BASIC TERMINOLOGIES

Computer Network

Computer network is a connection of autonomous computers for the purpose of resource sharing and communication between them.

Data communications

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable

Data Flow

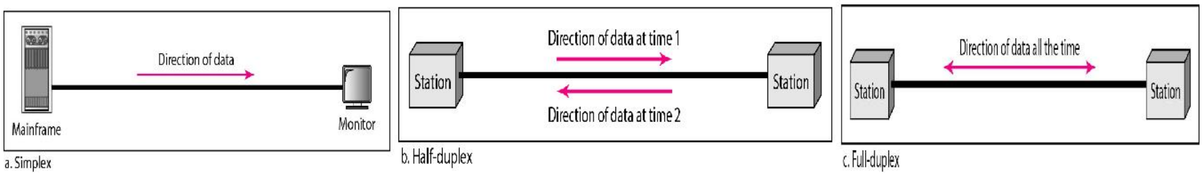
The three types of data flow are simplex, half-duplex and full-duplex.

- In **simplex mode**, the communication is unidirectional (Eg: keyboard, monitor). In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive

- In **half-duplex mode**, each station can both transmit and receive, but not at the same time (Eg. walkie-talkie). When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communicationin both directions at the same time; the entire capacity of the channel can be utilized foreach direction.

- In **full-duplex** (also called duplex), both stations can transmit and receive simultaneously (Eg. telephone network). The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction

-

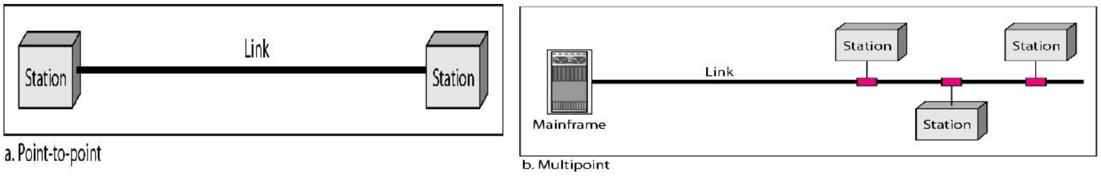

Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex b. Half-duplex c. Full-duplex

Type of Connection

The two types of connection are point-to-point and multi-point.

- A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Mostpoint-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible
- A multipoint connection is one in which more than two devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

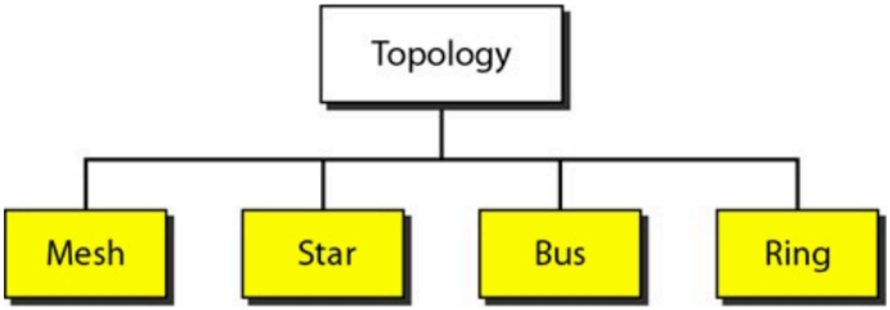


a. Point-to-point

b. Multipoint

Topology

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.



The four basic topologies are *mesh*, *star*, *bus*, and *ring*.

MESH TOPOLOGY - In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two
Devices.

A mesh topology is robust and secure. Installation is difficult and expensive. In a mesh topology, we need n (n – 1) / 2 duplex-mode links.

Advantages

- First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

- Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

- Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.

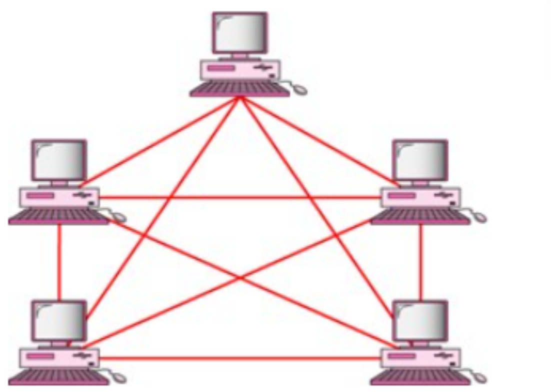
- Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems

Disadvantages

- First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive

Example

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.



n(n-1)/2 physical duplex links

Star Topology

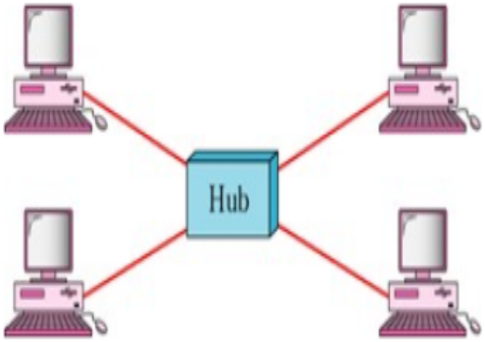
In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device

Advantages

- Less Expensive - In a star, each device needs only one link and one I/O port to connect it to any number of others.
- Easy to install and reconfigure
- Robustness. If one link fails, only that link is affected.
- Easy fault identification and fault isolation

Disadvantages

- Single point of failure. If the hub goes down, the whole system is dead



The star topology is used in local-area networks LANs

***Bus* Topology**

A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

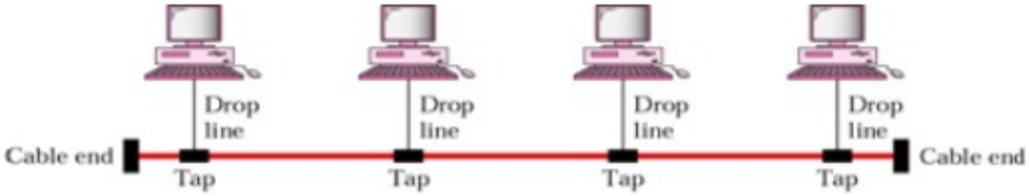
It is multi-point and signal gets weak as it travels through the long cable that acts as backbone. A fault in the bus stops the entire transmission

Advantage

- Ease of Installation
- Uses less cabling than mesh or star topologies.

