Communications Network Architecture

2.1 Introduction

In today's complex world, most companies have networks. In fact, most companies have a Web presence as well. A network can range from simply two computers that are linked together to the complexity of computers that can access data across continents. Networks are used to improve communication between departments, foster customer relationships, and share data throughout the world.

As a network administrator, it is your job to manage the network. To do this, you must understand the fundamental networking principles. Having this knowledge will help develop your planning and troubleshooting skills. This chapter provides you with those fundamental principles on which you will build knowledge and experience. It also focuses on the concept of a network, what makes it possible for devices to communicate, and what types of media are used for communication.

When you decide to connect computers to form a network, you have to ask yourself many questions.

- What type of network will you use?
- What operating systems do you have?
- Which operating systems do you want to add?
- How much money do you want to spend?
- What type of hardware and software is best for what you want to do?

The list goes on and on.

You may want to set up a quick and inexpensive network to enable file sharing between your desktop and laptop computers. You may want to build a more complex network that includes a server, six workstations, multiple printers, and other shared resources.

2.2 Understanding Network Basics

All networks use some basic hardware and software, but different configurations of this equipment define the type and uses of the network. For example, you may want to network two computers in the same room. The equipment you use to achieve this network can be different from the hardware you use to network two computers in different rooms or even in different buildings. Similarly, the hardware you use to enable two computers to use one Internet connection is different than the software you use for two computers sharing a printer. Understanding network uses and network types helps you plan your network.

Because networking your home or office is often involved and time-consuming, you need to understand the advantages and disadvantages of networking before planning your network. Understanding the pros and cons of networking helps you plan the exact network that's right for you and your family. In addition, before you can plan your network, buy the hardware and software, you need to understand some basic networking terms and technologies.

If you have two or more PCs in your home, you can save everyone time, energy, and money by networking the computers to share files, printers, and Internet access. There are many names for networks, often related to their size. Local area network (LAN) is perhaps the most common name for a network. A LAN contains two or more computers and is generally housed in one building. Home networks, however, are starting to be called by other names. TAN stands for tiny area network. Then there's HAN, which stands for home area network.

No matter how you use the PC—writing letters, balancing your checkbook, playing games, or surfing the Internet—you can benefit from networking your home computers. Remember, a network is a system that connects two or more computers so that they can communicate and share resources with each other. When you're a member of a network, you have access to more disk space, applications, files, and useful equipment. You can communicate with other users on the network without leaving your desk. You can share files without carrying a flash disk or CD back and forth from computer to computer. You can even share an expensive piece of equipment with everyone else in the building.

For the most part, you'll find that networking your computers benefits everyone in the house or office. Sharing resources makes your computer more efficient and effective, and gives you more equipment with which to work.

No matter what you do, however, there are always some disadvantages. The cost may be too much, for example, or security issues may bother you. Fortunately, there are enough options and solutions to your problems with networking to make the good outweigh the bad.

2.2.1 The Advantages

If you were installing a network for a corporation with hundreds of computers, you could expect a huge and difficult job. Installing a home network, however, is much easier. If you're planning to connect two to ten computers in your home, you can do it with little hassle and with great success.

Many Windows, Macintosh, and Linux computers include the networking software you need; you can purchase the networking hardware and install it all yourself. Alternatively, kits are available that include all the hardware you need to put together a home network. You can choose the features that are important to you, whether you desire speed, shared Internet access, security, or all these features. If you're hesitating about installing a home network, consider the following advantages.

Sharing Files

Share files with everyone on the network. Take some digital photographs and share them with your friends. It's quicker to transfer files across the network than saving them to a disc and copying them from that disc onto another computer. You might want to copy a large file, such as an application file, to your hard drive. You can copy it over the network instantly. Copying files is also an excellent method of backing up files; you can save extra copies of pictures, letters, and other valuable files on another computer on the network.

Sharing Disk Space

Disk space is always at a requirement in modern day computing. With graphic and image files, music files, large application files, and data files taking up your hard disk space, you can take advantage of a network and save files to any hard disk on the network. If you do not need your 60 gigabytes (GB) of hard disk

space, you can share it with your friend for saving pictures of the family or for storing music files.

