.


Unshielded Twisted-Pair (UTP) Cable
Protects the copper wire from physical damage
Outer Jacket
Protects the signal from interference
Twisted-Pair
Electrically isolates wires from each other and identifies each pair
Color-Coded Plastic Insulation

The twisting has the effect of canceling unwanted signals. When two wires in an electrical circuit are placed close together, external electromagnetic fields create the same interference in each wire. The pairs are twisted to keep the wires in as close proximity as is physically possible. When this common interference is present on the wires in a twisted pair, the receiver processes it in equal yet opposite ways. As a result, the signals caused by electromagnetic interference from external sources are effectively cancelled.

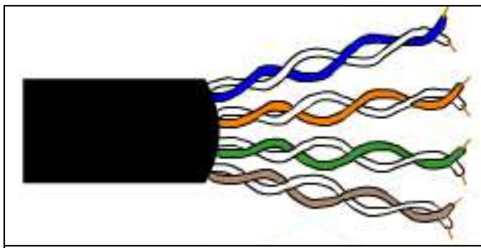
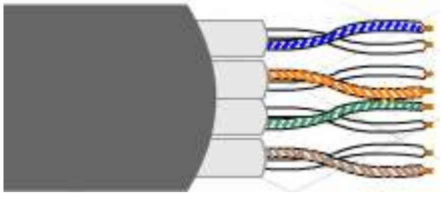
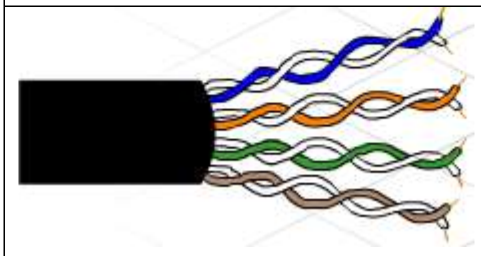
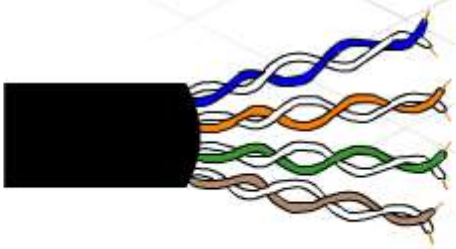
This cancellation effect also helps avoid interference from internal sources called crosstalk. Crosstalk is the interference caused by the magnetic field around the adjacent pairs of wires in the cable. When electrical current flows through a wire, it creates a circular magnetic field around the wire. With the current flowing in opposite directions in the two wires in a pair, the magnetic fields - as equal but opposite forces - have a cancellation effect on each other. Additionally, the different pairs of wires that are twisted in the cable use a different number of twists per meter to help protect the cable from crosstalk between pairs.

UTP Cabling Standards
The UTP cabling commonly found in workplaces, schools, and homes conforms to the standards established jointly by the Telecommunications Industry Association (TIA) and the Electronics Industries Alliance (EIA). TIA/EIA-568A stipulates the commercial cabling standards for LAN installations and is the standard most commonly used in LAN cabling environments. Some the elements defined are:

- Cable types
- Cable lengths
- Connectors

- Cable termination
- Methods of testing cable

The electrical characteristics of copper cabling are defined by the Institute of Electrical and Electronics Engineers (IEEE). IEEE rates UTP cabling according to its performance. Cables are placed into categories according to their ability to carry higher bandwidth rates. For example, Category 5 (Cat5) cable is used commonly in 100BASE-TX FastEthernet installations. Other categories include Enhanced Category 5 (Cat5e) cable and Category 6 (Cat6).

	Category 3 Cable (UTP) • Used for Voice communication • Most often used for phone lines
	Category 7 Cable (UTP) • Used for Data transmission • Individual pairs are wrapped in a shield and the entire four pairs wrapped in another shield • Supports 1000 Mbps-10 Gbps, though 10 Gbps is not recommended
	Category 6 Cable (UTP) • Used for Data transmission • An added separator is between each pair of wires allowing it to function at higher speeds • Supports 1000 Mbps-10 Gbps, though 10 Gbps is not recommended
	Category 5 and 5e Cable (UTP) • Used for Data transmission • Cat 5 supports 100 Mbps and can support 1000 Mbps but it is not recommended • Cat 5e supports 1000 Mbps

Cables in higher categories are designed and constructed to support higher data rates. As new gigabit speed Ethernet technologies are being developed and adopted, Cat5e is now the minimally acceptable cable type, with Cat6 being the recommended type for new building installations.Some people connect to data network using existing telephone systems. Often the cabling in these systems are some form of UTP that are lower grade than the current Cat5+ standards.Installing less expensive but lower rated cabling is potentially wasteful and shortsighted. If the decision is later made to adopt a faster LAN technology, total replacement of the installed cable infrastructure may be required.

UTP Cable Types

UTP cabling, terminated with RJ-45 connectors, is a common copper-based medium for interconnecting network devices, such as computers, with intermediate devices, such as routers and network switches.

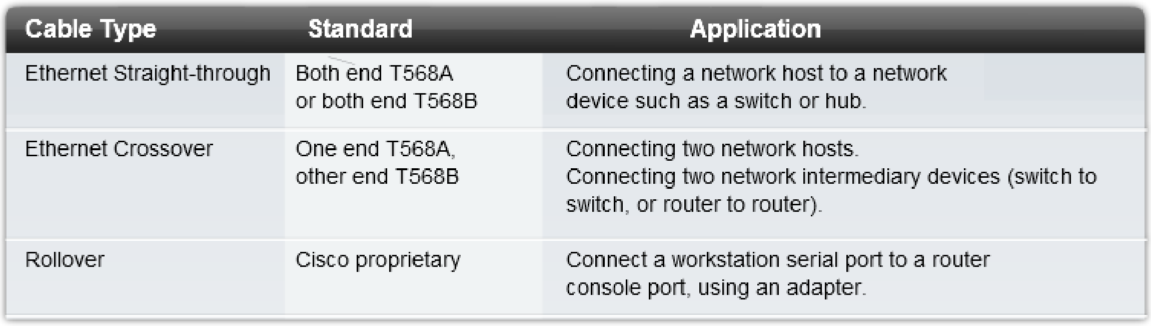
Different situations may require UTP cables to be wired according to different wiring conventions. This means that the individual wires in the cable have to be connected in different orders to different sets of pins in the RJ-45 connectors. The following are main cable types that are obtained by using specific wiring conventions:

- Ethernet Straight-through
- Ethernet Crossover
- Rollover

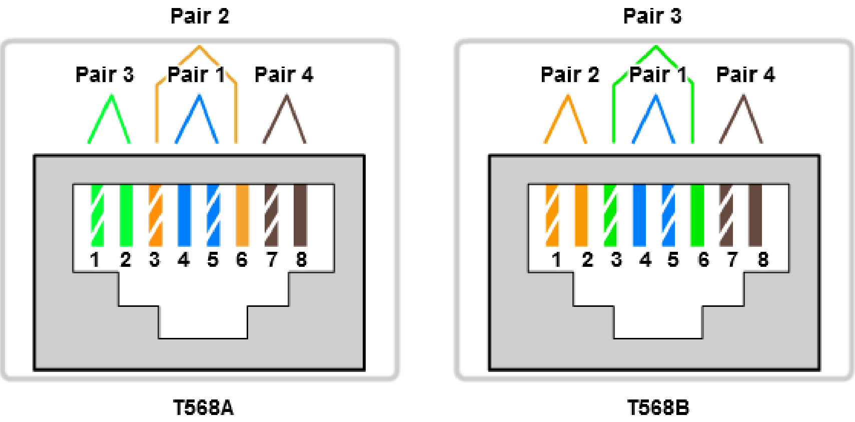
The figure shows the typical application of these cables as well as a comparison of these three cable types.