Disadvantages

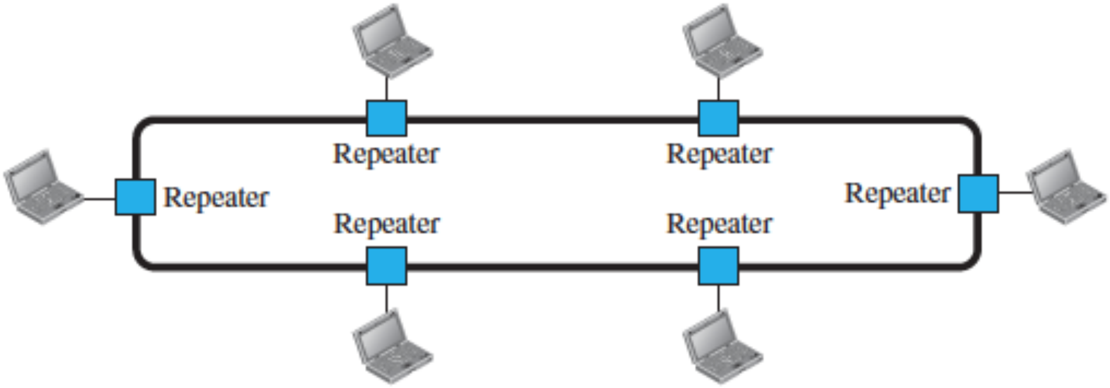
- Difficult reconnection and fault isolation
- A fault or break in the bus cable stops all transmission



Bus topology was the one of the first topologies used in the design of early local area networks. Traditional Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



1

Advantages

- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors.
- To add or delete a device requires changing only two connections
- In addition, fault isolation is simplified. Generally, in a ring a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm

Disadvantages

In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Example

Ring topology was prevalent when IBM introduced its local-area network, Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

NETWORK TYPES

Networks can be classified into LAN, WAN, MAN:

LAN – Local Area Network

- A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone’s home office, or it can extend throughout a company and include audio and video devices.

- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.

- In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet.

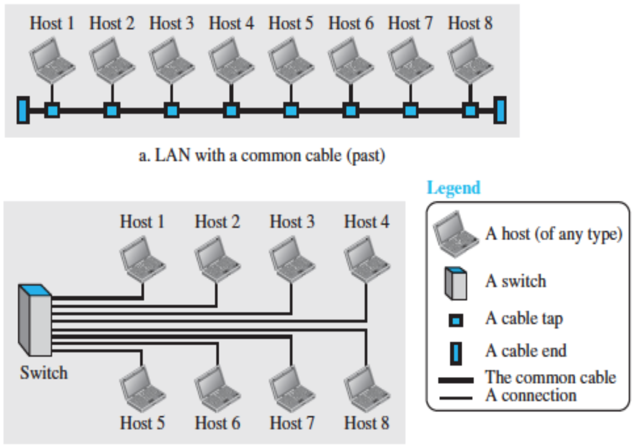
- Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts

- The LAN size is limited to a few kilometers. A LAN will use only one type of transmission medium.

- LANs are distinguished from other types of networks by their transmission media and topology. The most common LAN topologies are bus, ring, and star.

- Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps or even Gigabits.

- Wireless LANs are the newest evolution in LAN technology



a. LAN with a common cable (past)

b. LAN with a switch (today)

WAN – Wide Area Network

A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.

A wide area network (WAN) is also an interconnection of devices capable of communication. However, there are some differences between a LAN and a WAN.

- A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world.

- A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems.

- A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

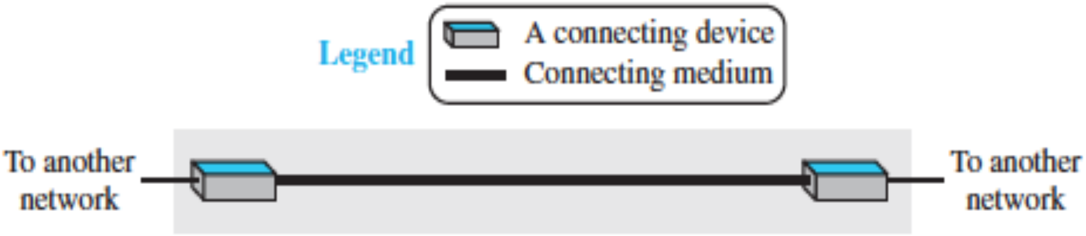
Types of WAN

- Point-to-point WANs and
- Switched WANs

Point-to-Point WAN

A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).

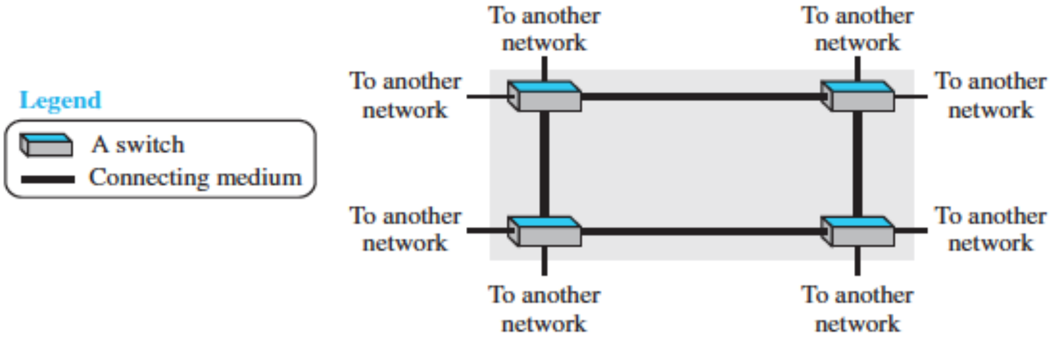
The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider.



Switched WAN

A switched WAN is a network with more than two ends. A switched WAN, is used in the backbone of global communication today.

We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches.



Metropolitan Area Networks

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or a city.
- It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.

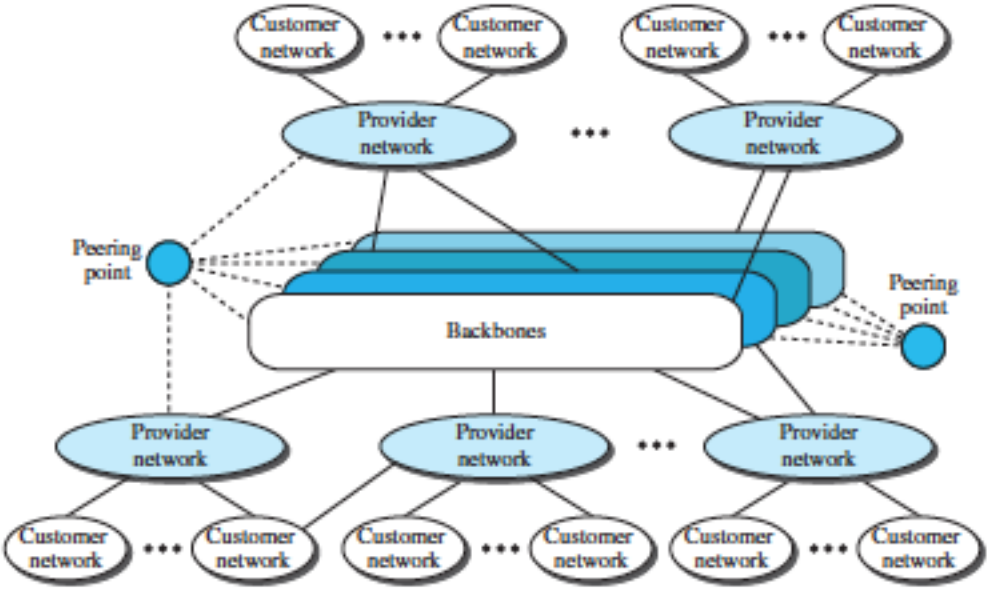
- A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.

