DATA COMMUNICATIONS AND COMPUTER NETWORKS

A local area network (LAN) is a specifically designed configuration of computers and other devices located within a confined area, such as a home or office building, and connected by wires or radio waves that permit the devices to communicate with one another to share data and services. Computers and other devices connected on a LAN can send and receive information from one another without confusion. Each device with an address that can be accessed to send or receive information is a node. A node can be a computer, a router, a printer, a video camera, a controller, or any number of other electronic devices. A host is always a computer. The network directs the communication passing through it and acts as a sort of electronic traffic cop to prevent collisions or mixing of data.

A LAN can be connected to the Internet, either through a direct cable connection or by a telephone link through a modem, so that workstations on the LAN have access to all the networks and sites linked to the global Web.

A host requires an operating system to manage its applications, hardware, and connection to the network. The operating system is also responsible for enabling the computers on the LAN to share their resources. The term resource refers to any files, databases, or printers installed on or attached to a host.

Basic network types

There are two basic types of networks that you'll encounter:

- **Peer-to-peer** network usually consists of several client computers that are connected to a network for simple file and printer sharing in a small office or home office. Each computer has a network card, which is connected to the network by a network cable or wireless network media. All the communication is between the client computers. There are often fewer than a dozen hosts on this type of network. Often times peer-to-peer network can be described as decentralized networking model—you must administer each user and computer on the network individually.

- **Client/server** network wherein computers called servers hold data and provide a wealth of services that users can share. Most of the communication on this type of network is between the client computers and the servers. Client/server networks scale much larger than peer-to-peer networks. A client/server network might also be described as a centralized networking model, because it enables users to administer computers and users as a group instead of individually.

Peer-to-peer model

In the peer-to-peer networking model, each host on the LAN has the same authority as other hosts. Each computer user is the administrator of his or her own computer and decides whether to share a resource on his or her computer (such as a file, database, or printer). The user is responsible for backing up data, installing software, sharing resources, enforcing security policies, and many other administrative tasks. All versions of Windows Vista, Windows XP, and Windows 2000 Professional are examples of client operating systems that support the peer-to-peer model.

In a peer-to-peer model, several hosts using different operating systems in a small business or home can be connected to form a small LAN.

A peer-to-peer network has no dedicated servers; instead, a number of workstations are connected together for the purpose of sharing information or devices. When there is no dedicated server, all workstations are considered equal; any one of them can participate as the client or the server. Peer-to-peer networks are designed to satisfy the

networking needs of home networks or of small companies that do not want to spend a lot of money on a dedicated server but still want to have the capability to share information or devices. For example, a small accounting firm with three employees that needs to access customer data from any of the three systems or print to one printer from any of the three systems may not want to spend a lot of money on a dedicated server. A small peer-to-peer network will allow these three computers to share the printer and the customer information with one another (see figure 1.1). The extra cost of a server was not incurred because the existing client systems were networked together to create the peer-to-peer network.

Most of the modern operating systems already have built-in peer-to-peer networking capabilities, which is why building a peer-to-peer network would be a "cheap" network solution. The disadvantage of a peer-to-peer network is the lack of centralized administration—with peer-to-peer networks, you need to build user accounts and configure security on each system.

It is important to note that peer-to-peer networks are designed for fewer than 10 systems, and with Microsoft client operating systems, only 10 concurrent network connections to those clients are allowed. This means that if you have 15 or 20 employees, you eventually will need to implement a server-based network.

Peer-to-peer authentication

In a peer-to-peer LAN consisting of Windows 2000 Professional, Windows 7, and Windows 8 computers, each user has his or her own computer and must enter his or her valid user ID and password to use the computer. If the user doesn't enter a valid user ID and password, he or she can't use the computer. The process of entering a correct user ID and password and gaining access to a computer is called authentication, validation, or logging on. In the peer-to-peer model, a user ID and password is authenticated by the local client operating system. All users have a user ID and password which allows them access only to their own computers. Using unique user IDs and passwords, they can't authenticate and gain access to someone else's computer. This is because their user accounts exist only on their own computers.

You can create additional local user accounts on a computer so that other users can access that computer's shared resources. A local user account is a collection of all the information that pertains to a user on a computer. This includes the user ID and password required for the user to authenticate and the permissions the user has for using and accessing resources on a computer. Individual users in a peer-to-peer model can make resources on their computers available to other network users.

Client/server model

A network operating system (NOS), such as Windows Server 2008 or 2003, Windows 2000 Server, UNIX, or Novell Open Enterprise Server or NetWare, can be installed on a server and used to manage network resources, including user accounts, printers, and file sharing across a LAN. User accounts are created on the NOS installed on a server. A trained system administrator is usually responsible for maintaining the server and NOS while managing resources to meet user needs. Users can authenticate and gain access to any host on the LAN by entering their single network user IDs and passwords. The user ID and password are authenticated against the NOS on the server instead of on each individual host.

In a client/server model, sometimes called a domain model, a server controls which resources on the LAN are shared and who can access these resources. In addition to creating user accounts in the NOS's directory, the system administrator assigns user permissions that control which resources users can access on the LAN. The server uses a database to store user account information, user permissions, security policies, printers, and other configuration settings. Software, files, printers, and other resources can be accessed by users on the LAN only when the system administrator has granted specific permission to a user account.

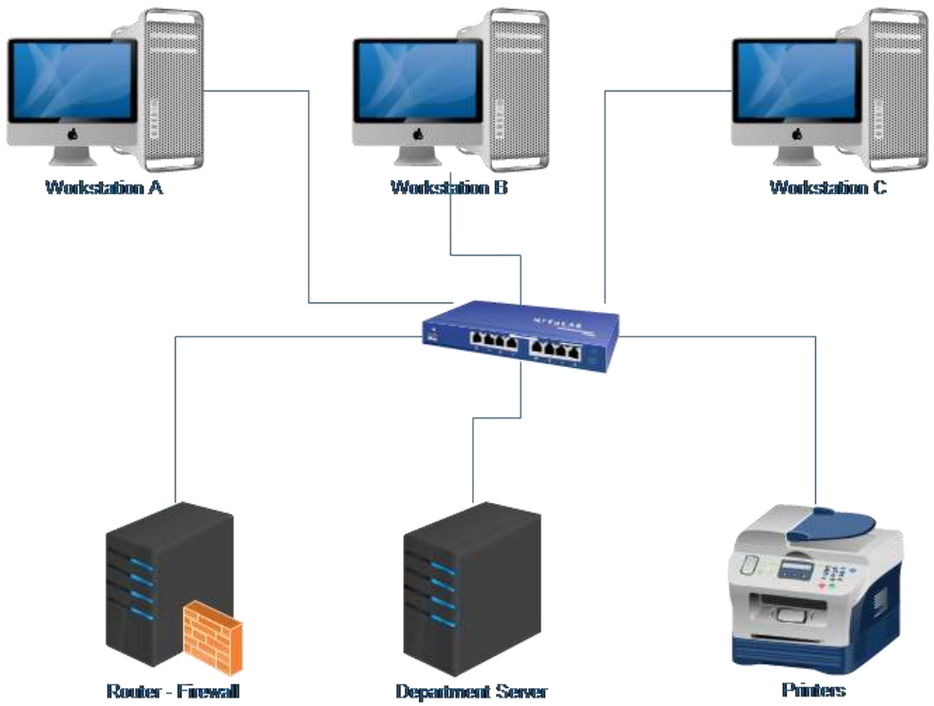

Figure 1.1 A sample Peer to Peer Network

In the client/server model, the local client operating system isn‘t responsible for authenticating user IDs and passwords. Instead, the client OS sends this information to the NOS on the server, which verifies the information based upon the information stored in its database. It does this by using a network client that‘s installed on the client computer. The network client is responsible for communicating with the NOS on the server.

In the client/server model, an administrator assigns users their own user IDs and passwords. This process, in turn, allows them to authenticate against the NOS and log on to access network resources (also called logging on to the network) to the computer and to the network resources.

If Novell Open Enterprise Server or NetWare is the NOS on the server and Windows 7 or Windows 8 is the client OS, the Novell Client for the client OS must be installed in order to serve as the network client. A server can be running Windows Server 2008 or 2003, or Windows 2000 Server as the NOS. In this case, the client OS (Windows 7, Windows 8) is used as the network client. Table 1.1 presents the comparison of the different networking model.

Table 1.1 Comparison of Networking Model

Attribute	Peer to Peer Network	Client/Server Network
Size	Recommended to a maximum of 10 computers	The size of the network is limited only by server size, network hardware, and budget. It can have thousands of connected systems.
Administration	Each individual is responsible for the administration of his or her own system. An administrator is not needed.	A skilled network administrator is often required to maintain and manage the network.
Security	Each individual is responsible for maintaining security for local files and devices connected to the system.	Security is managed from a central location but often requires a skilled administrator to correctly configure.
Cost	Minimal startup and implementation cost	Requires dedicated equipment and specialized hardware and administration, increasing the network’s cost.
Implementation	Easy to configure and set up.	Often requires complex setup procedures and skilled staff to set up.

