COMPUTER NETWORK

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resources-sharing among a wide range of users.

Before we discuss the more technical aspects of computer networks let us first focus on the merits and demerits derived from computer networks.

Need: If your business has more than one computer, chances are you could benefit from networking them. A local area network (LAN) connects your company's computers, allowing them to share and exchange a variety of information. While one computer can be useful on its own, several networked computers can be much more useful. Resource sharing and communication are two principal reasons of building and using computer networks.

Here are some of the ways a computer network can help your business:

a. **File sharing**
   Have you ever needed to access a file stored on another computer? A network makes it easy for everyone to access the same file and prevents people from accidentally creating different versions.
b. **Printer sharing**
   If you use a computer, chances are you also use a printer. With a network, several computers can share the same printer. Although you might need a more expensive printer to handle the added workload, it's still cheaper to use a network printer than to connect a separate printer to every computer in your office.
c. **Communication and collaboration**
   It's hard for people to work together if no one knows what anyone else is doing. A network allows employees to share files, view other people's work, and exchange ideas more efficiently. In a larger office, you can use e-mail and instant messaging tools to communicate quickly and to store messages for future reference.
d. **Organization**
   A variety of scheduling software is available that makes it possible to arrange meetings without constantly checking everyone's schedules. This software usually includes other helpful features, such as shared address books and to-do lists.
e. **Remote access**
   Having your own network allows greater mobility while maintaining the same level of productivity. With remote access in place, users are able to access the same files, data, and messages even when they're not in the office. This access can even be given to mobile handheld devices.
f. **Data protection**
   You should know by now that it's vital to back up your computer data regularly. A network makes it easier to back up all of your company's data on an offsite server, a set of tapes, CDs, or other backup systems. Of course, another aspect of data protection is data security.

MERITS OF COMPUTER NETWORKS

i. Enable multiple users to share a single hardware device like a printer or scanner.
ii. Make files easily shared among different users.
iii. Allow for the sharing of software or operating programs on remote systems.
iv. Enable network users communicate via email, instant messaging and video conferencing.
v. Make information easier to access and maintain among network users.
vi. Backup data stored on the file server.

vii. Security is good as users cannot see other user's file unlike on stand-alone machines.

DEMERITS OF COMPUTER NETWORK

a. Purchasing the network cables and file servers can be expensive.
b. Managing a large network is complicated and a trained network manager is needed.
c. If the file server breaks down, the files on the file server become inaccessible.
d. Virus can spread to other computers through a computer network.
e. There is a danger of hacking particularly with wide area networks.

DIFFERENT KINDS OF NETWORKS

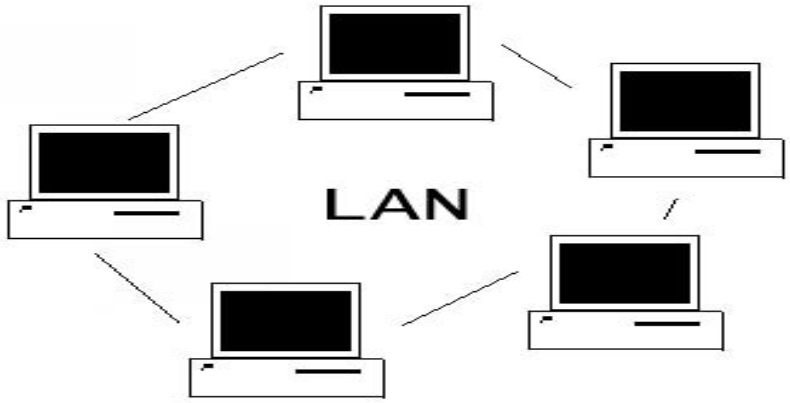
Networks can be classified in different ways based on geographical coverage, architecture, topology, communication medium used and in many other ways.

Classifying network based on geographical coverage, network can be broadly classified into three:

a) Local Area Network (LAN)
b) Metropolitan Area Network (MAN)
c) Wide Area Network (WAN)

a) LOCAL AREA NETWORK (LAN)

A Local Area Network or LAN refers to a computer network that is physically situated in a limited area such as one or more rooms or floors, or a building. The nodes (computer connected to the LAN) of the LAN are typically linked together by wired links. This is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. One computer is designated as the file server and stores the software that controls the network.



Local Area Network

A Local Area Network as shown in the figure above is a network in its simplest structure. Data transfer speeds over a Local Area Network can attain up to 10 Mbps (such as for an Ethernet network) and 1 Gbps (as with FDDI or Gigabit Ethernet). A Local Area Network can have as many as 100, or even 1000, users.

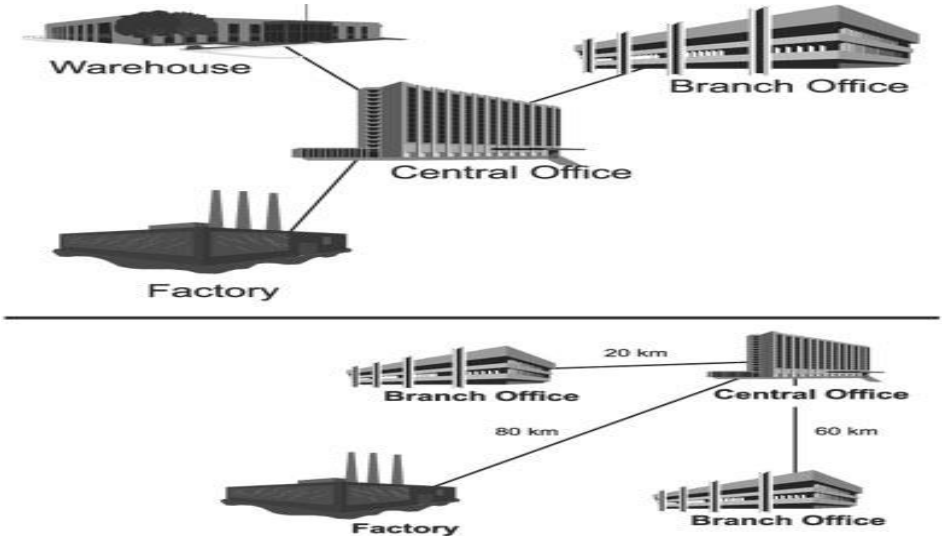
By expanding the definition of a LAN to the services that it provides, two different operating modes can be defined:

- The first is in a **"peer-to-peer"** network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- The second one is in a **"client/server"** environment, in which a central computer provides network services to users.

b) METROPOLITAN AREA NETWORK (MAN)

A Metropolitan Area Network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large Local Area Network (LAN) but smaller than the area covered by a Wide Area Network (WAN).

A Metropolitan Area Network (MAN) as shown in the figure below is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the borders of the immediate town/city. Routers, switches and hubs are connected to create a Metropolitan Area Network. MANs have the requirement of using telecommunication media such as voice channels or data channels. Branch offices are connected to head offices through MANs. Examples of organizations that use MANs are universities and colleges, grocery chains, and banks.



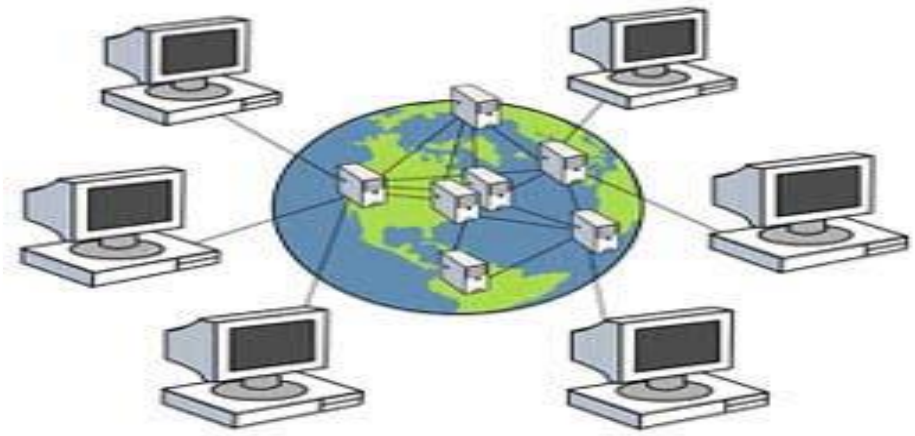
Metropolitan Area Network

c) WIDE AREA NETWORK (WAN)

As suggested by its name, a Wide Area Network is used to connect entire LANs and individual nodes, which are situated in different parts of the world. Wide Area Networks are linked together by a combination of wired and wireless links. The internet is a global wide area network

A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management.

A Wide Area Network as shown in the figure below is a network system connecting cities, countries, or continents together. WANs are connected together using one of the telecommunications mediums. The main difference between a MAN and a WAN is that the WAN uses Long Distance Carriers. Otherwise, the same protocols and equipment are used in MAN.



Wide Area Network

They may link the computers by means of cables, optical fibers, or satellites, but their users commonly access the networks via a modem (a device that allows computers to communicate over telephone lines). The largest wide – area network is the Internet, a collection of networks and gateways linking millions of computer users on every continent.

Networks for communications may also be classified as Intranet, Extranets and Internet.

a) **Intranet** are designed to be open, but secure private network accessible only to an organization's staff, that is, a wide range of information and services from an organization's internal information systems are not made available to the public, unlike the internet which is open to everybody.

b) **Extranets** are networks that link some of the intranet resources of an organization with other organizations and individuals. In other words, this is a private network that allows access to partners, (companies, organizations), vendors and supplies or authorized set of customers, to access some needed services of the organization's intranet, and without granting access to the organizations entire network.

c) **Internet** is a global system of interconnected computer networks that use internet protocol to link devices globally.

NETWORK TOPOLOGIES

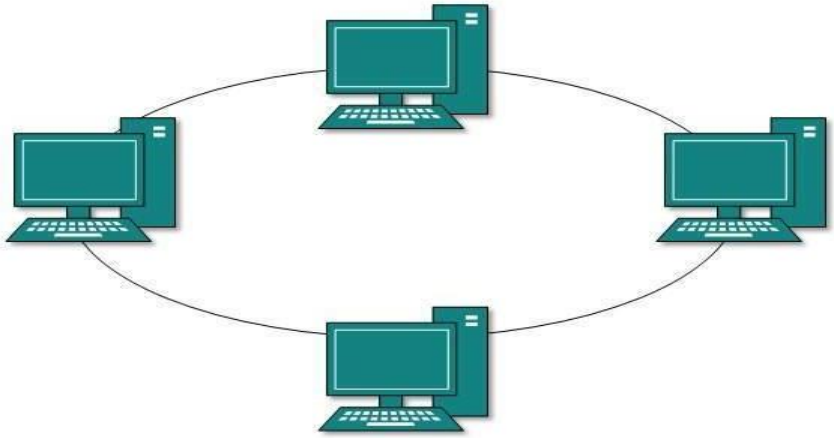
Network can be laid out in a different logical layouts or arrangements called a topology. The basic network topologies are:

a) **Bus-** All computers are connected to a common channel
b) **Star-** All computers are connected to a central server and hub
c) **Ring-** All computers are connected to a common channel.
d) **Tree-** Combines the characteristics of a linear bus and a star topology
e) **Mesh-** Peer-to-Peer Network

Computer networks, particularly Local Area Networks, can be described in terms of how the individual nodes are interconnected to one another. In addition, a network can also be described in terms of the roles played by individual computer unit. These two characteristics of a computer network are described by its topology. Network topology refers to the configuration used to connect computers and other devices within a computer network. In a network, computers are either used as a node or a server.

RING TOPOLOGY

In a ring topology as shown in the figure below, the first node is connected to the last node, which forms a ring-like structure. Messages or data are passed on from node to node until they reach their destination node. A malfunction in the connection of one node can stop the entire network from functioning properly. However, a ring network is like a one-way road where data travels in a single direction. Hence, collisions are avoided in a ring topology.



Ring Topology.

Advantages of Ring Topology

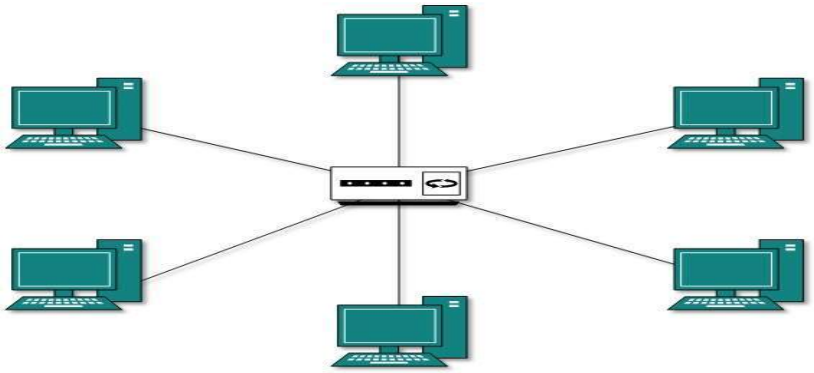
i. All traffic flows in only one direction thereby helping to reduce occurrence of collision.
ii. There is no need for network server to control the connectivity between workstations.
iii. Additional components do not affect the performance of the network.

Disadvantages of Ring Topology

i. Network is highly dependent on the wire which connects different components.
ii. If one workstation or port goes down, the entire network gets affected.
iii. Each packet of data must pass through all the nodes/computers between source and destination.

STAR TOPOLOGY

In a star topology as shown in the figure below, the nodes are connected to a server or a device called a hub. The server or the hub takes care of transmitting data from its sender to its destination without collisions. It can be said that the server or the hub acts as some sort of traffic policeman for the computer network. In addition, if a node's connection fails, the other nodes will remain operational because the hub still maintains the interconnection of the other nodes.



Star Topology

Advantages of a Star Topology

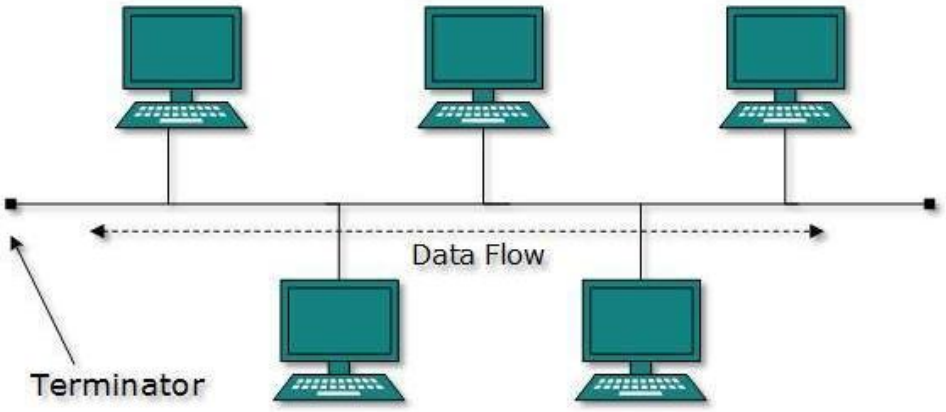
i. Centralised management. It helps in monitoring the network.
ii. Failure of one node or link does not affect the rest of the network.
iii. New node can be added or removed easily without affecting the rest of the network.
iv. Star topology gives far much better performance as signals do not necessarily get transmitted to all workstations/computers.

Disadvantages of a Star Topology

i. If the central device fails, the whole network goes down.
ii. The use of hub, router or switch as central device increases the overall cost of the network.
iii. Performance and number of nodes which can be added in such topology depend on the capacity of the central device.