Internetwork

When two or more networks are connected, they make an internetwork, or internet

The Internet

The most notable internet is called the Internet (uppercase I), and is composed of thousands of interconnected networks.



The figure shows the Internet as several backbones, provider networks, and customer networks.

At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT.

The backbone networks are connected through some complex switching systems, called peering points. At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.

The provider networks are connected to backbones and sometimes to other provider networks. The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet.

They pay fees to provider networks for receiving services. Backbones and provider networks are also called Internet Service Providers (ISPs). The backbones are often referred to as international ISPs; the provider networksare often referred to as national or regional ISPs.

INTERNET HISTORY

Early History

There were some communication networks, such as telegraph and telephone networks, before 1960. These networks were suitable for constant-rate communication at that time.

Birth of Packet-Switched Networks

The theory of packet switching for bursty traffic was first presented by Leonard Kleinrock in 1961 at MIT. At the same time, two other researchers, Paul Baran at Rand Institute and Donald Davies at National Physical Laboratory in England, published some papers about packet-switched networks.

ARPANET

In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency (ARPA)** in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for the Advanced Research Projects Agency Network (ARPANET), a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.

Birth of the Internet

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Project. They wanted to link dissimilar networks so that a host on one network could communicate with a host on another.

TCP/IP

Cerf and Kahn’s landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible.

Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection.

The new combination became known as TCP/IP. In 1981, under a Defence Department contract, UC Berkeley modified the UNIX operating system to include TCP/IP.

In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET. Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

MILNET

In 1983, ARPANET split into two networks: Military Network (MILNET) for military users and ARPANET for nonmilitary users.

CSNET

Another milestone in Internet history was the creation of CSNET in 1981. Computer Science Network (CSNET) was a network sponsored by the National Science Foundation (NSF).

NSFNET

With the success of CSNET, the NSF in 1986 sponsored the National Science Foundation Network (NSFNET), a backbone that connected five supercomputer centers located throughout the United States.

ANSNET

In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and Verizon, filled the void by forming a nonprofit organization called Advanced Network & Services (ANS) to build a new, high-speed Internet backbone called Advanced Network Services Network (ANSNET).

Internet Today

Today, we witness a rapid growth both in the infrastructure and new applications. The Internet today is a set of pier networks that provide services to the whole world. What has made the Internet so popular is the invention of new applications.

World Wide Web

The 1990s saw the explosion of Internet applications due to the emergence of the World Wide Web (WWW). The Web was invented at CERN by Tim Berners-Lee. This invention has added the commercial applications to the Internet.

Multimedia

Recent developments in the multimedia applications such as voice over IP (telephony), video over IP (Skype), view sharing (YouTube), and television over IP (PPLive) has increased the number of users and the amount of time each user spends on the network.

Internet Standards

An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft.

PROTOCOL LAYERING

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.

When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering.

Layering provides two features. First, it decomposes the problem of building a network into more manageable components. Second, it provides a more modular design. To add a new service, then it is only needed to modify the functionality at one layer, reusing the functions at all the other layers.

ISO

International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards.

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the 1980s.

OSI “ Open Systems Interconnection" Reference Model

OSI model was first introduced in 1984 by the International Organization for Standardization (ISO). It Outlines WHAT needs to be done to send data from one computer to another. Not HOW it should be done.

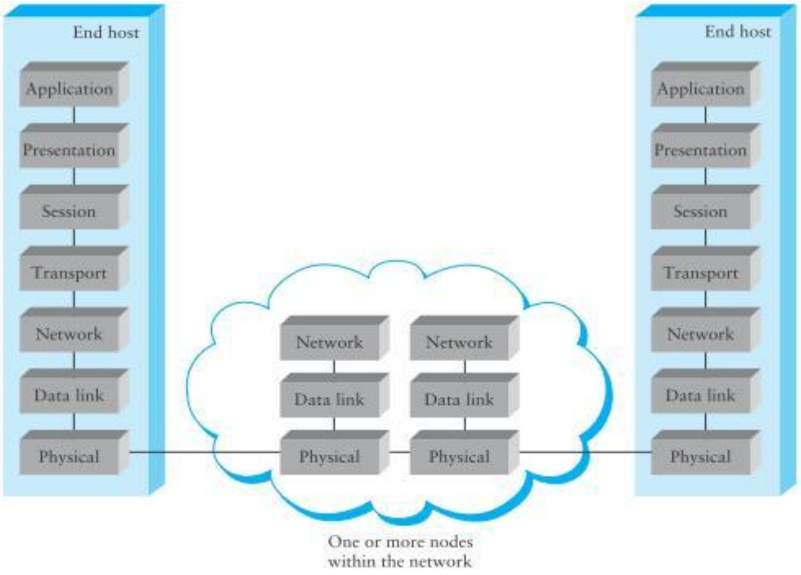
Protocols stacks handle how data is prepared for transmittal (to be transmitted) In the OSI model, The specification needed are contained in 7 different layers that interact with each other.

Commonly referred to as the OSI reference model. The OSI model is a theoretical blueprint that helps us understand how data gets from one user’s computer to another.

It is also a model that helps develop standards so that all of our hardware and software talks nicely to each other. It aids standardization of networking technologies by providing an organized structure for hardware and software developers to follow, to insure there products are compatible with current and future technologies.

OSI ARCHITECTURE

The ISO defined a common way to connect computers, called the Open Systems Interconnection (OSI) architecture. It defines partitioning of network functionality into seven layers as shown.



Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. Other responsibilities include:

Physical characteristics of interfaces and medium—It defines the characteristics of the interface between devices and transmission medium and type of medium.

Representation of bits—To be transmitted, bits must be encoded into signals, electrical or optical. The physical layer defines the type of encoding.

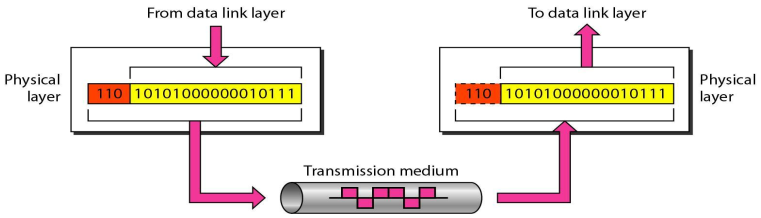
Data rate—It defines the transmission rate (number of bits sent per second).

Synchronization of bits—The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level.

Line configuration—The physical layer is concerned with the connection of devices to the media (point-to-point or multipoint configuration).