In addition to sharing hard disks, you can share file storage drives, such as tape drives, Zip drives, CD burners, and even flash disk drives. Sharing a flash disk that holds 1GB or 2GB of data means you can save your data files on one or two disks and access them whenever you want, even if they are on another computer in the network. Imagine sharing a CD burner—that's over 600MB of space. Share your DVD burner for over 4.5GB of space for each disc.

Creating Backups

Backing up your data files is important. You should always keep an extra copy of important files in case your hard disk goes bad, a file becomes corrupted, or someone accidentally deletes your work. You can back up all of your data quickly and easily over the network—on either a storage disk or on another hard disk. Restoring that data would also be quick and easy over the network. Backups are even more important in a small-business office, because accounts receivable and payable data, customer information, inventory, and other critical data can result in lost business if your hard disk crashes or becomes corrupted.

Sharing Peripherals

Expensive peripherals—such as a color inkjet or laser printer—are more affordable if everyone on the network can use them. If a printer isn't networked, only one person has continual use of that piece of equipment. Naturally, others can move to the computer to which it's attached, but that may not always be convenient or appropriate. If the peripheral is attached to the network, however, everyone can make use of it. You'll save money and time, and do more with less.

Working with Applications (Centralized Software Management)

One of the greatest benefits of installing a network in an organization is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.

Multiplayer games—such as Need for Speed —have gained popularity over the last year. Many games are available for two or more players to participate in concurrently. With Networked computers you can connect and share a game with your friends and have fun.

Additionally, suppose that you want to install a program from CD-ROM, but the CD-ROM drive attached to your computer is only a 2× speed. Your friend, however, has an 8× CD-ROM drive. Using the network, you can install the application from the 8× drive much more quickly.

Accessing the Internet

Sharing Internet access is ideal for many communities. If you have one Internet service provider (ISP) account but you have two, three, or more people who want to connect to the Internet, you can achieve that with a network without constraint, separate telephone lines, and separate Internet accounts. Using the right software or hardware, you can configure your modem—including telephone modem, Digital Subscriber Line (DSL), or cable modem—to connect to the Internet and simultaneously share that connection with other users. One person can collect e-mail, another can watch a movie, and a third can do facebook, all at the same time.

In addition to using the Internet for Web browsing, you can send and receive e-mail over the Internet. Similarly, you can set up your own e-mail system in your community eg Makerere Webmail. Send a memo to your loved one about a family gathering over the weekend; send notes to your dad about bills that are due or appointments to keep. Sending and receiving e-mail is one of the most popular computer pastimes in the world today, and you can set up your own mail system on your network or e-mail over the Internet, if you prefer.

Expanding your Network

As you begin using your network, you may decide to expand the network. You could, for example, attach to a network at work, via an extranet or a virtual private network (VPN). You may also want to develop your network to control more than just your computers.

If your job is one in which you can work from home, either part-time or full-time, you can not only network your home computers, but also attach to a work computer. E-mail your coworkers, print documents, send and receive files, and more, all from the comfort of your home.

Using your computer to control your heat and air conditioning, telephones, security systems, TV and video, and your PC network are not dreams of the future; they are available now. Networking your home can be as simple as sharing a printer or as complex as home automation.

Security

Sensitive files and programs on a network can be password protected. Then those files can only be accessed by the authorized users. This is another important advantage of networking when there are concerns about security issues. Also each and every user has their own set of privileges to prevent them accessing restricted files and programs.

2.2.2 The Disadvantages

While there are many advantages to installing a home or office network, there can be disadvantages too. If you're seriously thinking about setting up your own network, you should be informed about all of the advantages and disadvantages too.

Expensive to Install

For one, networks can be pricey to set up. While in the long term networks generally save you money, the initial costs of installation can be high. Cables, network cards, and software are expensive, and the installation may require the services of a technician, depending on how many computers are involved and what type of network it is.

Administrative Time Requirements

Proper maintenance of a network takes time and training. Many people will set up a network and find they have not budgeted for the required maintenance. Depending on the size of the network you may need to hire administrative support or take some informal training of your own.

File Server Failures

When a file server goes down, this can mean the entire network comes to a halt. While file servers are no more susceptible to failure than any other computer, the failure of a file server can mean a lot more productivity loss than the failure

of a workstation or stand-alone computer, since the entire network can lose access to needed programs and files.

Broken Cables:

While some network configurations can minimize the inconvenience of a broken cable, with other configurations, a broken cable can mean a halt to the entire network, when setting up your network, be aware of the impact of configuration on problems like this.