BUS TOPOLOGY

In a bus topology, individual node is connected to a main cabling system (see the figure below). The primary disadvantage of a bus topology is that a malfunction in the connection of one node can bring down the whole network. Data in a bus network makes use of the same channel, which leads to collisions. When there are collisions, the data is resent until it reaches its destination without colliding with other data.



Bus Topology

Advantages of Bus Topology

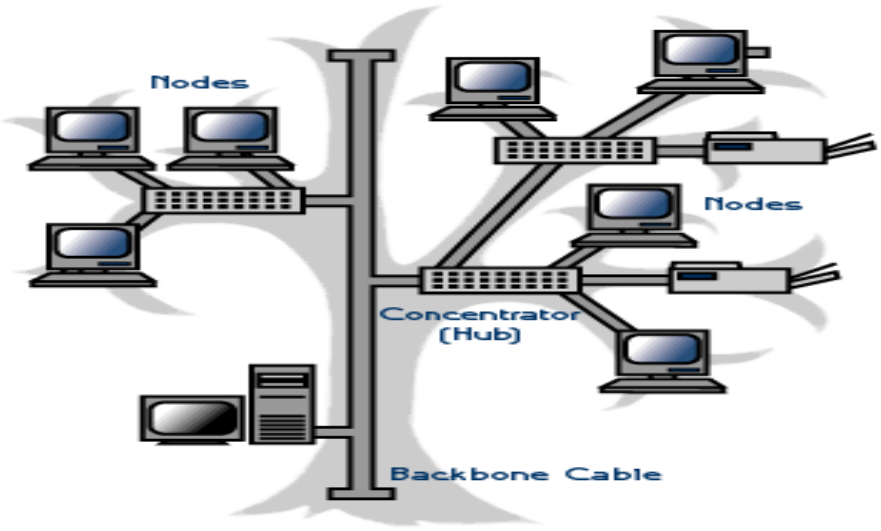
i. It is easy to setup and extend.
ii. Bus topology costs very less.
iii. Bus network is mostly used in small networks.
iv. Cable length required for this topology is the least compared to other networks.

Disadvantages of Bus Topology

i. Efficiency of bus network reduces as the number of devices connected to it increases.
ii. It is not suitable for networks with heavy traffic.
iii. Security is very low because all computers receive the sent signal from the source.
iv. If the main cable encounters some problem, the whole network breaks down.

TREE TOPOLOGY

The Tree topology shown in the figure below, integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.



A Tree topology

Advantages of a Tree Network topology

i. A Tree Topology is supported by many network vendors and even hardware vendors.
ii. A point-to-point connection is possible with Tree Networks.
iii. All the computers have access to the larger and their immediate networks.
iv. Best topology for branched out networks.

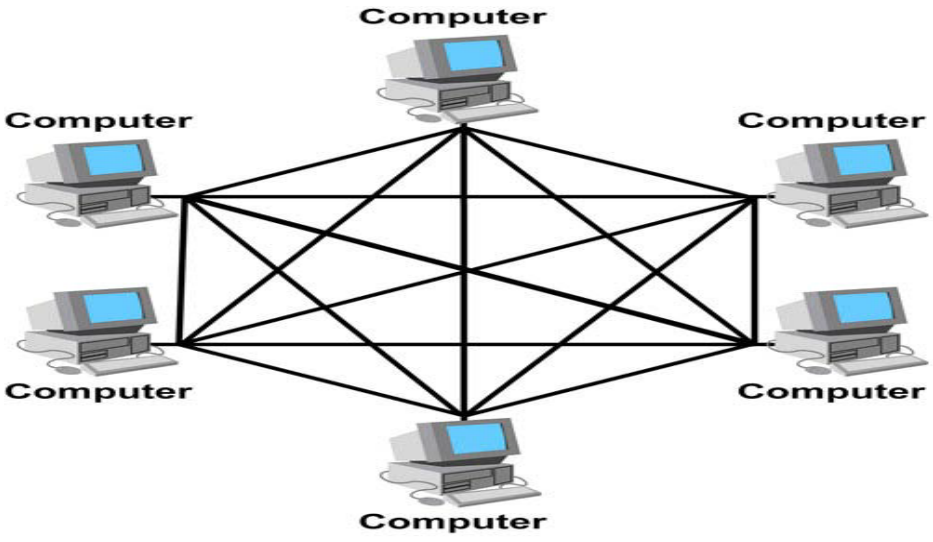
Disadvantages of a Tree Topology

i. In a Network Topology the length of the network depends on the type of cable that is being used.
ii. The Tree Topology network is entirely dependent on the trunk which is the main backbone of the network. If it fails then, the entire network will fail.
iii. Since the Tree Topology network is big, it is difficult to configure and can get complicated after a certain point.

MESH TOPOLOGY

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination, recall that even in a ring, although two cable paths exist, messages can only travel in one direction. Some WANs, most notably the Internet, employ mesh routing.

A mesh network in which every device connects to every other is called a full mesh. As shown in the figure below, partial mesh networks also exist in which some devices connect only indirectly to others. A peer-to-peer network is an example of a mesh topology because it allows users to share resources and file located on connected computer and to access shared resources found on other computers.



A Mesh Topology

Advantages of a Mesh Topology

i. It provides redundant paths between devices.
ii. The network can be expanded without disruption to current users.

iii. It is fault tolerant; since there is no gateway, nodes can connect to each other with no regard to the state of the rest of the network.
iv. In addition, nodes can create their own paths through the network because there is no gateway computer.

Disadvantages of a Mesh Topology

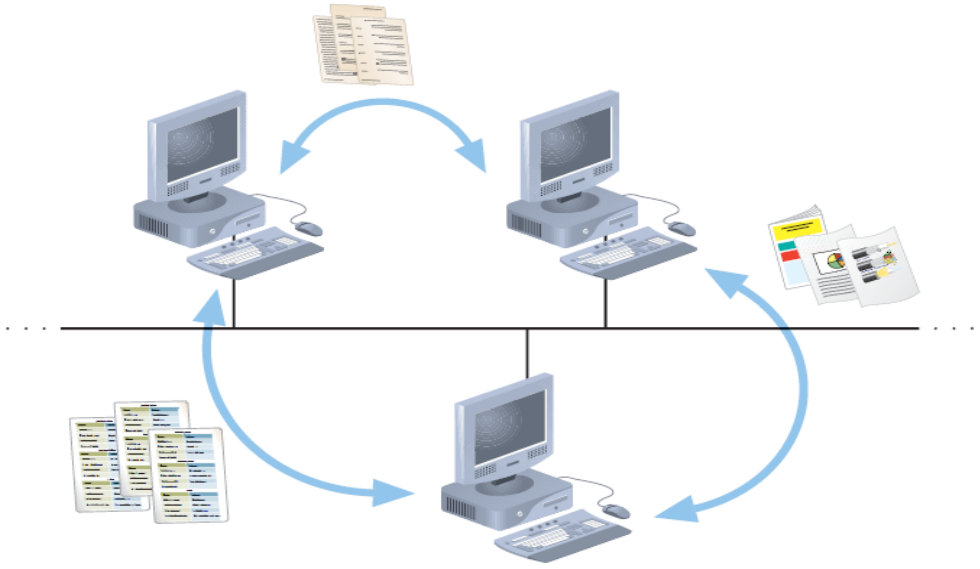
i. It requires more cable than the other LAN topologies.
ii. Complicated implementation may be experienced.
iii. Setup time can be quite time consuming.

TYPES OF NETWORKS

Computers can be positioned on a network in different ways relative to each other. They can have different levels of control over shared resources. They can also be made to communicate and share resources according to different schemes. The following sections describe two fundamental network models: peer-to-peer and client/server.

Peer-to-Peer Networks

The simplest form of a network is a peer-to-peer network. In a peer-to-peer network, every computer can communicate directly with every other computer. By default, no computer on a peer-to-peer network has more authority than another. However, each computer can be configured to share only some of its resources and prevent access to other resources. Traditional peer-to-peer networks typically consist of two or more general-purpose personal computers, with modest processing capabilities. Every computer is capable of sending and receiving information to and from every other computer, as shown in the Figure below.



Resource sharing on a simple peer-to-peer network

The following are advantages of using traditional peer-to-peer networks:

- They are simple to configure. For this reason, they may be used in environments in which time or technical expertise is scarce.
- They are often less expensive to set up and maintain than other types of networks. This fact makes them suitable for environments in which saving money is critical.

The following are disadvantages of using traditional peer-to-peer networks:

- They are not very flexible. As a peer-to-peer network grows larger, adding or changing significant elements of the network may be difficult.
- They are also not necessarily secure—meaning that in simple installations, data and other resources shared by network users can be easily discovered and used by unauthorized people.
- They are not practical for connecting more than a handful of computers, because they do not always centralize resources.

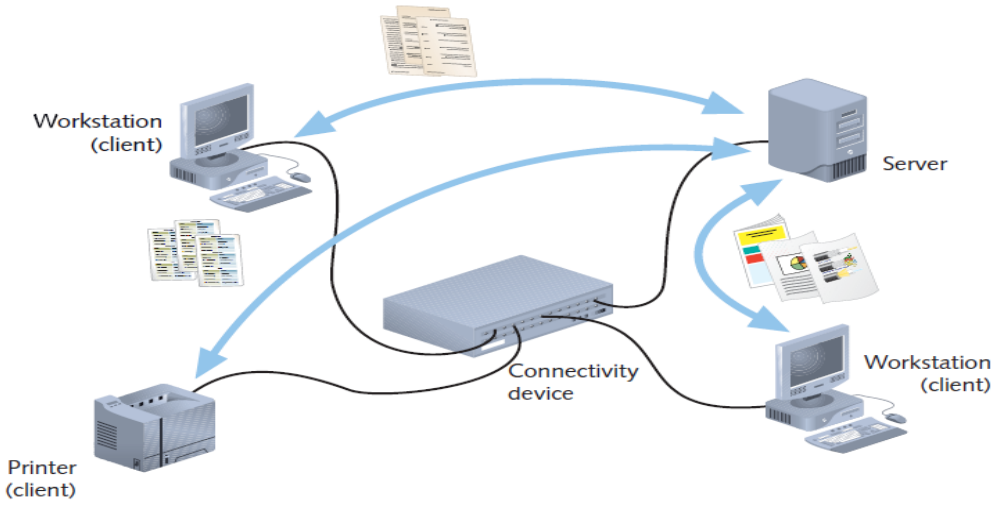
For example, if your computer is part of a peer-to-peer network that includes five other computers, and each computer user stores her spreadsheets and word-processing files on her own hard disk, whenever your colleagues want to edit your files, they must access your machine on the network. If one colleague saves a changed version of one of your spreadsheets on her hard disk, you'll find it difficult to keep track of which version is the most current. As you can imagine, the more computers you add to a peer-to-peer network, the more difficult it becomes to find and manage resources.

Client/Server Networks

Another way of designing a network is to use a central computer, known as a server, to facilitate communication and resource sharing between other computers on the network, which are known as clients. Clients usually take the form of personal computers, also known as workstations. A network that uses a server to enable clients to share data, data storage space, and devices is known as a client/server network. (The term client/server architecture is sometimes used to refer to the design of a network in which clients rely on servers for resource sharing and processing.) In terms of resource sharing and control, you can compare the client/server network to a public library. Just as a librarian manages the use of books and other media by patrons, a server manages the use of shared resources by clients. For example, if a patron does not have the credentials to check out books, the librarian prevents the patron from doing so. Similarly, a server allows only authorized clients to access its resources.

Every computer on a client/server network acts as a client or a server. (It is possible, but uncommon, for some computers to act as both.) Clients on a network can still run applications from and save data to their local hard disk. But by connecting to a server, they also have the option of using shared applications, data, and devices. Clients on a client/server network do not share their resources directly with each other, but rather use the server as an intermediary. Clients and servers communicate through connectivity devices such as switches or routers.

Figure below illustrates how resources are shared on a client/server network.



Resource sharing on a client/server network

Although client/server networks are typically more complex in their design and maintenance than peer-to-peer networks, they offer many advantages over peer-to-peer networks, such as:

- User logon accounts and passwords for anyone on a server-based network can be assigned in one place.
- Access to multiple shared resources (such as data files or printers) can be centrally granted to a single user or groups of users.
- Problems on the network can be monitored, diagnosed, and often fixed from one location.
- Servers are optimized to handle heavy processing loads and dedicated to handling requests from clients, enabling faster response time.
- Because of their efficient processing and larger disk storage, servers can connect more than a handful of computers on a network.

Together, these advantages make client/server networks easier to manage, more secure, and more powerful than peer-to-peer networks. They are also more scalable—that is, they can be more easily added onto and extended—than peer-to-peer networks.

To function as a server, a computer must be running an NOS (network operating system).
An NOS is a special type of software designed to do the following:

- Manage data and other resources for a number of clients.
- Ensure that only authorized users access the network.
- Control which types of files a user can open and read.
- Restrict when and from where users can access the network.
- Dictate which rules computers will use to communicate.
- Supply applications to clients.

Examples of popular network operating systems include various forms of UNIX and Linux, Microsoft Windows Server 2003 or Server 2008, and Mac OS X Server. (By contrast, a stand-alone computer, or a client computer, uses an operating system, such as Windows XP or Windows Vista, which has more limited resource management capabilities.)

COMMON MEDIA CHARACTERISTICS

Now that you are familiar with data-signalling characteristics, you are ready to learn more about the physical and atmospheric paths that these signals traverse. When deciding which kind of transmission media to use, you must match your networking needs with the characteristics of the media. This section describes the characteristics of several types of physical media, including throughput, cost, size and scalability, connectors, and noise immunity.

THROUGHPUT

Perhaps the most significant factor in choosing a transmission method is its throughput. All media are limited by the laws of physics that prevent signals from traveling faster than the speed of light. Beyond that, throughput is limited by the signalling and multiplexing techniques used in a given transmission method. Using fiber-optic cables allows faster throughput than copper or wireless connections. Noise and devices connected to the transmission medium can further limit throughput. A noisy circuit spends more time compensating for the noise and, therefore, has fewer resources available for transmitting data.

COST

The precise costs of using a particular type of cable or wireless connection are often difficult to pinpoint. For example, although a vendor might quote you the cost-per-foot for new network

cabling, you might also have to upgrade some hardware on your network to use that type of cabling. Thus, the cost of upgrading your media would actually include more than the cost of the cabling itself. Not only do media costs depend on the hardware that already exists in a network, but they also depend on the size of your network and the cost of labour in your area (unless you plan to install the cable yourself). The following variables can all influence the final cost of implementing a certain type of media:

- Cost of installation—Can you install the media yourself, or must you hire contractors to do it? Will you need to move walls or build new conduits or closets? Will you need to lease lines from a service provider?
- Cost of new infrastructure versus reusing existing infrastructure—Can you use existing wiring? In some cases, for example, installing all new Category 6 UTP wiring may not pay off if you can use existing Category 5 UTP wiring. If you replace only part of your infrastructure, will it be easily integrated with the existing media?
- Cost of maintenance and support—Reuse of an existing cabling infrastructure does not save any money if it is in constant need of repair or enhancement. Also, if you use an unfamiliar media type, it may cost more to hire a technician to service it. Will you be able to service the media yourself, or must you hire contractors to service it?
- Cost of a lower transmission rate affecting productivity—If you save money by reusing existing slower lines, are you incurring costs by reducing productivity? In other words, are you making staff wait longer to save and print reports or exchange e-mail?
- Cost of obsolescence—Are you choosing media that may become passing fads, requiring rapid replacement? Will you be able to find reasonably priced connectivity hardware that will be compatible with your chosen media for years to come?