Physical topology—It defines how devices are connected (mesh, star, ring, bus or hybrid) to make a network.

Transmission mode—The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex



Data Link Layer

The data link layer transforms a raw transmission facility to a reliable link. It makes the data appear error-free to the upper layer (network layer). Other responsibilities include:

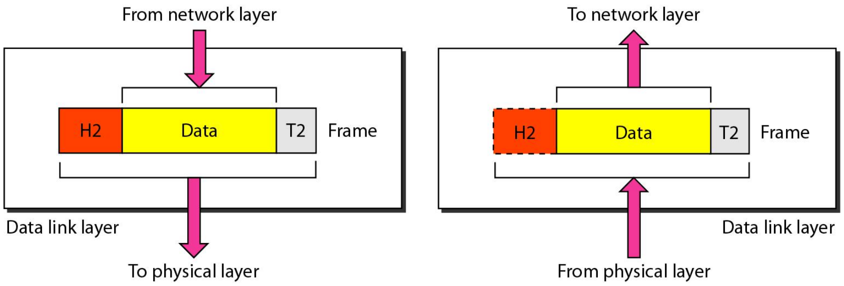
Framing—The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

Physical addressing—The data link layer adds a header to the frame to define the sender and/or receiver of the frame.

Flow control—If the receiving rate is less than the transmission rate, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Error control—The data link layer adds reliability to the physical layer by adding a trailer to detect and retransmit damaged/lost frames and to recognize duplicate frames.

Access control—When two or more devices are connected to the same link, data link layer protocols determines which device has control over the link at any given time.

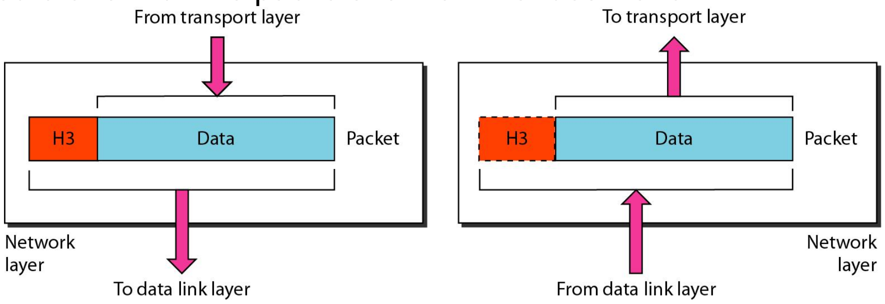


Network Layer

The network layer is responsible for the source-to-destination delivery of a packet. Other responsibilities of network layer include:

Logical addressing—The physical addressing given by the data link layer handles the addressing problem locally. If a packet passes the network boundary, then logical addressing system is required to help distinguish the source and destination systems.

Routing—When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called routers or *switches)* route or switch the packets to their final destination.



Transport Layer

The transport layer is responsible for *process-to-process* delivery of the entire message. A process is an application program running on a host. The network layer does not recognize any relationship between those packets and treats each one independently.

The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Other responsibilities include:

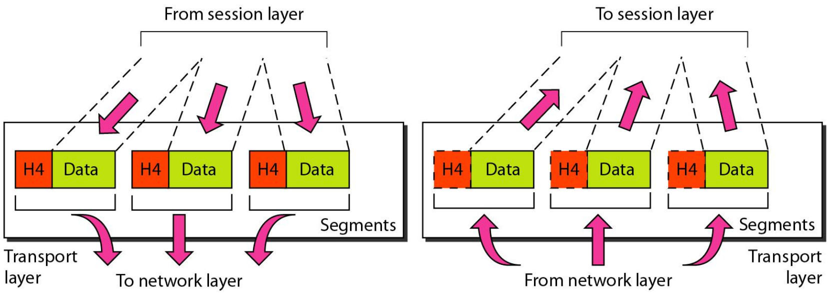
Service-point addressing—It includes a service-point address or *port* address so that a process from one computer communicates to a specific process on the other computer.

Segmentation and reassembly—A message is divided into transmittable segments, each containing a sequence number. These numbers enable the transport layer to reassemble the message correctly at the destination and to identify/replace packets that were lost.

Connection control—The transport layer can be either connectionless or connection-oriented. After all the data are transferred, the connection is terminated.

Flow control—The flow control at this layer is performed end to end.

Error control—The error control at this layer is performed process-to-process. Error correction is usually achieved through retransmission.

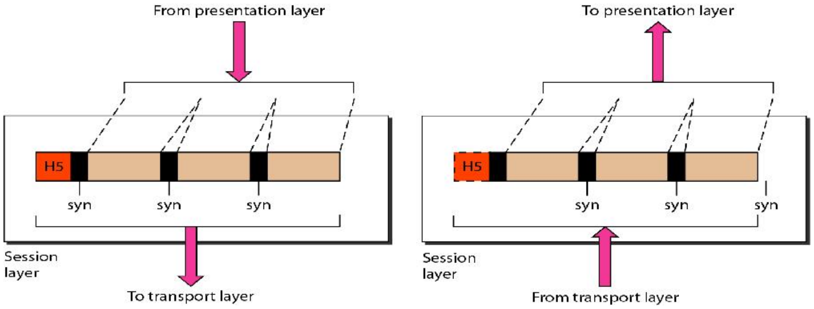


Session Layer

The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems. Other responsibilities include the following:

Dialog control—It allows two systems to enter into a dialog and communication between two processes to take place in either half-duplex / full-duplex mode.

Synchronization—The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, when checkpoints are inserted for every 100 pages and if a crash happens during transmission of page 523, then only pages 501 to 523 need to be resent.



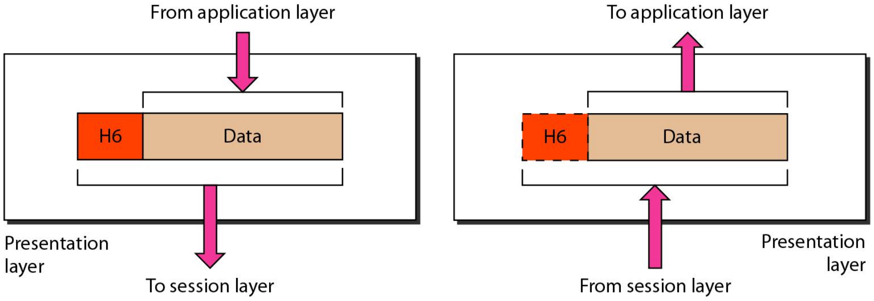
Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Specific responsibilities of the presentation layer include:

Translation—Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these encoding methods.

Encryption—To carry sensitive information, a system ensures privacy by encrypting the message before sending and decrypting at the receiver end.

Compression—Data compression reduces the number of bits contained in the information. It is particularly important in multimedia transmission.



Application Layer

The application layer enables the user, whether human or software, to access the network.

It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services. Specific services provided by the application layer include:

Network virtual terminal—A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.