Segments and backbones

Large networks are frequently broken down into manageable pieces called segments. A segment is the portion of the network on either side of two network transmission devices. Examples of network transmission devices include routers, bridges, repeaters, switches, and hubs. A network is segmented to extend allowable cable length, separate traffic to improve performance, and for security purposes.

Usually segments are connected directly to one another if they are in close proximity. In large buildings, or where the network spans more than one building, a backbone is constructed. The backbone is a high-speed network link connecting only segments (the nodes are connected to the segments). With this design, only data destined for another segment travels across the backbone. Preventing a data packet from traveling over the entire network is a key element in a well-designed network. Directing data over the shortest possible route to the destination increases network availability on those segments it doesn‘t need to travel across.

Network wiring

The computers in the network need a pathway to connect each other. This can be a physical connection of one type of wire or cabling or another. It can also be a connection through radio waves, infrared, or other wireless connection methods. Wiring is the heart of a network. It‘s also the part most vulnerable to performance problems caused by poor installation practices. Wiring in new construction is generally a straightforward process. Wiring in existing structures, whether done within the walls or on the surface, can be a frustrating experience. No network is better than the quality of the wiring on which it runs.

Fiber optic

Fiber optic cabling, which carries light-based data through strands of glass or plastic no thicker than a human hair, is currently the fastest and most expensive network transmission medium. Fiber optic cables are composed of a glass or a plastic strand through which light is transmitted. This core is clad in a glass tube designed to reflect the light back into the core, as the light bounces moving through the fiber core. An outer insulating, rubberized jacket covers the entire cable to protect it.

There are two types of fiber optic cable: single-mode fiber (SMF) and multi-mode fiber (MMF). Optic fibers which support many transmission (propagation) paths are referred to as multi-mode. Optic fibers which support only a single transmission path are single- mode. Multimode optic fibers generally have a large-diameter core, and are used for short distances, typically less than 300 meters. Fiber optic cable is used by the telephone and cable companies to deliver information across long distances. Fiber optic cabling is also used as the backbone for networks. For an end-user to use fiber optics, they must purchase conversion equipment that changes electrical impulses into photons. At present, the price of these devices is costly, but is certain to decline as the technology matures. This makes their widespread use in the future more likely.

Twisted pair

Until recently, most networks have used unshielded twisted pair (UTP) or shielded twisted pair (STP) cabling to connect the nodes in the network. Both types of cable are composed of four pairs of wires. The wires in each pair are twisted around each other, and the pairs are twisted together and bundled within a covering. The two wires (two halves of a single circuit) are wound together in order to cancel out electromagnetic interference (EMI) from external sources.

UTP cable comes in categories. Each category has a specific use, number of twists per foot, and speed. The more twists, the less crosstalk and electrical magnetic interference (EMI) affects the data on the cable. For networking, Cat3 cable used to be acceptable. However, Cat3 operates at up to only 10 Mbps with about two or three twists per foot. Most networks now use at least Cat5 cable, which operates at up to 100 Mbps, or Cat5e, which operates at up to 1 Gbps. Cat5 and Cat5e cables have 20

twists per foot. Cat6 cables use higher quality materials and have the potential to operate at up to 2.5 Gbps. The number of twists in Cat6 cable can vary. All twisted pair cabling has a maximum run length of approximately 100 meters. There is also a Cat6a cable that provides performance of up to 10Gbps. Cat7 is an emerging standard.

For the best wiring value and expansion capability, use composite cable, which combines Cat5 or Cat6 and other transmission cables within a single PVC jacket. It makes multiple-wire installation easier and saves on the cost of future wiring. Some of these cables contain two Cat5 or Cat6 wires for the network and two shielded RG-6 coaxial cables for cable and satellite television. The top-of-the-line, −future-proof‖ version of this type of cable contains Cat5 or Cat6 and RG-6 wires, and a fiber optic line—the fastest available transmission medium.

Coaxial

Coax cables contain a layer of braided wire or foil between the core and the outside insulating layer. The shielding provided by this layer helps protect the data from EMI problems. Another layer of plastic or rubberized material separates the central core from the shielding layer since, if these two layers touch, the data signal is damaged or lost. The type used for Ethernet networking is marked RG-58,. It‘s important that you don‘t mistake RG-59 cable for RG-58. RG-59 coaxial cable is used for low-power video and RF signal connections. You‘ll find it shipped with consumer electronic equipment, such as VCRs or digital cable and satellite receivers. In recent years, RG-6 type cables have become the standard for cable TV, replacing the smaller RG-59. RG-6 cables are most commonly used to deliver cable television signals to and within homes, and also aren‘t suitable for networking.

Thicknet cables are RG-8 or RG-11 cables. RG-8 cables, are 50- ohm stranded core cables, and RG-11 are 75-ohm solid core cables with dual shielding (foil and braided wires). Neither RG-8 nor RG-11 bends easily, because both are 10 mm in diameter (four-tenths of an inch). These cables can carry signals up to about 500 meters, so they‘re typically used for Ethernet network backbones rather than for drops to network nodes.

Thin Ethernet designs, wired with RG58/U coaxial cable, are limited by the attenuation (weakening due to distance travelled) of signals in the cable and can support network segments up to only 185 meters long. Thick Ethernet designs, wired with 50-ohm RG8/U coaxial, are more resistant to attenuation and can span up to 500 meters. Neither of these is being widely used now, because more advanced cable types can span distances up to 1,000 meters with less attenuation of network signals.

Serial

Using the serial ports on two computers, you can create a direct cable connection between two computers by using a single cable rather than a modem or other network interface device. In most cases, you make a direct cable connection with a null modem cable—a serial cable with RS-232 connectors on either end. Typical serial connectors are either 9-pin, or 25-pin. A null modem cable differs from ordinary serial cables in that the transmit and receive lines on the ends are reversed to enable direct two-way communication.

Duplex

Data is transmitted as simplex, half-duplex, or full-duplex. In simplex, data is transmitted in a single direction. In half-duplex, data is transmitted across the medium in both directions, but only in one direction at a time. In full-duplex, data can be transmitted across the medium in both directions at the same time. Network transmissions can be either half-duplex or full-duplex, although the majority are half-duplex.

- Simplex mode allows for one-way communication of data through the network, with the full bandwidth of the cable being used for the transmitting signal. One-way communication is of little use on LANs, making it unusual at best for network implementations.
- Far more common is half-duplex mode, which accommodates transmitting and receiving on the network, but not at the same time. Many networks are configured for half-duplex communication.

- The preferred dialog mode for network communication is full-duplex mode. To use full duplex, both the network card and the hub or switch must support full duplexing. Devices configured for full duplexing can transmit and receive simultaneously. This means that 100Mbps network cards theoretically can transmit at 200Mbps using full-duplex mode.

Wireless LAN

Wireless LAN (WLAN) technology uses radio waves or infrared light instead of cables to connect network nodes. Connections are made using a wireless NIC, which includes an antenna to send and receive signals. WLANs are popular in places where networking cables are difficult to install, such as outdoors or in a historic building with wiring restrictions, or where there are many mobile users, such as on a college campus.
Wireless devices can communicate directly (for example, a handheld device communicating with a computer via an infrared connection), or they can connect to a LAN by way of a wireless access point (WAP). Access points are placed so that nodes can access at least one access point from anywhere in the covered area. When devices use an access point, they communicate through the access point instead of communicating directly.

Benefits/drawbacks of wireless networks

The benefits of WLAN technology are many. The most obvious benefit is the increased flexibility and mobility that‘s created when using WLANs. Employees can move freely around the organization without disconnection from the network. Examples of how wireless networking can benefit an organization include the following:

- Inventory is more convenient when employees can freely walk around the warehouse or organization.
- Portable devices such as personal digital assistants (PDAs) and Tablet PCs can be used in hospital wards to track patients and doctor visits.
- Mobile workers moving between offices and telecommuters coming into the office can easily connect to the LAN from almost anywhere.
- Online information is always available for research or information retrieval.
- Production on manufacturing shop floors can be readily evaluated.
- Wireless network infrastructure can be moved to a new building more easily.
- The cost of providing network access to buildings is substantially lowered.

Although WLANs have some obvious advantages in places where running cables would be difficult or expensive, WLANs tend to be slower than wired networks, especially when they‘re busy. Another problem with WLANs is security. Companies are reluctant to use them when it‘s possible for an unauthorized person with a receiving device to intercept wireless LAN transmissions. Security on a WLAN is accomplished by filtering the MAC addresses of wireless NICs that are allowed to use the access point and by encrypting data sent over the wireless LAN.

Network protocols

Network protocols are the languages that computers, servers, and network devices use to communicate with each other. Protocols send data across the network in units called packets. Table 1.2 lists some common network LAN protocols that you can use in Windows networks.