Using a crossover or straight-through cable incorrectly between devices may not damage the devices, but connectivity and communication between the devices will not take place. This is a common error in the lab and checking that the device connections are correct should be the first troubleshooting action if connectivity is not achieved.

Straight-through, Crossover, and Rollover Cable Types



Cable Type	Standard	Application
Ethernet Straight-through	Both end T568A or both end T568B	Connecting a network host to a network device such as a switch or hub.
Ethernet Crossover	One end T568A, other end T568B	Connecting two network hosts. Connecting two network intermediary devices (switch to switch, or router to router).
Rollover	Cisco proprietary	Connect a workstation serial port to a router console port, using an adapter.



Other Copper Cable

Two other types of copper cable are used:

Coaxial Cable

Coaxial cable consists of a copper conductor surrounded by a layer of flexible insulation, as shown in the figure.

Over this insulating material is a woven copper braid, or metallic foil, that acts as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, also reduces the amount of outside electromagnetic interference. Covering the shield is the cable jacket.

All the elements of the coaxial cable encircle the center conductor. Because they all share the same axis, this construction is called coaxial, or coax for short.

Uses of Coaxial Cable

The coaxial cable design has been adapted for different purposes. Coax is an important type of cable that is used in wireless and cable access technologies. Coax cables are used to attach antennas to wireless devices. The coaxial cable carries radio frequency (RF) energy between the antennas and the radio equipment.

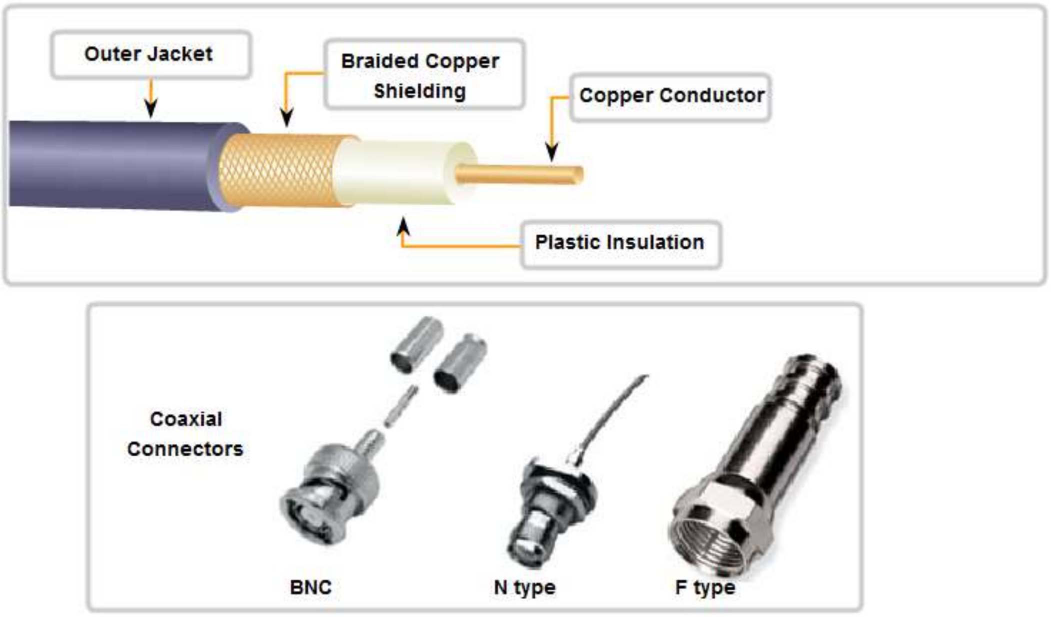
Coax is also the most widely used media for transporting high radio frequency signals over wire, especially cable television signals. Traditional cable television, exclusively transmitting in one direction, was composed completely of coax cable.

Cable service providers are currently converting their one-way systems to two-way systems to provide Internet connectivity to their customers. To provide these services, portions of the coaxial cable and supporting amplification elements are replaced with multi-fiber-optic cable. However, the final connection to the customer's location and the wiring inside the customer's premises is still coax cable. This combined use of fiber and coax is referred to as hybrid fiber coax (HFC).

In the past, coaxial cable was used in Ethernet installations. Today UTP offers lower costs and higher bandwidth than coaxial and has replaced as the standard for all Ethernet installations.

There are different types of connectors used with coax cable. The figure shows some of these connector types.

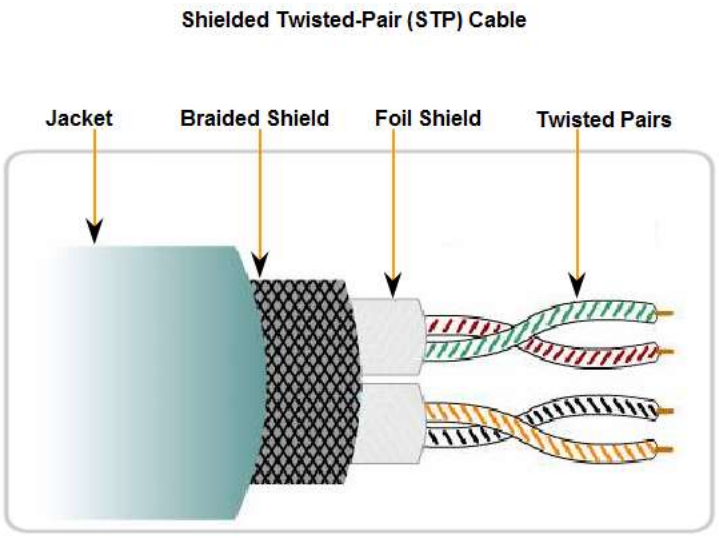
Coaxial Cable Design



Shielded Twisted-Pair (STP) Cable

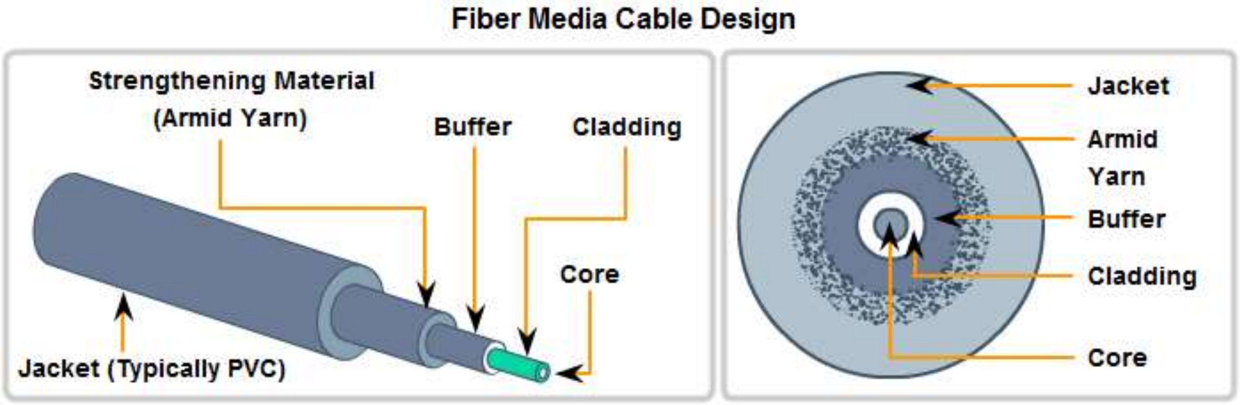
Another type of cabling used in networking is shielded twisted-pair (STP). As shown in the figure, STP uses two pairs of wires that are wrapped in an overall metallic braid or foil.

STP cable shields the entire bundle of wires within the cable as well as the individual wire pairs. STP provides better noise protection than UTP cabling, however at a significantly higher price.



For many years, STP was the cabling structure specified for use in Token Ring network installations. With the use of Token Ring declining, the demand for shielded twisted-pair cabling has also waned. The new 10 GB standard for Ethernet has a provision for the use of STP cabling. This may provide a renewed interest in shielded twisted-pair cabling.

Fiber Media



Fiber-optic cabling uses either glass or plastic fibers to guide light impulses from source to destination. The bits are encoded on the fiber as light impulses . Optical fiber cabling is capable of very large raw data bandwidth rates. Most current transmission standards have yet to approach the potential bandwidth of this media.

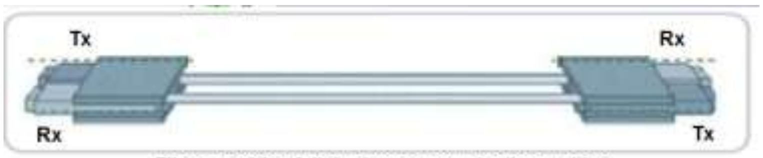
Fiber Compared to Copper Cabling

Given that the fibers used in fiber-optic media are not electrical conductors, the media is immune to electromagnetic interference and will not conduct unwanted electrical currents due to grounding issues. Because optical fibers are thin and have relatively low signal loss, they can be operated at much greater lengths than copper media, without the need for signal regeneration. Some optical fiber Physical layer specifications allow lengths that can reach multiple kilometers.

Optical fiber media implementation issues include:
More expensive (usually) than copper media over the same distance (but for a higher capacity)
Different skills and equipment required to terminate and splice the cable infrastructure
More careful handling than copper media

At present, in most enterprise environments, optical fiber is primarily used as backbone cabling for high-traffic point-to-point connections between data distribution facilities and for the interconnection of buildings in multi-building campuses. Because optical fiber does not conducts electricity and has low signal loss, it is well suited for these uses.

Cable Construction



Fiber provides full duplex communications with a cable dedicated to each direction.

Optical fiber cables consist of a PVC jacket and a series of strengthening materials that surround the optical fiber and its cladding. The cladding surrounds the actual glass or plastic fiber and is designed to prevent light loss from the fiber.

Because light can only travel in one direction over optical fiber, two fibers are required to support full duplex operation. Fiber-optic patch cables bundle together two optical fiber cables and terminate them with a pair of standard single fiber connectors. Some fiber connectors accept both the transmitting and receiving fibers in a single connector.

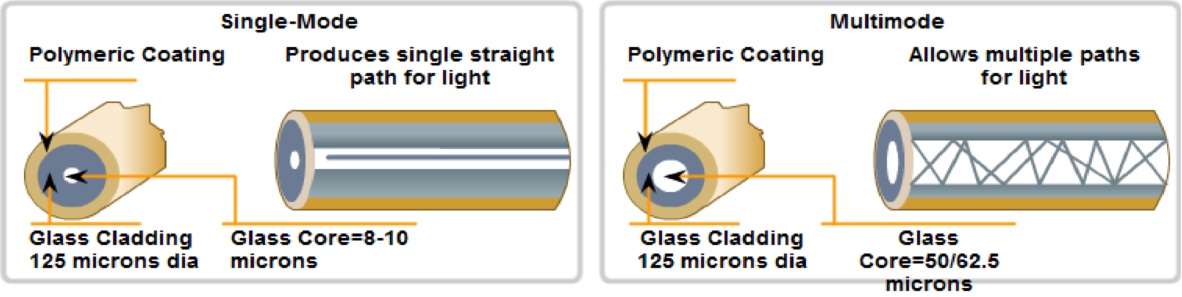
Generating and Detecting the Optical Signal

Either lasers or light emitting diodes (LEDs) generate the light pulses that are used to represent the transmitted data as bits on the media. Electronic semi-conductor devices called photodiodes detect the light pulses and convert them to voltages that can then be reconstructed into data frames.

Note: The laser light transmitted over fiber-optic cabling can damage the human eye. Care must be taken to avoid looking into the end of an active optical fiber.

Fiber optic cables can be broadly classified into two types: single-mode and multimode.

Single-mode optical fiber carries a single ray of light, usually emitted from a laser. Because the laser light is uni-directional and travels down the center of the fiber, this type of fiber can transmit optical pulses for very long distances.


Single-Mode
Polymeric Coating
Produces single straight path for light
Glass Cladding 125 microns dia
Glass Core=8-10 microns
Multimode
Polymeric Coating
Allows multiple paths for light
Glass Cladding 125 microns dia
Glass Core=50/62.5 microns

- Small Core
- Less Despersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters

- Larger core than single-mode cable (50 microns or greater)
- Allows greater dipersion and therefore, loss of signal
- Used for long distance appllication, but shorter than single-mode (up to ~2km, 6560 ft)
- Uses LEDs as the light source often within LANs or distances of couple hundred meters within a campus network

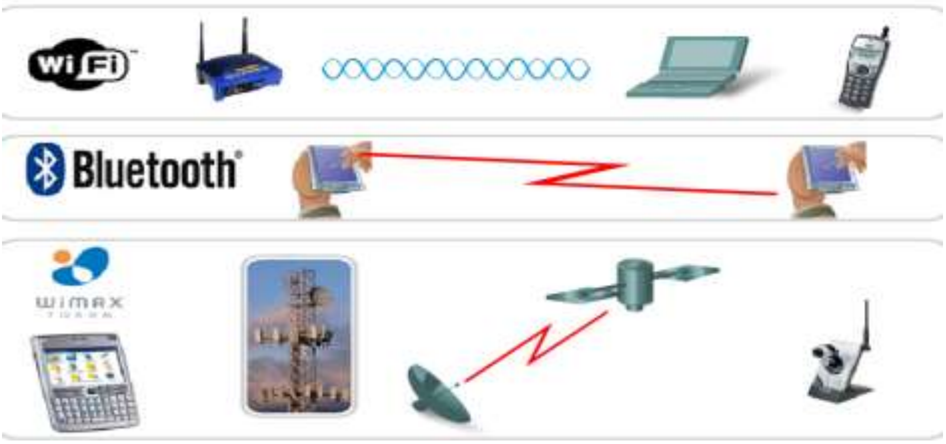
Multimode fiber typically uses LED emitters that do not create a single coherent light wave. Instead, light from an LED enters the multimode fiber at different angles. Because light entering the fiber at different angles takes different amounts of time to travel down the fiber, long fiber runs may result in the pulses becoming blurred on reception at the receiving end. This effect, known as modal dispersion, limits the length of multimode fiber segments.

Multimode fiber, and the LED light source used with it, are cheaper than single-mode fiber and its laser-based emitter technology.

Wireless Media

Types of Wireless Networks

Wireless Media Standards and Types



The IEEE and telecommunications industry standards for wireless data communications cover both the Data Link and Physical layers. Four common data communications standards that apply to wireless media are:

- Standard IEEE 802.11 - Commonly referred to as Wi-Fi, is a Wireless LAN (WLAN) technology that uses a contention or non-deterministic system with a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) media access process.
- Standard IEEE 802.15 - Wireless Personal Area Network (WPAN) standard, commonly known as "Bluetooth", uses a device pairing process to communicate over distances from 1 to 100 meters.
- Standard IEEE 802.16 - Commonly known as WiMAX (Worldwide Interoperability for Microwave Access), uses a point-to-multipoint topology to provide wireless broadband access.
- Global System for Mobile Communications (GSM) - Includes Physical layer specifications that enable the implementation of the Layer 2 General Packet Radio Service (GPRS) protocol to provide data transfer over mobile cellular telephony networks.

Other wireless technologies such as satellite communications provide data network connectivity for locations without another means of connection. Protocols including GPRS enable data to be transferred between earth stations and satellite links.

The Wireless LAN

WLAN Access Points and Adapters

A common wireless data implementation is enabling devices to wirelessly connect via a LAN. In general, a wireless LAN requires the following network devices:

Wireless Access Point (AP) - Concentrates the wireless signals from users and connects, usually through a copper cable, to the existing copper-based network infrastructure such as Ethernet.