File transfer, access, and management—This application allows a user to access/retrieve files in a remote host, and to manage or control files in a remote computer locally.

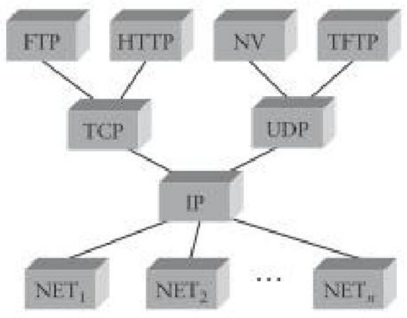
Mail services—This application provides the basis for e-mail forwarding and storage.

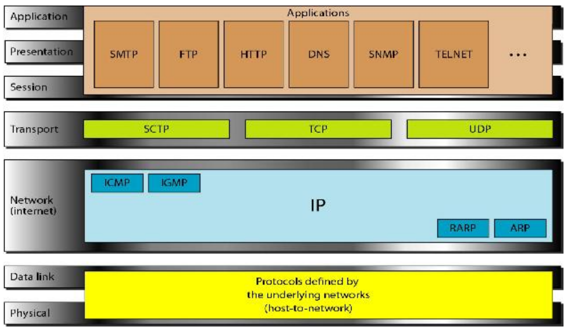
Directory services—This application provides distributed database sources and access for global information about various objects and services.

The following figure shows three application services X4OO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM).

INTERNET (TCP/IP) ARCHITECTURE

The Internet architecture is also known as TCP/IP architecture after its two main protocols. The Internet architecture evolved out of packet-switched network called the ARPANET.





At the lowest level **(physical & data link layers of OSI)** TCP/IP does not define any specific protocol. It supports all standard and proprietary protocols such as Ethernet, FDDI, etc. These protocols are implemented by a combination of hardware and software.

The network layer consists of a major protocol, the *Internetworking Protocol* (IP). It supports the interconnection of multiple networking technologies into a logical internetwork. It is an unreliable and connectionless protocol. IP transports data in packets called *datagrams,* each of which is transported separately. The other protocols are:

- Address Resolution Protocol (ARP) is used to determine the physical address when logical address is known and

- Reverse Address Resolution Protocol (RARP) is used to determine the logical address when physical address is known

- Internet Control Message Protocol (ICMP) to send any notification to the sender.

- Internet Group Message Protocol (IGMP) for simultaneous transmission of a message to a group of recipients

The transport layer is responsible for delivery of a message from one process to another process. The protocols:

- *Transmission Control Protocol* (TCP) for a reliable byte-stream channel (connection-oriented).

- *User Datagram Protocol (UDP)* for an unreliable datagram delivery channel (connectionless).

- *Stream Control Transmission Protocol* (SCTP) is a combination of TCP/UDP.

Running above the transport layer are a range of application protocols, such as FTP, TFTP (Trivial File Transport Protocol), Telnet (remote login), SMTP, etc., that enable the interoperation of popular applications. The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model

The striking features of Internet architecture are:

- The Internet architecture does not imply *strict layering*. The application is free to bypass the defined transport layers and to directly use IP or one of the underlying networks.

- IP serves as the focal point for the architecture i.e., it defines a common method for exchanging packets among a wide collection of networks.

PERFORMANCE

Network Performance metrics are measured as Bandwidth, Throughput, Delay or Latency.

Bandwidth
One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second.

Bandwidth in Hertz
Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds
The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

Throughput
The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different.

A link may have a bandwidth of B bps, but we can only send T bps through this link with T always less than B.

In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data.

For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Example Problem to Calculate Throughput
A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution
We can calculate the throughput as

Throughput = (12,000 x 10,000) / 60 = 2 Mbps

The throughput is almost one-fifth of the bandwidth in this case.

Latency (Delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = Distance / (Propagation Speed)

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal. For example, in a vacuum, light is propagated with a speed of 3×10^8 m/s. It is lower in air; it is much lower in cable.

Example

What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in cable.

Solution

We can calculate the propagation time as

Propagation time = (12,000 x 1000) / (2.4 x 10^8) = 50 ms

The example shows that a bit can go over the Atlantic Ocean in only 50 ms if there is a direct cable between the source and the destination.

Transmission Time

In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later. The transmission time of a message depends on the size of the message and the bandwidth of the channel.

Transmission time = (Message size) / Bandwidth.

What are the propagation time and the transmission time for a 2.5-KB (kilobyte) message (an email) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution

Propagation time = (12,000 3 1000) / (2.4 3 108) 5 50 ms

Transmission time = (2500 x 8) / 10^9 = 0.020 ms

Jitter

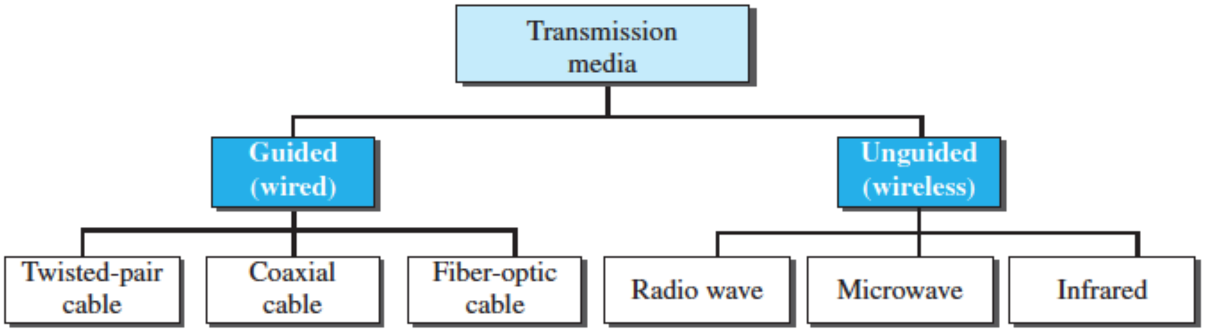
Another performance issue that is related to delay is jitter. We can roughly say that jitter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time-sensitive (audio and video data, for example). If the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

Transmission Medium

A transmission medium can be broadly defined as anything that can carry information from a source to a destination.

The transmission medium is usually free space, metallic cable, or fiber-optic cable. The information is usually a signal that is the result of a conversion of data from another form.

Transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space



GUIDED MEDIA

Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.

A signal traveling along any of these media is directed and contained by the physical limits of the medium.

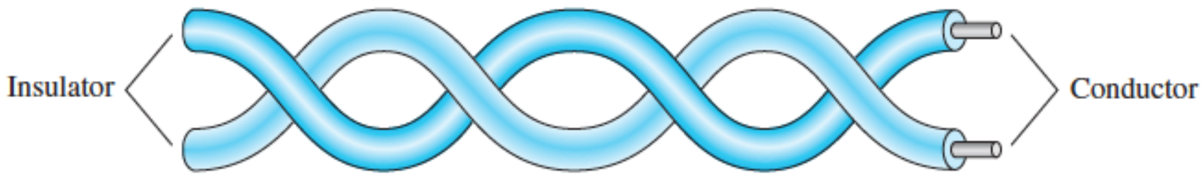
Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light

Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together.