Table 1.2 Network Protocols in Windows networks

Protocol	Description
Transmission Control Protocol/Internet Protocol (TCP/IP)	A routable, non-proprietary protocol that‘s the predominant Windows network protocol. It‘s supported by all versions of Windows and most other non-Microsoft operating systems. TCP/IP is also the protocol of the Internet.
Internetwork PacketExchange/Sequenced Packet	A routable, proprietary protocol that was the native protocol in early versions of Novell NetWare. Later versions of NetWare supported TCP/IP as the native protocol. Windows computers can connect to

Exchange(IPX/SPX)	IPX/SPX networks and NetWare servers by using Microsoft‘s version of IPX/SPX, called NWLink. To share files and printers on a NetWare server, you must install the Microsoft Client for NetWare.
Appletalk	A routable network protocol supported by Apple Macintosh computers. Windows NT and Windows 2000 support AppleTalk. Mac OS X (10.2 and later) supports TCP/IP and can connect to Windows networks without requiring AppleTalk support. AppleTalk computers are called nodes and can be configured as part of zones for sharing resources. As with other networks, each node on an AppleTalk network must be configured with a unique network address.
NetBEUI	A non-routable, proprietary Microsoft protocol that‘s supported in Windows 9x/Me, Windows NT, and Windows 2000. NetBEUI uses Network Basic Input/Output System (NetBIOS) services to communicate with other computers on a network. (NetBIOS helps with computer names and some basic communication services.) Although it isn‘t technically supported in Windows XP, you can install NetBEUI by manually copying files from the installation CD- ROM. What‘s nice about NetBEUI is that it has no settings to configure. You install the protocol, connect the computer to the network, and it just works. The drawback is that it isn‘t routable, so it can‘t pass data from one network segment to another. This means that it can‘t be used for remote access or any communication outside a single segment.

Wireless network protocols

Wireless networks send and receive information using one of four major wireless protocols:

- Wi-Fi (Wireless Fidelity) is the most widely used wireless technology at present. Wi-Fi began as 802.11b IEEE standard, although most implementations have been upgraded to use the newer 802.11g IEEE standard. 802.11b and 802.11g have an indoor transmission range of up to 35 meters.
- Bluetooth is a short-range wireless technology limited to transmission distances of about 100 meters or less, which generally confines it to connecting nodes within a single room or adjacent rooms.
- 802.11a is an improved version of the original Wi-Fi technology and is also based on the same IEEE 802 standard. 802.11a has an indoor transmission range of up to 35 meters. 802.11a isn‘t compatible with 802.11b.
- WiMAX (IEEE 802.16 Air Interface Standard) is a point-to-multipoint broadband wireless access standard. It‘s an emerging wireless connection standard for long distances.

A network‘s architecture consists of:

- The design of its wiring or radio wave connections.
- The configuration of its other physical components.
- Its software (programming).
- The protocols by which it operates.

All of these parts must be tightly organized into a physical structure with consistent operating methodology to establish a communication system that works smoothly among all the devices connected to the network. The most common types of network architecture used today are Ethernet, Token Ring, and wireless. Each has advantages and limitations. The bandwidth, that is, the amount of data (measured in megabits per second) that the network can handle at once, varies among these architectures.

Network designs

The design of a networks 'wiring or radio wave connections is called its physical topology. It's helpful to think of a topology as a shape. Common network topologies include the star, bus, ring, and mesh.

The star

In a star topology (Figure 1.2), each node is connected to a central network transmission device such as a hub or a switch, which serves as a distribution device. The central network transmission device then passes the information packets it receives from any device to the other devices connected to it. In a star, each computer has its own wired or wireless connection to the hub. The benefit of the star design is that because each computer has its own connection to the central network transmission device, when a single connection fails, it doesn't affect the communication ability of other computers connected to the same network transmission device. However, if the central network transmission device fails, all of the computers connected to that device will no longer be able to communicate on the network. Currently the star design is the most popular LAN physical topology.

Advantages of a Star Topology

One advantage of a star topology is scalability and ease of adding another system to the network. If you need to add another workstation to the network with a star topology, you simply connect that system to an unused port on the hub. Another benefit is the fact that if there is a break in the cable it affects only the system that is connected to that cable. Centralizing network components can make an administrator's life much easier in the long run. Centralized management and monitoring of network traffic can be vital to network success. With a star configuration, it is also easy to add or change configurations because all of the connections come to a central point.

Disadvantages of a Star Topology

On the flip side, if the hub fails in a star topology, the entire network comes down, so we still have a central point of failure. But this is a much easier problem to troubleshoot than trying to find a cable break with a bus topology. Another disadvantage of a star topology is cost. To connect each workstation to the network, you will need to ensure that there is a hub with an available port, and you will need to ensure you have a cable to go from the workstation to the hub. Today, the cost is increasingly less of a disadvantage because of the low prices of devices such as hubs and switches.

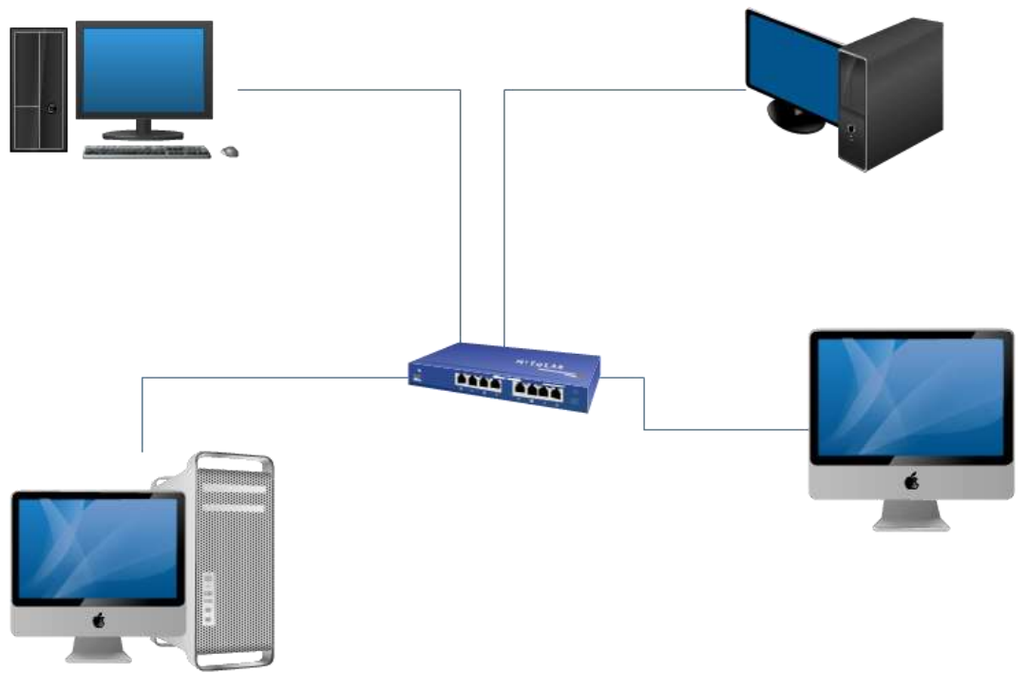

Figure 1.2 Star Topology

The bus

A bus topology uses one cable as a main trunk to connect all of the systems together (Figure 1.3). A bus topology is very easy to set up and requires no additional hardware such as a hub. The cable is also called a trunk, a backbone, or a segment.

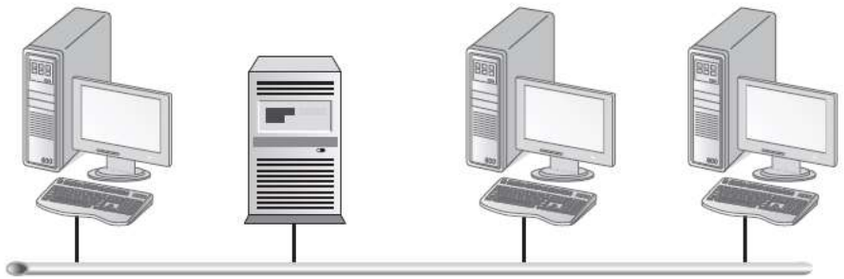

Figure 1.3 Bus Topology

In a bus topology, each node is connected to the next by a direct line so that a continuous line is formed. There‘s no central point in this arrangement. Each node is simply connected to the next one on either side of it. The bus design incorporates coaxial cable and T connectors to connect the individual computers to the bus. When the end of the line is reached and there are no further nodes to be connected, the bus is closed off with a terminator device specific to the cabling used. In a bus Ethernet, data is sent on the network line in both directions from the source node. The data passes from one node to the next until it reaches the terminator at the end of the network. The terminator simply cancels the data signal, discarding the data so it can‘t echo back on the network line and head back to the node it just came from. All information on the network passes through each node but only once. There‘s no replication or broadcasting of data as in a star configuration. Each node determines if data it receives is addressed to it. If it is, the data is read and receipt is confirmed. If it isn‘t, the packet is passed on to the next node. The benefit of a bus topology is that it‘s simple and inexpensive to set up. However, if there‘s a break in the line anywhere, all communication on that segment stops. The technology used is also not very scalable. Currently the bus design isn‘t used much in LAN physical topologies.