Wireless NIC adapters - Provides wireless communication capability to each network host.

As the technology has developed, a number of WLAN Ethernet-based standards have emerged. Care needs to be taken in purchasing wireless devices to ensure compatibility and interoperability.

Standards include:

- IEEE 802.11a - Operates in the 5 GHz frequency band and offers speeds of up to 54 Mbps. Because this standard operates at higher frequencies, it has a smaller coverage area and is less effective at penetrating building structures. Devices operating under this standard are not interoperable with the 802.11b and 802.11g standards described below.

- IEEE 802.11b - Operates in the 2.4 GHz frequency band and offers speeds of up to 11 Mbps. Devices implementing this standard have a longer range and are better able to penetrate building structures than devices based on 802.11a.

- IEEE 802.11g - Operates in the 2.4 GHz frequency band and offers speeds of up to 54 Mbps. Devices implementing this standard therefore operate at the same radio frequency and range as 802.11b but with the bandwidth of 802.11a.

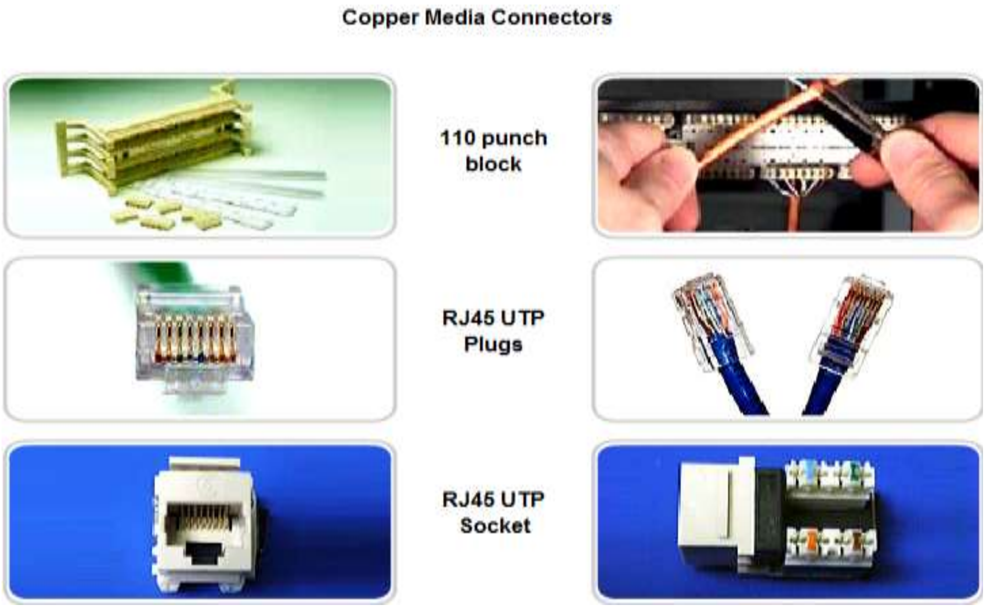
- IEEE 802.11n
- The IEEE 802.11n standard is currently in draft form. The proposed standard defines frequency of 2.4 Ghz or 5 GHz. The typical expected data rates are 100 Mbps to 210 Mbps with a distance range of up to 70 meters.

The benefits of wireless data communications technologies are evident, especially the savings on costly premises wiring and the convenience of host mobility. However, network administrators need to develop and apply stringent security policies and processes to protect wireless LANs from unauthorized access and damage.

These wireless standards and Wireless LAN implementations will be covered in more detail in the LAN Switching and Wireless course.

Media Connectors

Common Copper Media Connectors



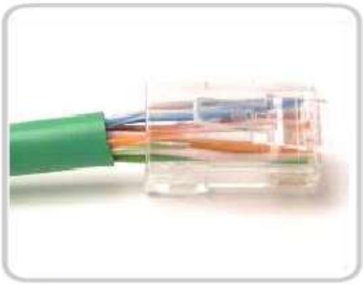
Different Physical layer standards specify the use of different connectors. These standards specify the mechanical dimensions of the connectors and the acceptable electrical properties of each type for the different implementations in which they are employed.

Although some connectors may look the same, they may be wired differently according to the Physical layer specification for which they were designed. The ISO 8877 specified RJ-45 connector is used for a range of Physical layer specifications, one of which is Ethernet. Another specification, EIA-TIA 568, describes the wire color codes to pin assignments (pinouts) for Ethernet straight-through and crossover cables.

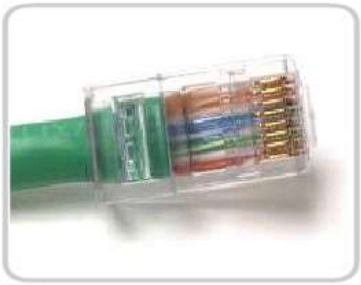
Although many types of copper cables can be purchased pre-made, in some situations, especially in LAN installations, the termination of copper media may be performed onsite. These terminations include crimped connections to terminate Cat5 media with RJ-45 plugs to make patch cables, and the use of punched down connections on 110 patch panels and RJ-45 jacks. The figure shows some of the Ethernet wiring components.

Correct Connector Termination

Each time copper cabling is terminated, there is the possibility of signal loss and the introduction of noise to the communication circuit. Ethernet workplace cabling specifications stipulate the cabling necessary to connect a computer to an active network intermediary device. When terminated improperly, each cable is a potential source of Physical layer performance degradation. It is essential that all copper media terminations be of high quality to ensure optimum performance with current and future network technologies.



Bad connector - Wires are untwisted for too great a length.



Good connector - Wires are untwisted to the extent necessary to attach the connector.

In some cases, for example in some WAN technologies, if an improperly wired RJ-45-terminated cable is used, damaging voltage levels may be applied between interconnected devices. This type of damage will generally occur when a cable is wired for one Physical layer technology and is used with a different technology.

Common Optical Fiber Connectors

Fiber-optic connectors come in a variety of types. The figure shows some of the most common:

- Straight-Tip (ST) (trademarked by AT &T) - a very common bayonet style connector widely used with multimode fiber.

- Subscriber Connector (SC) - a connector that uses a push-pull mechanism to ensure positive insertion. This connector type is widely used with single-mode fiber.

- Lucent Connector (LC) - A small connector becoming popular for use with single-mode fiber and also supports multi-mode fiber.

Terminating and splicing fiber-optic cabling requires special training and equipment. Incorrect termination of fiber optic media will result in diminished signaling distances or complete transmission failure.

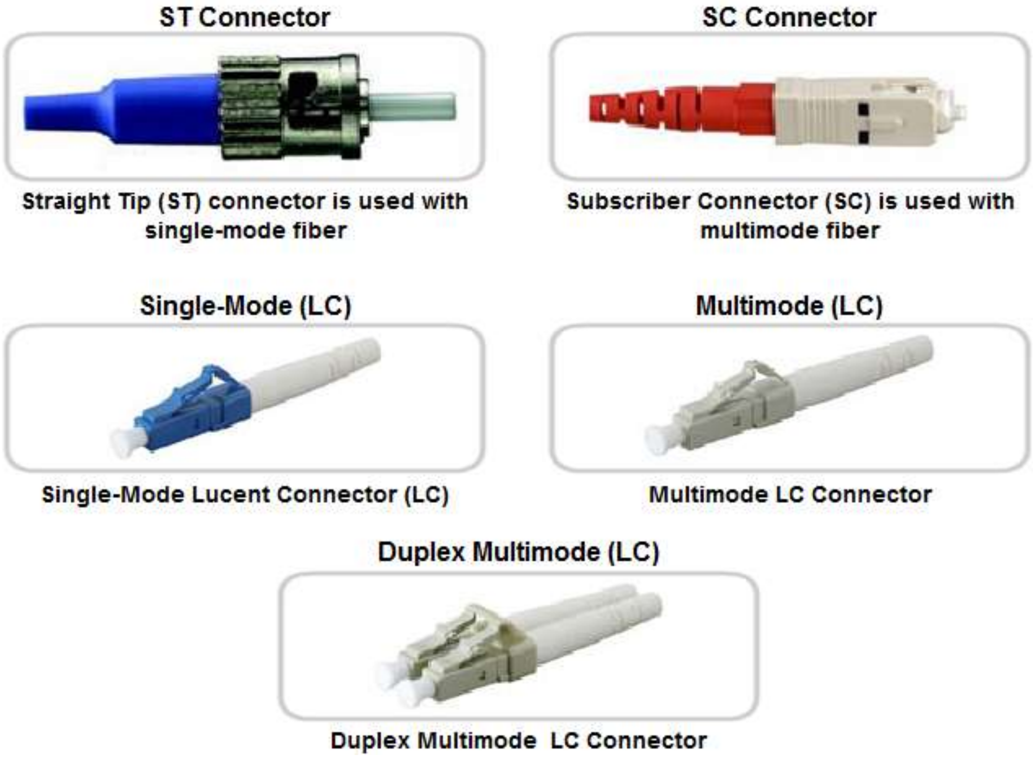
Three common types of fiber-optic termination and splicing errors are:

- Misalignment - the fiber-optic media are not precisely aligned to one another when joined.
- End gap - the media do not completely touch at the splice or connection.
- End finish - the media ends are not well polished or dirt is present at the termination.

It is recommended that an Optical Time Domain Reflectometer (OTDR) be used to test each fiber-optic cable segment. This device injects a test pulse of light into the cable and measures back scatter and reflection of light detected as a function of time. The OTDR will calculate the approximate distance at which these faults are detected along the length of the cable.

A field test can be performed by shining a bright flashlight into one end of the fiber while observing the other end of the fiber. If light is visible, then the fiber is capable of passing light. Although this does not ensure the performance of the fiber, it is a quick and inexpensive way to find a broken fiber.

Fiber Media Connectors



ST Connector

Straight Tip (ST) connector is used with single-mode fiber

SC Connector

Subscriber Connector (SC) is used with multimode fiber

Single-Mode (LC)

Single-Mode Lucent Connector (LC)

Multimode (LC)

Multimode LC Connector

Duplex Multimode (LC)

Duplex Multimode LC Connector

Cabling

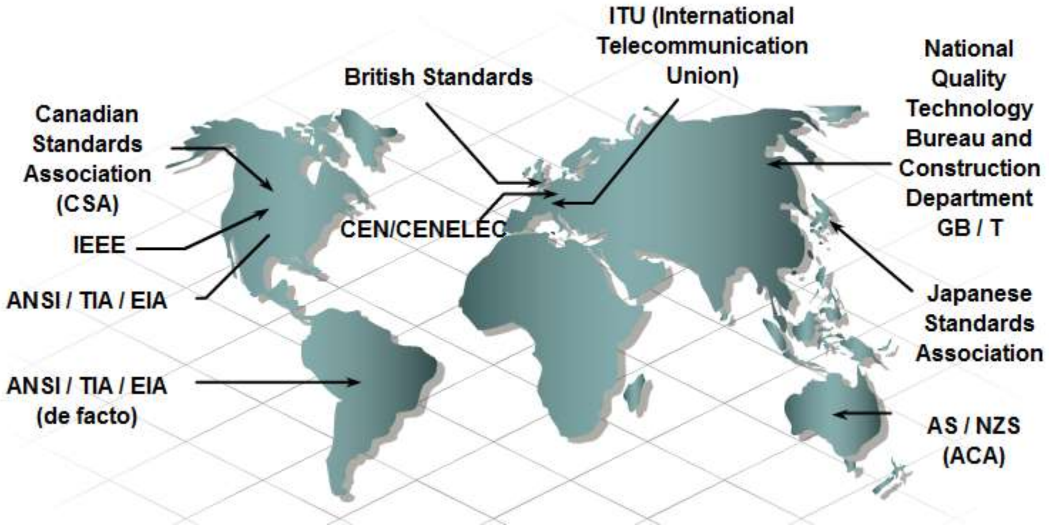
Cabling is an integral part of building any network. When installing cabling, it is important to follow cabling standards, which have been developed to ensure data networks operate to agreed levels of performance.

Standards

Cabling standards are a set of specifications for the installation and testing of cables. Standards specify types of cables to use in specific environments, conductor materials, pinouts, wire sizes, shielding, cable lengths, connector types and performance limits.

There are many different organizations involved in the creation of cabling standards. While some of these organizations have only local jurisdiction many offer standards that are adopted around the world.

Some of the organizations and the areas that they manage are seen in the graphic.


ITU (International Telecommunication Union)
British Standards
National Quality Technology Bureau and Construction Department GB / T
Canadian Standards Association (CSA)
IEEE
CEN/CENELEC
ANSI / TIA / EIA
Japanese Standards Association
ANSI / TIA / EIA (de facto)
AS / NZS (ACA)

Working with Twisted Pair

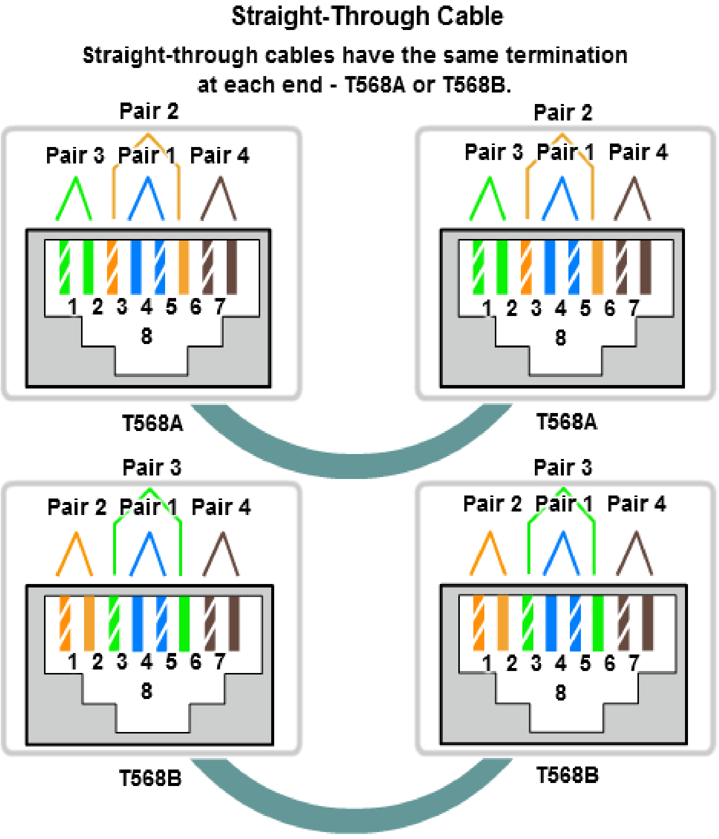
Twisted pair cable is most commonly used in network installations. The TIA/EIA organization defines two different patterns, or wiring scheme, called T568A and T568B. Each wiring scheme defines the pinout, or order of wire connections, on the end of the cable.

The two schemes are similar except two of the four pairs are reversed in the termination order. The graphic shows this color-coding and how the two pairs are reversed.

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 already employed.

Using the T568A and T568B wiring standards, 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

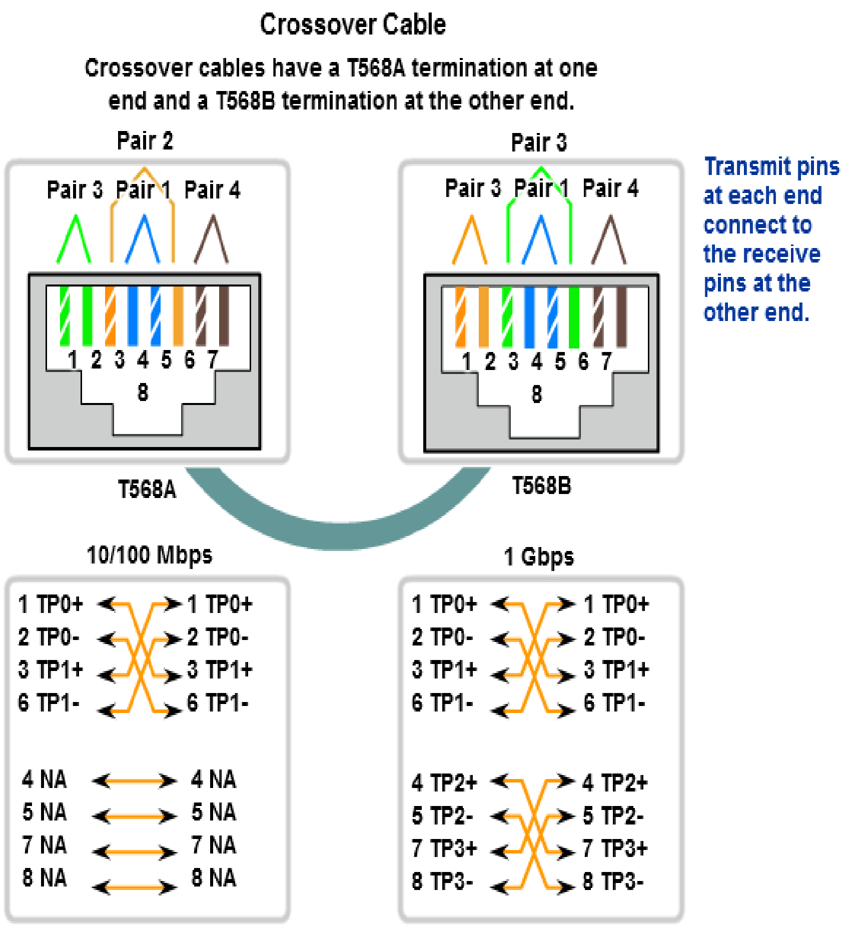

Straight-Through Cable

Straight-through cables have the same termination at each end - T568A or T568B.

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.

It is the type of straight-through cable (T568A or T568B) used on the network that defines the wiring scheme for the network.

Crossover Cable



Transmit pins at each end connect to the receive pins at the other end.

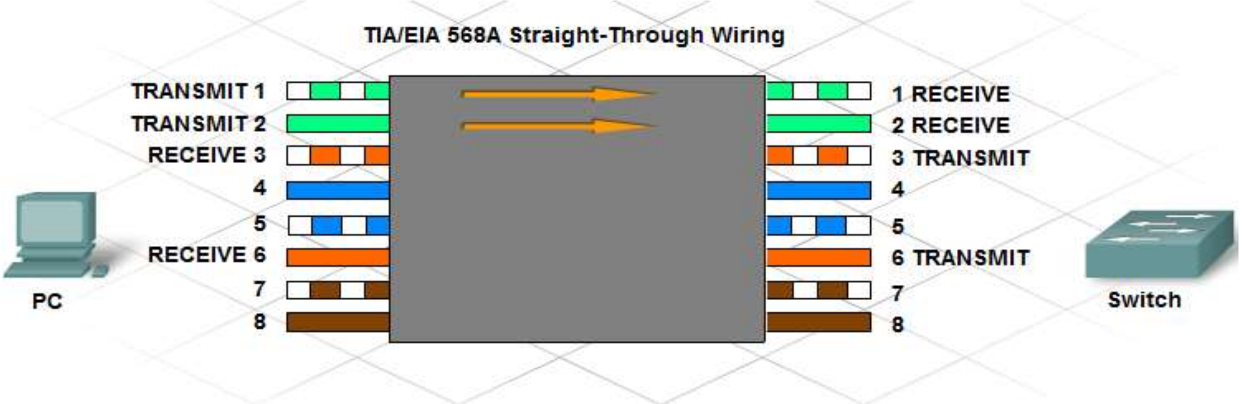
A crossover cable uses both wiring schemes. T568A on one end of the cable and T568B on the other end of the same cable. This means that the order of connection on one end of the cable does not match the order of connections on the other.

The straight-through and crossover cables each have a specific use on the network. The type of cable needed to connect two devices depends on which wire pairs the devices use to transmit and receive data.

Specific pins on the connector are associated with a transmit function and a receive function. The transmit pin versus the receive pin is determined based on the device.

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. 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.

Unlike Devices



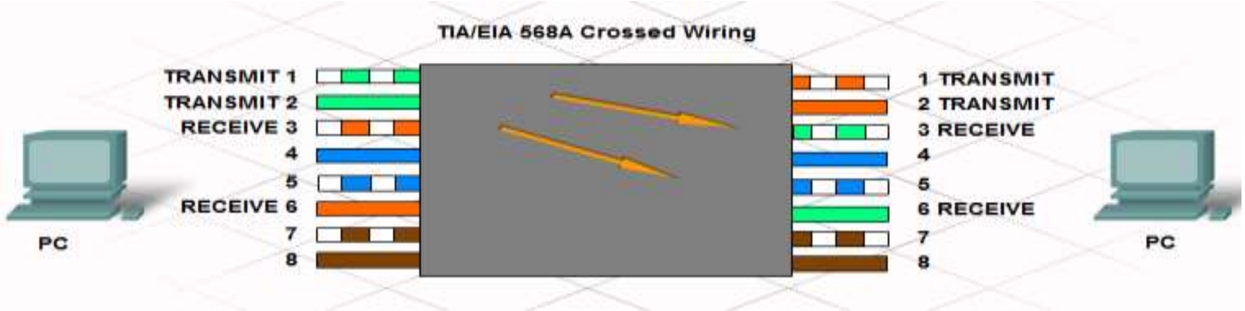
The pins on the RJ-45 data connector of a PC have pins 1 and 2 as transmit and pins 3 and 6 as receive. The pins on the data connector of a switch have pins 1 and 2 as receive and pins 3 and 6 as transmit. The pins used for transmit on the PC correspond to those used for receive on the switch. Therefore, a straight-through cable is necessary.

The wire connected to pin 1 (transmit pin) on the PC on one end of the cable, is connected to pin 1 (receive pin) on the switch on the other end of the cable.

Other examples of unlike devices that require a straight-through cable include:

- Switch port to router port
- Hub port to PC

Like Devices



If a PC is directly connected to another PC, pins 1 and 2 on both devices are transmit pins and pins 3 and 6 are receive pins.

A crossover cable would ensure that the green wire connected to pins 1 and 2 (transmit pins) on one PC connect to pins 3 and 6 (receive pins) on the other PC.

If a straight-through cable were used, the wire connected to pin 1, the transmit pin, on PC1 would be connected to pin 1, the transmit pin, on PC2. It is not possible to receive data on a transmit pin.

Other examples of 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.

MDI/MDIX Selection
Many devices allow the UTP Ethernet port to be set to MDI or MDIX. This can be done in one of three ways, depending on the features of the device:

1. On some devices, ports may have a mechanism that electrically swaps the transmit and receive pairs. The port can be changed from MDI to MDIX by engaging the mechanism.

2. As part of the configuration, some devices allow for selecting whether a port functions as MDI or as MDIX.

3. Many newer devices have an automatic crossover feature. This feature allows the device to detect the required cable type and configures the interfaces accordingly. On some devices, this auto-detection is performed by default. Other devices require an interface configuration command for enabling MIDX auto-detection.

UTP Cable Termination

UTP and STP cable is usually terminated into an RJ-45 connector.

The RJ-45 connector is considered a male component, which is crimped to the end of the cable. When a male connector is viewed from the front with the metal contacts facing up, the pin locations are numbered from 8 on the left to 1 on the right.

The jack is considered the female component and is located in networking devices, wall outlets, or patch panels. The RJ-45 connector on the wire plugs into the jack.

Cables can be purchased that are pre-terminated with RJ-45 connectors. They can also be manually terminated, onsite, using a crimping tool. When manually terminating UTP cable into an RJ-45 connector, untwist only a small amount of wire to minimize crosstalk. Also be sure that the wires are pushed all the way into the end of the connector and that the RJ45 connector is crimped onto the wire jacket. This ensures good electrical contact and provides strength to the wire connection.

Terminating UTP at Patch Panel and Wall Jacks

Front of Patch Panel

Rear of Patch Panel

Close Up of Back of Patch Panel

Punchdown Tool

Network devices are usually connected to patch panels. Patch panels act like switchboards that connect workstations cables to other devices. The use of patch panels enables the physical cabling of the network to be quickly rearranged as equipment is added or replaced. These patch panels use RJ-45 jacks for quick connection on the front, but require the cables to be punched down on the reverse side of the RJ-45 jack.

Patch panels are no longer confined to enterprise network installations. They can be found in many small businesses and even homes where they provide a central connection point for data, telephone and even audio systems.

The RJ-45 jack has eight conductors, and is wired according to either T568A or T568B. At the patch panel a device known as a punchdown tool is required to push the wires into the connector. The wires should be matched up to the appropriate insulation displacement connector (IDC) by color before punching them down. The punchdown tool also cuts off any excess wire.

A punchdown tool is not required to terminate most wall jacks. To terminate these connectors the cables are untwisted and placed into the appropriate IDC. Placing the cap on the jack pushes the cables into the IDC and cuts through the insulation on the wires. Most of these connectors then require the installer to manually trim away excess cable.

In all cases, untwisting more cable than is necessary will increase the amount of crosstalk and degrade overall network performance.

Cable Testing

When a new or repaired cable run is terminated, it is important to verify that the cable operates correctly and meets connectivity standards. This can be done through a series of tests.

The first test is a visual inspection, which verifies that all wires are connected according to T568A or B.

In addition to visual examination, check the cable electrically in order to determine problems or flaws in a network cabling installation. The following are tools that can be used for cable diagnostics:

- Cable testers
- Cable certifiers
- Multimeters

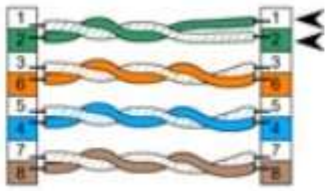
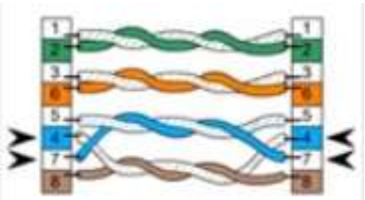
The cable tester is used to perform initial diagnostics. The first test usually is called a continuity test and it verifies that there is end-to-end connectivity. It can also detect common cabling faults such as opens and shorts.

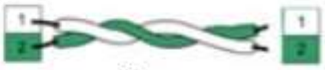
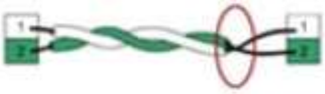
An open circuit occurs when the wire is not properly pushed into the connector and there is no electrical contact. An open can also occur if there is a break in the wire.

A short occurs when the copper conductors touch each other. As the electric pulse travels down the wire, it will cross onto the touching wire. This creates an unintended path in the flow of the signal to its destination.

A cable tester can also create wire maps that will verify that the cable is terminated correctly. A wire map shows which wire pairs connect to which pins on the plugs and sockets. The wire map test verifies that all eight wires are connected to the correct pins and indicates if cabling faults are present such as split pairs or reversals.

If any of these faults are detected, the easiest way to correct them is to reterminate the cable.

 Reversed Pair	The reversed-pair fault occurs when a wire pair is correctly installed on one connector, but reversed on the other connector. For example if the white/green wire is terminated on pin 1 and the green wire is terminated on pin 2 at one end of a cable, but reversed at the other end, then the cable has a reversed-pair fault.
 Split Pair	A split-pair fault occurs when one wire from one pair is switched with one wire from a different pair at both ends. Look carefully at the pin numbers in the graphic to detect the wiring fault. A split pair creates two transmit or receive pairs each with two wires that are not twisted together. This mixing hampers the cross-cancellation process and makes the cable more susceptible to crosstalk and interference.

 Open	An error in wiring that is caused by a break in the continuity of a circuit.
 Short	A short occurs when the copper portions of two wires touch each other.

Specialized cable testers provide additional information, such as the level of attenuation and crosstalk.

Attenuation
Attenuation, also commonly referred to as insertion loss, is a general term that refers to the reduction in the strength of a signal. Attenuation is a natural consequence of signal transmission over any medium. Attenuation limits the length of network cabling over which a message can be sent. A cable tester measures attenuation by injecting a signal in one end and then measuring its strength at the other end.

Crosstalk
Crosstalk is the leakage of signals between pairs. If this is measured near the transmitting end it is termed near-end crosstalk (NEXT). If measured at the receiving end of the cable it is termed far-end crosstalk (FEXT). Both forms of crosstalk degrade network performance and are often caused by untwisting too much cable when terminating. If high crosstalk values are detected, the best thing to do is check the cable terminations and re-terminate as necessary.

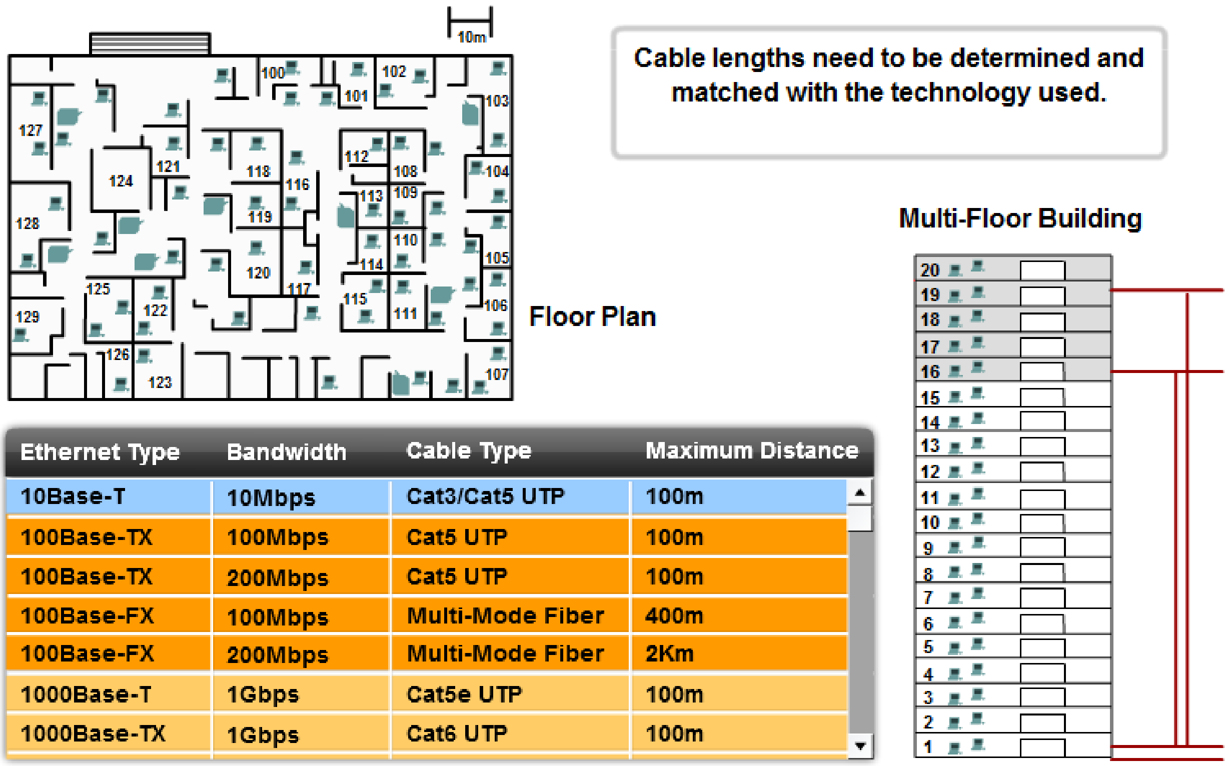
Cable Length and Cost
The total length of cable required to connect a device includes all cables from the end devices in the work area to the intermediary device in the telecommunication room (usually a switch). This includes cable from the devices to the wall plug, the cable through the building from wall plug to the cross-connecting point, or patch panel, and cable from patch panel to the switch. If the switch is located in a telecommunication rooms on different floors in a building or in different buildings, the cable between these points must be included in the total length.

Attenuation is reduction of the strength of a signal as it moves down a media. The longer the media, the more attenuation will affect the signal. At some point, the signal will not be detectable. Cabling distance is a significant factor in data signal performance. Signal attenuation and exposure to possible interference increase with cable length.

For example, when using UTP cabling for Ethernet, the horizontal (or fixed) cabling length needs to stay within the recommended maximum distance of 90 meters to avoid attenuation of the signal. Fiber-optic cables may provide a greater cabling distance-up to 500 meters to a few kilometers depending on the technology. However, fiber-optic cable can also suffer from attenuation when these limits are reached.

The cost associated with LAN cabling can vary from media type to media type, and the staff might not realize the impact on the budget. In a perfect setting, the budget would allow for fiber-optic cabling to every device in the LAN. Although fiber provides greater bandwidth than UTP, the material and installation costs are significantly higher. In practice, this level of performance is not usually required and is not a reasonable expectation in most environments. Network designers must match the performance needs of the users with the cost of the equipment and cabling to achieve the best cost/performance ratio.

Cable Length and Cost



Cable lengths need to be determined and matched with the technology used.

Ethernet Type	Bandwidth	Cable Type	Maximum Distance
10Base-T	10Mbps	Cat3/Cat5 UTP	100m
100Base-TX	100Mbps	Cat5 UTP	100m
100Base-TX	200Mbps	Cat5 UTP	100m
100Base-FX	100Mbps	Multi-Mode Fiber	400m
100Base-FX	200Mbps	Multi-Mode Fiber	2Km
1000Base-T	1Gbps	Cat5e UTP	100m
1000Base-TX	1Gbps	Cat6 UTP	100m

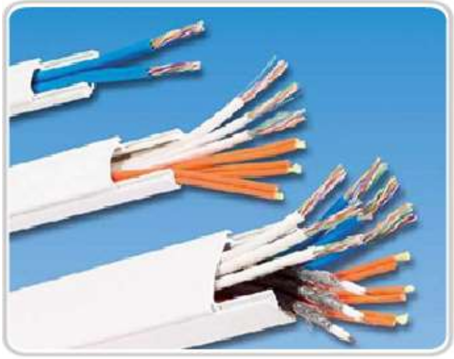
Bandwidth

The devices in a network have different bandwidth requirements. When selecting the media for individual connections, carefully consider the bandwidth requirements.

For example, a server generally has a need for more bandwidth than a computer dedicated to a single user. For a server connection, consider media that will provide high bandwidth, and can grow to meet increased bandwidth requirements and newer technologies. A fiber cable may be a logical choice for a server connection.

Currently, the technology used in fiber-optic media offers the greatest bandwidth available among the choices for LAN media. Given the seemingly unlimited bandwidth available in fiber cables, much greater speeds for LANs are expected. Wireless is also supporting huge increases in bandwidth, but it has limitations in distance and power consumption.

Ease of Installation


UTP Cable Raceway

Fiber Cable Raceway

The ease of cable installation varies according to cable types and building architecture. Access to floor or roof spaces, and the physical size and properties of the cable influence how easily a cable can be installed in various buildings. Cables in buildings are typically installed in raceways.

As shown in the figure, a raceway is an enclosure or tube that encloses and protects the cable. A raceway also keeps cabling neat and easy to thread.

UTP cable is relatively lightweight and flexible and has a small diameter, which allows it to fit into small spaces. The connectors, RJ-45 plugs, are relatively easy to install and are a standard for all Ethernet devices.

Many fiber-optic cables contain a thin glass fiber. This creates issues for the bend radius of the cable. Crimps or sharp bends can break the fiber. The termination of the cable connectors (ST, SC, MT-RJ) are significantly more difficult to install and require special equipment.

Wireless networks require cabling, at some point, to connect devices, such as access points, to the wired LAN. Because there are fewer cables required in a wireless network, wireless is often easier to install than UTP or fiber cable. However, a wireless LAN requires more careful planning and testing. Also, there are many external factors, such as other radio frequency devices and building construction that can effect its operation.

Electromagnetic Interference/Radio Frequency Interference

Electromagnetic Interference (EMI) and Radio Frequency Interference (RFI) must be taken into consideration when choosing a media type for a LAN. EMI/RFI in an industrial environment can significantly impact data communications if the wrong cable is used.

Interference can be produced by electrical machines, lighting, and other communications devices, including computers and radio equipment.

As an example, consider an installation where devices in two separate buildings are interconnected. The media used to interconnect these building will be exposed the possibility of lightening strikes. Additionally, there maybe a great distance between these two buildings. For this installation, fiber cable is the best choice.

Wireless is the medium most susceptible to RFI. Before using wireless technology, potential sources of interference must be identified and, if possible, minimized.

Cabling Best Practice

The following steps, called best practices, ensure that cable termination is successful.

1. It is important that the type of cables and components used on a network adhere to the standards required for that network. Modern converged networks carry voice, video and data traffic on the same wires; therefore the cables used on converged networks must be able to support all these applications.

2. Cable standards specify maximum lengths for different types of cables. Always adhere to the length restrictions for the type of cable being installed.

3. UTP, like all copper cable, is susceptible to EMI. It is important to install cable away from sources of interference such as high-voltage cables and fluorescent lighting. Televisions, computer monitors and microwaves are other possible sources of interference. In some environments it may be necessary to install data cables in conduit to protect them from EMI and RFI.

4. Improper termination and the use of low quality cables and connectors can degrade the signal carrying capacity of the cable. Always follow the rules for cable termination and test to verify that the termination has been done properly.

5. Test all cable installations to ensure proper connectivity and operation.

6. Label all cables as they are installed, and record the location of cables in network documentation.

Structured cabling is a method for creating an organized cabling system that can be easily understood by installers, network administrators, and any other technicians who deal with cables. One component of structured cabling is cable management.

Cable management serves multiple purposes. First, it presents a neat and organized system which aids in the isolation of cabling problems. Second, by following cable management best practices, the cables are protected from physical damage which greatly reduces the number of problems experienced.

Cables should be considered a long term investment. What may be sufficient now may not be in the near future. Always plan for the future by complying with all current standards. Remember that standards help to ensure that the cables will be able to deliver acceptable performance as the technology evolves.

It is important to observe cabling best practices in all environments. Strict adherence to these practices, in home and business environments, helps reduce the number of potential problems. It will save a great amount of time, money and frustration.

Adapted and Compiled from:

CCNA IT Essential, “PC Hardware and Software” version 4.0, Cisco Networking Academy
CCNA Discovery 1, “Networking for Home and Small Businesses”, Cisco Networking Academy
CCNA Discovery 2, “Working at a Small-to-Medium Business of ISP”, Cisco Networking Academy
CCNA Exploration 1, “Network Fundamentals”, Cisco Networking Academy
Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide, Cisco Press