Security Threats

Security threats are always problems with large networks. There are hackers who are trying to steal valuable data of large companies for their own benefit. So it is necessary to take utmost care to facilitate the required security measures.

Bandwidth Issues

In a network there are users who consume a lot more bandwidth than others. Because of this some other people may experience difficulties in using a shared resource.

Although there are disadvantages to networking, it is a vital need in today's environment. People need to access the Internet, communicate and share information and they can't live without that. Therefore engineers need to find alternatives and improved technologies to overcome issues associated with networking. Therefore we can say that computer networking is always beneficial to have even if there are some drawbacks.

2.3 Network Line Configuration

Network Line configuration refers to the way two or more communication devices attached to a link. Line configuration is also referred to as connection. A link is a communication medium through which data is communicated between devices. For communication to occur between two devices, they must be connected to the same link at the same time. The two possible types of line configurations or connections are discussed in the next sections.

2.3.1 Point-to-Point Connection

The point-to-point connection provides a dedicated link between two communication devices. In this type of network, when a message is sent from one computer to another, it usually has to be sent via other computers in the network. A point-to-point network shown in Figure 2-1 below consists of many connections between individual pairs of computers. As a general rule, large networks such as Wide Area Networks are organized in this fashion. This type of network is sometimes called a store and forward network or a packet switched network. It Provides a dedicated link between two devices use actual length of wire or cable to connect the two end including microwave & satellite link. Infrared remote control & tvs remote control.

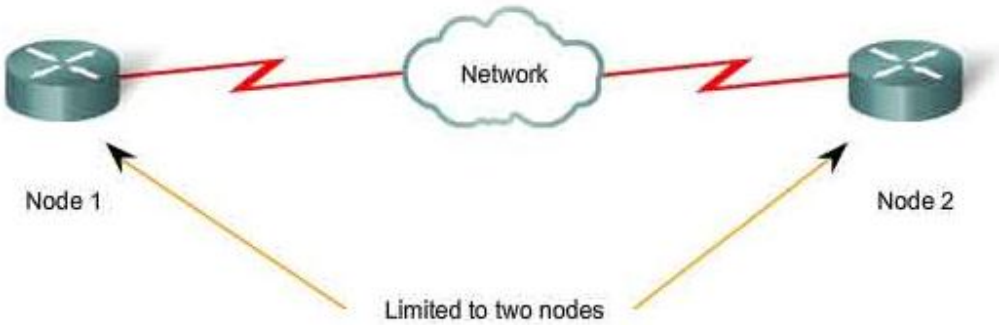

Figure 2-1: Point to Point Network

A good example of a point-to-point network is a computer that is connected to a local printer by a USB cable. Although highly reliable, there is no way for either node to connect to anything else using that one USB connection. Also, without any redundancy, the entire connection is dependent on the USB cable as well. However, the point-point network is impractical from a networking standpoint because rarely is only one connection between two nodes adequate. The point-to-point network can be compared to two soup cans connected by a string. Although there is nothing to interrupt the connection, there is no ability for the network to branch out and make more connections.

2.3.2 Multipoint Connection

Multipoint connection is also referred to as multidrop connection. This type of connection allows multiple devices (more than two devices) to share a single link. The multipoint connection or line configuration is shown in Figure 2-2

below. A typical example of a multipoint connection is the internet where more than one device can access a dedicated server.

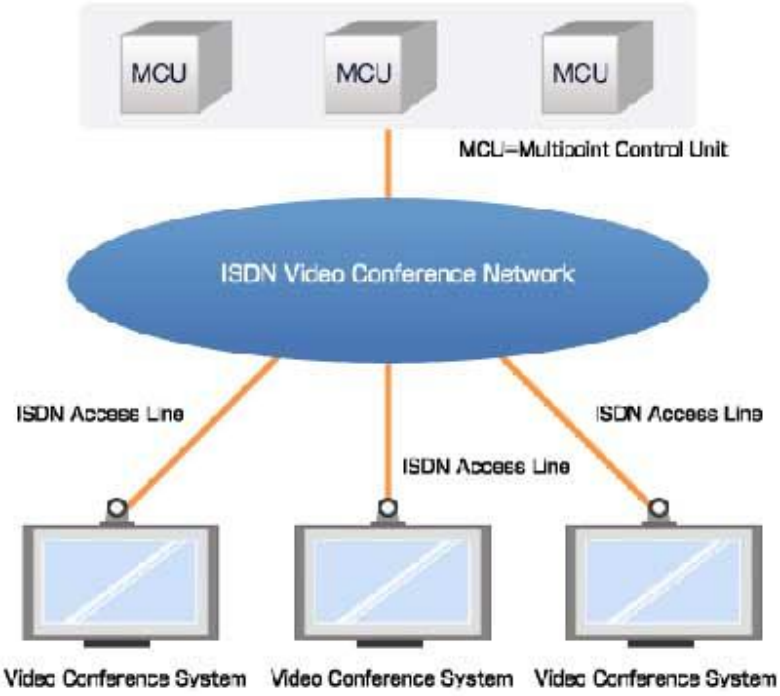

Figure 2-2: Multipoint Connection

2.4 Network Topologies

In simple terms, a computer network consists of two or more connected computers. When computers are connected, we must choose network infrastructure, which is the combination of all the physical and logical components. Network topology defines the structure of the network. It falls into two categories: Physical and Logical topology. Physical topology is the actual layout of the wire or media. The physical topologies used in Local Area Networks (LAN) are shown in Figure 2-3 below:

- Ring topology, which connects one host to the next and the last host to the first. This creates a physical ring of cable.
- A mesh topology is implemented to provide as much protection as possible from interruption of service. As seen in the graphic, each host has its own connections to all other hosts. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.

- Star topology, which connects all cables to a central point of concentration.

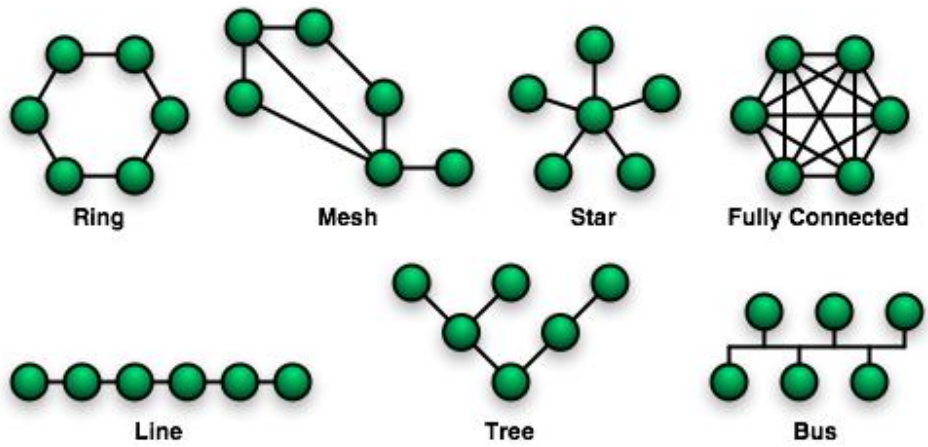

Figure 2-3: Physical Topologies Used in Local Area Networks

- The Line topology connects one host to the next and the last host doesn't connect to the first. This creates a physical line of cable.
- A tree (hierarchical) topology is similar to an extended star. However, instead of linking the hubs and/or switches together, the system is linked to a computer that controls the traffic on the topology.
- Bus topology, which uses a single backbone cable that is terminated at both ends. All the hosts connect directly to this backbone. A backbone is the part of a network that handles the major traffic, consisting of many different networks and running long distances. It is made up of a large collection of interconnected commercial, government, academic and other high-capacity data routes and core routers that carry data across the countries, continents and oceans of the world.

The **logical topology** of a network is how the hosts communicate across the medium. The two most common types of logical topologies are broadcast and token passing.

Broadcast topology simply means that each host sends its data to all other hosts on the network medium. There is no order that the stations must follow to

use the network. It is first come, first serve. Ethernet works this way as will be explained later in the course.

Token passing which controls network access by passing an electronic token sequentially to each host. When a host receives the token, that host can send data on the network. If the host has no data to send, it passes the token to the next host and the process repeats itself. Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (FDDI).

2.5 Networking and Internetworking Devices

2.5.1 A Router

A router is an intelligent connecting device that can send packets to the correct LAN segment to take them to their destination. Routers form the backbone of the internet. A router directs data packets from one network to another as shown in Figure 2-4. Routers link LAN segments at the network layer of the OSI Reference Model for computer- to-computer communications. The networks connected by routers can use similar or different networking protocols. A router may be one or more of the following types:

- **Central** Acts as a network backbone, connecting many LANs.
- **Peripheral** Connects individual LANs to either a central router or to another peripheral router.
- **Local** Operates within its LAN driver's cable-length limitations.
- **Remote** Connects beyond its device\ driver limitations, perhaps through a modem\ or remote connection.
- **Internal** Part of a network file server.
- **External** Located in a workstation on the network.

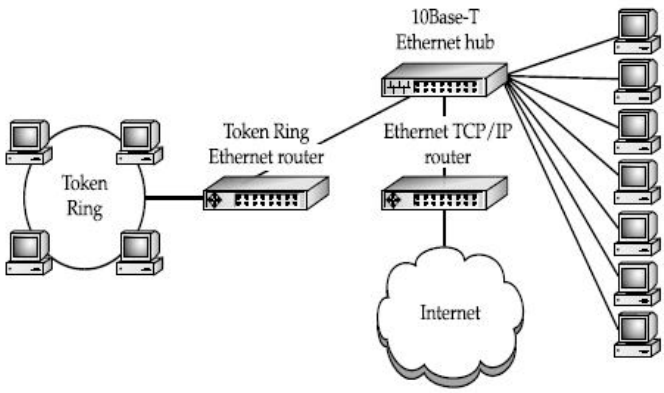

Figure 2-4: Networking Using a Router

2.5.2 A Hub

A hub, sometimes called a concentrator, is a device that connects a number of network cables coming from client computers to a network. Hubs come in many different sizes, supporting from as few as two computers up to large hubs that may support 60 computers or more. (The most common hub size supports 24 network connections.) All the network connections on a hub share a single collision domain, which is a fancy way of saying all the connections to a hub "talk" over a single logical wire and are subject to interference from other computers connected to the same hub. A typical hub is shown in Figure 2-5.

Figure 2-5: A Typical Hub

2.5.3 A Switch

A switch is wired very similar to a hub, and actually looks just like a hub. However, on a switch all of the network connections are on their own collision domain. The switch makes each network connection a private one, and then collects the data from each of the connections and forwards the data to a network backbone, which usually runs at a much higher speed than the individual switch connections. Often, switches are used to connect many hubs to a single network backbone. Switches are a lot like bridges, except that they have many ports and otherwise look like a hub. You might think of a switch as a sort of multiport bridge. Figure 2-6 shows a typical switch and hub wiring arrangement.

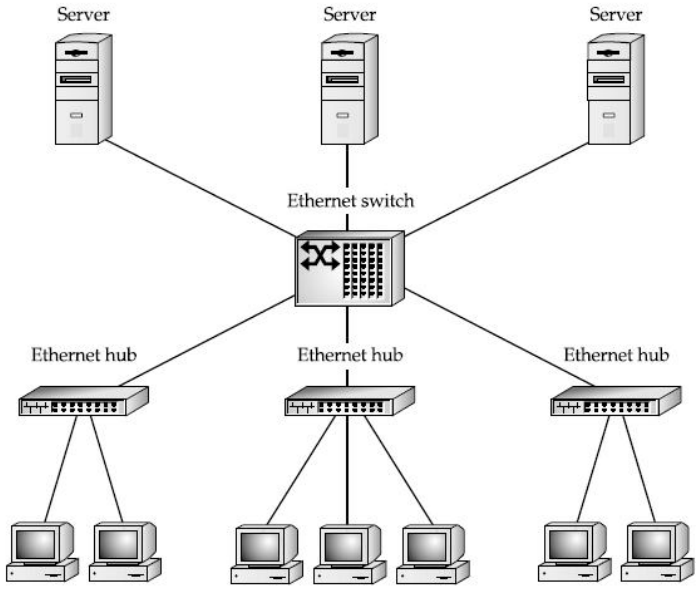

Figure 2-6: Using Hubs and Switches

2.5.4 Repeaters

A repeater is a device that extends the distance of a particular network run. It takes a weak network signal in on one side, boosts the signal, then sends it out its other side. For instance, if you have to run a 10Base-T cable longer than 100 meters, a repeater enables you to double that distance. Repeaters operate at the physical layer of the OSI networking model. They do not have the intelligence to understand the signals that they are transmitting. Repeaters merely amplify the signal coming in either side and repeat it out their other side. (Remember, however, they also amplify any noise on the cable!)

Repeaters are only used to connect the same type of media, such as 10Base-2 to 10Base-2, or Token Ring to Token Ring. Repeaters do have a small amount of intelligence that can be useful. They can segment one of their connections from the other when there is a problem. For example, consider two segments of Thin Ethernet that are connected using a repeater. If one of those segments is broken, the repeater still allows the good segment to continue working within itself. Users on the good segment will be unable to connect to resources on the broken segment, but they can continue to use the good segment without trouble. (Remember, though, this capability does you little good if your servers are on the broken segment and your workstations are on the good segment!) Figure 2-7 shows a network extension using repeaters.

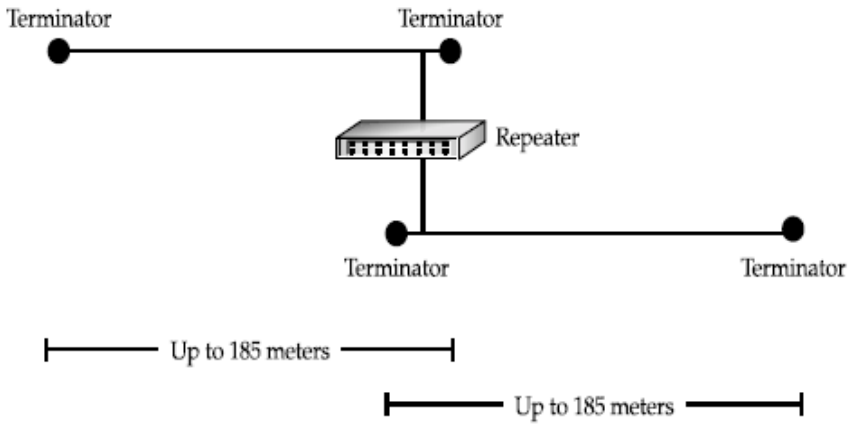

Figure 2-7: Using a repeater to increase network length

2.5.5 A Bridge

Bridges are basically more intelligent versions of repeaters. Bridges can connect two network segments together, but they have the intelligence to pass traffic from one segment to another only when that traffic is destined for the other segment. Bridges are, therefore, used to segment networks into smaller pieces. Some bridges are also available that can span different networking systems and media, such as from coaxial Thin Ethernet to twisted-pair Token Ring.

Bridges operate one layer higher, at the data-link layer (Layer 2). Bridges examine the Media Access Control (MAC) address of each packet they encounter to determine whether they should forward the packet to the other network. Bridges contain address information about all the parts of your network, through either a static routing table that you program or a dynamic, learning-tree system that discovers all the devices and addresses on the network.

2.6 Connection-oriented and connectionless services

The two primary types of services which are made available by a particular network layer and which actually are also useful classifications for many non-technical types of service industries are known as connection-oriented and connectionless communication.

2.6.1 Connection-oriented Services

One of the easiest ways to understand what a connection-oriented protocol is would be to think of a very familiar service upon which it's based: the telephone

system. When you pick up the phone, you have an open circuit, and the dial tone carrier signal allows you to connect to a destination of your choice.

Given valid input parameters, the service:

- Establishes the connection.
- Allows you to utilize the connection.
- Tears down the connection when you done using it.

The primary difference between this method and that of a connectionless service is that in a connection-oriented system, all of your communications are taking place on the same transmission channel. On the other hand, with a connectionless service, all transmissions are independently routed, and perhaps re-assembled in some order at the other end -- the service in between has no inherent responsibility for ensuring ordinality -- it need only assure that each transmission gets delivered from its source to its destination.

2.6.2 Connectionless Services

A good analogy for a connectionless service is the process of sending letters through the postal system. Each transmission (the "letter") contains the full destination address and is processed independent of related messages. As described above, the service has only to ensure that each reaches its host within certain time parameters. Unlike a connection-oriented service, the system has free reign on what happens enroute between the sender and receiver:

- A message can be delayed to ensure another arrives first
- Widely different channels of communication can be used for transmitting messages
- A message can be handed off to a trusted third party in the distribution network
- A message can be intercepted by a third party, copied or logged, and passed on to the intended receiver

These operations are basically impossible for a connection-oriented service.