With a bus topology, when a computer sends out a signal, the signal travels the cable length in both directions from the sending computer. When the signal reaches the end of the cable length, it bounces back and returns in the direction it came from. This is known as signal bounce. Signal bounce is a problem, because if another signal is sent on the cable length at the same time, the two signals will collide and be destroyed and then must be retransmitted. For this reason, at each end of the cable there is a terminator. The terminator is designed to absorb the signal when the signal reaches the end, preventing signal bounce. If there is no termination, the entire network fails because of signal bounce, which also means that if there is ever a break in the cable, you will have un-terminated ends and the entire network will go down.

A bus is a passive topology, which means that the workstations on the bus are not responsible for regenerating the signal as it passes by them. Since the workstations do not play an active role, the workstations are not a requirement of a functioning bus, which means that if a workstation fails, the bus does not fail. But if there is an un-terminated end in the bus, the entire network will fail.

Advantages of a Bus Topology

One advantage of a bus topology is cost. A bus topology uses less cable than a star topology or a mesh topology, and you do not need to purchase any additional devices such as hubs. Another advantage of a bus topology is the ease of installation. With a bus topology, you simply connect the workstation to the cable segment or backbone. You need only the amount of cable to connect the workstation to the backbone. The most economical choice for a network topology is a bus topology, because it is easy to work with and a minimal amount of additional devices are required. Most importantly, if a computer fails, the network stays functional.

Disadvantages of a Bus Topology

The main disadvantage of a bus topology is the difficulty of troubleshooting it. When the network goes down, it is usually due to a break in the cable segment. With a large network, this problem can be tough to isolate. Scalability is an important consideration in the dynamic world of networking. Being able to make changes easily within the size and layout of your network can be important in future productivity or downtime. The bus topology is not very scalable.

The ring

In a ring topology, each node is connected to a central device by two wires (Figure 1.4). In Token Ring networks, this device is referred to as a multistation access unit (MSAU, although it is sometimes referred to as MAU). Communication is enabled by passing a token around the ring to each node—if a node has the token, it can transmit data. The token packet is always present somewhere on the network. It travels from the central device up one connecting wire to a node and back to the central device through the other wire, then up one wire to the next node and back through the other. It passes through the central device after each node and, after passing through all of them and returning to the central device, it travels back to its starting point at the other end of the central device through the main ring cable. The token travels in a circle or ring on the network in a single direction, even though the nodes are physically arranged as a star.

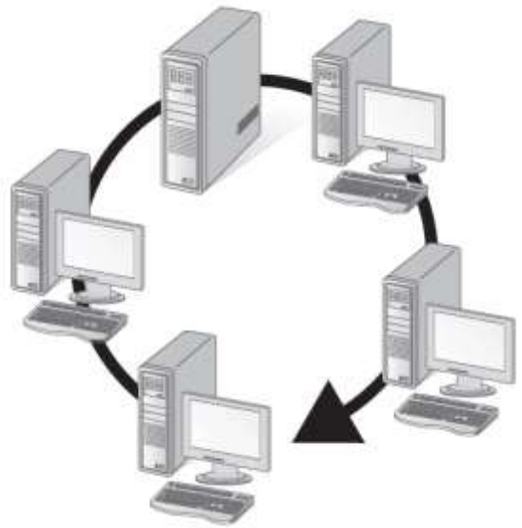

Figure 1.4 Ring Topology

Advantages of a Ring Topology

A major advantage of a ring topology is that signal degeneration is low because each workstation is responsible for regenerating or boosting the signal. With the other topologies, as the signal travels the wire, it gets weaker and weaker as a result of outside interference: eventually, it becomes unreadable if the destination system is too far away. Because each workstation in a ring topology regenerates the signal, the signal is stronger when it reaches its destination and seldom needs to be retransmitted.

Disadvantages of a Ring Topology

The biggest problem with ring topologies is that if one computer fails or the cable link is broken, the entire network could go down. With newer technology, however, this isn't always the case. The concept of a ring topology today is that the ring will not be broken when a system is disconnected; only that system is dropped from the ring. Isolating a problem can be difficult in some ring configurations. (With newer technologies, a workstation or server will put out a beacon if it notices a break in the ring.) Another disadvantage is that if you make a cabling change to the network or move a workstation, the brief disconnection can interrupt or bring down the entire network.

The mesh

In a mesh topology, all nodes in the mesh have independent connections to all other nodes in the mesh. This configuration makes it very fault- tolerant and scalable. Mesh topologies require computers to have multiple network cards installed, and due to the complexity of wiring and support are rarely used for user computers. Figure 1.5 shows an example of a mesh topology.

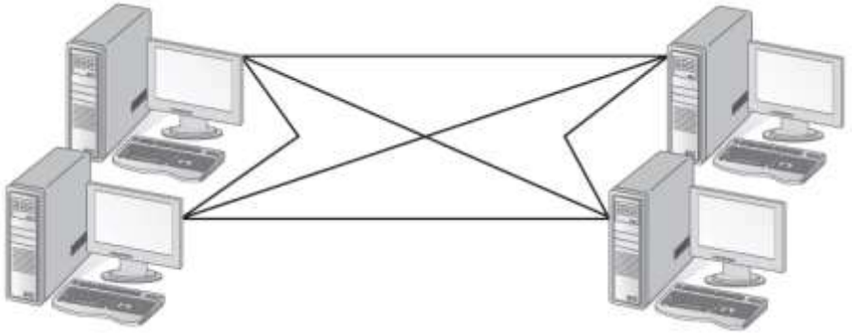

Figure 1.5 A Mesh Topology

Advantages of a Mesh Topology
The biggest advantage of a mesh topology is fault tolerance, meaning that, if there is a break in a cable segment, traffic can be rerouted through a different pathway because there are multiple pathways to send data from one system to another. This fault tolerance means that it is almost impossible for the network to go down due to a cable fault.

Disadvantages of a Mesh Topology
A disadvantage of a mesh topology is the cost of the additional cabling and network interfaces to create the multiple pathways between each system. A mesh topology is very hard to administer and manage because of the numerous connections.

The hybrid
In a hybrid network topology two or more different types of network topologies are combined together into one network(Figure 1.6). For example, a large LAN might use a combination star and bus design with nodes connected to several hubs and the hubs connected in a bus configuration. This design is useful for constructing large networks with a minimum of wiring, but because all the hubs must still broadcast their data to the nodes, it tends to slow down as the amount of data flowing in it multiplies.

It is important to note that it is typical for networks to implement a mixture of topologies to form a hybrid topology. For example, a very popular hybrid topology is a star-bus topology, in which a number of star topologies are connected by a central bus. This is a popular topology because the bus will connect hubs that are spread over distance.

Another very popular hybrid topology is the star-ring topology. The star-ring topology is popular because it looks like a star but acts as a ring. For example, there is a network architecture known as Token Ring that uses a central “hub” type device, but the internal wiring makes a ring. Physically it looks like a star, but logically it acts as a ring topology.

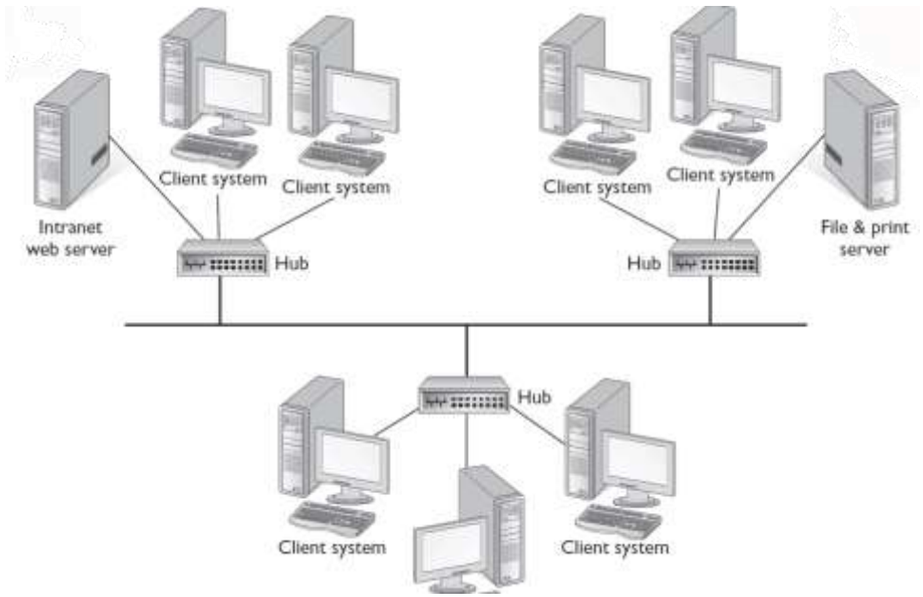

Figure 1.6 A Hybrid Topology

Wireless Topologies
A wireless topology is one in which few cables are used to connect systems. The network is made up of transmitters that broadcast the packets using radio frequencies. The network contains special transmitters called cells, or wireless access points, which extend a radio sphere in the shape of a bubble around the transmitter.

This bubble can extend to multiple rooms and possibly floors in a building. The PCs and network devices have a special transmitter-receiver, which allows them to receive broadcasts and transmit requested data back to the access point. The access point is connected to the physical network by a cable, which allows it, and any wireless clients, to communicate with systems on the wired network. A wireless network topology is shown in figure 1.7.