One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

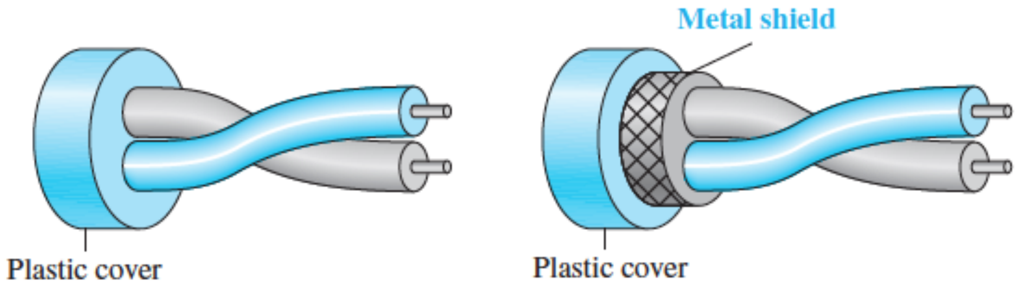
In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.



Types of Twisted Pair

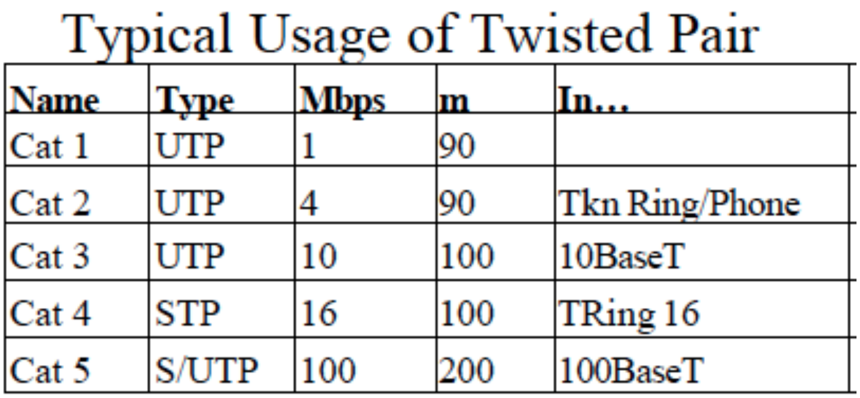
- Unshielded twisted-pair (UTP)
- Shielded twisted-pair (STP) (IBM)

STP cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.



a. UTP

b. STP



Typical Usage of Twisted Pair

Name	Type	Mbps	m	In…
Cat 1	UTP	1	90	
Cat 2	UTP	4	90	Tkn Ring/Phone
Cat 3	UTP	10	100	10BaseT
Cat 4	STP	16	100	TRing 16
Cat 5	S/UTP	100	200	100BaseT

Pros and Cons of Twisted Pair Cable

- Cheap
- Easy to work with

– Can use as digital or analog

- Limited bandwidth/data rate

– Generally 1Mhz and 100Mbps

- Short range

– 2km for digital, 5km for analog

- Direct relationship between data rate and range

– Gigabit Ethernet

- 1000Mbps over 4 Cat5 UTP up to 100 meters

– IEEE 802.3ab standard in 1999

- 1000Mbps over 1 Cat5 UTP up to 24 meters

Unshielded Twisted Pair (UTP)

– Ordinary telephone wire
– Cheapest
– Easiest to install
– Suffers from external EM interference

Shielded Twisted Pair (STP)

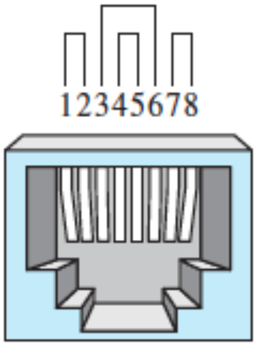
– Metal braid or sheathing that reduces interference
– More expensive

- Harder to handle (thick, heavy)

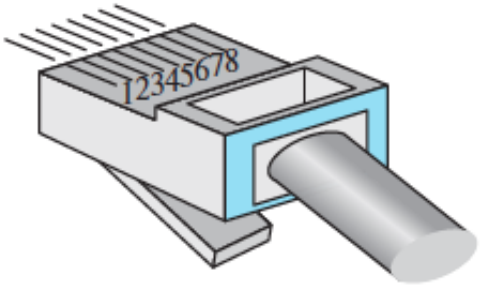
Connectors

The most common UTP connector is RJ45 (RJ stands for registered jack)

The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.



RJ-45 Female



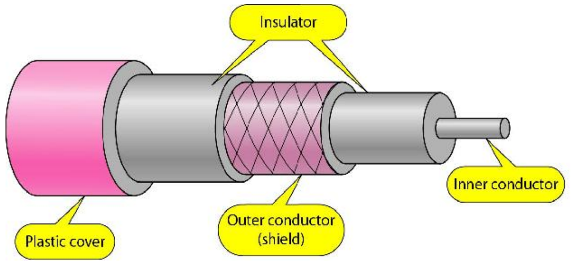
RJ-45 Male

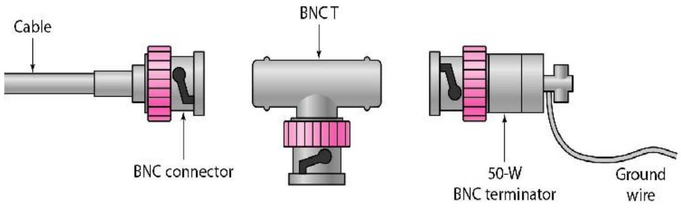
Coaxial cable

- Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently.

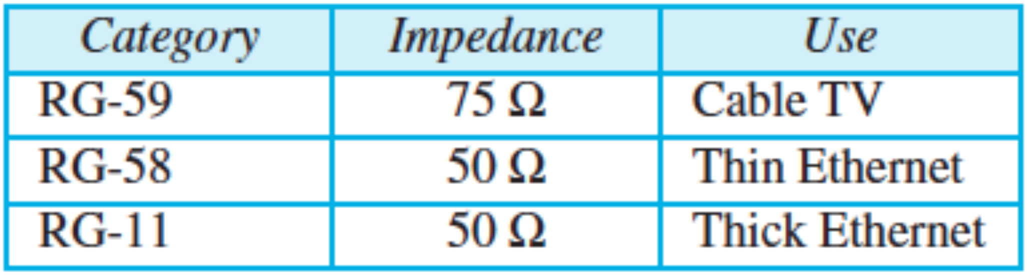
- Instead of having two wires, coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two.

- The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit.





Coaxial Cable Standards Coaxial cables are categorized by their Radio Government (RG) ratings.



Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial Cable Connectors

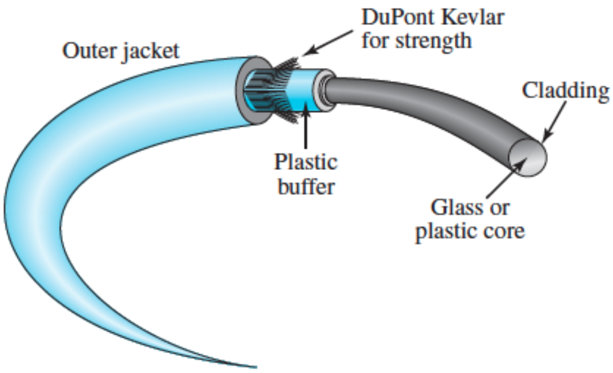
The most common type of connector used today is the Bayonet Neill-Concelman (BNC) connector.

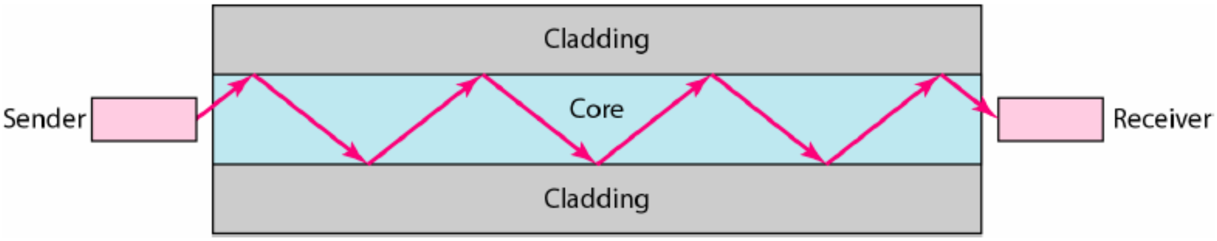
Applications

- Cable TV networks. Cable TV uses RG-59 coaxial cable.
- Ethernet LANs
- The 10Base-2, or Thin Ethernet, uses RG-58 coaxial cable with BNC connectors to transmit data at 10 Mbps with a range of 185 m.
- The 10Base5, or Thick Ethernet, uses RG-11 (thick coaxial cable) to transmit 10 Mbps with a range of 5000 m.

Fiber-Optic Cable

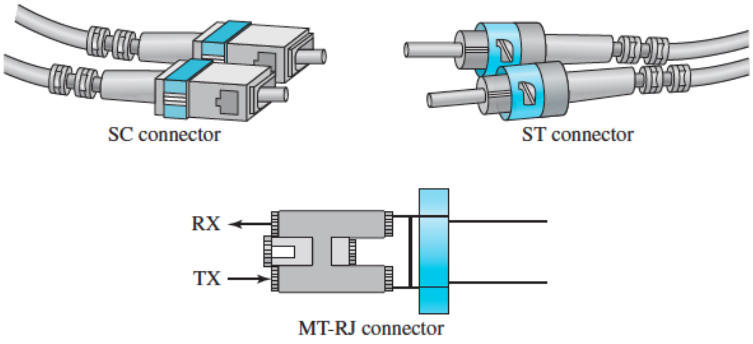
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- It transmits light rather than electronic signals It is the standard for connecting networks between buildings, due to its immunity to the effects of moisture and light
- Fiber optic cable has the ability to transmit signals over much longer distances than coaxial or twisted pair
- It can also carry information at vastly greater speeds
- Fiber optic cable is more difficult to install than other cabling





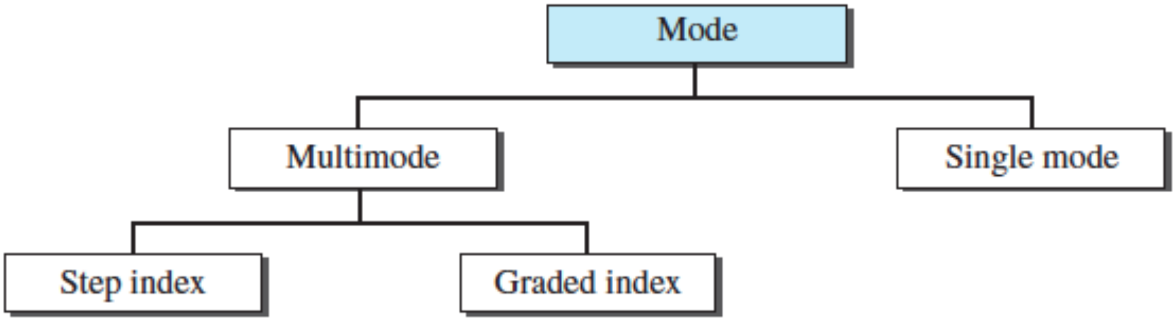
Fiber-Optic Cable Connectors

- There are three types of connectors for fiber-optic cables,
- The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system.
- The straight-tip (ST) connector is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.
- MT-RJ is a connector that is the same size as RJ45.



Propagation Modes

- Current technology supports two modes (multimode and single mode) for propagating light along optical channels.
- Multimode can be implemented in two forms: step-index or graded-index



Multimode

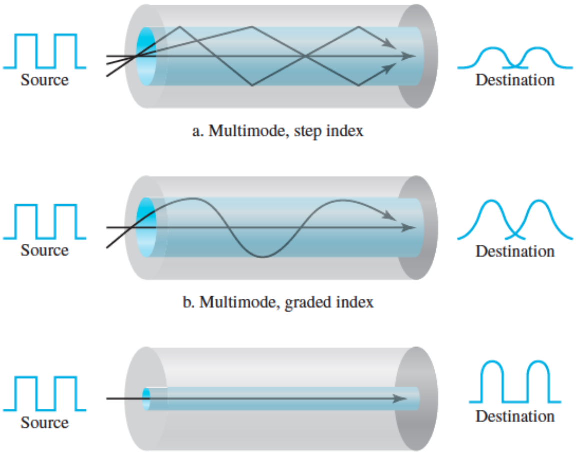
Multimode is so named because multiple beams from a light source move through the core in different paths.

In multimode step-index fiber, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding

A second type of fiber, called multimode graded-index fiber, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction. As we saw above, the index of refraction is related to density. A gradedindex fiber, therefore, is one with varying densities.