NOISE IMMUNITY

As you learned earlier, noise can distort data signals. The extent to which noise affects a signal depends partly on the transmission media. Some types of media are more susceptible to noise than others. The type of media least susceptible to noise is fiber-optic cable, because it does not use electric current, but light waves, to conduct signals.

On most networks, noise is an ever-present threat, so you should take measures to limit its impact on your network. For example, install cabling well away from powerful electromagnetic forces. If your environment still leaves your network vulnerable, choose a type of transmission media that helps to protect the signal from noise. For example, wireless signals are more apt to be distorted by EMI/RFI than signals traveling over a cable. It is also possible to use anti-noise algorithms to protect data from being corrupted by noise. If these measures don't ward off interference, in the case of wired media, you may need to use a metal conduit, or pipeline, to contain and further protect the cabling.

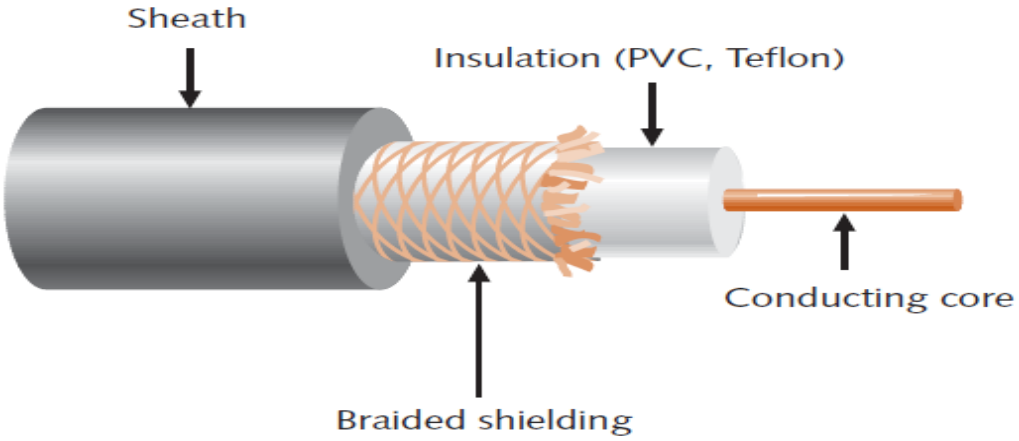
Now that you understand data transmission and the factors to consider when choosing a transmission medium, you are ready to learn about different types of transmission media. To qualify for Network+ certification, you must know the characteristics and limitations of each type of media, how to install and design a network with each type, how to troubleshoot networking media problems, and how to provide for future network growth with each option.

SIZE AND SCALABILITY

Three specifications determine the size and scalability of networking media: maximum nodes per segment, maximum segment length, and maximum network length. In cabling, each of these specifications are based on the physical characteristics of the wire and the electrical characteristics of data transmission. The maximum number of nodes per segment depends on attenuation and latency. Each device added to a network segment causes a slight increase in

the signal's attenuation and latency. To ensure a clear, strong, and timely signal, you must limit the number of nodes on a segment.
The maximum segment length depends on attenuation and latency plus the segment type. A network can include two types of segments: populated and unpopulated. A populated segment is a part of a network that contains end nodes. For example, a switch connecting users in a classroom is part of a populated segment. An unpopulated segment, also known as a link segment, is a part of the network that does not contain end nodes, but simply connects two networking devices such as routers.
Segment lengths are limited because after a certain distance, a signal loses so much strength that it cannot be accurately interpreted. The maximum distance a signal can travel and still be interpreted accurately is equal to a segment's maximum length. Beyond this length, data loss is apt to occur. As with the maximum number of nodes per segment, maximum segment length varies between different cabling types. The same principle of data loss applies to maximum network length, which is the sum of the network's segment lengths.

COAXIAL CABLE
Coaxial cable, called "coax" for short, was the foundation for Ethernet networks in the 1970s and remained a popular transmission medium for many years. Over time, however, twisted pair and fiber-optic cabling have replaced coax in modern LANs. If you work on long established networks or cable systems, however, you might have to work with coaxial cable.
Coaxial cable consists of a central metal core (often copper) surrounded by an insulator, a braided metal shielding, called braiding or shield, and an outer cover, called the sheath or jacket.



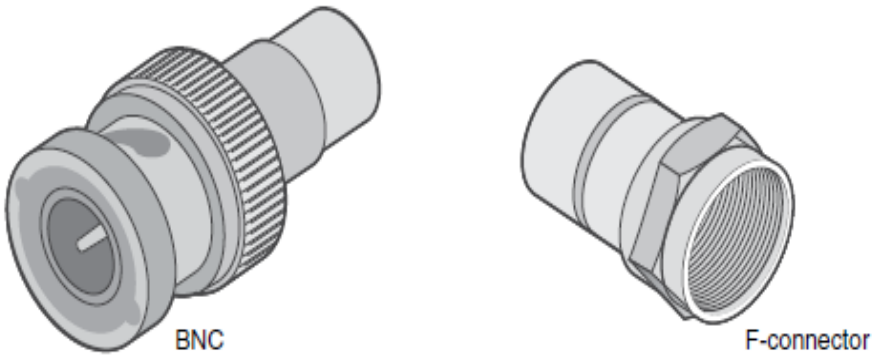
Coaxial cable
The picture above depicts a typical coaxial cable. The core may be constructed of one solid metal wire or several thin strands of metal wire. The core carries the electromagnetic signal, and the braided metal shielding acts as both a shield against noise and a ground for the signal. The insulator layer usually consists of a plastic material such as PVC (polyvinyl chloride) or Teflon. It protects the core from the metal shielding, because if the two made contact, the wire would short-circuit. The sheath, which protects the cable from physical damage, may be PVC or a more expensive, fire-resistant plastic.
Because of its shielding, most coaxial cable has a high resistance to noise. It can also carry signals farther than twisted pair cabling before amplification of the signals becomes necessary (although not as far as fiber-optic cabling). On the other hand, coaxial cable is more expensive than twisted pair cable because it requires significantly more raw materials to manufacture.
Coaxial cabling comes in hundreds of specifications, although you are likely to see only two or three types of coax in use on data networks. All types have been assigned an RG specification

number. (RG stands for radio guide, which is appropriate because coaxial cabling is used to guide radio frequencies in broadband transmission.) The significant differences between the cable types lie in the materials used for their shielding and conducting cores, which in turn influence their transmission characteristics, such as impedance (or the resistance that contributes to controlling the signal, as expressed in ohms), attenuation, and throughput. Each type of coax is suited to a different purpose. When discussing the size of the conducting core in a coaxial cable, we refer to its American Wire Gauge (AWG) size. The larger the AWG size, the smaller the diameter of a piece of wire. Following is a list of coaxial cable specifications used with data networks:

- RG-6
- RG-8
- RG-58
- RG-59

Common connectors used on coaxial cables are as follows:

- BNC: A Bayonet Neill-Concelman (BNC) connector (British Naval-Connector in some literature) can be used for a variety of applications, including as a connector in a 10BASE2 Ethernet network. A BNC coupler could be used to connect two coaxial cables together back-to-back.
- F-connector: An F-connector is often used for cable TV (including cable modem) connections. Notice that some refer to it is simply as F-type, including CompTIA.



TWISTED PAIR CABLE

Twisted pair cable consists of color-coded pairs of insulated copper wires, each with a diameter of 0.4 to 0.8 mm (approximately the diameter of a straight pin). Every two wires are twisted around each other to form pairs, and all the pairs are encased in a plastic sheath, as shown in Figure 3-19. The number of pairs in a cable varies, depending on the cable type.

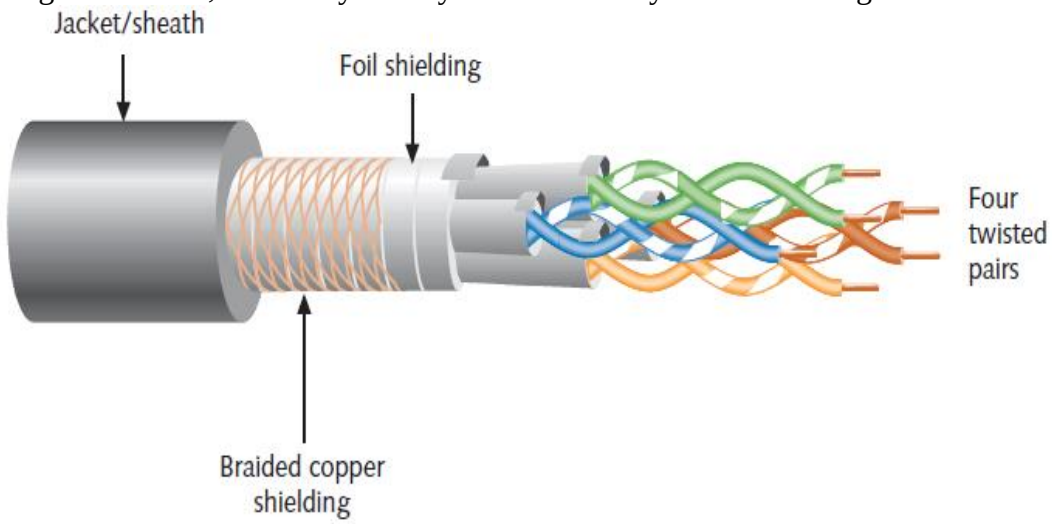
The more twists per foot in a pair of wires, the more resistant the pair will be to cross talk. Higher-quality, more expensive twisted pair cable contains more twists per foot. The number of twists per meter or foot is known as the twist ratio. Because twisting the wire pairs more tightly requires more cable, however, a high twist ratio can result in greater attenuation. For optimal performance, cable manufacturers must strike a balance between minimizing cross talk and reducing attenuation.

Because twisted pair is used in such a wide variety of environments and for a variety of purposes, it comes in hundreds of different designs. These designs vary in their twist ratio, the number of wire pairs that they contain, the grade of copper used, the type of shielding (if any), and the materials used for shielding, among other things. A twisted pair cable may contain from

1 to 4200 wire pairs. Modern networks typically use cables that contain four wire pairs, in which one pair is dedicated to sending data and another pair is dedicated to receiving data.
Twisted pair cable is relatively inexpensive, flexible, and easy to install, and it can span a significant distance before requiring a repeater (though not as far as coax). Twisted pair cable easily accommodates several different topologies, although it is most often implemented in star or star-hybrid topologies. Furthermore, twisted pair can handle the faster networking transmission rates currently being employed. Due to its wide acceptance, it will probably continue to be updated to handle the even faster rates that will emerge in the future. All twisted pair cable falls into one of two categories: STP (shielded twisted pair) or UTP (unshielded twisted pair).

STP (SHIELDED TWISTED PAIR)

STP (shielded twisted pair) cable consists of twisted wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil. Some STP use a braided copper shielding. The shielding acts as a barrier to external electromagnetic forces, thus preventing them from affecting the signals traveling over the wire inside the shielding. It also contains the electrical energy of the signals inside. The shielding may be grounded to enhance its protective effects. The effectiveness of STP's shield depends on the level and type of environmental noise, the thickness and material used for the shield, the grounding mechanism, and the symmetry and consistency of the shielding.

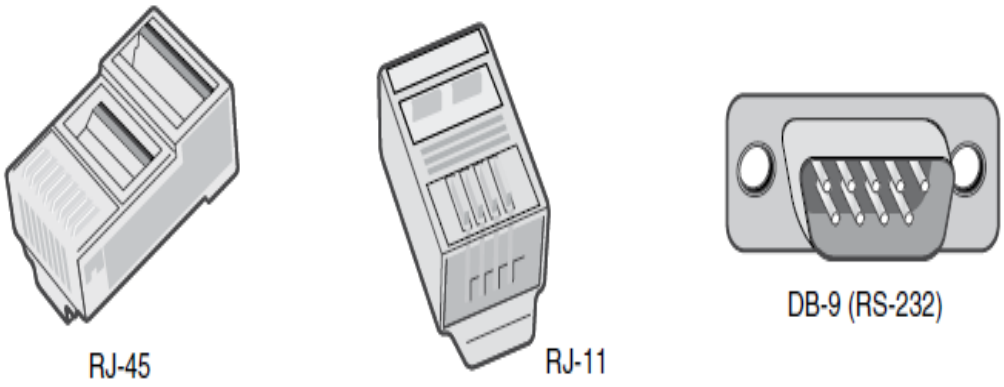


UTP (UNSHIELDED TWISTED PAIR)

UTP (unshielded twisted pair) cabling consists of one or more insulated wire pairs encased in a plastic sheath. As its name implies, UTP does not contain additional shielding for the twisted pairs. As a result, UTP is both less expensive and less resistant to noise than STP. Figure below depicts a typical UTP cable.

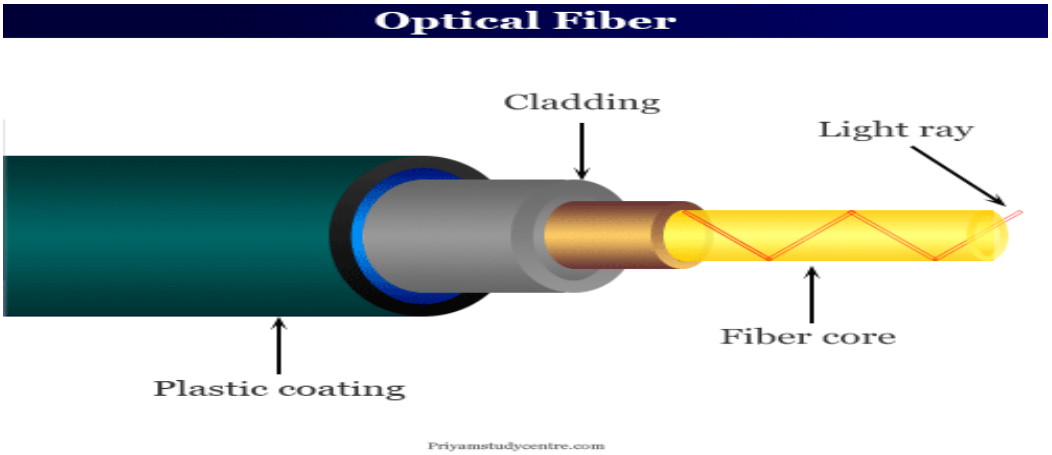
Common connectors used on twisted-pair cables are as follows:

- RJ-45: A type 45 registered jack (RJ-45) is an eight-pin connector found in most Ethernet networks. However, most Ethernet implementations only use four of the eight pins.
- RJ-11: A type 11 registered jack (RJ-11) has the capacity to be a six-pin connector. However, most RJ-11 connectors have only two or four conductors. An RJ-11 connector is found in most home telephone networks. However, most home phones only use two of the six pins.
- DB-9 (RS-232): A nine-pin D-subminiature (DB-9) connector is an older connector used for low-speed asynchronous serial communications, such as a PC to a serial printer, a PC to a console port of a router or switch, or a PC to an external modem. Do not confuse the DB-9 with a DB-25. The DB-25 connector was also used for the serial or parallel ports of early personal computers.



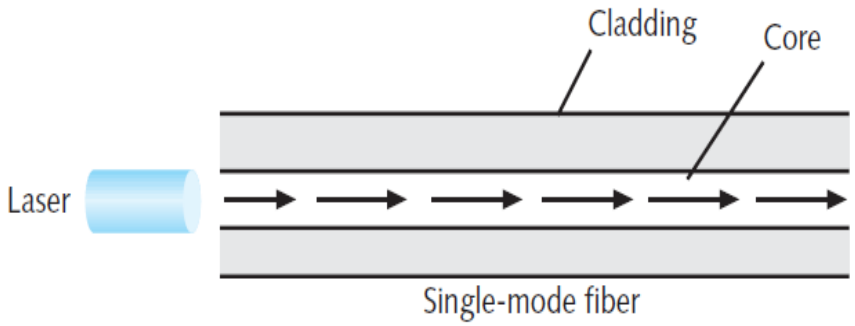
FIBER-OPTIC CABLE

Fiber-optic cable, or simply fiber, contains one or several glass or plastic fibers at its center, or core. Data is transmitted via pulsing light sent from a laser (in the case of 1- and 10- Gigabit technologies) or an LED (light-emitting diode) through the central fibers. Surrounding the fibers is a layer of glass or plastic called cladding. The cladding has a different density from the glass or plastic in the strands. It reflects light back to the core in patterns that vary depending on the transmission mode. This reflection allows the fiber to bend around corners without diminishing the integrity of the light-based signal. Outside the cladding, a plastic buffer protects the cladding and core. Because the buffer is opaque, it also absorbs any light that might escape. To prevent the cable from stretching, and to protect the inner core further, strands of Kevlar (a polymeric fiber) surround the plastic buffer. Finally, a plastic sheath covers the strands of Kevlar. Figure below shows a fiber-optic cable with multiple, insulated fibers.



Like twisted pair and coaxial cabling, fiber-optic cabling comes in a number of different varieties, depending on its intended use and the manufacturer. For example, fiber-optic cables used to connect the facilities of large telephone and data carriers may contain as many as 1000 fibers and be heavily sheathed to prevent damage from extreme environmental conditions. At the other end of the spectrum, fiber-optic patch cables for use on LANs may contain only two strands of fiber and be pliable enough to wrap around your hand.
However, all fiber cable variations fall into two categories: single-mode and multimode.

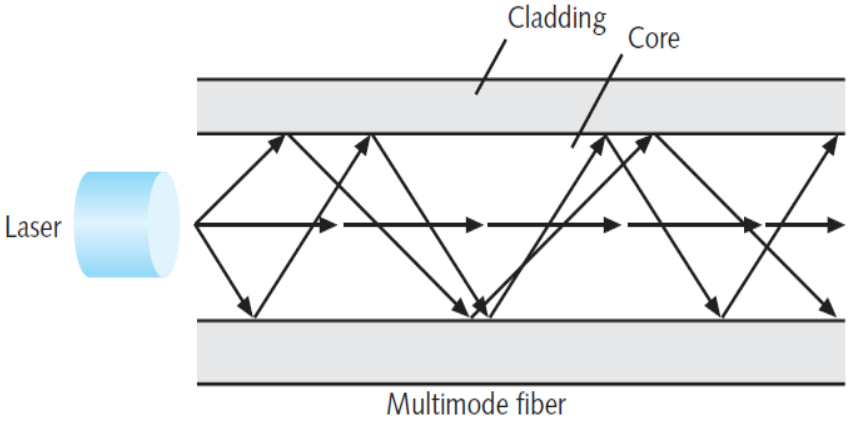
SMF (Single-Mode Fiber)
SMF (single-mode fiber) uses a narrow core (less than 10 microns in diameter) through which light generated by a laser travel over one path, reflecting very little. Because it reflects little, the light does not disperse as the signal travels along the fiber. This continuity allows single-mode fiber to accommodate the highest bandwidths and longest distances (without requiring repeaters) of all network transmission media. Single-mode fiber may be used to connect a carrier's two facilities. However, it costs too much to be considered for use on typical LANs and WANs. Figure 3-31 depicts a simplified version of how signals travel over single-mode fiber.



MMF (Multimode Fiber)
MMF (multimode fiber) contains a core with a larger diameter than single-mode fiber (between 50 and 115 microns in diameter; the most common size is 62.5 microns) over which many pulses of light generated by a laser or LED travel at different angles. It is commonly found on cables that connect a router to a switch or a server on the backbone of a network. Figure 3-32 depicts a simplified view of how signals travel over multimode fiber.
Because of its reliability, fiber is currently used primarily as a cable that connects the many segments of a network. Fiber-optic cable provides the following benefits over copper cabling:

- Extremely high throughput
- Very high resistance to noise
- Excellent security
- Ability to carry signals for much longer distances before requiring repeaters than copper cable
- Industry standard for high-speed networking

The most significant drawback to the use of fiber is that covering a certain distance with fiber-optic cable is much more expensive than using twisted pair cable. Also, fiber-optic cable requires special equipment to splice, which means that quickly repairing a fiber-optic cable in the field (given little time or resources) can be difficult.



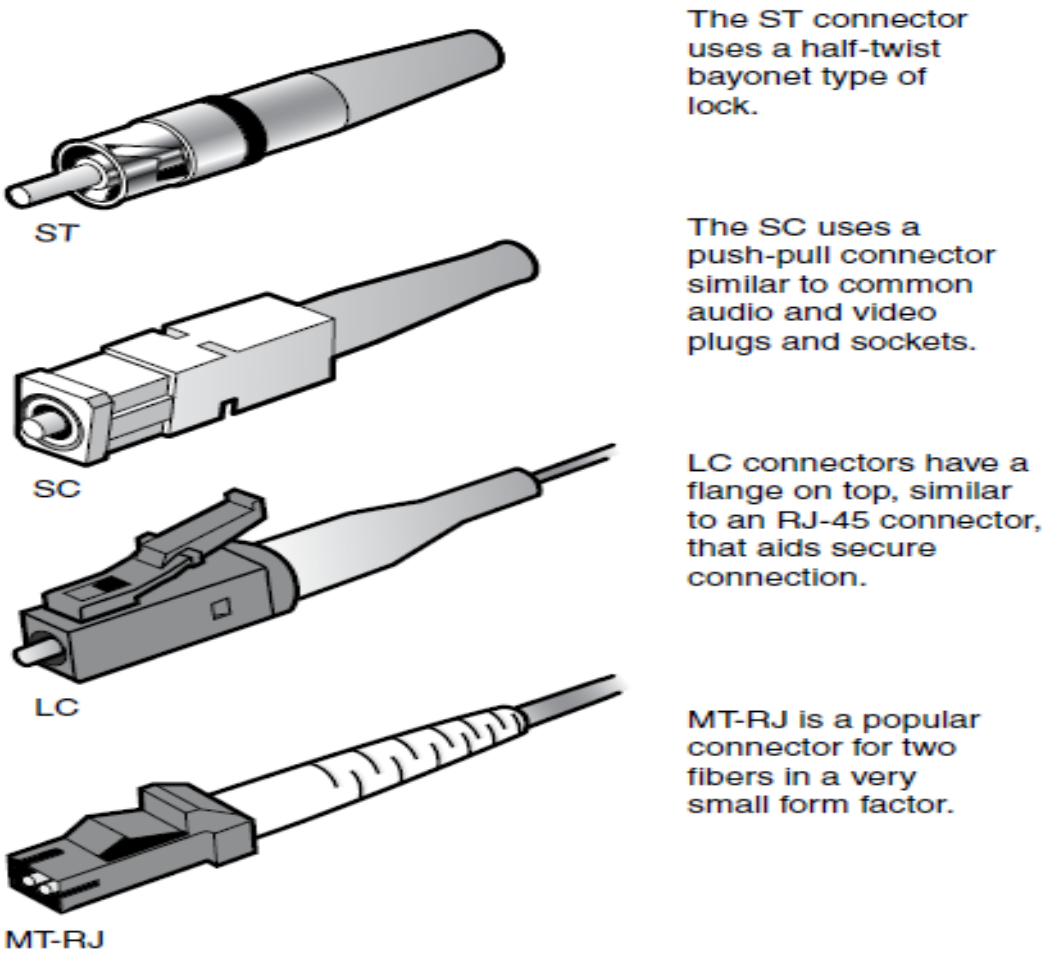
Some common connectors used on fiber-optic cables are as follows:

- ST: A straight tip (ST) connector is sometimes referred to as a bayonet connector, because of the long tip extending from the connector. ST connectors are most commonly used with MMF. An ST connector connects to a terminating device by pushing the connector into the terminating equipment and then twisting the connector housing to lock it in place.

- SC: Different literature defines an SC connector as subscriber connector, standard connector, or square connector. The SC connector is connected by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device. The connector has slight variants within the industry, with the major types being APC, UPC, and MTRJ. Always consult with the vendor or IT staff member regarding the exact requirements.

- LC: A Lucent connector (LC) connects to a terminating device by pushing the connector into the terminating device, and it can be removed by pressing the tab on the connector and pulling it out of the terminating device.

- MTRJ: The most unique characteristic of a media termination recommended jack (MTRJ) connector is that two fiber strands (a transmit strand and a receive strand) are included in a single connector. An MTRJ connector is connected by pushing the connector into the terminating device, and it can be removed by pulling the connector from the terminating device.



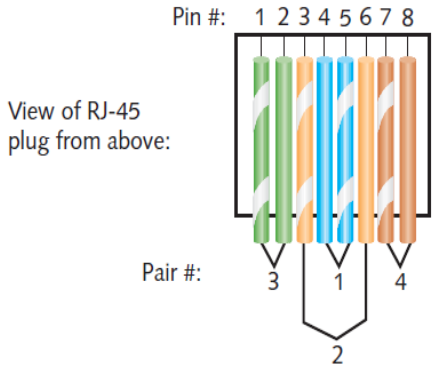
Terminating Twisted Pair Cable

Imagine you have been sent to one of your employer's remote offices and charged with upgrading all the old Cat 3 patch cables in a data closet with new, Cat 6 patch cables. A patch cable is a relatively short (usually between 3 and 25 feet) length of cabling with connectors at both ends. Based on the company's network documentation, you brought 50 premade cables with RJ-45 plugs on both ends, which you purchased from an online cable vendor. At the remote location, however, you discover that its data closet actually contains 60 patch cables that need replacing. No additional premade cables are available at that office, and you don't have time to order more. Luckily, you have brought your networking tool kit with spare RJ-45 plugs and a spool of Cat 6 cable. Knowing how to properly terminate Cat 6 cables allows you to make all the new patch cables you need and complete your work. Even if you are never faced with this situation, it's likely that at some point you will have to replace an RJ-45 connector on an existing cable. This section describes how to terminate twisted pair cable.

Proper cable termination is a basic requirement for two nodes on a network to communicate. Beyond that, however, poor terminations can lead to loss or noise—and consequently, errors—in a signal. Closely following termination standards, then, is critical. TIA/EIA has specified two different methods of inserting twisted pair wires into RJ-45 plugs: TIA/EIA 568A and TIA/EIA 568B. Functionally, there is no difference between the standards. You only have to be certain that you use the same standard on every RJ-45 plug and jack on your network, so that data is transmitted and received correctly. The figure below depicts pin numbers and assignments (or pinouts) for the TIA/EIA 568A standard when used on an Ethernet network. The second figure depicts pin numbers and assignments for the TIA/EIA 568B standard.

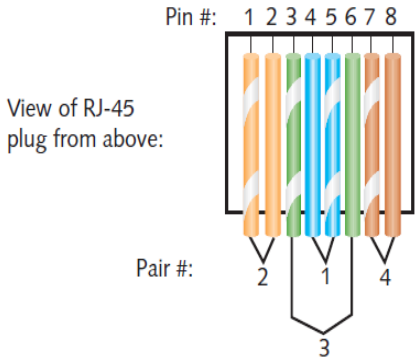
(Although networking professionals commonly refer to wires in the two figures as transmit and receive, their original T and R designations stand for Tip and Ring, terms that come from early telephone technology but are irrelevant today.)

If you terminate the RJ-45 plugs at both ends of a patch cable identically, following one of the TIA/EIA 568 standards, you will create a straight-through cable. A straight-through cable is so named because it allows signals to pass "straight through" from one end to the other. This is the type used to connect a workstation to a hub or router, for example. However, in some cases you may want to reverse the pin locations of some wires—for example, when you want to connect two workstations without using a connectivity device or when you want to connect two hubs through their data ports. This can be accomplished through the use of a crossover cable, a patch cable in which the termination locations of the transmit and receive wires on one end of the cable are reversed, as shown in Figure A. In this example, the TIA/EIA 568B standard is used on the left side, whereas the TIA/EIA 568A standard is used on the right side. Notice that only pairs 2 and 3 are switched, because those are the pairs sending and receiving data.



Pin #	Color	Pair #	Function
1	White with green stripe	3	Transmit +
2	Green	3	Transmit -
3	White with orange stripe	2	Receive +
4	Blue	1	Unused
5	White with blue stripe	1	Unused
6	Orange	2	Receive -
7	White with brown stripe	4	Unused
8	Brown	4	Unused

TIA/EIA 568A standard terminations



Pin #	Color	Pair #	Function
1	White with orange stripe	2	Transmit +
2	Orange	2	Transmit -
3	White with green stripe	3	Receive +
4	Blue	1	Unused
5	White with blue stripe	1	Unused
6	Green	3	Receive -
7	White with brown stripe	4	Unused
8	Brown	4	Unused

TIA/EIA 568B standard terminations

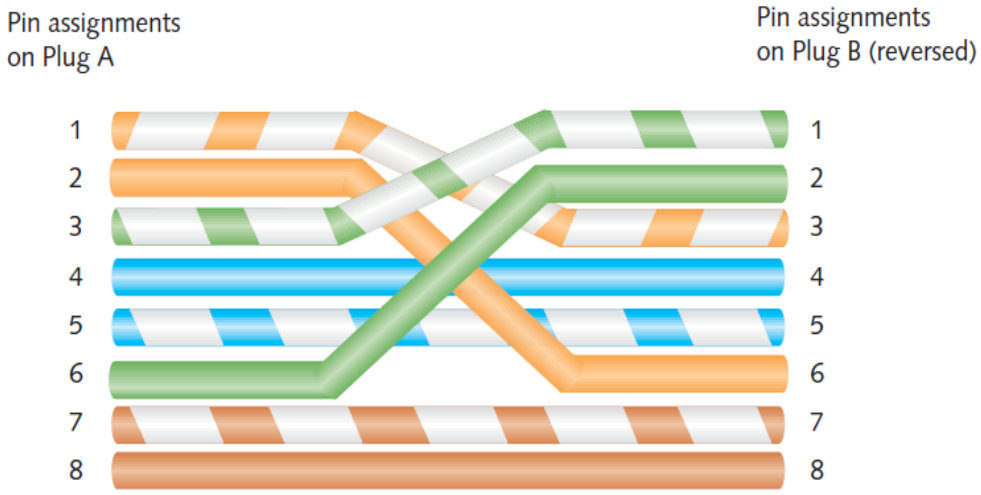


Figure A: RJ-45 terminations on a crossover cable

The tools you'll need to terminate a twisted-pair cable with an RJ-45 plug are a wire cutter, wire stripper, and crimping tool, which are pictured in Figures B, C and D, respectively. (In fact, you can find a single device that contains all three of these tools.)

Following are the steps to create a straight-through patch cable. To create a crossover cable, you would simply reorder the wires in Step 4 to match Figure A. The process of fixing wires inside the connector is called crimping, and it is a skill that requires practice—so don't be discouraged if the first cable you create doesn't reliably transmit and receive data. You'll get to practice making cables in the end-of-chapter Hands-on Projects:

1. Using the wire cutter, make a clean cut at both ends of the twisted-pair cable.
2. Using the wire stripper, remove the sheath off of one end of the twisted-pair cable, beginning at approximately one inch from the end. Be careful to neither damage nor remove the insulation that's on the twisted pairs inside.
3. Separate the four wire pairs slightly. Carefully unwind each pair no more than ½ inch.
4. To make a straight-through cable, align all eight wires on a flat surface, one next to the other, ordered according to their colors and positions listed in TIA/EIA 568B. (It might be helpful first to "groom"—or pull steadily across the length of—the unwound section of each wire to straighten it out and help it stay in place.)
5. Keeping the wires in order and in line, gently slide them all the way into their positions in the RJ-45 plug.
6. After the wires are fully inserted, place the RJ-45 plug in the crimping tool and press firmly to crimp the wires into place. (Be careful not to rotate your hand or the wire as you do this, otherwise only some of the wires will be properly terminated.) Crimping causes the internal RJ-45 pins to pierce the insulation of the wire, thus creating contact between the two conductors.
7. Now remove the RJ-45 connector from the crimping tool. Examine the end and see whether each wire appears to be in contact with the pin. It may be difficult to tell simply by looking at the connector. The real test is whether your cable will successfully transmit and receive signals.
8. Repeat Steps 2 through 7 for the other end of the cable. After completing Step 7 for the other end, you will have created a straight-through patch cable.

Even after you feel confident making your own cables, it's a good idea to verify that they can transmit and receive data at the necessary rates using a cable tester.

NETWORKING STANDARDS AND THE OSI MODEL

Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed. Many different industries use standards to ensure that products, processes, and services suit their purposes. Because of the wide variety of hardware and software in use today, standards are especially important in the world of networking. Without standards, it would be very difficult to design a network because you could not be certain that software or hardware from different manufacturers would work together. For example, if one manufacturer designed a network cable with a 1-centimeter-wide plug and another company manufactured a wall plate with a 0.8-centimeter-wide opening, you would not be able to insert the plug into the wall plate.

When purchasing networking equipment, therefore, you want to verify that equipment meets the standards your network requires. However, bear in mind that standards define the minimum acceptable performance of a product or service—not the ideal. So, for example, you might purchase two different network cables that comply with the minimum standard for transmitting at a certain speed, but one cable might exceed that standard, allowing for better network performance. In the case of network cables, exceeding minimum standards often follows from the use of quality materials and careful production techniques.

A complete list of the standards that regulate computers and networking would fill an encyclopedia. Although you don't need to know the fine points of every standard, you should be familiar with the groups that set networking standards and the critical aspects of standards required by your network.

ANSI

ANSI (American National Standards Institute) is an organization composed of more than a thousand representatives from industry and government who together determine standards for the electronics industry and other fields, such as chemical and nuclear engineering, health and safety, and construction. ANSI also represents the United States in setting international standards. **This organization does not dictate that manufacturers comply with its standards, but requests voluntarily compliance.** Of course, manufacturers and developers benefit from compliance, because compliance assures potential customers that the systems are reliable and can be integrated with an existing infrastructure. **New electronic equipment and methods must undergo rigorous testing to prove they are worthy of ANSI's approval.** You can purchase ANSI standards documents online from ANSI's Web site (www.ansi.org) or find them at a university or public library. You need not read complete ANSI standards to be a competent networking professional, but you should understand the breadth and significance of ANSI's influence.

EIA and TIA

Two related standards organizations are EIA and TIA. EIA (**Electronic Industries Alliance**) is a trade organization composed of representatives from electronics manufacturing firms across the United States. **EIA not only sets standards for its members, but also helps write ANSI standards and lobbies for legislation favorable to the growth of the computer and electronics industries.**

In 1988, one of the EIA's subgroups merged with the former United States Telecommunications Suppliers Association (USTSA) to form TIA (**Telecommunications Industry Association**). **TIA focuses on standards for information technology, wireless, satellite, fiber optics, and telephone equipment.** Both TIA and EIA set standards, lobby

governments and industry, and sponsor conferences, exhibitions, and forums in their areas of interest.
Probably the best-known standards to come from the TIA/EIA alliance are its guidelines for how network cable should be installed in commercial buildings, known as the "TIA/EIA 568-B Series." You can find out more about TIA from its Web site, www.tiaonline.org, and EIA from its Web site, www.eia.org.

IEEE
The IEEE (Institute of Electrical and Electronics Engineers), or "I-triple-E," is an international society composed of engineering professionals. **Its goals are to promote development and education in the electrical engineering and computer science fields.** To this end, IEEE hosts numerous symposia, conferences, and local chapter meetings and publishes papers designed to educate members on technological advances. It also maintains a standards board that establishes its own standards for the electronics and computer industries and contributes to the work of other standards-setting bodies, such as ANSI.
IEEE technical papers and standards are highly respected in the networking profession. Among other places, you will find references to IEEE standards in the manuals that accompany NICs. You can purchase IEEE documents online from IEEE's Web site (www.ieee.org) or find them in a university or public library.

ISO
ISO (International Organization for Standardization), headquartered in Geneva, Switzerland, is a collection of standards organizations representing 157 countries. **ISO's goal is to establish international technological standards to facilitate global exchange of information and barrier free trade.** Given the organization's full name, you might expect it to be called IOS, but ISO is not meant to be an acronym. In fact, iso is the Greek word for equal. Using this term conveys the organization's dedication to standards.
ISO's authority is not limited to the information-processing and communications industries. It also applies to the fields of textiles, packaging, distribution of goods, energy production and utilization, shipbuilding, and banking and financial services. The universal agreements on screw threads, bank cards, and even the names for currencies are all products of ISO's work. In fact, fewer than 3000 of ISO's more than 17,000 standards apply to computer-related products and functions. You can find out more about ISO at its Web site: www.iso.org.

ITU
The ITU (International Telecommunication Union) is a specialized United Nations agency **that regulates international telecommunications, including radio and TV frequencies, satellite and telephony specifications, networking infrastructure, and tariffs applied to global communications.** It also provides developing countries with technical expertise and equipment to advance those nations' technological bases.
The ITU was founded in Paris in 1865. It became part of the United Nations in 1947 and relocated to Geneva, Switzerland. Its standards arm contains members from 191 countries and publishes detailed policy and standards documents that can be found on its Web site: www.itu.int. Typically, ITU documents pertain more to global telecommunications issues than to industry technical specifications. However, the ITU is deeply involved with the implementation of worldwide Internet services. As in other areas, the ITU cooperates with several different standards organizations, such as ISOC (discussed next), to develop these standards.

ISOC

ISOC (Internet Society), founded in 1992, is a professional membership society **that helps to establish technical standards for the Internet.** Some current ISOC concerns include the rapid growth of the Internet and keeping it accessible, information security, and the need for stable addressing services and open standards across the Internet. ISOC's membership consists of thousands of Internet professionals and companies from 90 chapters around the world.
ISOC oversees groups with specific missions, such as the IAB (Internet Architecture Board). IAB is a technical advisory group of researchers and technical professionals interested in overseeing the Internet's design and management. As part of its charter, IAB is responsible for Internet growth and management strategy, resolution of technical disputes, and standards oversight.
You can learn more about ISOC and its member organizations, IAB and IETF, at their Web site: www.isoc.org.

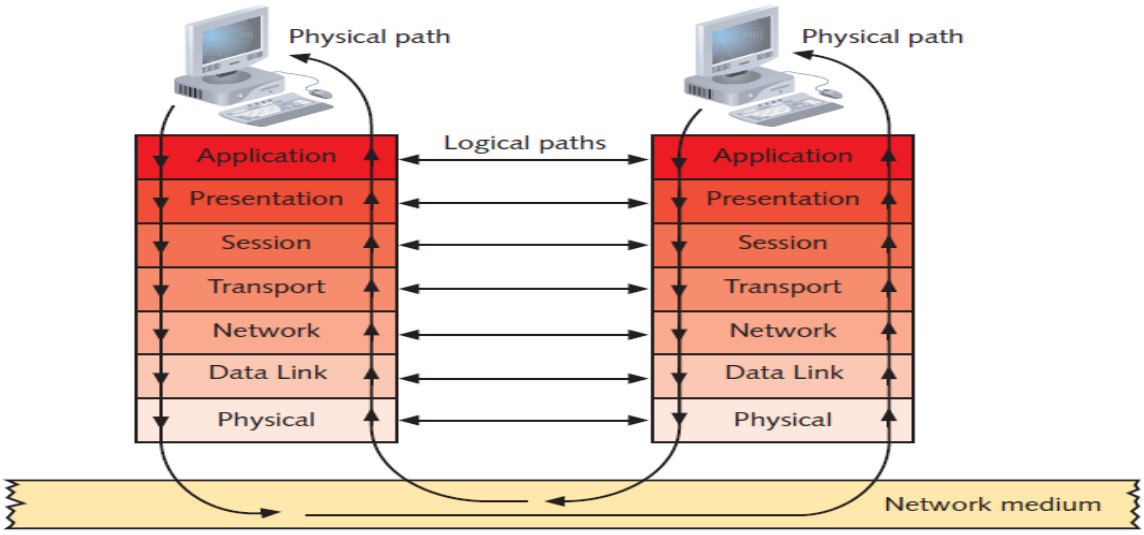
IANA and ICANN
You have learned that every computer on a network must have a unique address. On the Internet, this is especially important because millions of different computers must be available to transmit and receive data at any time. Addresses used to identify computers on the Internet and other TCP/IP-based networks are known as IP (Internet Protocol) addresses. To ensure that every Internet-connected device has a unique IP address, organizations across the globe rely on centralized authorities.
In early Internet history, a non-profit group called the **IANA (Internet Assigned Numbers Authority)** kept records of available and reserved IP addresses and determined how addresses were doled out. Starting in 1997, IANA coordinated its efforts with three RIRs (Regional Internet Registries): ARIN (American Registry for Internet Numbers), APNIC (Asia Pacific Network Information Centre), and RIPE (Réseaux IP Européens). An RIR is a not-for-profit agency that manages the distribution of IP addresses to private and public entities. In the late 1990s, the United States Department of Commerce (DOC), which funded IANA, decided to overhaul IP addressing and domain name management. The DOC recommended the formation of **ICANN (Internet Corporation for Assigned Names and Numbers)**, a private, non-profit corporation. ICANN is now ultimately responsible for IP addressing and domain name management. Technically speaking, however, IANA continues to perform the system administration.
Individuals and businesses do not typically obtain IP addresses directly from an RIR or IANA. Instead, they lease a group of addresses from their ISP (Internet service provider), a business that provides organizations and individuals with access to the Internet and often, other services, such as e-mail and Web hosting. An ISP, in turn, arranges with its RIR for the right to use certain IP addresses on its network. The RIR obtains its right to dole out those addresses from ICANN. In addition, the RIR coordinates with IANA to ensure that the addresses are associated with devices connected to the ISP's network.
You can learn more about IANA and ICANN at their Web sites, www.iana.org and www. icann.org, respectively.

THE OSI MODEL
In the early 1980s, ISO began work on a universal set of specifications that would enable computer platforms across the world to communicate openly. The result was a helpful model for understanding and developing computer-to-computer communications over a network. This model, called the OSI (Open Systems Interconnection) model, divides network communications into seven layers: **Physical, Data Link, Network, Transport, Session, Presentation, and Application.** At each layer, protocols perform services unique to that layer. While performing those services, the protocols also interact with protocols in the layers directly

above and below. In addition, at the top of the OSI model, Application layer protocols interact with the software you use (such an e-mail or spreadsheet program). At the bottom, Physical layer services act on the networking cables and connectors to issue and receive signals.
The OSI model is a theoretical representation of what happens between two nodes communicating on a network. It does not prescribe the type of hardware or software that should support each layer. Nor does it describe how software programs interact with other software programs or how software programs interact with humans. Every process that occurs during network communications can be associated with a layer of the OSI model, so you should be familiar with the names of the layers and understand the key services and protocols that belong to each.

Networking professionals often devise a mnemonic way of remembering the seven layers of the OSI model. One strategy is to make a sentence using words that begin with the same first letter of each layer, starting with either the lowest (Physical) or the highest (Application) layer. For example, you might choose to remember the phrase "Programmers Dare Not Throw Salty Pretzels Away." Quirky phrases are often easiest to remember.

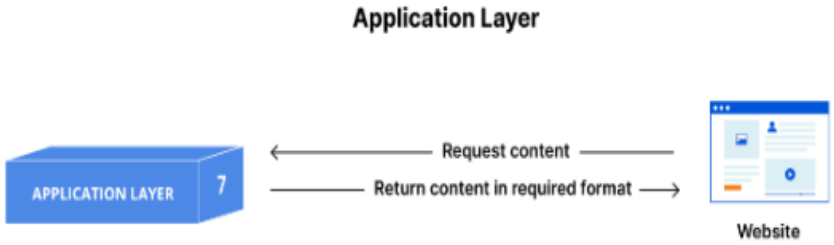
The path that data takes from one computer to another through the OSI model is illustrated in the Figure below



Flow of data through the OSI model

What is the OSI Model?
The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other.
The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.
Each layer of the OSI Model handles a specific job and communicates with the layers above and below itself. DDoS attacks target specific layers of a network connection; application layer attacks target layer 7 and protocol layer attacks target layers 3 and 4.

The seven abstraction layers of the OSI model can be defined as follows, from top to bottom:
7. The application layer



This is the only layer that directly interacts with data from the user. Software applications like web browsers and email clients rely on the application layer to initiate communications. But it should be made clear that client software applications are not part of the application layer; rather the application layer is responsible for the protocols and data manipulation that the software relies on to present meaningful data to the user.
Application layer protocols include HTTP as well as SMTP (Simple Mail Transfer Protocol is one of the protocols that enables email communications).

6. The presentation layer

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.
Two communicating devices communicating may be using different encoding methods, so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.
If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.
Finally the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

5. The session layer

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

The session layer also synchronizes data transfer with checkpoints. For example, if a 100 megabyte file is being transferred, the session layer could set a checkpoint every 5 megabytes. In the case of a disconnect or a crash after 52 megabytes have been transferred, the session could be resumed from the last checkpoint, meaning only 50 more megabytes of data need to be transferred. Without the checkpoints, the entire transfer would have to begin again from scratch.

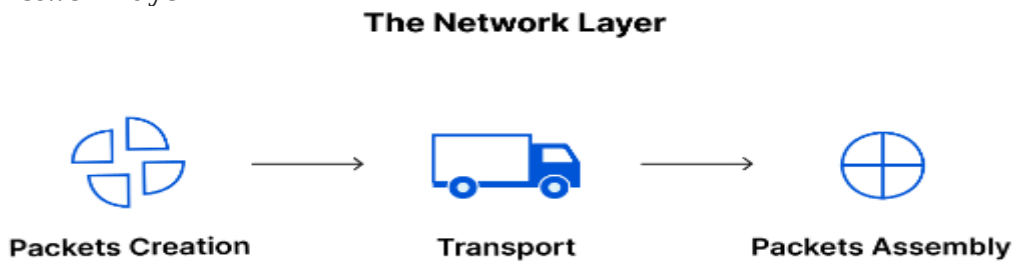
4. The transport layer

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection does not overwhelm a receiver with a slow connection. The transport layer performs error control on the receiving end by ensuring that the data received is complete, and requesting a retransmission if it isn't.

Transport layer protocols include the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

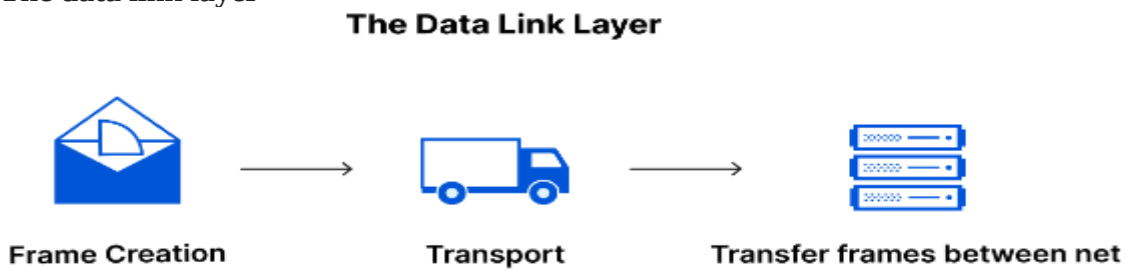
3. The network layer



The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

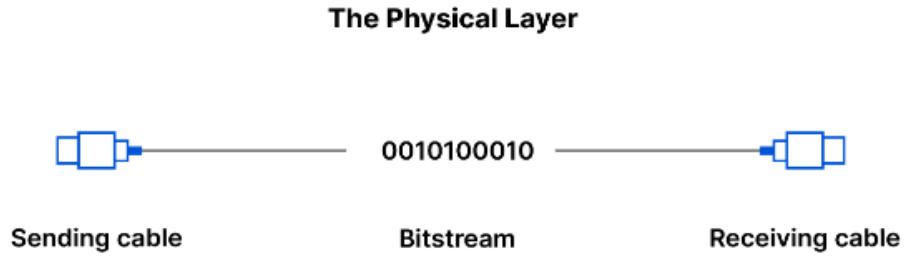
Network layer protocols include IP, the Internet Control Message Protocol (ICMP), the Internet Group Message Protocol (IGMP), and the IPsec suite.

2. The data link layer



The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the *same* network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

1. The physical layer



This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

How data flows through the OSI Model

In order for human-readable information to be transferred over a network from one device to another, the data must travel down the seven layers of the OSI Model on the sending device and then travel up the seven layers on the receiving end.

For example: Mr. Cooper wants to send Ms. Palmer an email. Mr. Cooper composes his message in an email application on his laptop and then hits 'send'. His email application will pass his email message over to the application layer, which will pick a protocol (SMTP) and pass the data along to the presentation layer. The presentation layer will then compress the data and then it will hit the session layer, which will initialize the communication session.

The data will then hit the sender's transportation layer where it will be segmented, then those segments will be broken up into packets at the network layer, which will be broken down even further into frames at the data link layer. The data link layer will then deliver those frames to the physical layer, which will convert the data into a bitstream of 1s and 0s and send it through a physical medium, such as a cable.

Once Ms. Palmer's computer receives the bit stream through a physical medium (such as her wifi), the data will flow through the same series of layers on her device, but in the opposite order. First the physical layer will convert the bitstream from 1s and 0s into frames that get passed to the data link layer. The data link layer will then reassemble the frames into packets for the network layer. The network layer will then make segments out of the packets for the transport layer, which will reassemble the segments into one piece of data.

The data will then flow into the receiver's session layer, which will pass the data along to the presentation layer and then end the communication session. The presentation layer will then remove the compression and pass the raw data up to the application layer. The application layer will then feed the human-readable data along to Ms. Palmer's email software, which will allow her to read Mr. Cooper's email on her laptop screen.

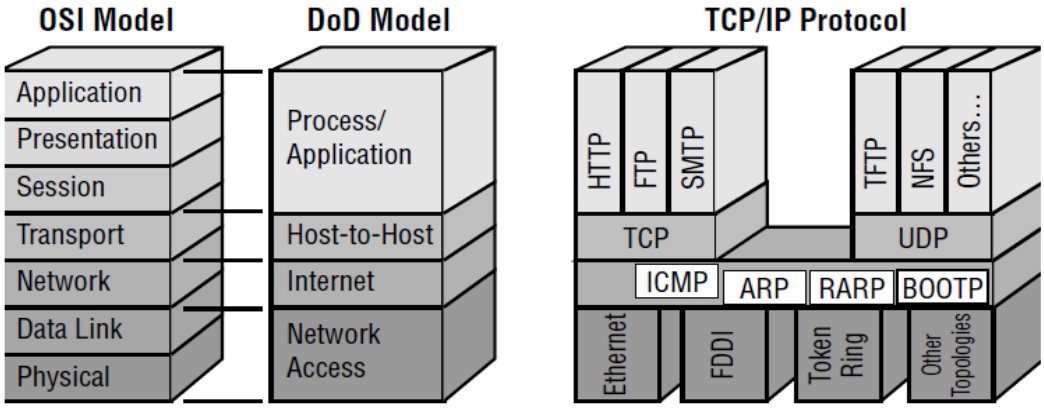
Advantages of the OSI Model

The advantages of the OSI Model are the following: -

- Help network administrators in determining the required hardware and software to build their network.
- Encourage hardware manufacturers to create networking products that can communicate with each other over the network.
- Provide a teaching tool to understand the communication process used between networking components.
- Separate a complex function into simpler components.
- Make troubleshooting easier, as network administrators can troubleshoot issues more quickly and effectively by looking in a layer that is causing the issue rather than finding it in the entire network.

TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL

As ISO was hammering out details of the OSI model, another network architecture that was already in place quietly continued to gain currency. The TCP/IP protocol suite, which was not created by standards-making organization but by a group of computer scientists, incorporates the TCP and IP protocols and has in fact always been more popular than the OSI model. The TCP/IP protocol suite does not have rigidly defined layers as the OSI model does, some textbooks describe five TCP/IP layers, while other describe four.



- **Application layer** – This layer is equivalent to OSI's application and presentation layers. Frequently used applications include File Transfer Protocol, Telnet, Simple mail Transfer protocol, Simple Network Management, and Hypertext Transfer Protocol. All these applications will be discussed in the later unit of this course.
- **Transport layer** – This layer is equivalent to OSI's transport layer. This layer commonly uses the TCP to maintain an error-free end-to-end connection. User

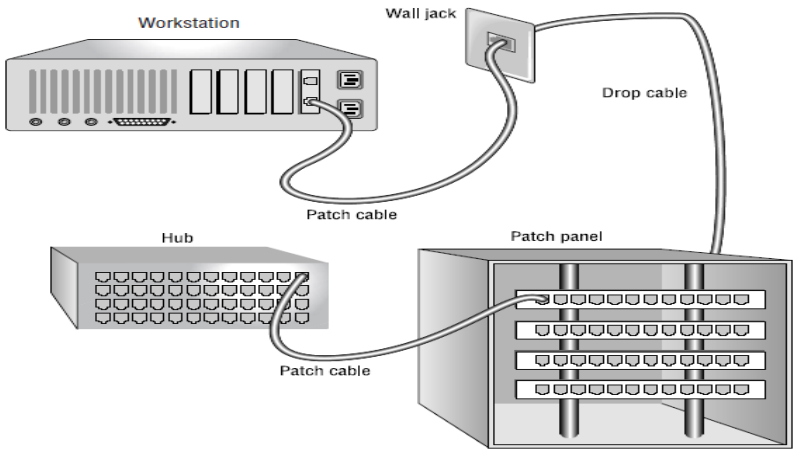
datagram protocol is an alternative that is also used, though less frequently, in the TCP/IP protocol suite.

- **Network (Internet or internetwork) layer** – This layer is equivalent to OSI's network layer. The protocol that is used at this layer to transfer data within and between networks is the Internet Protocol (IP).
- **Network access (data link/physical) laye**r – This layer is roughly equivalent to OSI's data link and physical layers.

NETWORK COMPONENTS

Now that we have discussed what you need to do before you install or upgrade, let's examine some of the components you may actually be installing.

In this section, we'll look at a typical UTP (unshielded twisted-pair) installation to illustrate the components that connect a LAN. Figure below shows some of these components. Notice that the only hard-wired cables (those you can't simply unplug) run from the wall jack to the patch panel. The workstation connects to the cable run through the wall jack via a patch cable, which is usually less than 3 meters (about 10 feet). Also, the hub connects to the patch panel with multiple patch cables (although in the Figure below, only one cable is shown to illustrate a single connection from end to end). In addition to the components shown in the figure below, we will also discuss some of the network connectivity devices you will need when installing the network.



Patch Panel

A *patch panel* is a central wiring point for multiple devices on a UTP network and itself contains no electronic circuits. The following advantages are associated with using a patch panel:

- Upgrading is easier.
- Troubleshooting is easier.
- You can avoid physical damage to the cable since it isn't necessary to move it when you upgrade the network.

When you use a patch panel on a UTP network, you connect components with patch cables. A *patch cable* is any cable that connects one network device to the main cable. For example, patch cables can connect workstations to the main cable and connect the main cable through the patch panel to the hub. Instead of plugging the long run of cable directly into the hub, you connect it to a patch panel and then connect the patch panel port that represents that cable into the hub using a patch cable.

Be careful, though, because the total segment length of the network includes the patch cables at both ends. For example, let's say you are using Ethernet over UTP in the 10BaseT configuration. The maximum segment length is 100 meters (a little more than 300 feet). Thus, the maximum distance from hub to NIC can be 100 meters. Some people mistake this and put in a 100-meter cable run from patch panel to wall plate. They then install a 10-meter workstation to wall-plate patch cable and a 3-meter patch panel to hub patch cable. This brings the total distance to 113 meters, and the workstation using that cable run may not be able to communicate correctly with the rest of the network.

The Repeater

A *repeater* amplifies (or repeats) network signals to extend the maximum reach of a network. Repeaters receive network signals on one port, amplify them, and repeat them out the other port. Since they operate only at the Physical layer of the OSI model, repeaters can interconnect different media types but cannot convert protocols.

The main purpose of a repeater is to extend the maximum distance of a single network segment. Let's say you have a workstation that is 150 meters (about 450 feet) from a hub. If your network is 10BaseT Ethernet, you won't be able to connect the workstation directly to the hub because the distance between the hub and the workstation is longer than the maximum segment length of 10BaseT Ethernet (100 meters). For this reason, you place a repeater about 50 to 100 meters between the two.

If it's practical, you could also move the hub. But since hubs are usually close to where all wires come together, this is often neither the best nor the most practical solution.

A repeater is the least expensive of all network devices, but since a repeater can do nothing to segment network traffic, it does little to decrease network traffic. A repeater can actually do more harm than good because it propagates everything, including noise and error packets.

The Hub

A *hub*, is the central device in a star topology. Hubs are most commonly used in 10BaseT or 100BaseT Ethernet networks. Most hubs are simple multiport repeaters. That is, they receive a signal on one port and repeat it to all other ports. As with repeaters, though, they also repeat any noise or corrupt signals to all ports.

There are three types of hubs:

- A *passive hub* simply makes physical, electrical connections between all incoming cables and stations so that stations can communicate. Because they don't do any repeating, passive hubs don't require power. ARCNet is an example of a topology that uses passive hubs.
- An *active hub* is powered and contains circuitry to amplify the network signals it receives. Active hubs are used most often in UTP installations of Ethernet (the most common method of cabling for Ethernet). The majority of hubs are active hubs.
- An *intelligent hub* is really a subtype of active hub. All intelligent hubs are active, but not all active hubs are intelligent. An intelligent hub is any hub that contains special features for management and configuration.

Many hubs today can manage individual ports, collect traffic statistics, and power up/power down from a remote station on the network. These features make an intelligent hub more complex and, thus, more expensive.

When you install a hub, you simply plug patch cables from the patch panel into the ports on the hub. These hub–to–patch-panel patch cables are typically very short (less than 1 meter, or about 3 feet). If you have an intelligent hub, you may be able to configure ports to be active or inactive using special hub-configuration software.

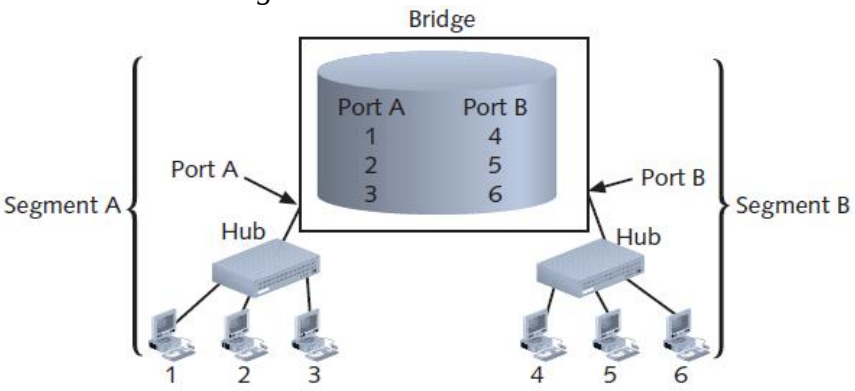
A stand-alone hub

The Bridge

A *bridge* is a network device that logically separates a single network into two segments. The primary use for a bridge is to keep traffic meant for stations on one segment on that side of the bridge and not let that traffic pass to the other side. It does this by creating a table of MAC (media access control) addresses of all stations, indicating which stations are on which segment.

When the bridge receives an incoming packet, it examines the MAC address, determines which segment that station is on, and sends the packet only to that segment.

If power to a bridge is lost, the MAC address table is lost, requiring a rebuild when power is restored. Working at the Data Link layer of the OSI model (IEEE MAC sublayer), a bridge knows nothing about protocols and simply passes packets to the correct segment. Bridges can improve network performance because traffic is not propagated unnecessarily on all network segments. It is possible to create a bridge by placing two NICs in one computer. This is commonly called an *internal bridge.*



A bridge's use of a filtering database

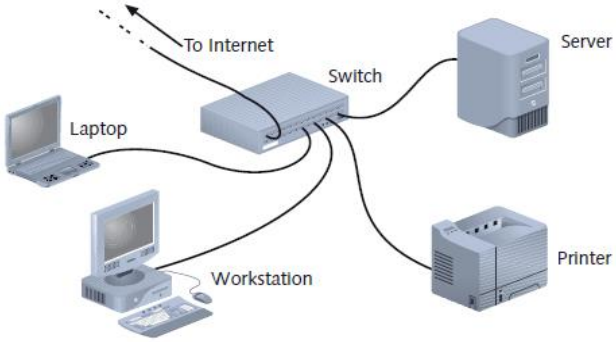
SWITCHES

Switches are connectivity devices that subdivide a network into smaller logical pieces, or segments. Traditional switches operate at the Data Link layer of the OSI model, while more modern switches can operate at Layer 3 or even Layer 4. As with bridges, switches interpret MAC address information. In fact, they can be described as multiport bridges. Figure 6-16 depicts two switches. On the right is a 24-port switch, useful for connecting nodes in a workgroup, and on the left is a high-capacity switch that contains multiple redundant features (such as two NICs) and offers security, automated traffic management, and even routing functions.

Switches vary greatly in size and function, so there's no such thing as a "typical" switch. Most switches have at least an internal processor, an operating system, memory, and several ports that enable other nodes to connect to it.

Because they have multiple ports, switches can make better use of limited bandwidth and prove more cost-efficient than bridges. Each port on the switch acts like a bridge, and each device connected to a switch effectively receives its own dedicated channel. In other words, a switch can turn a shared channel into several channels. From the Ethernet perspective, each dedicated channel represents a collision domain. Because a switch limits the number of devices in a collision domain, it limits the potential for collisions.

Switches



A switch on a small network

The Router

Routers connect logical networks and provide a way for data to move between those networks. A router is more like a special-purpose computer than a simple electronic device. The classic definition of a router is a device that reads the source and destination address of a packet and forwards it based on the information it gathers about the network. Routers can make intelligent decisions about the best way to forward packets, based on Network layer information. These decisions are based primarily on *hop count* (also referred to as *cost*). A hop occurs each time a packet traverses a router to get from one network to another. Hop count is established through communication with other routers. The router chooses the route with the lowest hop count to the packet's destination. If a link in the network is down, the router may choose a route that does not have the lowest hop count.

You usually configure a router via a serial port connection to a computer that contains configuration software. Others may use a command-line interface and require either a terminal or PC-emulated terminal for configuration.

Some routers are expandable with plug-in modules. These expansion modules allow you to make a router that uses any of the different types of port configuration, including Ethernet,

Token Ring, FDDI (Fiber Distributed Data Interface), ATM (Asynchronous Transfer Mode), and any other network topology.

ROUTER FUNCTIONS

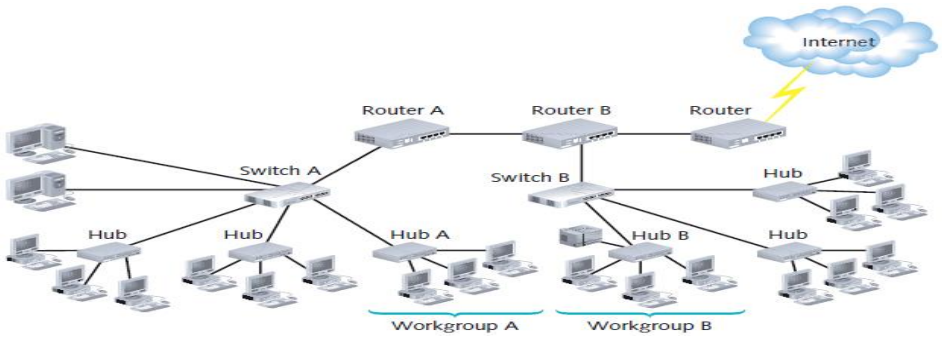
A router is a very flexible device. Although any one can be specialized for a variety of tasks, all routers can do the following:

- Connect dissimilar networks.
- Interpret Layer 3 addressing and other information (such as quality of service indicators).
- Determine the best path for data to follow from point A to point B.
- Reroute traffic if a primary path is down but another path is available.

In addition to performing these basic functions, routers may perform any of the following optional functions:

- Filter out broadcast transmissions to alleviate network congestion.
- Prevent certain types of traffic from getting to a network, enabling customized segregation and security.
- Support simultaneous local and remote connectivity.
- Provide high network fault tolerance through redundant components such as power supplies or network interfaces.

Routers



The placement of routers on a LAN

ROUTING

Routing is used for taking a packet from one device and sending it through the network to another device on a different network. If your net work has no routers, then you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:

- Destination address.
- Neighbor routers from which it can learn about remote networks.
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table that describes how to find the remote networks. If the network is directly connected, then the router already knows how to get to the network. If the networks are not attached, the router must learn how to get to the remote network with either ***static routing,*** which means that the administrator must hand-type all network locations into the routing table, or use dynamic routing. ***Dynamic routing*** is the process of routing protocols running on the router communicating with neighbor routers. The routers then update each other about all the networks they know about. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the change. If static routing is used, the administrator is responsible for updating all changes by hand into all routers.

PROTOCOLS

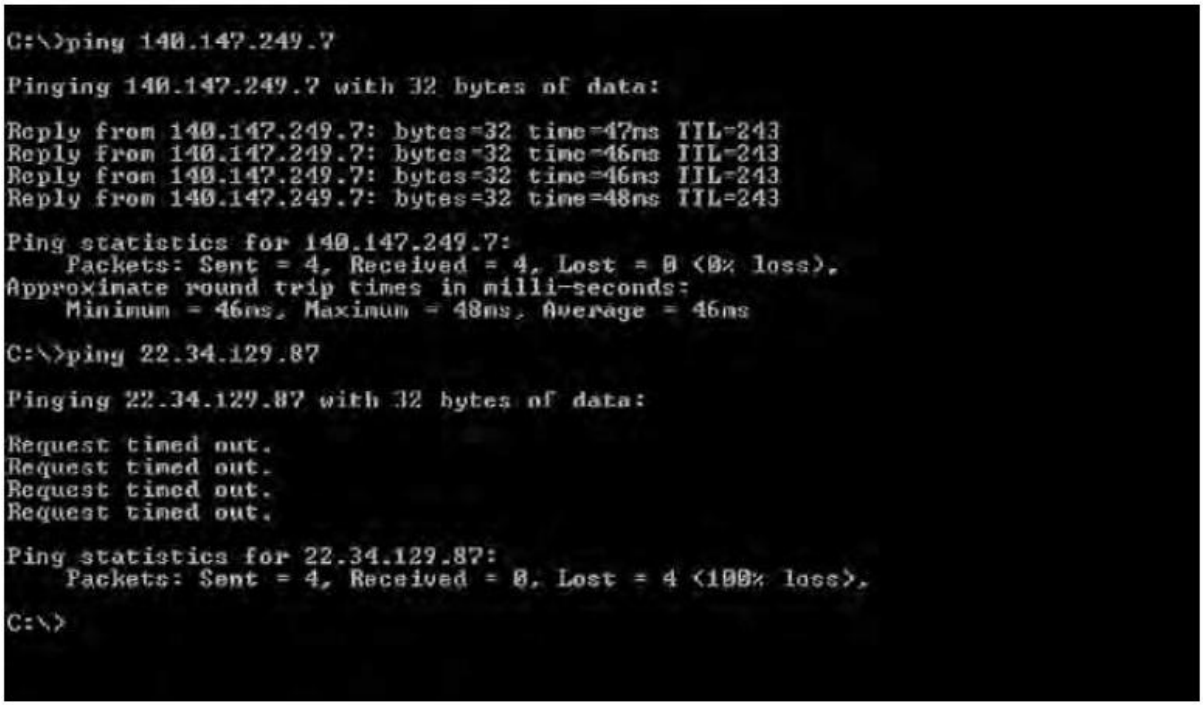
PING (Packet Internet Groper)

PING (Packet Internet Groper) is a utility that can verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating with the network. It is often employed simply to determine whether a host is responding (or "up"). PING uses ICMP services to send echo request and echo reply to messages that determine the validity of an IP address.

These two types of messages work in much the same way that sonar operates. First, a signal, called an echo request, is sent out to another computer. The other computer then rebroadcasts the signal, in the form of an echo reply, to the sender. The process of sending this signal back and forth is known as pinging.

You can ping either an IP address or a host name. For example, to determine whether the www.loc.gov site is responding, you could type ping www.loc.gov and press Enter. Alternately, you could type ping 140.147.249.7 (the IP address of this site at the time this book was written) and press Enter. If the site is operating correctly, you receive a response that includes multiple replies from that host. If the site is not operating correctly, you will receive a response indicating that the request timed out or that the host was not found. You could also receive a "request timed out" message if your workstation is not properly connected to the network, or if the network is malfunctioning. Figure below gives examples of a successful and an unsuccessful ping test.

By pinging the loopback address, 127.0.0.1, you can determine whether your workstation's TCP/IP services are running. By pinging a host on another subnet, you can determine whether the problem lies with a connectivity device between the two subnets.



Output from successful and unsuccessful PING tests

TELNET

Telnet is a terminal emulation protocol used to log on to remote hosts using the TCP/IP protocol suite. Using Telnet, a TCP connection is established and keystrokes on the user's machine act like keystrokes on the remotely connected machine. Often, Telnet is used to connect two dissimilar systems (such as PCs and UNIX machines). Through Telnet, you can control a remote host over LANs and WANs such as the Internet. For example, network managers can use Telnet to log on to a router from a computer elsewhere on their LAN and modify the router's configuration. Telnet, however, is notoriously insecure (meaning that someone with malicious intent could easily falsify the credentials Telnet requires to log on to a device successfully), so telnetting to a router across a public network would not be wise. Other, more secure methods of remotely connecting to a host have replaced Telnet for that reason.

FTP (File Transfer Protocol)

FTP (File Transfer Protocol) is an application layer protocol used to send and receive files via TCP/IP. In FTP exchanges, a host running the FTP server portion accepts commands from another host running the FTP client portion. FTP clients come with a set of simple commands that make up its user interface. To exchange data, the client depends on an FTP server that is always waiting for requests. After a client connects to the FTP server, FTP data is exchanged via TCP, which means that FTP provides some assurance of delivery.

TFTP (Trivial File Transfer Protocol)

TFTP (Trivial File Transfer Protocol) is another TCP/IP Application layer protocol that enables file transfers between computers, but it is simpler (or more trivial) than FTP. A significant difference between FTP and TFTP is that TFTP relies on UDP at the Transport layer. Its use of UDP means that TFTP is connectionless and does not guarantee reliable delivery of data. Also, TFTP does not require users to log on to the remote host with an ID and password in order to gain access to a directory and transfer files. Instead, when you enter the TFTP command, your computer issues a simple request to access the host's files.

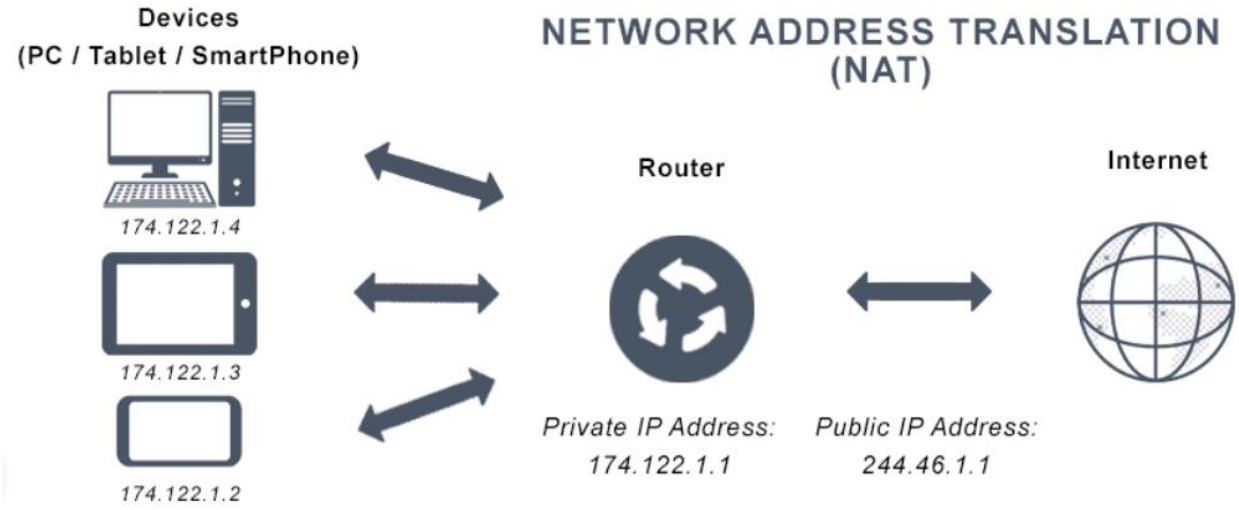
Difference and similarities of FTP and TFTP

NTP (Network Time Protocol)

NTP (Network Time Protocol) is a simple Application layer protocol used to synchronize the clocks of computers on a network. NTP depends on UDP for Transport layer services. Although it is simple, it is also important. Time is critical in routing to determine the most efficient path for data over a network. Time synchronization across a network is also important for time-stamped security methods and maintaining accuracy and consistency between multiple storage systems. NTP is a protocol that benefits from UDP's quick, connectionless nature at the Transport layer. NTP is time sensitive and cannot wait for the error checking that TCP would require.

Network Address Translation Definition

Network Address Translation (NAT) is a process that enables one, unique IP address to represent an entire group of computers. In network address translation, a network device, often a router or NAT firewall, assigns a computer or computers inside a private network a public address. In this way, network address translation allows the single device to act as an intermediary or agent between the local, private network and the public network that is the internet. NAT's main purpose is to conserve the number of public IP addresses in use, for both security and economic goals.



What is Network Address Translation?

Network Address Translation (NAT) conserves IP addresses by enabling private IP networks using unregistered IP addresses to go online. Before NAT forwards packets between the networks it connects, it translates the private internal network addresses into legal, globally unique addresses.

NAT configurations can reveal just one IP address for an entire network to the outside world as part of this capability, effectively hiding the entire internal network and providing additional security. Network address translation is typically implemented in remote-access environments, as it offers the dual functions of address conservation and enhanced security.

What is the Purpose of NAT?

To communicate with the internet, a networking system requires a unique IP address. This 32-bit number identifies and locates the network device so a user can communicate with it.

The IPV4 addressing scheme of past decades technically made billions of these unique addresses available, but not all could be assigned to devices for communication. Instead, some were exempted and used for testing, broadcast, and certain reserved military purposes. While that left over 3 billion for communication, the proliferation of the internet has meant the addresses were near exhaustion.

The IPv6 addressing scheme was introduced as the solution to this weakness in the IPv4 addressing scheme. IPv6 recreates the addressing system so there are more options for allocating addresses, but it has taken several years to alter the networking system infrastructure and to implement. NAT was introduced by Cisco in the meantime and widely deployed.

How Does NAT Work?

Let's say that there is a laptop connected to a home network using NAT. That network eventually connects to a router that addresses the internet. Suppose that someone uses that laptop to search for directions to their favorite restaurant. The laptop is using NAT. So, it sends this request in an IP packet to the router, which passes that request along to the internet and the search service you're using. But before your request leaves your home network, the router first changes the internal IP address from a private local IP address to a public IP address. Your router effectively translates the private address you're using to one that can be used on the internet, and then back again. Now you know that your humble little cable modem or DSL router has a little, automated translator working inside of it.

If the packet keeps a private address, the receiving server won't know where to send the information back to. This is because a private IP address cannot be routed onto the internet. If your router were to try doing this, all internet routers are programmed to automatically drop private IP addresses. The nice thing is, though, that all routers sold today for home offices and small offices can readily translate back and forth between private IP address and publicly-routed IP addresses.

NAT Types

There are three different types of NATs. People and organizations use them for different reasons, but they all still work as a NAT.

Static NAT

When the local address is converted to a public one, this NAT chooses the same one. This means there will be a consistent public IP address associated with that router or NAT device.

Dynamic NAT

Instead of choosing the same IP address every time, this NAT goes through a pool of public IP addresses. This results in the router or NAT device getting a different address each time the router translates the local address to a public address.

PAT

PAT stands for port address translation. It's a type of dynamic NAT, but it bands several local IP addresses to a singular public one. Organizations that want all their employees' activity to use a singular IP address use a PAT, often under the supervision of a network administrator.

Advantages of NAT

1. **Address conservation.** NAT conserves IP addresses that are legally registered and prevents their depletion.
2. **Network address translation security.** NAT offers the ability to access the internet with more security and privacy by hiding the device IP address from the public network, even when sending and receiving traffic. NAT rate-limiting allows users to limit the maximum number of concurrent NAT operations on a router and rate limit the number of NAT translations. This provides more control over the use of NAT addresses, but can also be used to limit the effects of worms, viruses, and denial-of-service (DoS) attacks. Dynamic NAT implementation creates a firewall between the internal network and the internet automatically. Some NAT routers offer traffic logging and filtering.
3. **Flexibility.** NAT provides flexibility; for example, it can be deployed in a public wireless LAN environment. Inbound mapping or static NAT allows external devices to initiate connections to computers on the stub domain in some cases.
4. **Simplicity.** Eliminates the need to renumber addresses when a network changes or merges. Network address translation allows you to create an inside network virtual host to coordinate TCP load-balancing for internal network servers.
5. **Speed.** Compared to proxy servers, NAT is transparent to both destination and source computers, allowing for quicker direct dealing. In addition, proxy servers typically work at the transport layer or layer 4 of the OSI Reference Model or higher, making them slower than network address translation, which is a network layer or layer 3 protocol.
6. **Scalability.** NAT and dynamic host configuration protocol (DHCP) work well together, with the DHCP server doling out unregistered IP addresses for the stub domain from the list as necessary. Scaling up is easier, since you can increase the available range of IP addresses the DHCP configures to make room for additional network computers immediately instead of requesting more IP addresses from IANA as needs increase.
7. **Multi-homing.** Multiple connections to the internet, called multi-homing, helps maintain a reliable connection and reduces the chance of a shutdown in case of a failed connection. This also enables load-balancing via reducing the number of computers using any single connection. Multi-homed networks often connect to multiple ISPs, each assigning a range of IP addresses or a single IP address to the organization.

Disadvantages of NAT

1. **Resource consumption.** Network address translation is a technology that consumes memory resources and processor space, because it must translate IPv4 addresses for all outgoing and incoming IPv4 datagrams and retain the details from translation in memory.
2. **Delays.** Path delays are caused by translation results in switching path delays. Functionality. Some applications and technologies will not function as expected with NAT enabled.
3. **Traceability.** Network address translation complicates protocols for tunneling. IPsec is the secure protocol recommended for network address translation.

4. **Layer issue.** A router is a device for the network layer, yet as a NAT device it is required to tamper with the transport layer in the form of port numbers.

ROUTING

Routing is used for taking a packet from one device and sending it through the network to another device on a different network. If your network has no routers, then you are not routing. Routers route traffic to all the networks in your internetwork. To be able to route packets, a router must know, at a minimum, the following:

- Destination address.
- Neighbor routers from which it can learn about remote networks.
- Possible routes to all remote networks.
- The best route to each remote network.
- How to maintain and verify routing information.

The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table that describes how to find the remote networks. If the network is directly connected, then the router already knows how to get to the network. If the networks are not attached, the router must learn how to get to the remote network with either *static routing*, which means that the administrator must hand-type all network locations into the routing table, or use dynamic routing. *Dynamic routing* is the process of routing protocols running on the router communicating with neighbor routers. The routers then update each other about all the networks they know about. If a change occurs in the network, the dynamic routing protocols automatically inform all routers about the change. If static routing is used, the administrator is responsible for updating all changes by hand into all routers.

Static Routing

Static routing is the process of an administrator manually adding routes in each router's routing table. There are benefits and disadvantages to all routing processes.

Static routing has the following benefits:

- No overhead on the router CPU
- No bandwidth usage between routers
- Security (because the administrator only allows routing to certain networks)

Static routing has the following disadvantages:

- The administrator must really understand the internetwork and how each router is connected to configure the routes correctly.
- If one network is added to the internetwork, the administrator must add a route to it on all routers.
- It's not feasible in large networks because it would be a full-time job.

Default Routing

Default routing is used to send packets with a remote destination network not in the routing table to the next hop router. You can only use default routing on stub networks, which means that they have only one exit port out of the network.

Dynamic Routing

Dynamic routing is the process of using protocols to find and update routing tables on routers. This is easier than static or default routing, but you use it at the expense of router CPU processes and bandwidth on the network links. A routing protocol defines the set of rules used by a router when it communicates between neighbor routers.

The routing protocols are Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP).

Routing Protocols

There are three classes of routing protocols:

Distance vector: The distance-vector routing protocols use a distance to a remote network to find the best path. Each time a packet goes through a router, it's called a hop. The route with the least number of hops to the network is determined to be the best route. The vector is the determination of direction to the remote network. Examples of distance-vector routing protocols are RIP and IGRP.

Link state: Typically called shortest path first, the routers each create three separate tables. One of these tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used for the routing table. Link-state routers know more about the internetwork than any distance-vector routing protocol. An example of an IP routing protocol that is completely link state is OSPF.

Hybrid Uses aspects of distance vector and link state, for example, EIGRP.

There is no set way of configuring routing protocols for use with every business. This is a task that is performed on a case-by-case basis. However, if you understand how the different routing protocols work, you can make good business decisions. This course and equivalent exam only cover distance-vector routing protocols and theory.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) is an automated means of assigning a unique IP address to every device on a network. DHCP, like BOOTP, belongs to the Application layer of the OSI model. It was developed by the IETF as a replacement for BOOTP. DHCP operates in a similar manner to BOOTP, but unlike BOOTP, DHCP does not require the network administrator to maintain a table of IP and MAC addresses on the server. Thus, the administrative burden of running DHCP is much lower. DHCP does, however, require the network administrator in charge of IP address management to install and configure the DHCP service on a DHCP server.

Reasons for implementing DHCP include the following:

- To reduce the time and planning spent on IP address management—Central management of IP addresses eliminates the need for network administrators to edit the TCP/IP configuration on every network workstation, printer, or other device.
- To reduce the potential for errors in assigning IP addresses—With DHCP, almost no possibility exists that a workstation will be assigned an invalid address or that two workstations will attempt to use the same IP address. (Occasionally, the DHCP server software may make a mistake.)
- To enable users to move their workstations and printers without having to change their TCP/IP configuration—As long as a workstation is configured to obtain its IP address from a central server, the workstation can be attached anywhere on the network and receive a valid address.
- To make IP addressing transparent for mobile users—A person visiting your office, for example, could attach to your network and receive an IP address without having to change his laptop's configuration.

Will there be a problem in a network where there are statically and dynamically assigned IP addresses?

DHCP (Dynamic Host Configuration Protocol) is an automated means of assigning a unique IP address to every device on a network.

There is nothing wrong with having both static and dynamic IP addresses on the same network; as long as you make sure the static IP address is not overlapping the DHCP server's address pool, is in the same subnet, and you have specified the correct Default gateway and DNS addresses to match the dynamic connections.

If a static IP address is assigned inside the range of the DHCP server's address pool in the router, or is assigned outside the address pool but not in the same subnet, you could have a problem.

A network administrator might separate traffic to accomplish the following:

1. **Enhance security**—Subnetworks must be connected via routers or other Layer 3 devices. As you know, these devices do not retransmit incoming frames to all other nodes on the same segment (as a hub does). Instead, they forward frames only as necessary to reach their destination. Because every frame is not indiscriminately retransmitted, the possibility for one node to tap into another node's transmissions is reduced.
2. **Improve performance**—For the same reason that subnetting enhances security, it also improves performance on a network. When data is selectively retransmitted, unnecessary transmissions are kept to a minimum. Subnetting is useful for limiting the amount of broadcast traffic—and, therefore, the number of potential collisions on Ethernet networks—by decreasing the size of each broadcast domain. The more efficient use of bandwidth results in better overall network performance.
3. **Simplify troubleshooting**—For example, a network administrator might subdivide an organization's network according to geography, assigning a separate subnet to the nodes in the downtown office, west-side office, and east-side office of her company. Suppose one day the network has trouble transmitting data only to a certain group of 10 1.4 Designing TCP/IP-Based Networks 487 IP addresses—those located on the

west-side office subnet. When troubleshooting, rather than examining the whole network for errors or bottlenecks, the network administrator needs only to see that the faulty transmissions are all associated with addresses on the west-side subnet to know that she should zero in on that subnet.

TCP (TRANSMISSION CONTROL PROTOCOL)

TCP (Transmission Control Protocol) operates in the Transport layer of the OSI model and provides reliable data delivery services. TCP is a connection-oriented sub-protocol, which means that a connection must be established between communicating nodes before this protocol will transmit data. TCP further ensures reliable data delivery through sequencing and checksums. Without such measures, data would be transmitted indiscriminately, without checking whether the destination node was offline, for example, or whether the data became corrupt during transmission. Finally, TCP provides flow control to ensure that a node is not flooded with data.

TCP THREE-WAY HANDSHAKE.

One of the reasons why TCP is reliable and secure is because it is a connection-oriented protocol. This mean that before two hosts can exchange messages, that there must be "a mutual agreement" between the transmitter and the receiver on the terms (e.g., Windowing, Rate of transmission) of transmission before message(s) are sent.
For the three-way handshake to take place, according to figure below, initially, user A sends a SYN request to any other system (Server B) on the network it wants to exchange message with. The other system (Server B) will communicate back with a SYN/ACK if it is able to allow the request. When the user A receives the SYN/ACK from the second system, it responds with an ACK packet, and the communication between the two systems can proceed. As shown in figure 2:

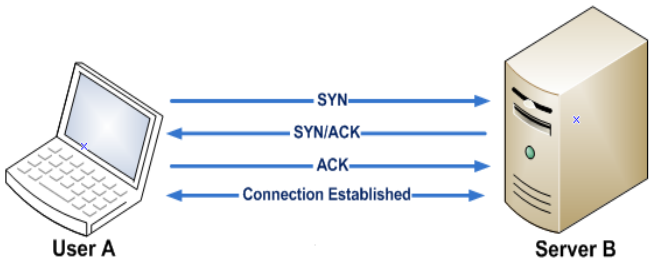


Figure 2: The TCP three-way handshake

UDP (USER DATAGRAM PROTOCOL)

UDP (User Datagram Protocol), like TCP, belongs to the Transport layer of the OSI model. Unlike TCP, however, UDP is a connectionless transport service. In other words, UDP offers no assurance that packets will be received in the correct sequence. In fact, this protocol does not guarantee that the packets will be received at all. Furthermore, it provides no error checking or sequencing. Nevertheless, UDP's lack of sophistication makes it more efficient than TCP. It can be useful in situations in which a great volume of data must be transferred quickly, such as live audio or video transmissions over the Internet. In these cases, TCP—with its acknowledgments, checksums, and flow control mechanisms—would only add more overhead

to the transmission. UDP is also more efficient for carrying messages that fit within one data packet.

THE SOFTWARE TOOL IS PING

Ping is undoubtedly the most frequent gadget in the network; it is mainly used to determine the network connectivity issues. The ping program uses the ICMP (Internet Message Control Protocol) protocol to simply send a network packet and request a response. The destination host receiving the request sends back the same data again using ICMP, so that ping can send and receive each packet time to report and report the percentage of packets without impact, which is useful in determining whether the network is properly connected and the status of the network connection (packet loss rate). Ping is one of the Windows operating system integrated TCP / IP applications that can be executed directly in 'Start-Run'

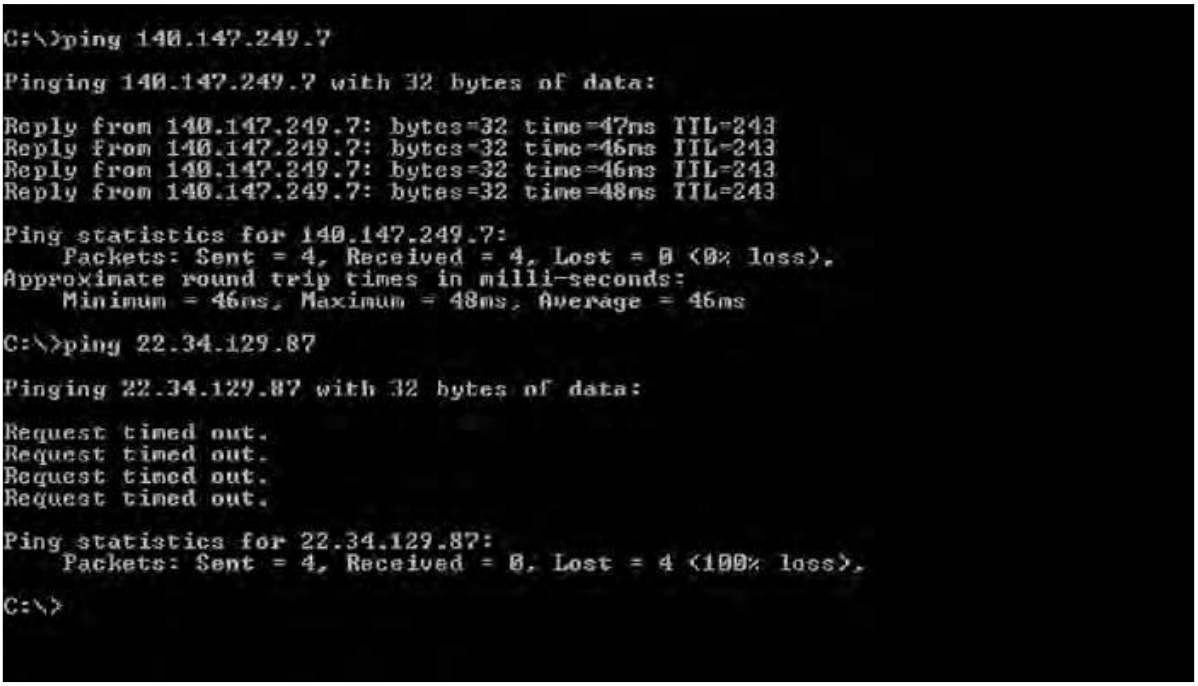
LOOPBACK ADDRESS: An IP address reserved for communicating from a node to itself (used mostly for troubleshooting purposes). The IPv4 loopback address is always cited as 127.0.0.1, although in fact, transmitting to any IP address whose first octet is 127 will contact the originating device. In IPv6, the loopback address is represented as:1.

LOOPBACK TEST: An attempt to contact one's own machine for troubleshooting purposes. In TCP/IP-based networking, a loopback test can be performed by communicating with an IPv4address that begins with an octet of 127. Usually, this means pinging the address 127.0.0.1.

Such as ping 127.0.0.1 (any computer will see 127.0.0.1 as its own IP address) You can check whether the computer has a network card installed; whether the correct installation of the TCP/IP protocol; correctly configured IP address and subnet mask or host name.

By pinging the loopback address, 127.0.0.1, you can determine whether your workstation's TCP/IP services are running. By pinging a host on another subnet, you can determine whether the problem lies with a connectivity device between the two subnets.

For example, suppose that you have recently moved your computer from the Accounting Department to the Advertising Department, and now you cannot access the Web. The first test you should perform is pinging the loopback address. If that test is successful, then you know that your workstation's TCP/IP services are running correctly. Next, you might try pinging your neighbor's machine. If you receive a positive response, you know that your network connection is working. You should then try pinging a machine on another subnet that you know is connected to the network



Output from successful and unsuccessful PING tests

Reference Books:

1. Network+ Study Guide. By David Groth
2. Introduction to Computer Security. Matt Bishop
3. Network+ Guide to Networks, Fifth Edition Tamara Dean
4. Network+ Study Guide Fourth Edition David Groth Toby Skandier