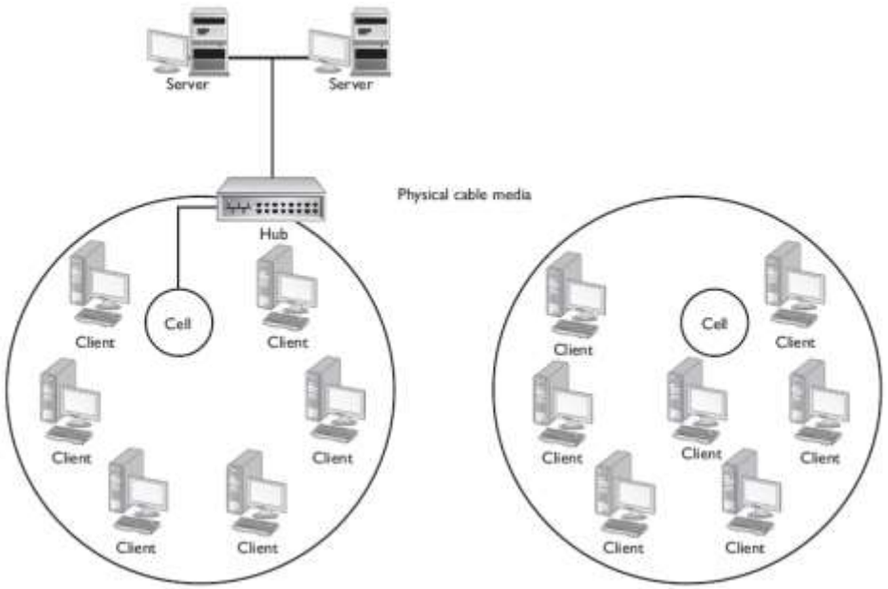

Figure 1.7 A Wireless Topology

Notice in the figure that the wireless cells, or access points, are connected to the network by connecting into the hub or switch that has a connection to the rest of the wired network. Also notice that the clients do not have cables connecting them to the network. These are wireless clients, and they will get access to the network through the wireless cell (or access point).

Another option for wireless networks is the use of a radio antenna on or near the building, which allows one cell to cover the building and the surrounding area. This approach is best in a campus-type arrangement, where many buildings that need to be included in the cell are in a close geographical area. This setup does not easily Point-to-point versus point-to-multipoint. Each of the preceding network designs uses point-to-point or point-to-multipoint connections. In a point-to-point connection, there is a dedicated connection between two nodes—only those two nodes communicate over the connection, the connection between a wireless network and a LAN is typically a point-to-point connection—there‘s a dedicated communication line between the wireless access point and a LAN network transmission device. Another example of a point-to-point connection is the dial-up connection from a computer to an ISP.

In a point-to-multipoint connection, there are multiple connections that connect a single node to multiple nodes. Network transmission devices, such as switches and hubs are point-to-multipoint devices.

Wireless networks typically are implemented using one of two wireless topologies:

- The infrastructure, or managed, wireless topology
- The ad hoc, or unmanaged, wireless topology

Infrastructure Wireless Topology

The infrastructure wireless topology is commonly used to extend a wired LAN to include wireless devices. Wireless devices communicate with the wired LAN through a base station known as an access point (AP) or wireless access point. The AP forms a bridge between a wireless and wired LAN, and all transmissions between wireless stations, or between a system and a wired network client, go through the AP. APs are not mobile and have to stay connected to the wired network; therefore, they become part of the wired network infrastructure (thus the name). In infrastructure wireless networks, there might be several access points providing wireless coverage for a large area or only a single access point for a small area, such as a single home or small building. Figure 1.8 shows an infrastructure wireless network.

Ad Hoc Wireless Networking

In a wireless ad hoc topology, devices communicate directly between themselves without using an access point. This peer-to-peer network design is commonly used to connect a small number of computers or wireless devices. For example, an ad hoc wireless network may be set up temporarily between laptops in a boardroom or to connect systems in a home instead of using a wired solution.

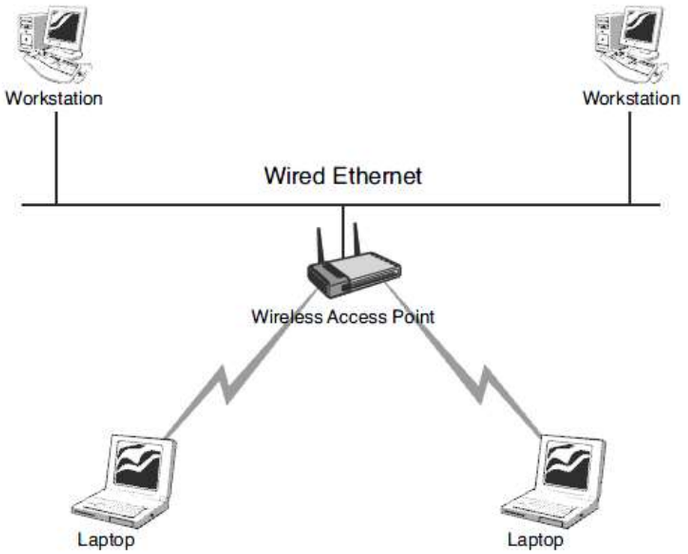

Figure 1.8 Infrastructure Wireless Network

The ad hoc wireless design provides a quick method to share files and resources between a small number of systems. Figure 1.9 shows an ad hoc wireless network.

Point-to-Point Networks

As the name suggests, in a point-to-point (PtP) wireless configuration, the communication link travels from one node directly to one other node. Wireless point-to-point systems often are used in wireless backbone systems such as microwave relay communications, or as a replacement for a single wired communication cable. Figure 1.10 shows a point-to-point wireless configuration.

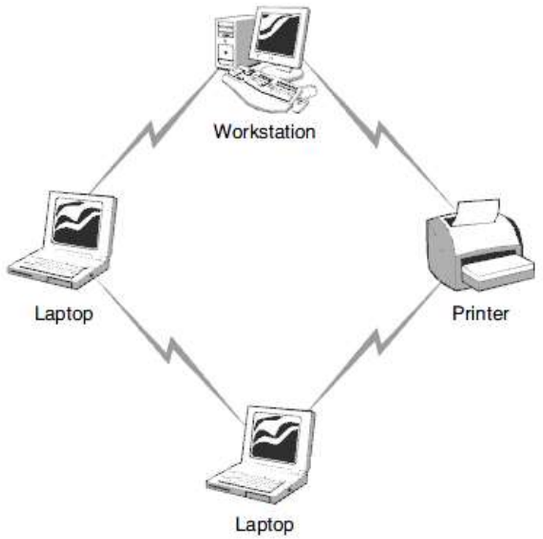

Figure 1.9 Ad Hoc Wireless Network

As shown in figure 1.11, the point-to-point wireless link connects two remote locations. Not having to run cable such as fiber makes it an economic way to provide a communication link. However, a typical point-to-point wireless configuration has no redundancy. This means that if the wireless link should fail, communication between the locations is unavailable.

The point-to-point link is often used for organizations that need a direct link between two remote office buildings. These point-to-point wireless connections typically are easy to install and require no external outdoor casing, cables, or other accessories. Because there is no need for the cabling infrastructure, a point-to-point wireless solution is a cost-effective method of connecting two remote locations.

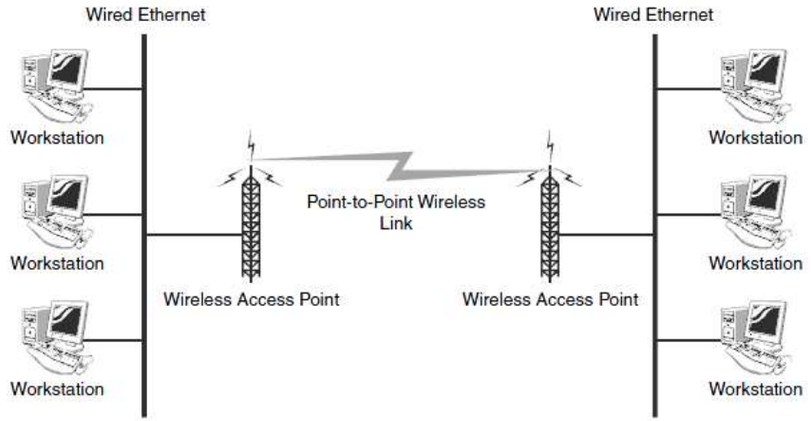

Figure 1.10 Point to Point Wireless Configuration

Point-to-Multipoint Networks

A point-to-multipoint (PtMP) wireless connection is designed to link multiple wired networks. Signals in point-to-multipoint networks travel from a central node such as a base station of a cellular system, an access point of a WLAN, or a satellite. The function of the multipoint wireless topology is to interconnect multiple locations, enabling them to access and share resources. Multipoint networks use a base station as the "hub" and client networks as the connection points communicating with the base station. These point-to-multipoint networks are used in wireless Internet service providers (WISPs), large corporate campuses, interconnected branch offices, and more.

The reliability of the PtMP network topology depends on the quality of the central node and each connecting node. The location of the central node is very important to ensure the range and strength of the wireless signal.

Wireless Mesh Networks

As discussed earlier, wired mesh networks are costly due to the cabling required to interconnect all computer systems. Wireless mesh networks obviously do not need cables running between systems, making wireless mesh networks fairly common in the networking world. In the wireless mesh network, as with the wired mesh, each network node is interconnected to other nodes on the network.

With a wired mesh, the wireless signal starts at a wireless base station (access point) attached to a wired network. A wireless mesh network extends the transmission distance by relaying the signal from one computer to another. Unlike the wired mesh, in which a complex and expensive collection of physical cables is required to create the mesh, the wireless mesh is inexpensive to implement. Figure 1.11 shows a wireless mesh network.

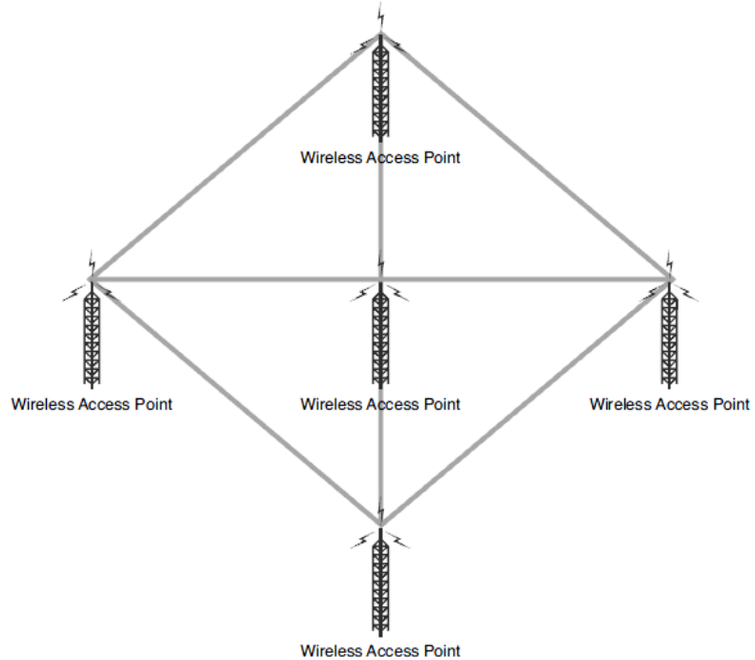

Figure 1.11 Wireless Mesh Network

The wireless mesh network has several key advantages. Because a wireless mesh network is interconnected with one or more nodes on the network, the data can travel multiple paths to reach its destination. When a new node is added, it provides new paths for other nodes, which in turn improves network performance and decreases congestion. Advantages of the wireless mesh include the following:

- Self-healing: Wireless mesh networks are known as self-healing, which refers to the network's ability to adapt to network failure and even function should a node be moved from one location to another. Self-healing in a wireless mesh environment is possible because of the interconnected connections and because of the wireless media.
- Scalable: Wireless mesh networks are highly scalable. Using wireless, it is possible to add new systems to the network without the need for expensive cables.
- Reliability: Of all network topologies, the mesh network provides the greatest reliability. The redundant number of paths for the data to travel ensures that data can reach its destination.
- Cost: One disadvantage of the wired mesh is the cost associated with running the cabling and the support costs of such a complex network. Wireless mesh networks are essentially self-configuring and do not have cabling requirements. Therefore, systems can be added, removed, and relocated with little cost or disruption to the network.

Packet versus circuit switching networks

In a packet switching network, data is broken up into packets before it's sent over the network. Each packet is transmitted individually and is able to follow different routes to its destination. At the destination network node, the packets are queued as they arrive. Once all the packets forming the original data arrive at the destination, they're recompiled into the original form. In a circuit switching network, a dedicated line is allocated for the transmission of data between two network nodes.

Circuit-switching is the best choice when data needs to be transmitted quickly and must arrive in the same order in which it's sent, such as with most real-time data (live audio and video.) Packet switching is more efficient for data that can withstand delays in transmission, such as e-mail messages and Web pages.

Ethernet

Ethernet is the most popular form of LAN in use today. It's popular because it strikes a good balance between ease of setup and use, speed, and cost. Four types of Ethernet architecture are available now. Each is distinguished primarily by the speed at which it operates.

- 10 Gigabit Ethernet (also called 10GbE) is the fastest of the Ethernet standards. With a data rate of 10 gigabits per second, it is ten times faster than Gigabit Ethernet.
- 1000-Mbps Ethernet (also called Gigabit Ethernet) operates at a speed of 1000 Mbps (1 gigabit per second). It's used for large, high-speed LANs and heavy-traffic server connections. Few, if any, home networks require Gigabit Ethernet.
- 100-Mbps Ethernet (also called Fast Ethernet) operates at a speed of 100 Mbps. It can also handle data at 10 Mbps, and this feature allows devices running at the slower speed to operate on the same network along with those operating at 100 Mbps.
- 10-Mbps Ethernet (also called Twisted Pair Ethernet) operates at a speed of 10 megabits per second (Mbps) of data. The first Ethernet version was developed by the Xerox Corporation in the 1970s. It later became known as Ethernet IEEE 802.3.

Each Ethernet version can be set up using various types of wire or cable, but the different speeds of the versions and the conditions in which they operate usually dictate what type of connecting wires you need to use. Designations for the different Ethernet standards are based on the medium each standard uses:

- BASE-X and BASE-R standards—Run over fiber optic cable.
- BASE-W standards—Run over fiber optic cables; referred to as Wide Area Network Physical Layer (WAN PHY). Uses the same types of fiber and

support the same distances as 10GBASE-R standards, however with these standards Ethernet frames are encapsulated in SONET frames.

- BASE-T standards—Run over twisted pair cable; shielded or unshielded.
- BASE-CX standards—Run over shielded copper twisted pair cable.

Most current Ethernet installations use shielded twisted-pair (STP) cable, unshielded twisted-pair (UTP) cable, or fiber optic cable. Older Ethernet installations used either 50-ohm RG58/U coaxial cable, also known as thin Ethernet and 10Base2, or 50-ohm RG8/U coaxial, known as thick Ethernet and 10Base5, but these are both obsolete now.

Gigabit Ethernet standards

Table 1.3 lists the 10 Gigabit Ethernet (10GbE) standards and their specifications.

Table 1.3 10 Gigabit Ethernet Standards (10GbE)

Standard	Medium	Distance up to	Notes
10GBASE-T	Copper twisted pair—shielded or unshielded	100 meters with CAT6a; up to 55 meters with CAT6	
10GBASE-SR	Multi-mode fiber	26 meter or 82 meters depending on cable type 300 meters over 50 µm 2000 MHz·km OM3 multi-mode fiber	Preferred choice for optical cabling within buildings
10GBASE-LR 10GBASE-LW	Single-mode fiber	10 kilometers	Used to connect transceivers
10GBASE-ER	Single-mode fiber	40 kilometers	
10GBASE-EW			
10GBASE-ZR 10GBASE-ZW	Single-mode fiber	80 kilometers	Not specified in standards; built to Cisco optical specification

1000 Mbps - Gigabit Ethernet standards

Table 1.4 lists the gigabit Ethernet standards and their specifications.

Table 1.4 Gigabit Ethernet Standards

Standard	Medium	Distance up to	Notes
1000BASE-T	Unshielded twisted pair – Cat5, Cat5e or Cat6	100 meters per network segment	Requires all four wire pairs
1000BASE-CX	Balanced copper shielded twisted-pair	25 meters	An initial standard for gigabit Ethernet connections
1000BASE-LX	Single-mode optic fiber	5 km*	
1000BASE-LX10	Single-mode optic fiber	10 km	Wavelength of 1270 to 1355 nm
1000BASE-BX10	Single-mode optic fiberover single-strand fiber	10 km	Different wavelength going in each direction - 1490 nm downstream, 1310 nm upstream
1000BASE-LH	Single-mode optic fiber	10 km	Wavelength of 1300 or 1310nm. Non-standard implementation.

			Very similar to 1000BASE-LX, but achieves longer distances due to higher quality optics. 1000BASE-LH is backwards compatible with 1000BASE-LX.
1000BASE-ZX	Single-mode optic fiber	70 km	1550 nm wavelength. Non-standard implementation
1000BASE-SX	Multi-mode optic fiber	500 km	

* The 1000BASE-LX standard specifies transmission over a single-mode optic fiber, at distances of up to 5 km over 9 μm (micron or micrometer). In practice, it often operates correctly over a much greater distance. Many manufacturers guarantee operation up to 10 to 20 km, provided that their equipment is used at both ends of the link. 1000BASE-LX can also run over multi-mode fiber with a maximum segment length of 550 m. Link distances greater than 300 m might require a special launch conditioning patch cord. The launch conditioning patch cord launches the laser at a precise offset from the center of the fiber. This causes the laser to spread across the diameter of the fiber core, reducing differential mode delay. Differential mode delay occurs when the laser couples onto a limited number of available modes in the multi-mode fiber.

Fast Ethernet standards

Table 1.5 lists the Fast Ethernet standards and their specifications.

Table 1.5 Fast Ethernet Standards

Standard	Medium	Distance up to	Notes
100BASE-TX	Twisted-pair copper—CAT5 or higher	100 meters per network segment	Runs over two pairs—one pair of twisted wires in each direction The most common Fast Ethernet.
100BASE-T4	Twisted-pair copper – CAT3		Requires four pairs—one pair for transmit, one for receiving, and remaining pairs switch direction as negotiated. An early implementation of Fast Ethernet.
100BASE-T2	Twisted-pair copper		Runs over two pairs.
100BASE-FX	Singe or multi-mode pair	400 meters for half-duplex 2 km for full-duplex over MMF	Uses two strands—one for receiving and one for transmitting Not compatible with 10BASE-FL.
100BASE-SX	Multi-mode fiber	300 meters	Uses two strands of MMF—one for receiving and one for transmitting. Backwards-compatible with 10BASE-FL.
100BASE-BX	Single-mode fiber	20 km	Uses a single strand of SMF.

Ethernet bonding

Ethernet bonding combines the bandwidth of two network interface cards as a cost-effective way to increase bandwidth available for data transfers for critical servers, such as firewalls and production servers. Ethernet bonding can also provide fault tolerance, so that when one NIC fails, you can replace it without disabling client access to the server.

Ethernet networks

Ethernet networks can be physically arranged in either of two configurations, which refer to how the nodes (devices) are connected to the Ethernet:

- Bus topology
- Star topology

A star Ethernet might be slower than a bus Ethernet, especially if there are many nodes on the network. This happens because the hub generates a lot of data traffic that isn‘t used. It replicates all the data it receives from any source and sends it to every node. The amount of data being sent increases for every node added to the network, even though most of the data sent to each node isn‘t intended for that node and is discarded on arrival.

A node on an Ethernet network waits to send information to the network until it determines that no other node is transmitting information, and then begins transmitting itself. During transmission, the system also listens in on the media. If it senses that another node is also transmitting, a collision event occurs.

When this happens, the node quits transmitting for a random period of time and then checks the media again to see if it is okay to transmit. Any station might transmit when it senses that the carrier is free. If a collision is detected, each station will wait for a randomly determined interval before retransmitting.

As the amount of data sent increases, more and more data packets from different nodes competing for bandwidth on the LAN collide with one another. The network detects these collisions and resends the data packets involved, but the collisions and replication of data transmissions slow down the network. Most network operating systems track retransmissions, which are a good indication of the number of collisions occurring on the network.

Collisions slow cable throughput. At some point in its growth, an Ethernet network might encounter a reduction in performance. This depends on the amount of traffic generated by each workstation.

Channel access methods

The channel access method determines the physical methodology by which data is sent across the transmitting media. Today, there are various channel access methods through which conversation is made possible. These technologies are analogous to two of the ways that people communicate. For example, imagine that a specific problem and its possible resolutions are discussed in a meeting. This phase of the meeting is more of a free for all in which there might be moments where everyone talks and other times where most hold off speaking, yielding to only one speaker, after which everyone again attempts to communicate their thoughts. Now, consider yourself in a departmental staff meeting discussing project status. Each member of the team waits his turn to communicate the successes and failures for the week. After completing, the next person communicates his status. This process continues in an orderly fashion until all have had a chance to speak.

The example of several people talking at once is an example of a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) communications methodology. CSMA/CD networks are more popularly known as Ethernet networks. CSMA/CD is the most common implementation of channel access.

- Carrier sensing—Listens for someone talking.
- Multiple access — All have concurrent access to the media.
- Collision detection—If two or more systems transmit at once, the system realizes the message did not get through and repeats the message.

Transmission failures can be caused by:

- Bad cabling
- Improper termination
- Collisions

- Improper cable length

The terms Ethernet and 802.3 are used interchangeably. There are some small differences, but both are CSMA/CD specifications. Ethernet was originally developed by Xerox, Intel, and DEC in the late 1970s, with specifications first released in 1980. The IEEE 802.3 specification differs from Ethernet primarily with respect to the frame format. Other differences involve pinouts and the Signal Quality Error (SQE) signal, also known as a heartbeat. A variation on this theme is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This methodology doesn‘t detect collisions as much as it attempts to avoid collisions. An alert message notifies nodes of an impending transmission. Any collisions that occur will be during this alert sequence rather than during actual data transmission. Because the alert sequence is shorter than an actual data transmission, the retransmit of lengthy data is avoided.

Token Ring networks

Token Ring LAN technology was developed by IBM Corporation. It operates at slower speeds than Ethernet, 4 Mbps or 16 Mbps depending on the Token Ring network, but it‘s physically arranged in a star topology, one of the designs also used by Ethernet. Token Ring LANs are so named because their protocol for data control uses a token, a small packet of data, to determine which node on the network can transmit data, and because all data actually travels in a circle or ring on the network.

In a Token Ring, each node is connected to a central device, referred to as a Multistation Access Unit (MSAU), by two wires. A token packet is always present somewhere on the network, traveling from the MSAU up one connecting wire to a node and back to the MSAU through the other wire, then up one wire to the next node and back through the other. It passes through the MSAU after each node and, after passing through all of them and returning to the MSAU, it travels back to its starting point at the other end of the MSAU through the Token Ring‘s main ring cable. While the Token Ring network physically appears to be a star, it‘s actually a ring. You can think of this design as a ring in a box.

Wireless LANs

Wireless LANs don‘t use wires to connect the nodes of the network. The nodes aren‘t physically connected at all to one another or to a central device. They communicate with an access point or wireless hub using a wireless network interface card (NIC), which includes a transceiver and an antenna. The wireless NIC allows the node to communicate over relatively short distances using radio waves, which it sends to, and receives from, the nearest hub.

Wireless connections can be made from a node to a hub through walls and other obstructions, because radio waves pass through solid obstructions fairly easily. This ability makes wireless LANs very useful and cost-effective in already finished buildings where retrofitting wiring is both difficult and expensive. It‘s also an advantage where hardwiring a network might be impossible, such as on the beach at a summer home, or to a boat tied up at a private dock. Wireless LANs are limited, however, both by the low transmitting power of their NICs and hubs and by the fact that dense metals, especially ferrous metals, as well as heavy layers of concrete, stone, brick, or dirt, absorb radio waves. These factors restrict the distance over which a wireless network can be extended and might require more hubs than anticipated to obtain full-area coverage. Hubs or access points must be placed so that the wireless NICs of nodes can access at least one of them from any location within the LAN‘s defined area. Wireless networked nodes communicate with one another only through a hub, rather than directly node to node, as in a bus Ethernet. Hubs must be wired together or connected by wireless technology into a network that allows all hubs to communicate with one another and transmit the data they receive from their wireless nodes. A wireless LAN isn‘t entirely free of wired connections. It‘s usually connected to a cable network by its hubs, which constitute nodes on a wired LAN.

WAN bandwidth technologies

A wide area network (WAN) spans larger geographical distances and connects multiple LANs together using high-speed communication lines. Wide area networks expand the basic LAN model by linking LANs to communicate with one another. By traditional definition, a LAN becomes a WAN when you expand the network configuration beyond your own premises and many times lease data communication

lines from a public carrier. WANs support data transmissions across public carriers by using facilities such as dial-up lines, dedicated lines, or packet switching.

There are several ways to create WAN connections, depending on location and available hardware:

- Dial-up networking (DUN)—Uses a modem to connect through regular, analog phone lines.
- Virtual private network (VPN)—A network connection that uses encryption and security protocols to create a private network over a public network.
- Digital Subscriber Line (DSL)—High-speed connections made over regular analog phone lines.
- Cable—Connections made over the same lines that carry cable television signals.
- Satellite—Connections made by sending and receiving signals from satellites in orbit around the earth.
- Wireless—Used to connect users in hotspots, where wireless Internet service is provided by an employer, business, or governmental unit, such as a city. Wireless connections can also be made over cellular telephone networks.
- Cellular—Connections made through a cell phone or laptop‘s cellular network PC card on a cellular phone network.

Faster WAN technologies are used to connect a small ISP or large business to a regional ISP, and a regional ISP to an Internet backbone. These technologies include the following:

- T lines and E lines
- X.25 and frame relay
- ATM

POTS/PSTN

The slowest but least expensive Internet connection to an ISP is affectionately known as plain old telephone service (POTS). Also referred to as the public switched telephone network (PSTN), it‘s the network of the world‘s public circuit-switched telephone networks. This is the most common method of home connection and uses a dialup system each time the connection to the ISP is made over the telephone line. The connection isn‘t continuous, and when the line isn‘t connected to an ISP, it can be used for regular telephone service or any other telecommunications function. Data speed on a regular telephone line is a maximum of 56 Kbps.

A technology called modem bonding allows multiple dial-up links over POTS to be combined for redundancy or increased throughput.

ISDN

Integrated Services Digital Network (ISDN) technology also uses a telephone line to transmit data, but unlike POTS, the data isn‘t converted to analog form—the modem used must be a digital modem. An ISDN line is digital and consists of two phone circuits, both carried on one pair of wires along with a slower, third circuit used for control signals. Each data circuit can transmit data at up to 64 Kbps and the two circuits can be combined to move data at a speed of 128 Kbps. This configuration of an ISDN line is known as the basic rate interface (BRI) and is intended for home and small- business users. Another higher-cost ISDN level of service is called primary service interface (PRI) and is intended for larger users. It has 23 data channels and a control channel.

DSL

A Digital Subscriber Line (DSL) is a high-speed data and voice transmission line that still uses telephone wires for data transmission but carries the digital data at frequencies well above those used for voice transmission. This makes possible the transmission of voice and digital data on the same line at the same time. The regular voice telephone line must be dialed for each use, but the DSL part of the line is always connected to the computer. A DSL can transmit data at speeds up to 1.5 Mbps in both directions, or it can be set up as an asymmetric line (ADSL), which can transmit up to 640 Kbps upstream (to the ISP) and 7.1 Mbps downstream (from the ISP). Higher bandwidth can be achieved by bonding multiple DSL lines, similar to the modem bonding technology described for POTS.

Cable
A cable modem connects to the cable television line that‘s already installed or available in most homes. These devices are actually transceivers (transmitter/receivers), rather than modems, but are commonly known as cable modems. With a cable modem, digital data is converted to analog signals and placed on the cable at the same time as the incoming television signal. Incoming analog data signals are converted to digital for the computer by the modem. The data frequencies differ from the television signal frequencies, and the two signals don‘t interfere with one another on the cable. Depending on the individual configuration, a cable modem can transmit data at speeds from 500 Kbps up to 5 Mbps. Many cable companies now offer Voice over IP (VoIP) service, also known as digital phone service, to their users. With VoIP, you can make telephone calls over a data network such as the Internet. VoIP converts the analog signals from digital back to voice at the other end so you can speak to anyone with a regular phone number.

Satellite
A satellite link Internet connection to an ISP is now available nationwide. It‘s especially attractive in rural areas where telephone-based services may be limited, and cable sometimes isn‘t available. A satellite communication link uses a dish similar to a satellite television dish mounted on the building to communicate with a stationary satellite in orbit. The server is connected to the dish antenna. Incoming Internet data travels from the ISP to the satellite in orbit, then down to the dish and into the LAN server. The speed of the connection varies according to the ISP but can go up to 1.5 Mbps. The uplink connection from the LAN to the ISP is usually by a telephone line/modem connection and isn‘t as fast as the satellite downlink. A digital radio signal from the LAN up to the satellite, which in turn sends the signal to the ISP, is also available but at a much higher cost than the telephone connection, which is usually adequate for sent data.

Wireless
The term ―wireless‖ refers to several technologies and systems that don‘t use cables for communication, including public radio, cellular telephones, one-way paging, satellite, infrared, and private, proprietary radio. With the expense and the concern that increasing the use of wireless might affect our health, airplane control systems, pacemakers, and other similar items, wireless isn‘t as popular as wired data transmission. Wireless is an important technology for mobile devices and for Internet access in remote locations where other methods aren‘t an option.

For Internet access, two popular applications of wireless are:

- Fixed-point wireless, sometimes called Wireless Local Loop (WLL)
- Mobile wireless

Cellular
All the major cellular phone companies now provide Internet connection service for their customers. Wherever you have cell phone service reception, you can connect to the Internet using your Internet capable phone or laptop using a cellular network PC card. Cell phone companies typically charge an additional monthly fee for this service. The connection speed for cellular Internet service is faster than dial-up, but is slower than DSL or cable. There are currently three connection technologies in use—Enhanced Data rates for GSM Evolution (EDGE), Evolution-Data Optimized (EV-DO), and High-Speed Downlink Packet Access (HSDPA).

T lines and E lines
The first successful system that supported digitized voice transmission was introduced in the 1960s and was called a T-carrier. A T-carrier works with a leased digital communications line provided through a common carrier, such as BellSouth or AT&T. Although it was originally intended for voice, the line also works with data. The system has become a popular choice for Internet access for larger companies. The leased lines are permanent connections that use multiplexing, a process of dividing a single channel into multiple channels that can be used to carry voice, data, video, or other signals.

Several variations of T-carrier lines are available; the most popular are T1 and T3 lines.

- For a T1 line, multiplexing allows the line to carry 24 channels, and each channel is capable of transmitting 64 Kbps. A 24-channel T1 line can transmit

a total of 1.544 Mbps. If a T1 is used for voice only, it can support 24 separate telephone lines, one for each channel.

- A T3 line can carry 672 channels, giving it a throughput of 44.736 Mbps. T1 and T3 lines can be used by a business to support both voice and data, with some channels allocated to each.

The E-carrier is the European equivalent of the American T-carrier. The E-carrier is a digital transmission format devised by ITU. The ITU Web site can be found at www.itu.int. An E1 line can transmit data at a rate of 2.048 Mbps, and an E3 line can work at speeds of 34.368 Mbps.

Both T-carriers and E-carriers use four wires, two for receiving and two for sending. Originally copper wires were used (telephone wiring), but digital signals require a clearer connection, so shielded twisted-pair wiring became the preferred wire. The carriers need repeaters that can regenerate the signal every 6,000 feet. Businesses with multiple T1 lines generally use coaxial, fiber optic, or microwave cabling, a high-end, high-performance cabling that can support microwave frequencies. With T3, microwave or fiber optic cabling is required.

A fractional T1 line is an option for organizations that don‘t need a full T1 line. The fractional T1 allows businesses to lease some of the channels of a T1 line rather than leasing all 24 channels. This arrangement is also good for businesses that expect to grow into a T1 line eventually. Each T1 channel has a throughput of 64 Kbps, so a fractional T1 can be leased in 64-Kbps increments.

X.25 and frame relay

Both X.25 and frame relay are packet-switching communication protocols designed for long-distance data transmission rather than the circuit-switching technology used by the telephone system. Packet-switching technology divides data into packets and sends each packet separately; it‘s the technology used by the Internet. Each packet might be sent on a different path. This technology works well, because it can use the bandwidth more efficiently.

Frame relay is based on X.25, but it‘s a digital version, whereas X.25 is an analog technology. Frame relay is digital, so it can support higher throughput of up to 1.544 Mbps, compared with X.25, which supports up to 56 Kbps. X.25 was popular for about 20 years and was the most common packet-switching technology used on WANs. Frame relay, which was standardized in 1984, has largely replaced X.25.

Both X.25 and frame relay use a permanent virtual circuit (PVC). PVC is a logical connection between two nodes. PVCs aren‘t dedicated lines, as the T-carriers are. Rather, when you lease a PVC, you specify the nodes (two endpoints) and the amount of bandwidth required, but the carrier reserves the right to send the data along any number of paths between the two stationary endpoints. You then share the bandwidth with other users who lease the X.25 or frame relay circuit.

The biggest advantage of X.25 and frame relay is that you have to pay for only the amount of bandwidth you require. Frame relay is less expensive than newer technologies, and it has worldwide standards already established. Both X.25 and frame relay use shared lines, so throughput decreases as traffic increases.

Circuits for X.25 aren‘t readily available in North America, but frame relay circuits can be found easily. International businesses that communicate overseas might use frame relay to connect offices.

ATM

Asynchronous Transfer Mode (ATM) is a very fast network technology that can be used with LANs as well as WANs. It uses fixed-length packets, called cells, to transmit data, voice, video, and frame relay traffic. Each cell is 53 bytes, 48 bytes of data plus a 5-byte header. The header contains the information necessary to route the packet. All the packets used by ATM are 53 bytes; it‘s easy to determine the number of packets and the traffic flow, which helps utilize bandwidth.

ATMs also use virtual circuits, meaning the two endpoints are stationary, but the paths between these two endpoints can change. They can use either PVCs or switched virtual circuits (SVCs). SVCs are logical, point-to-point connections that depend on

the ATM to decide the best path along which to send the data. The routes are determined before the data is even sent. In contrast, an Ethernet network transmits the data before determining the route it takes; the routers and switches are responsible for deciding the paths.

ATMs achieve a throughput of 622 Mbps. This makes them popular for large LANs, because they‘re faster than Ethernet at 100 Mbps. An ATM network works best with fiber optic cable, so it can attain high throughput, however, it also works with coaxial or twisted-pair cable. The following table compares a number of communication bandwidth technologies, their common uses, and their speeds.

WAN mesh topology

A mesh network topology is highly reliable and is used when the network reliability is critical and can justify the added expense. A mesh topology provides multiple point-to- point links between routers in a WAN, giving more than one choice on how data can travel from router to router. In a mesh topology, a router searches out multiple paths and determines the best one to take. Routers can make these decisions, based on how busy a network is, how many hops are between two remote networks, how much bandwidth is available, and the cost of using a network. A mesh topology offers added security, because routers can have their own dedicated line connections. A mesh topology also offers added reliability, because there‘s more than one option between routers.

In addition, if one router fails, the WAN can still function. On the other hand, a mesh topology can be rather expensive, as added network cards and cabling are required. It‘s sometimes used on an ATM LAN or WAN.