Single-Mode

Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density

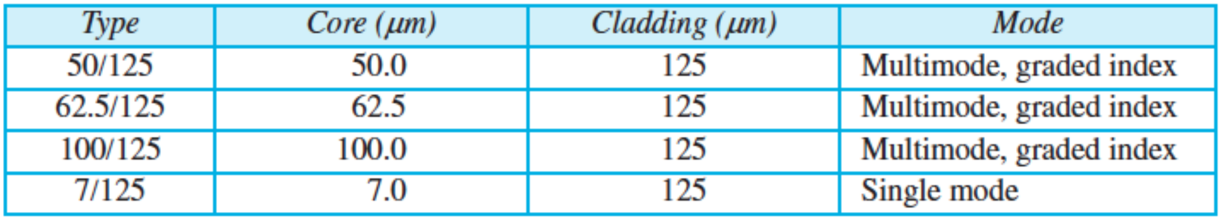


a. Multimode, step index

b. Multimode, graded index

c. Single mode

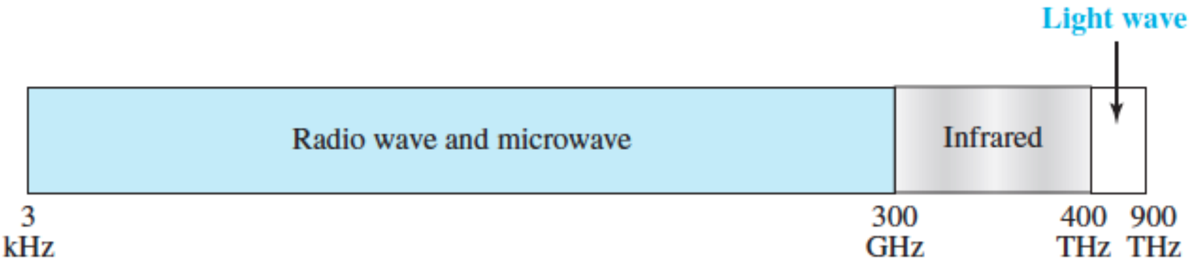
Fiber Optic Types



Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

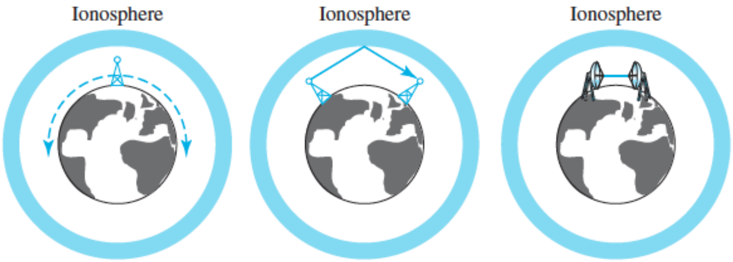
UNGUIDED MEDIA: WIRELESS

- Unguided medium transport electromagnetic waves without using a physical conductor.
- This type of communication is often referred to as wireless communication .
- Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
- Electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.
- Unguided signals can travel from the source to the destination in several ways: ground propagation, sky propagation, and line-of-sight propagation.



Propagation Mode

- In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth.
- In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth
- In line-of-sight propagation, very high-frequency signals are transmitted in straight lines directly from antenna to antenna.

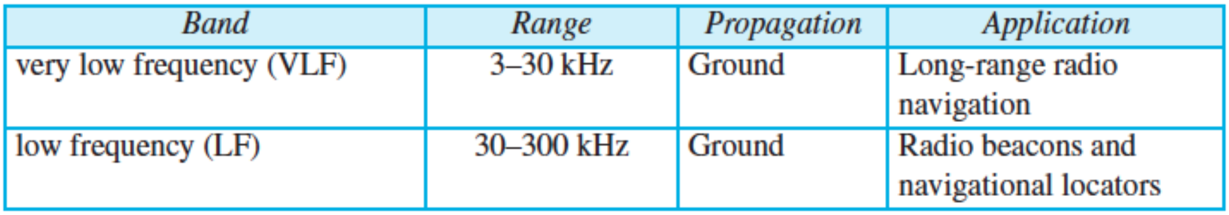


Ground propagation (below 2 MHz)

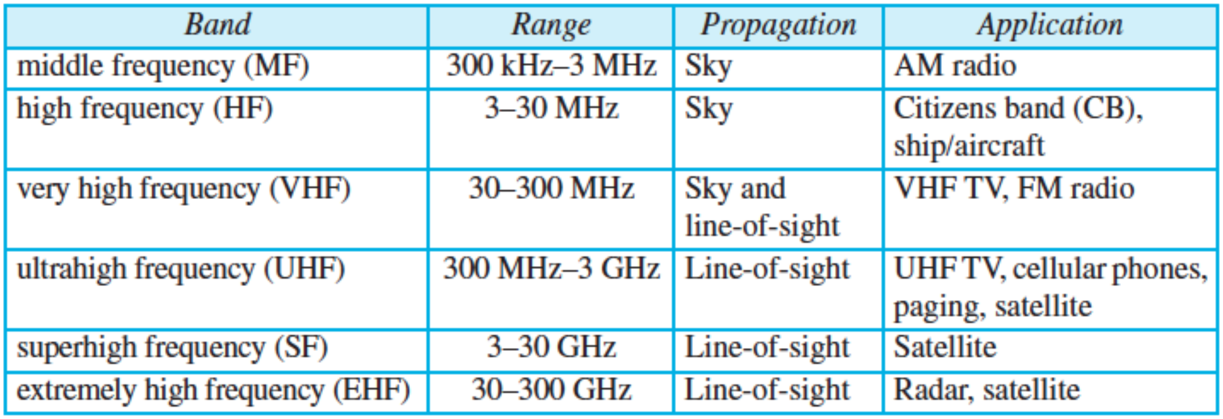
Sky propagation (2–30 MHz)

Line-of-sight propagation (above 30 MHz)

Bans



Band	*Range*	*Propagation*	*Application*
very low frequency (VLF)	3–30 kHz	Ground	Long-range radio navigation
low frequency (LF)	30–300 kHz	Ground	Radio beacons and navigational locators



Band	*Range*	*Propagation*	*Application*
middle frequency (MF)	300 kHz–3 MHz	Sky	AM radio
high frequency (HF)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft
very high frequency (VHF)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
ultrahigh frequency (UHF)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
superhigh frequency (SF)	3–30 GHz	Line-of-sight	Satellite
extremely high frequency (EHF)	30–300 GHz	Line-of-sight	Radar, satellite

Types of Wireless Medium

- Radio waves,
- Microwaves, and
- Infrared waves.

Radio Wave

• Although there is no clear-cut demarcation between radio waves and microwaves, electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves;

• Waves ranging in frequencies between 1 and 300 GHz are called microwaves.

• Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions.

• This means that the sending and receiving antennas do not have to be aligned.

• Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

Applications

- The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers.
- AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Disadvantage

- Interference
- The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.

Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwaves, they can be narrowly focused.
- This means that the sending and receiving antennas need to be aligned.
- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall.
- Microwaves are used for unicast communication such as cellular telephones, satellite networks, and wireless LANs.

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn.

Infrared

• Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.

• Infrared waves, having high frequencies, cannot penetrate walls.

•This advantageous characteristic prevents interference between one system and another; a shortrange communication system in one room cannot be affected by another system in the next room.

• However, infrared signals useless for long-range communication.

• In addition, we cannot use infrared waves outside a building because the sun’s rays contain infrared waves that can interfere with the communication.

Application

The Infrared Data Association (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers.