NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

INTRANET CABLING AND COMMUNICATION TECHNIQUES

Graduation Project
EE- 400

Student: Osama Al-najjar (980678)

Supervisor: Assoc. Prof. Dr Doğan Akay

Lefkoşa - 2002

TABLE OF CONTENTS

AKNOWLEDGMENTS

At the beginning I would like to thank Dr Doğan Akay for being my advisor in this work. Under his supervision I was able to pass through many difficult problems in my project, I learned a lot from him about the network and the internet, he always answered my questions generously, and his answers were more than enough for me. I really appreciate his efforts in supporting me scientifically and immaterially.

Thanks to faculty of engineering specially and to Near East University generally for providing such an interesting educational environment.

Special thanks to Mr. İsmail, Murat, and all the family there in Microsolutions. With there experience in networks, I had a lot of practice, and I successfully overcome many competitive problems. Thanks for Microsolutions for having such a good emulative environment.

Personal thank to my fiancé. With her considerateness and support I felt the ability to face and surmount very difficult and despair moments.

I also want to thank my life friends: Adnan, Hussein, Ramadan, Mohammed, Omran, and Samer. Being with them made 4 years of my life full of exciting, wonderful and fascinating moments, which I will never forgot.

Thanks to the partner who I passed with him the most difficult, exciting and interesting journey in my life- or I should say "Until know at least"- SMB.

Finally, I want to thank my family, especially my parents. There continuous support and endless love, brought me to this position. I would like to dedicate this work as a humble thank to them. I wish them a place in the heaven after a long healthy and happy life.

ABSTRACT

These papers introduces the basic concepts and principles that underlie computer networking, from the simplest peer-to-peer local area networks to the vastly complex wide area networks that reach across international boundaries and around the world. Presents an overview of networking terminology, examine different network topologies and architectures, and focus on the physical components of computer networks, including server and client computers, and cabling and connectors. Also investigates what occurs within computers when they are linked and how they send and receive messages, including the standards and protocols that govern network communication. It also describes the basic implementation of a network, including detailed information about network topologies, cables, protocols and a lot of network components. It discusses system accessing methods and data transmission through different media. It provides several solutions for difficult conditions.

INTRODUCTION

The human beings are always looking for the perfect ness, that is why you can hear about a new invention every day, the needs that met the people mad them in thinking and creation mod almost every second in there life's. No body could believe that from where you are setting, you can talk to a friend who is in the other end of the world, but this became a true when the telephone first was invented, but it didn't end up there, human tried again and again to modify the solution to have better results, results which are faster, easier and cheaper, the solution was unclear, its way was difficult and took a lot of time, but at the end the results were achieved and the solution was THE INTERNET.

This thesis aimed to highlight on the basics of the internet, those small, medium and large intranets.

The thesis consists of the introduction, four chapters and conclusion.

Chapter one introduces the networks. We discuss some basic principles of computer-based networking and looks at different network configurations.

Chapter two presents the cabling system of the networks. We focus on the cables that connect the network and examine there construction.

Chapter three describes the network architecture. We study the accessing methods and discuss how the network handles data.

Chapter four is devoted to the network protocols. We explore different types of protocols and focus on the major protocol being used nowadays, which is TCP/IP.

The conclusion summarizes an important results obtained by the author of the thesis showing the depth of the networking job.

CHAPTER 1

INTRODUCTION TO NETWORKING

1.1 Introduction

As all the technologies, the network were an invention created first to serve military needs. It all started during the world wars, and continued after the second world war, the related nations stared to think of a fast, easy and cheap communication method to use in order to defeat the enemy, we can notice that by looking where the networks were first invented, without specifications, definitely in one or more of the fighter nations. After that these technologies released to the public to allow them to get the most benefit form it.

Far away from the internet as an example of a network, humans are almost using the networks in every aspect in there life's, in the universities for example, network became the major require that should be available for students, at lest to grant the access to the internet- which is the riches resource available on the earth nowadays-to every site there. Considering a commercial view of point, the internet became the cheapest communication method all over the world, so it was obvious that most of the companies are using the internet as it's main communication way. Form that sense, granting access to the internet for more than one line was impossible without using networks, and off course using network has a lot more benefits where ever it has been used, then just granting access to the internet.

This chapter introduces some basic principles of computer-based networking, discusses advantages of networking, presents the idea of connecting computers together to form a local area network (such as a corporate intranet) and a wide area network (such as the Internet), looks at different network configurations and explores the major features and advantages of different kinds of networks and describes designs for connecting computers.

1.2 What is networking?

1.2.1 The Concept of Networking

The idea of networking has been around for a long time and has taken on many meanings. If you were to look up "network" in your dictionary, you might find any of the following definitions:

- An openwork fabric; netting
- A system of interlacing lines, tracks, or channels
- Any interconnected system; for example, a television-broadcasting network
- A system in which a number of independent computers are linked together to share data and peripherals, such as hard disks and printers

Obviously, the last definition is the one we are concerned with in this course. The key word in the definition is "share." Sharing is the purpose of computer networking. The ability to share information efficiently is what gives computer networking its power and its appeal. And when it comes to sharing information, human beings are in many ways similar to computers. Just as computers are little more than collections of the information they have been given, so we are, in large part, collections of our experiences and the information given to us. When we want to expand our knowledge, we broaden our experience and gather more information. For example, to learn more about computers, we might talk informally with friends in the computer industry, go back to school and take a class, or work through a self-paced training course like this one. Whichever options we choose, when we seek to share the knowledge and experiences of others, we are networking.

Another way to think of networking is to envision a network as a team. This might be a sports team, such as a football team, or a project team, such as the one that created this training course. Through the efforts of all involved—the sharing of time, talent, and resources—a goal is accomplished or a project is completed. Similarly, managing a computer network is not unlike managing a team of people. Sharing and communicating can be simple and easy (a quarterback calling a play in the huddle) or complex (a virtual project team located in different time zones around the world that communicates through

teleconferencing, e-mail, and multimedia presentations over the Internet to complete a project).

1.2.2 Introducing Computer Networking

At its most elementary level, a computer network consists of two computers connected to each other by a cable that allows them to share data. All computer networking, no matter how sophisticated stems from that simple system. While the idea of connecting two computers by a cable may not seem extraordinary, in retrospect it has proven to be a major achievement in communications.

Computer networking arose as an answer to the need to share data in a timely fashion. Personal computers are powerful tools that can process and manipulate large amounts of data quickly, but they do not allow users to share that data efficiently. Before networks, users needed either to print out documents or copy document files to a disk for others to edit or use them. If others made changes to the document, there was no easy way to merge the changes. This was, and still is, known as "working in a stand-alone environment." (See Figure 1.1.)

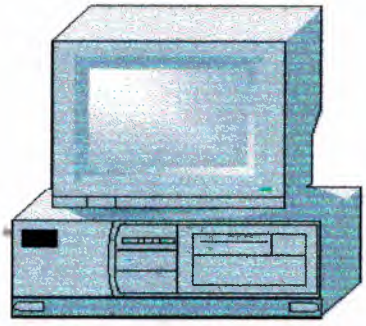

Figure 1.1 *Stand-alone environment*

Copying files onto floppy disks and giving them to others to copy onto their computers was sometimes referred to as the "sneakernet." This early form of computer networking is one that many of us have used and perhaps still use today. See Figure 1.2; it might bring back some fond memories.

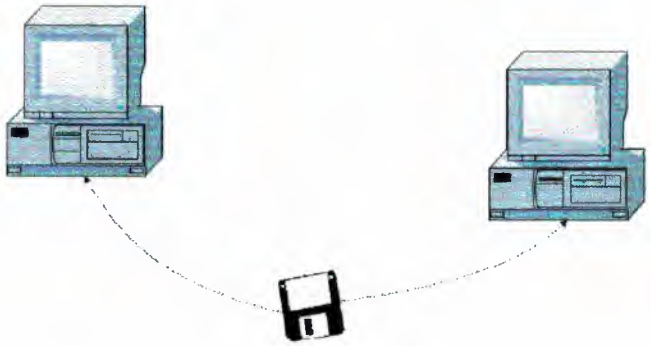

Figure 1.2 *The sneakernet*

This system works well in certain situations and has its advantages—it allows us to stop for a cup of coffee or socialize with a friend while we exchange and merge data—but it is far too slow and inefficient to meet the needs and expectations of today's computer users. The amount of data available to be shared and the distances we want the data to travel far exceed the capabilities of the sneakernet.

But what if the computer shown in Figure 1.1 were to be connected to other computers? Then, it could share data with the other computers and send documents to the other printers. This connecting together of computers and other devices is called a *network*, and the concept of connected computers sharing resources is called networking. (See Figure 1.3.)

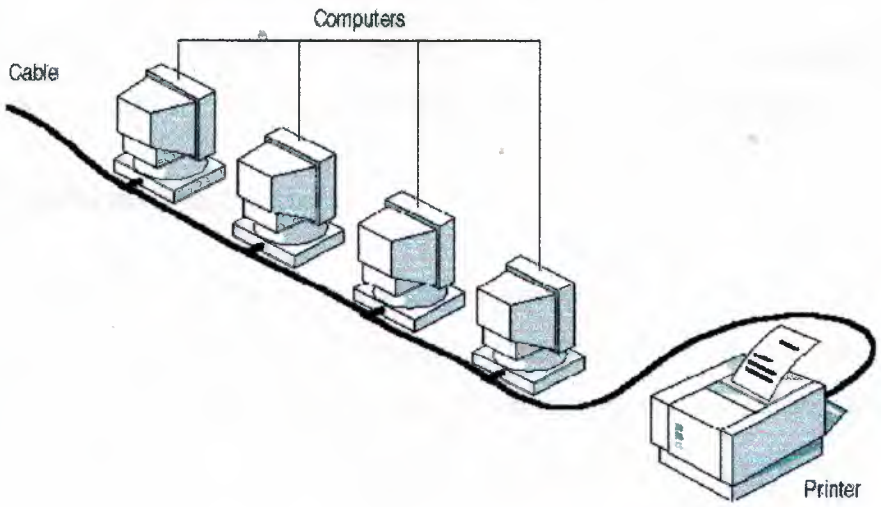

Figure 1.3 *A simple computer network*

1.2.3 Why Use a Computer Network?

With the availability and power of today's personal computers, you might ask why networks are needed. From the earliest networks to today's high-powered personal computers, the answer has remained the same: networks increase efficiency and reduce costs. Computer networks achieve these goals in three primary ways:

- Sharing information (or data)
- Sharing hardware and software
- Centralizing administration and support

More specifically, computers that are part of a network can share:

- Documents (memos, spreadsheets, invoices, and so on).
- E-mail messages.
- Word-processing software.
- Project-tracking software.
- Illustrations, photographs, videos, and audio files.
- Live audio and video broadcasts.
- Printers.
- Fax machines.
- Modems.
- CD-ROM drives and other removable drives, such as Zip and Jaz drives.
- Hard drives.

And more sharing options exist. The capabilities of networks are constantly expanding as new ways are found to share and communicate by means of computers.

1. Sharing Information (or Data)

The ability to share information quickly and inexpensively has proven to be one of the most popular uses of networking technology. It has been reported that e-mail is by far the number-one activity of people who use the Internet. Many businesses have invested in networks specifically to take advantage of network-based e-mail and scheduling programs.

By making information available for sharing, networks can reduce the need for paper communication, increase efficiency, and make nearly any type of data available simultaneously to every user who needs it. Managers can use these utilities to communicate quickly and effectively with large numbers of people and to organize and schedule meetings with people drawn from an entire company or business enterprise far more easily than was previously possible. (See Figure 1.4.)

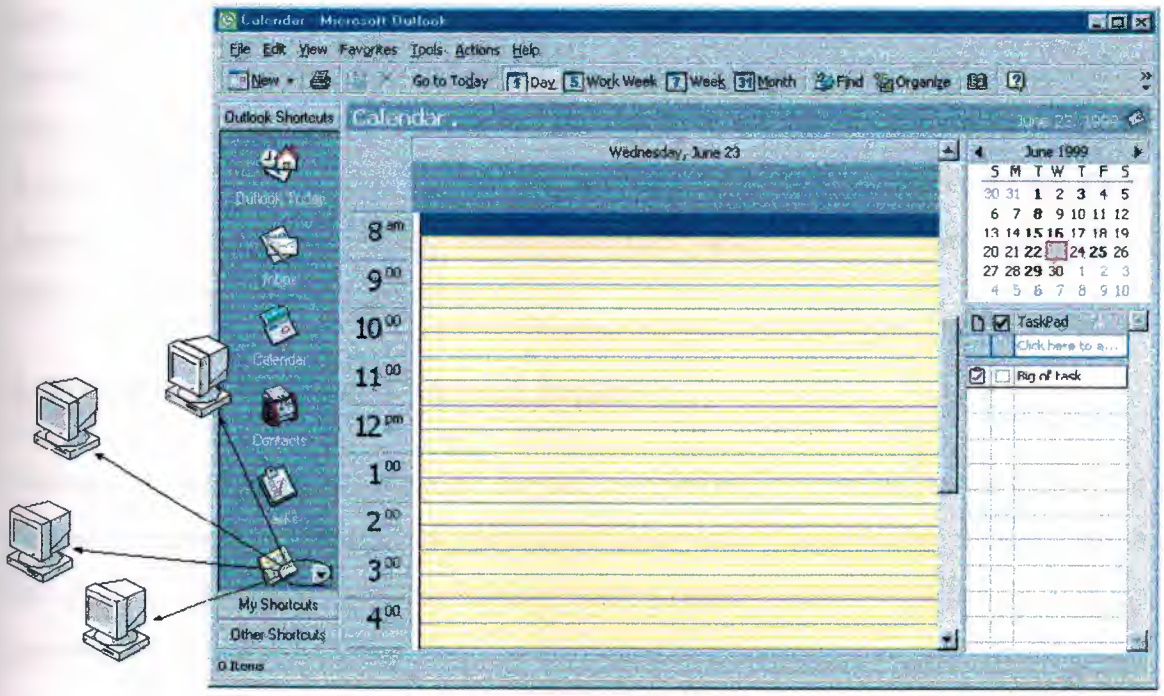

Figure 1.4 *Scheduling a meeting with Microsoft Outlook*

2. Sharing Hardware and Software

Before the advent of networks, computer users needed their own printers, plotters, and other peripherals; the only way users could share a printer was to take turns sitting at the computer connected to the printer. Figure 1.5 shows a typical stand-alone workstation with a printer.

Networks make it possible for several people to share data and peripherals simultaneously. If many people need to use a printer, they can all use the printer available on the network. Figure 1.6 shows a typical network environment in which five workstations share a single printer.

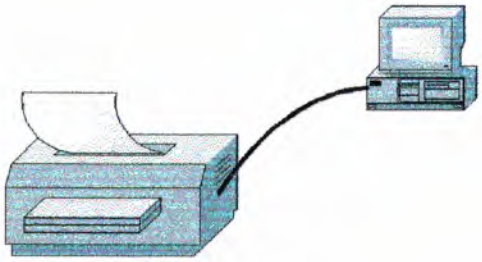

Figure 1.5 *A printer in a stand-alone environment*

Networks can be used to share and standardize applications, such as word processors, spreadsheets, inventory databases, and so on, to ensure that everyone on the network is using the same applications and the same versions of those applications. This allows documents to be shared easily and creates training efficiencies: it is easier for people to master one word processing application thoroughly than to try to learn four or five different word processing applications.

3. Centralizing Administration and Support

Networking computers can simplify support tasks as well. It is far more efficient for technical personnel to support one version of one operating system or application and to set up all computers in the same manner than to support many individual and unique systems and setups.

1.2.4 The Two Major Types of Networks: LANs and WANs

Computer networks are classified into one of two groups, depending on their size and function. A *local area network (LAN)* is the basic building block of any computer network. A LAN can range from simple (two computers connected by a cable) to complex (hundreds of connected computers and peripherals throughout a major corporation). (See Figure 1.7.) The distinguishing feature of a LAN is that it is confined to a limited geographic area.

A *wide area network (WAN),* on the other hand, has no geographical limit (see Figure 1.8). It can connect computers and other devices on opposite sides of the world. A WAN is made up of a number of interconnected LANs. Perhaps the ultimate WAN is the Internet.

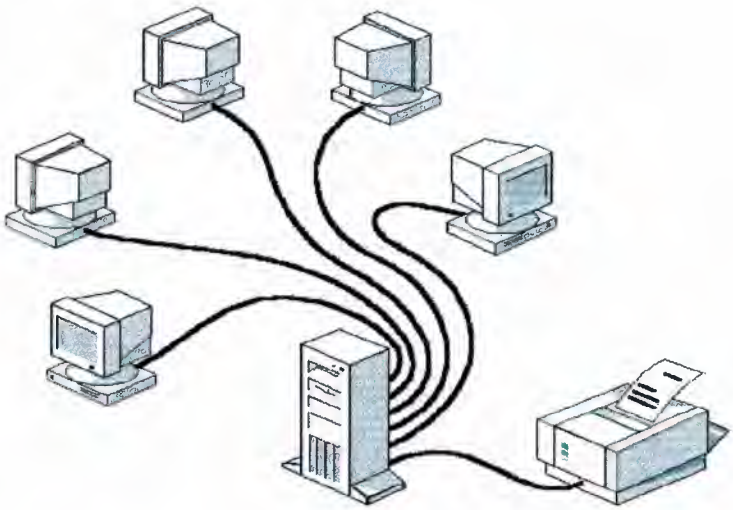

Figure 1.6 *Sharing a printer in a networking environment*

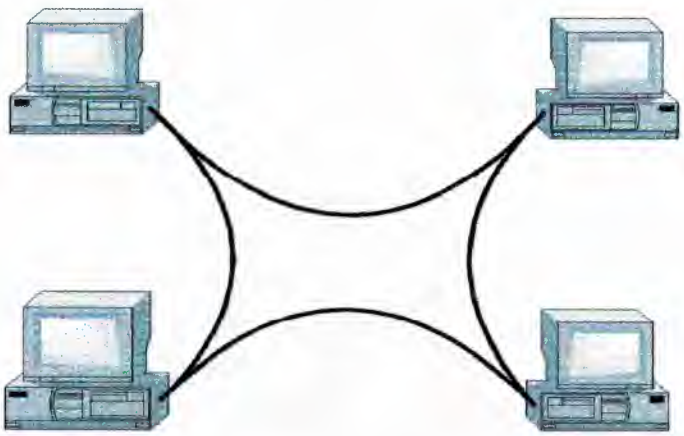

Figure 1.7 *A local area network (LAN)*

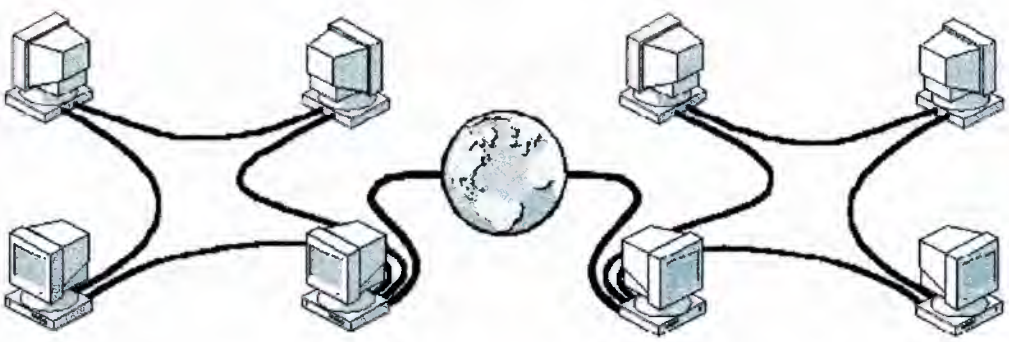

Figure 1.8 *A wide area network (WAN)*

1.3 Network configuration

1.3.1 Network Configuration Overview

In general, all networks have certain components, functions, and features in common, shown in Figure 1.9. These include:

- Servers—Computers that provide shared resources to network users.
- Clients—Computers that access shared network resources provided by a server.
- Media—The wires that make the physical connections.
- Shared data—Files provided to clients by servers across the network.
- Shared printers and other peripherals—Additional resources provided by servers.
- Resources—Any service or device, such as files, printers, or other items, made available for use by members of the network.

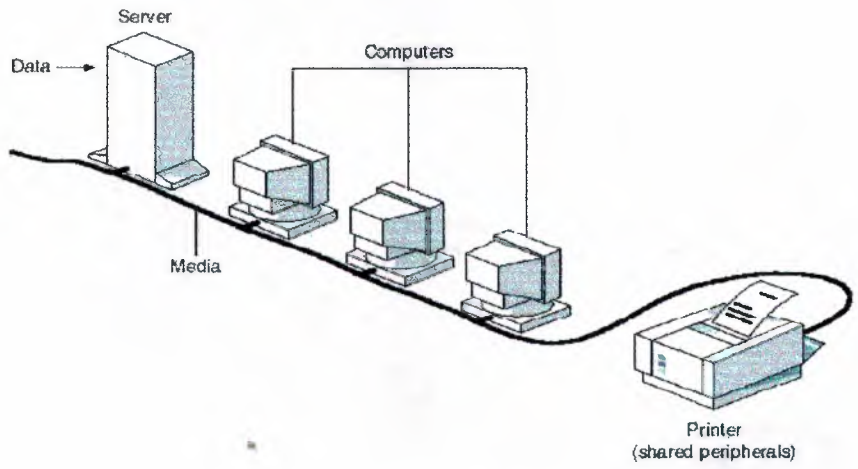

Figure 1.9 *Common network elements*

Even with these similarities, networks are divided into two broad categories, illustrated in Figure 1.10:

- Peer-to-peer networks
- Server-based networks

The distinction between peer-to-peer and server-based networks is important because each type has different capabilities. The type of network you choose to implement will depend on factors such as the:

- Size of the organization.
- Level of security required.
- Type of business.
- Level of administrative support available.
- Amount of network traffic.
- Needs of the network users.
- Network budget.

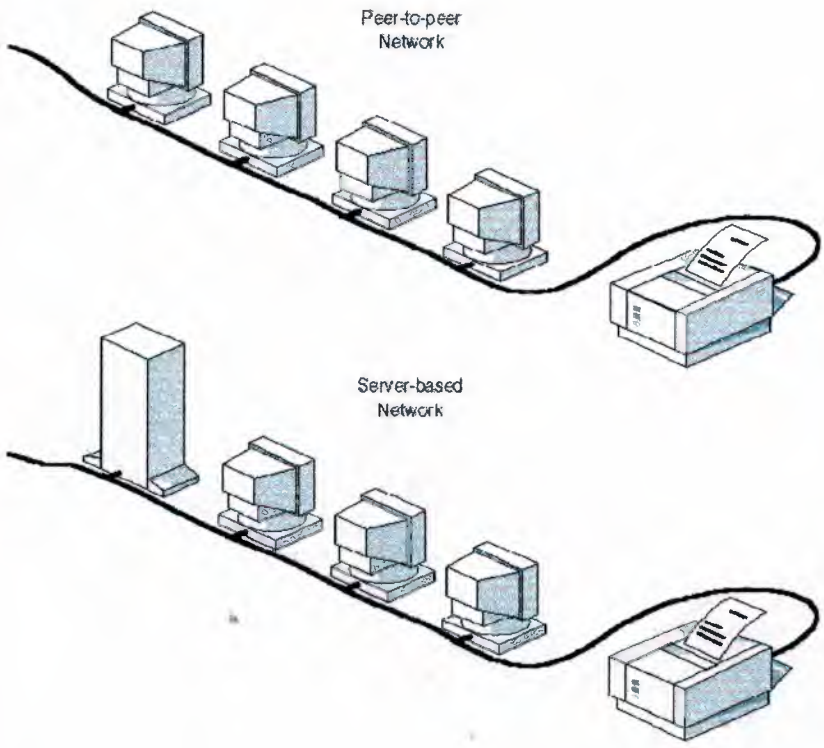

Figure 1.10 *Typical peer-to-peer and server-based networks*

1.3.2 Peer-to-Peer Networks

In a peer-to-peer network, there are no dedicated servers, and there is no hierarchy among the computers. All the computers are equal and therefore are known as peers. Each computer functions as both a client and a server, and there is no administrator

responsible for the entire network. The user at each computer determines what data on that computer is shared on the network. Figure 1.11 shows a peer-to-peer network in which each computer functions as both a client and a server.

- **Size**

Peer-to-peer networks are also called *workgroups*. The term "workgroup" implies a small group of people. There are typically 10 or fewer computers in a peer-to-peer network.

- **Cost**

Peer-to-peer networks are relatively simple. Because each computer functions as a client and a server, there is no need for a powerful central server or for the other components required for a high-capacity network. Peer-to-peer networks can be less expensive than server-based networks.

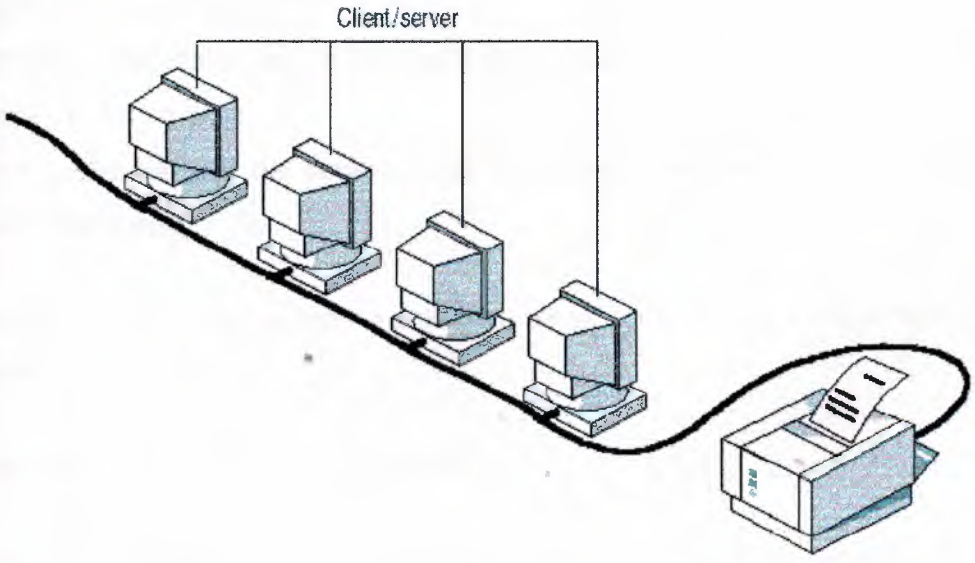

Figure 1.11 *Peer-to-peer network computers act as both clients and servers*

- **Operating Systems**

In a peer-to-peer network, the networking software does not require the same standard of performance and level of security as the networking software designed for dedicated

servers. Dedicated servers function only as servers and not as clients or workstations. They are discussed in more detail later in this lesson.

Peer-to-peer networking is built into many operating systems. In those cases, no additional software is required to set up a peer-to-peer network.

- **Implementation**

In typical networking environments, a peer-to-peer implementation offers the following advantages:

- Computers are located at users' desks.
- Users act as their own administrators and plan their own security.
- Computers in the network are connected by a simple, easily visible cabling system.

Where a Peer-to-Peer Network Is Appropriate

Peer-to-peer networks are good choices for environments where:

- There are 10 users or fewer.
- Users share resources, such as files and printers, but no specialized servers exist.
- Security is not an issue.
- The organization and the network will experience only limited growth within the foreseeable future.

Where these factors apply, a peer-to-peer network will probably be a better choice than a server-based network.

Peer-to-Peer Network Considerations

Although a peer-to-peer network might meet the needs of small organizations, it is not appropriate for all environments. The rest of this section describes some of the considerations a network planner needs to address before choosing which type of network to implement.

1. Administration

Network administration tasks include:

- Managing users and security.
- Making resources available.
- Maintaining applications and data.
- Installing and upgrading application and operating system software.

In a typical peer-to-peer network, no system manager oversees administration for the entire network. Instead, individual users administer their own computers.

2. Sharing Resources

All users can share any of their resources in any manner they choose. These resources include data in shared directories, printers, fax cards, and so on.

3. Server Requirements

In a peer-to-peer environment, each computer must:

- Use a large percentage of its resources to support the user at the computer, known as the *local user*.
- Use additional resources such as hard-disk space and memory, to support the user's accessing resources on the network, known as the *remote user*.

While a server-based network relieves the local user of these demands, it requires at least one powerful, dedicated server to meet the demands of all the clients on the network.

4. Security

On a computer network, *security* (making computers and data stored on them safe from harm or unauthorized access) consists of setting a password on a resource, such as a directory, that is shared on the network. All peer-to-peer network users set their own security, and shared resources can exist on any computer rather than on a centralized server only; consequently, centralized control is very difficult to maintain. This lack of control has a big impact on network security because some users may not implement any

security measures at all. If security is an issue, a server-based network might be a better choice.

5. Training

Because every computer in a peer-to-peer environment can act as both a server and a client, users need training before they are able to function properly as both users and administrators of their computers.

1.3.3 Server-Based Networks

In an environment with more than 10 users, a peer-to-peer network—with computers acting as both servers and clients—will probably not be adequate. Therefore, most networks have dedicated servers. A *dedicated* server is one that functions only as a server and is not used as a client or workstation. Servers are described as "dedicated" because they are not themselves clients, and because they are optimized to service requests from network clients quickly and to ensure the security of files and directories. Server-based networks (see Figure 1.12) have become the standard models for networking.

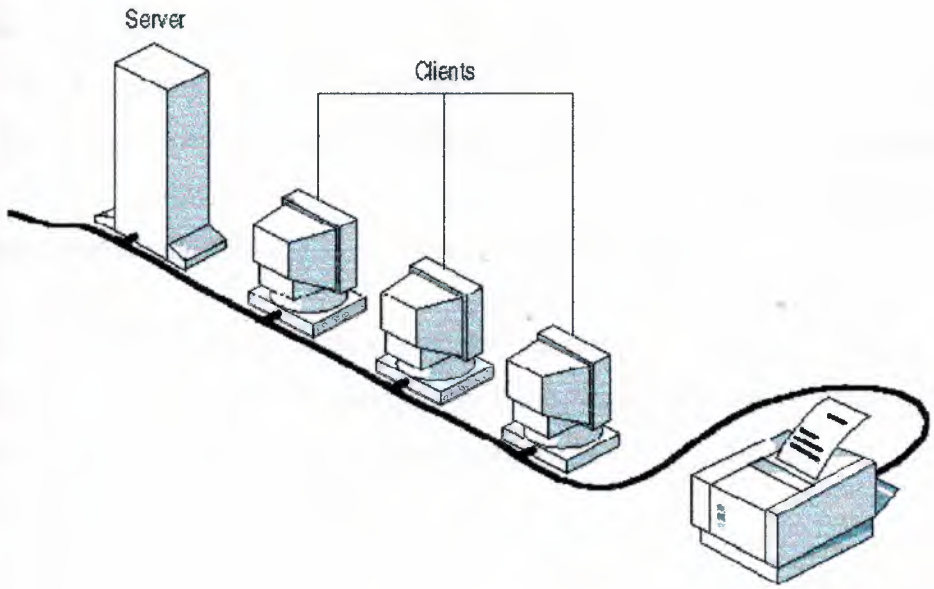

Figure 1.12 *Server-based network*

As networks increase in size (as the number of connected computers, and the physical distance and traffic between them, grows), more than one server is usually needed. Spreading the networking tasks among several servers ensures that each task will be performed as efficiently as possible.

- **Specialized Servers**

Servers must perform varied and complex tasks. Servers for large networks have become specialized to accommodate the expanding needs of users. Following are examples of different types of servers included on many large networks. (See Figure 1.13.)

- **File and Print Servers**

File and print servers manage user access and use of file and printer resources. For example, when you are running a word-processing application, the word-processing application runs on your computer. The word-processing document stored on the file and print server is loaded into your computer's memory so that you can edit or use it locally. In other words, file and print servers are used for file and data storage.

- **Application Servers**

Application servers make the server side of client/server applications, as well as the data, available to clients. For example, servers store vast amounts of data that is organized to make it easy to retrieve. Thus, an application server differs from a file and print server. With a file and print server, the data or file is downloaded to the computer making the request. With an application server, the database stays on the server and only the results of a request are downloaded to the computer making the request.

A client application running locally accesses the data on the application server. For example, you might search the employee database for all employees who were born in November. Instead of the entire database, only the result of your query is downloaded from the server onto your local computer.

- **Mail Servers**

Mail servers operate like application servers in that there are separate server and client applications, with data selectively downloaded from the server to the client.

- **Fax Servers**

Fax servers manage fax traffic into and out of the network by sharing one or more fax modem boards.

- **Communications Servers**

Communications servers handle data flow and e-mail messages between the servers' own networks and other networks, mainframe computers, or remote users who dial in to the servers over modems and telephone lines.

- **Directory Services Servers**

Directory services servers enable users to locate, store, and secure information on the network. For example, some server software combines computers into logical groupings (called *domains*) that allow any user on the network to be given access to any resource on the network.

Planning for specialized servers becomes important with an expanded network. The planner must take into account any anticipated network growth so that network use will not be disrupted if the role of a specific server needs to be changed.

The Role of Software in a Server-Based Environment

A network server and its operating system work together as a unit. No matter how powerful or advanced a server might be, it is useless without an operating system that can take advantage of its physical resources. Advanced server operating systems, such as those from Microsoft and Novell, are designed to take advantage of the most advanced server hardware

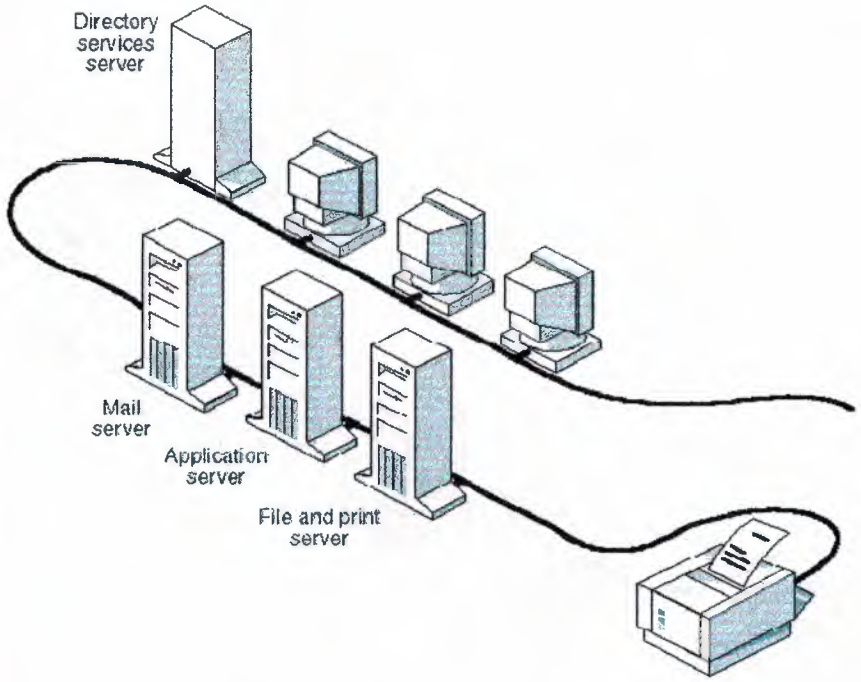

Figure 1.13 *Specialized servers*

Server-Based Network Advantages

Although it is more complex to install, configure, and manage, a server-based network has many advantages over a simple peer-to-peer network.

A) Sharing Resources

A server is designed to provide access to many files and printers while maintaining performance and security for the user.

Server-based data sharing can be centrally administered and controlled. Because these shared resources are centrally located, they are easier to find and support than resources on individual computers.

B) Security

Security is often the primary reason for choosing a server-based approach to networking. In a server-based environment, one administrator who sets the policy and applies it to every user on the network can manage security. Figure 1.14 depicts security being centrally administered.

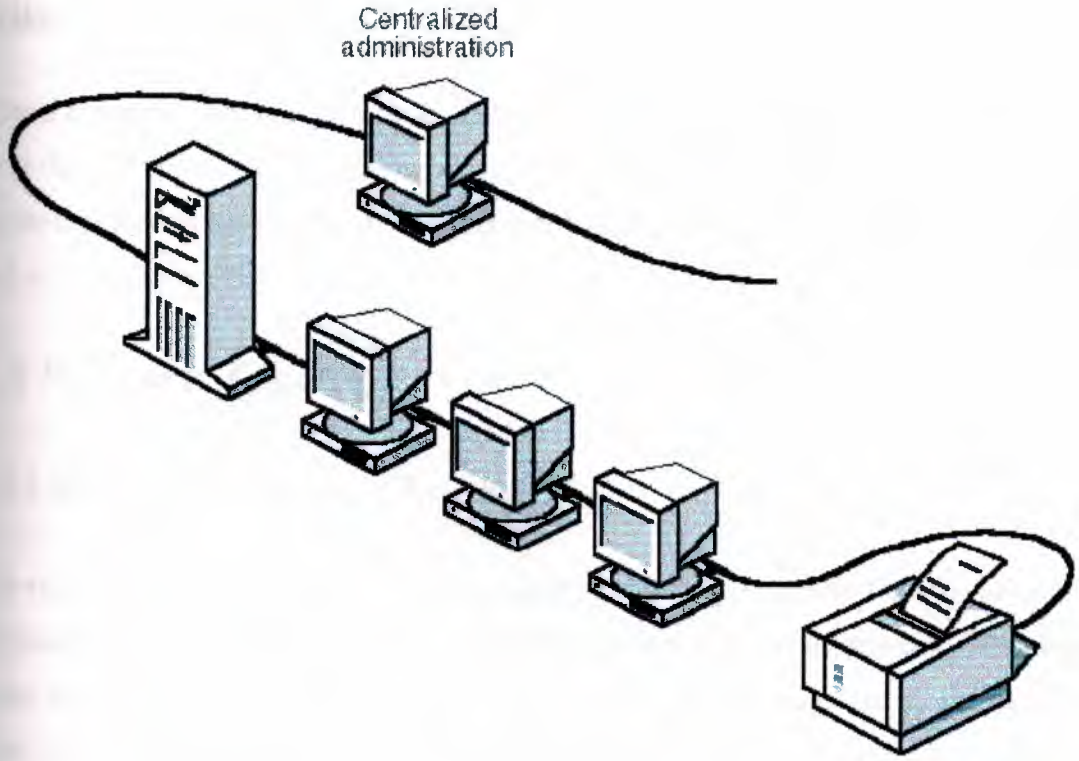

Figure 1.14 *One administrator handles network security*

C) Backup

Backups can be scheduled several times a day or once a week depending on the importance and value of the data. Server backups can be scheduled to occur automatically, according to a predetermined schedule, even if the servers are located on different parts of the network.

D) Redundancy

Through the use of backup methods known as *redundancy systems*, the data on any server can be duplicated and kept online. Even if harm comes to the primary data storage area, a backup copy of the data can be used to restore the data.

E) Number of Users

A server-based network can support thousands of users. This type of network would be impossible to manage as a peer-to-peer network, but current monitoring and network-management utilities make it possible to operate a server-based network for large numbers of users.

F) Hardware Considerations

Client computer hardware can be limited to the needs of the user because clients do not need the additional random access memory (RAM) and disk storage needed to provide server services. A typical client computer often has no more than a Pentium processor and 32 megabytes (MB) of RAM.

1.4 Network Topology

1.4.1 Designing a Network Topology

The term *topology*, or more specifically, network topology, refers to the arrangement or physical layout of computers, cables, and other components on the network. "Topology" is the standard term that most network professionals use when they refer to the network's basic design. In addition to the term "topology," you will find several other terms that are used to define a network's design:

- Physical layout
- Design
- Diagram
- Map

A network's topology affects its capabilities. The choice of one topology over another will have an impact on the:

- Type of equipment the network needs.
- Capabilities of the equipment.
- Growth of the network.
- Way the network is managed.

Developing a sense of how to use the different topologies is a key to understanding the capabilities of the different types of networks.

Before computers can share resources or perform other communication tasks they must be connected. Most networks use cable to connect one computer to another.

However, it is not as simple as just plugging a computer into a cable connecting other computers. Different types of cable—combined with different network cards, network operating systems, and other components—require different types of arrangements.

To work well, a network topology takes planning. For example, a particular topology can determine not only the type of cable used but also how the cabling runs through floors, ceilings, and walls.

Topology can also determine how computers communicate on the network. Different topologies require different communication methods, and these methods have a great influence on the network.

1.4.2 Standard Topologies

All network designs stem from four basic topologies:

- Bus
- Star
- Ring
- Mesh

A *bus topology* consists of devices connected to a common, shared cable. Connecting computers to cable segments that branch out from a single point, or hub, is referred to as setting up a *star topology*. Connecting computers to a cable that forms a loop is referred to as setting up a *ring topology*. A *mesh topology* connects all computers in a network to each other with separate cables.

These four topologies can be combined in a variety of more complex hybrid topologies.

Bus

The bus topology is often referred to as a "linear bus" because the computers are connected in a straight line. This is the simplest and most common method of networking computers. Figure 1.15 shows a typical bus topology. It consists of a single cable called a *trunk* (also called a backbone or segment) that connects all of the computers in the network in a single line.

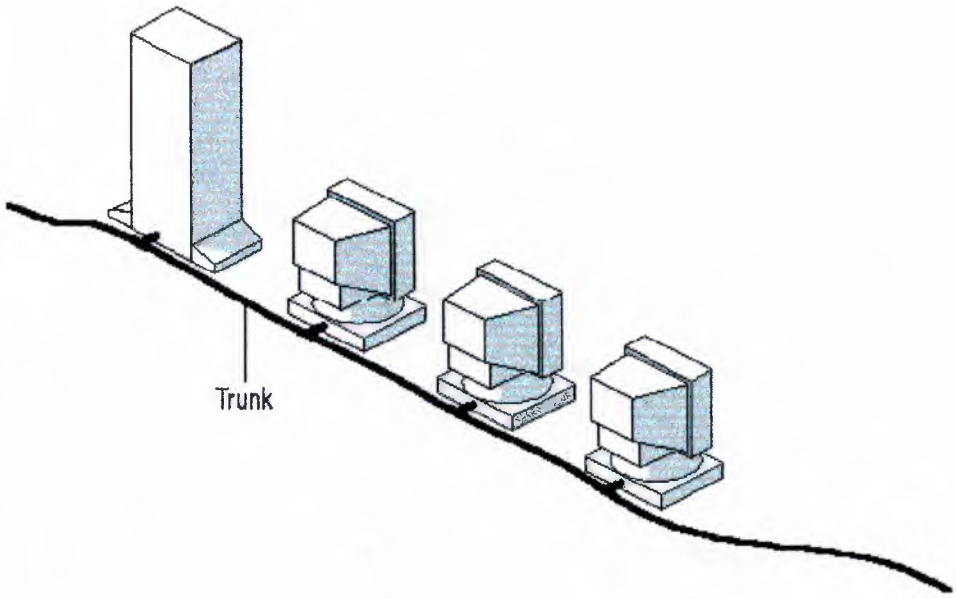

Figure 1.15 *Bus topology network*

- **Communication on the Bus**

Computers on a bus topology network communicate by addressing data to a particular computer and sending out that data on the cable as electronic signals. To understand how computers communicate on a bus, you need to be familiar with three concepts:

- Sending the signal
- Signal bounce
- Terminator

Sending the Signal Network data in the form of electronic signals is sent to all the computers on the network. Only the computer whose address matches the address encoded in the original signal accepts the information. All other computers reject the data. Figure 1.16 shows a message being sent from 0020af151d8b to 02608c133456. Only one computer at a time can send messages.

Because only one computer at a time can send data on a bus network, the number of computers attached to the bus will affect network performance. The more computers there are on a bus, the more computers will be waiting to put data on the bus and, consequently, the slower the network will be.

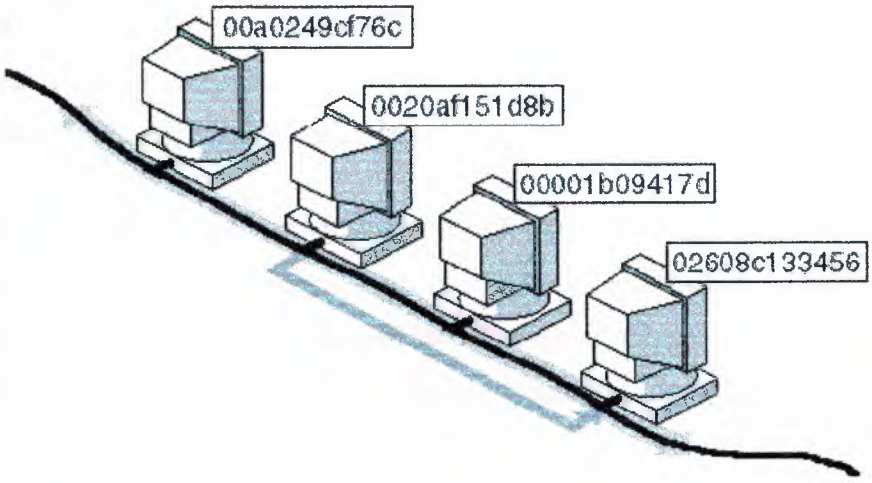

Figure 1.16 *Data is sent to all computers, but only the destination computer accepts it*

There is no standard way to measure the impact of a given number of computers on the speed of any given network. The effect on performance is not related solely to the number of computers. The following is a list of factors that—in addition to the number of networked computers—will affect the performance of a network:

- Hardware capabilities of computers on the network
- Total number of queued commands waiting to be executed
- Types of applications (client-server or file system sharing, for example) being run on the network
- Types of cable used on the network
- Distances between computers on the network

Computers on a bus either transmit data to other computers on the network or listen for data from other computers on the network. They are not responsible for moving data from one computer to the next. Consequently, if one computer fails, it does not affect the rest of the network.

Signal Bounce Because the data, or electronic signal, is sent to the entire network, it travels from one end of the cable to the other. If the signal is allowed to continue uninterrupted, it will keep bouncing back and forth along the cable and prevent other computers from sending signals. Therefore, the signal must be stopped after it has had a chance to reach the proper destination address.

Terminator To stop the signal from bouncing, a component called a *terminator* is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data.

Both ends of each cable segment on the network must be plugged into something. For example, a cable end can be plugged into a computer or a connector to extend the cable length. Any open cable ends not plugged into something must be terminated to prevent signal bounce. Figure 1.17 shows a properly terminated bus topology network.

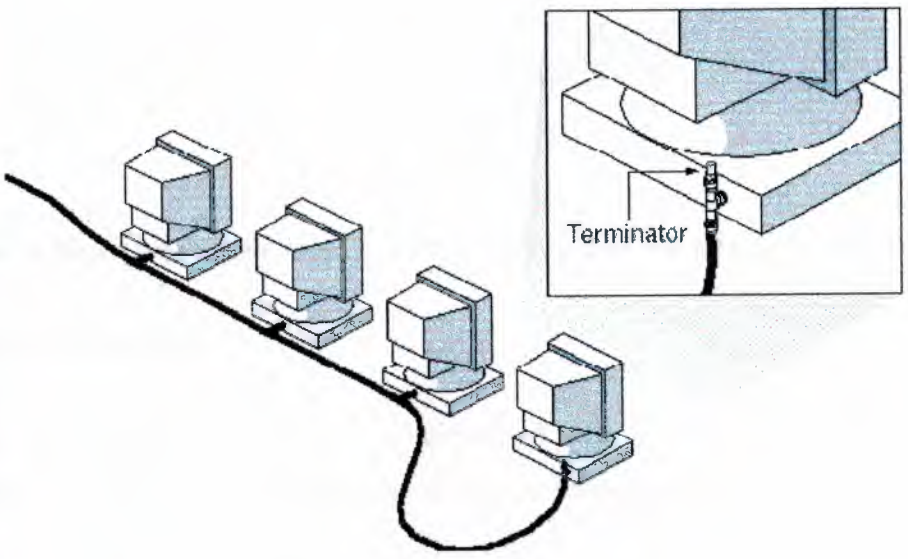

Figure 1.17 *Terminators absorb free signals*

- **Disrupting Network Communication**

A break in the cable will occur if the cable is physically separated into two pieces or if at least one end of the cable becomes disconnected. In either case, one or both ends of the cable will not have a terminator, the signal will bounce, and all network activity will stop. This is one of several possible reasons why a network will go "down." Figure 1.18 shows a bus topology with a disconnected cable. This network will not work because it now has unterminated cables.

The computers on the network will still be able to function as stand-alone computers; however, as long as the segment is broken, they will not be able to communicate with each other or otherwise access shared resources. The computers on the down segment

will attempt to establish a connection; while they do so, workstation performance will be slower.

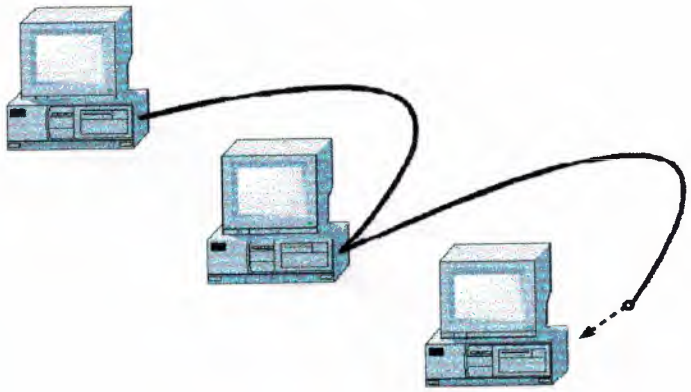

Figure 1.18 *An unplugged cable is not terminated and will take down the network*

- **Network Expansion**

As the physical size of the site grows, the network will need to grow as well. Cable in the bus topology can be extended by one of the two following methods:

- A component called a *barrel connector* can connect two pieces of cable together to make a longer piece of cable (see Figure 1.19). However, connectors weaken the signal and should be used sparingly. One continuous cable is preferable to connecting several smaller ones with connectors. Using too many connectors can prevent the signal from being correctly received.

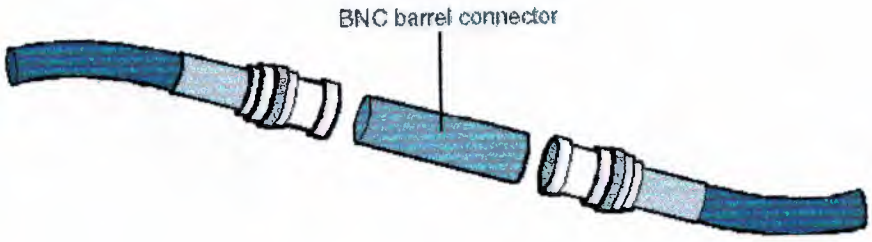

Figure 1.19 *Barrel connectors can be used to combine cable segments*

- A device called a *repeater* can be used to connect two cables. A repeater actually boosts the signal before it sends the signal on its way. Figure 1.20 shows a repeater boosting a weakened signal. A repeater is better than a connector or a longer piece of cable because it allows a signal to travel farther and still be correctly received.

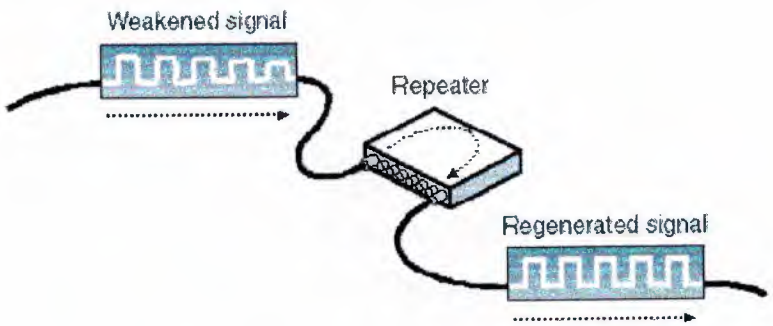

Figure 1.20 *Repeaters connect cables and amplify the signal*

Star

In the star topology, cable segments from each computer are connected to a centralized component called a *hub*. Figure 1.21 shows four computers and a hub connected in a star topology. Signals are transmitted from the sending computer through the hub to all computers on the network. This topology originated in the early days of computing when computers were connected to a centralized mainframe computer.

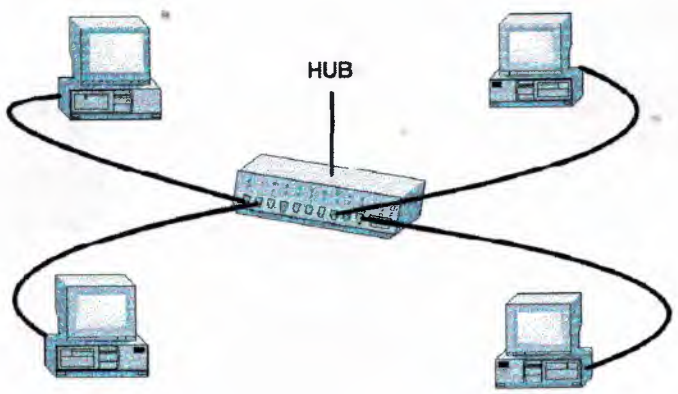

Figure 1.21 *Simple star network*

The star network offers the advantage of centralized resources and management. However, because each computer is connected to a central point, this topology requires a great deal of cable in a large network installation. Also, if the central point fails, the entire network goes down.

If one computer—or the cable that connects it to the hub—fails on a star network, only the failed computer will not be able to send or receive network data. The rest of the network continues to function normally.

Ring

The ring topology connects computers on a single circle of cable. Unlike the bus topology, there are no terminated ends. The signals travel around the loop in one direction and pass through each computer, which can act as a repeater to boost the signal and send it on to the next computer. Figure 1.22 shows a typical ring topology with one server and four workstations. The failure of one computer can have an impact on the entire network.

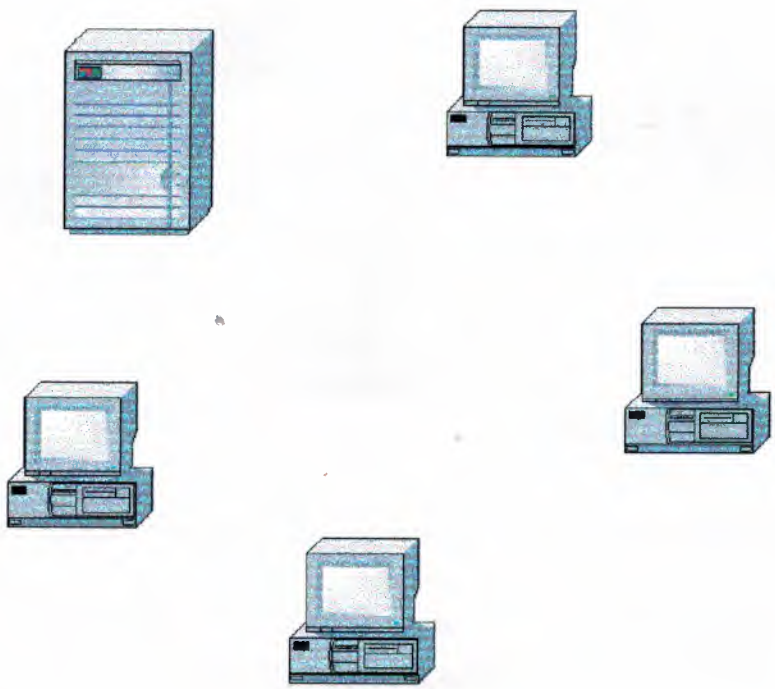

Figure 1.22 *Simple ring network showing logical ring*

Token Passing

One method of transmitting data around a ring is called *token passing*. (A *token* is a special series of bits that travels around a token-ring network. Each network has only one token.) The token is passed from computer to computer until it gets to a computer that has data to send. Figure 1.23 shows a token ring topology with the token. The sending computer modifies the token, puts an electronic address on the data, and sends it around the ring.

The data passes by each computer until it finds the one with an address that matches the address on the data.

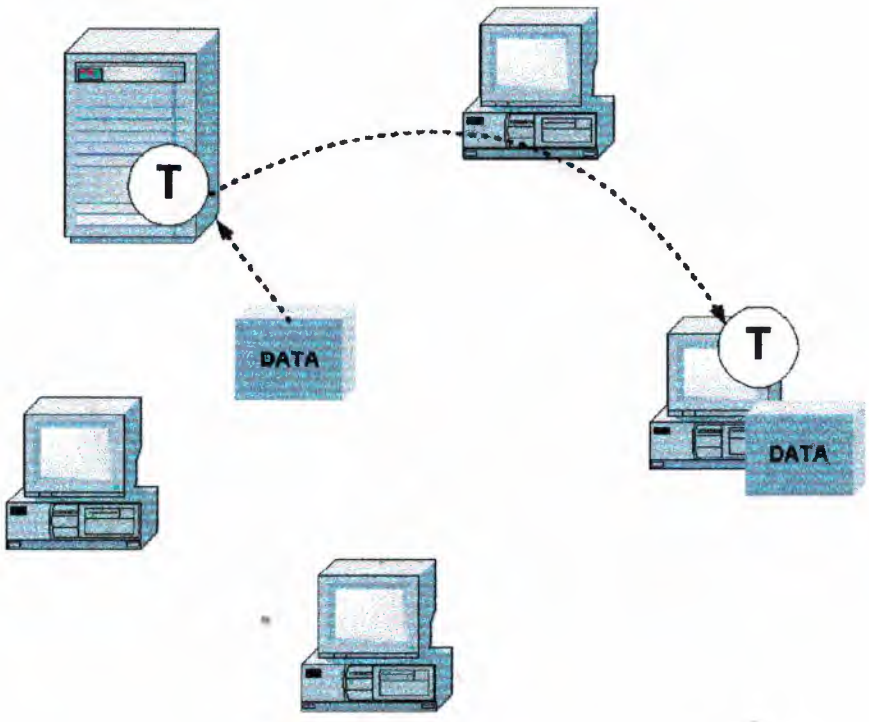

Figure 1.23 *A computer grabs the token and passes it around the ring*

The receiving computer returns a message to the sending computer indicating that the data has been received. After verification, the sending computer creates a new token and releases it on the network. The token circulates within the ring until a workstation needs it to send data.

It might seem that token passing would take a long time, but the token actually travels at roughly the speed of light. A token can circle a ring 200 meters (656 feet) in diameter about 477,376 times per second.

Mesh

A mesh topology network offers superior redundancy and reliability. In a mesh topology, each computer is connected to every other computer by separate cabling. This configuration provides redundant paths throughout the network so that if one cable fails, another will take over the traffic. While ease of troubleshooting and increased reliability are definite pluses, these networks are expensive to install because they use a lot of cabling. Often, a mesh topology will be used in conjunction with other topologies to form a hybrid topology.

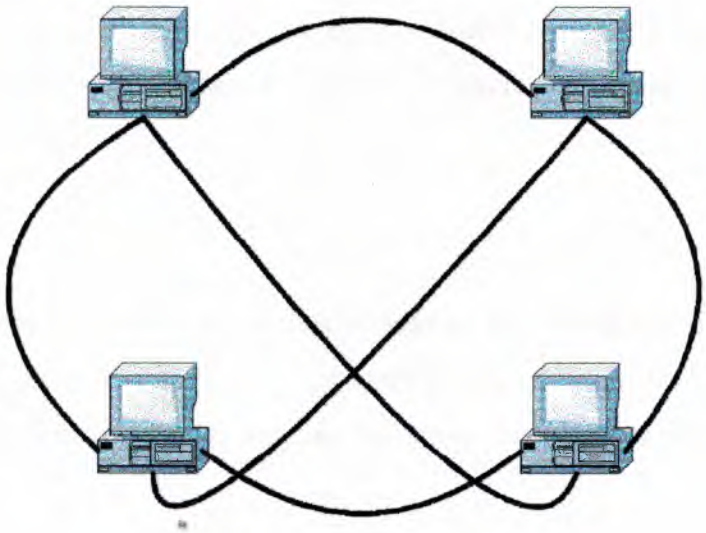

Figure 1.24 *In a mesh topology, all computers are connected to each other by separate cables*

1.4.3 Hubs

One network component that has become standard equipment in networks is the hub. Figure 1.25 shows a hub as the central component in a star topology.

It might seem that token passing would take a long time, but the token actually travels at roughly the speed of light. A token can circle a ring 200 meters (656 feet) in diameter about 477,376 times per second.

Mesh

A mesh topology network offers superior redundancy and reliability. In a mesh topology, each computer is connected to every other computer by separate cabling. This configuration provides redundant paths throughout the network so that if one cable fails, another will take over the traffic. While ease of troubleshooting and increased reliability are definite pluses, these networks are expensive to install because they use a lot of cabling. Often, a mesh topology will be used in conjunction with other topologies to form a hybrid topology.

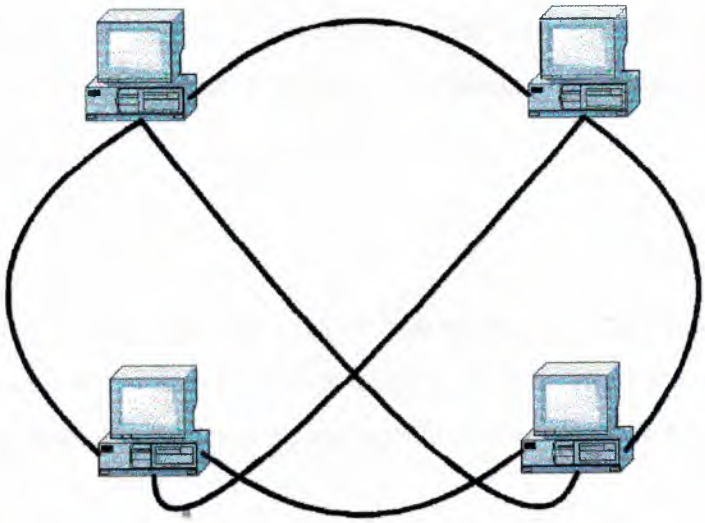

Figure 1.24 *In a mesh topology, all computers are connected to each other by separate cables*

1.4.3 Hubs

One network component that has become standard equipment in networks is the hub. Figure 1.25 shows a hub as the central component in a star topology.

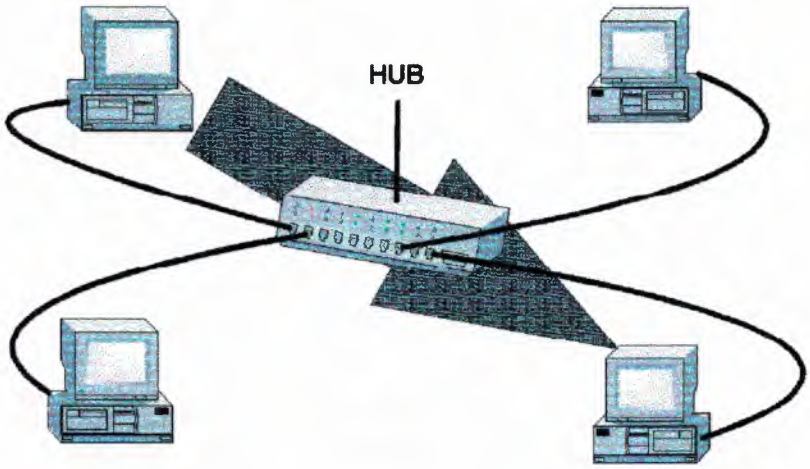

Figure 1.25 *A hub is the central point in a star topology*

1. Active Hubs

Most hubs are active; that is, they regenerate and retransmit signals in the same way as a repeater does. Because hubs usually have eight to twelve ports for network computers to connect to, they are sometimes called multiport repeaters. Active hubs require electrical power to run.

2. Passive Hubs

Some types of hubs are passive; examples include wiring panels or punch-down blocks. They act as connection points and do not amplify or regenerate the signal; the signal passes through the hub. Passive hubs do not require electrical power to run.

3. Hybrid Hubs

Advanced hubs that will accommodate several different types of cables are called *hybrid hubs*. Figure 1.26 shows a main hub (the hybrid) with three sub-hubs.

Hub Considerations

Hub-based systems are versatile and offer several advantages over systems that do not use hubs.

In the standard linear-bus topology, a break in the cable will take the network down. With hubs, however, a break in any of the cables attached to the hub affects only a limited segment of the network. Figure 1.27 shows that a break or disconnected cable affects only one workstation while the rest of the network keeps functioning.

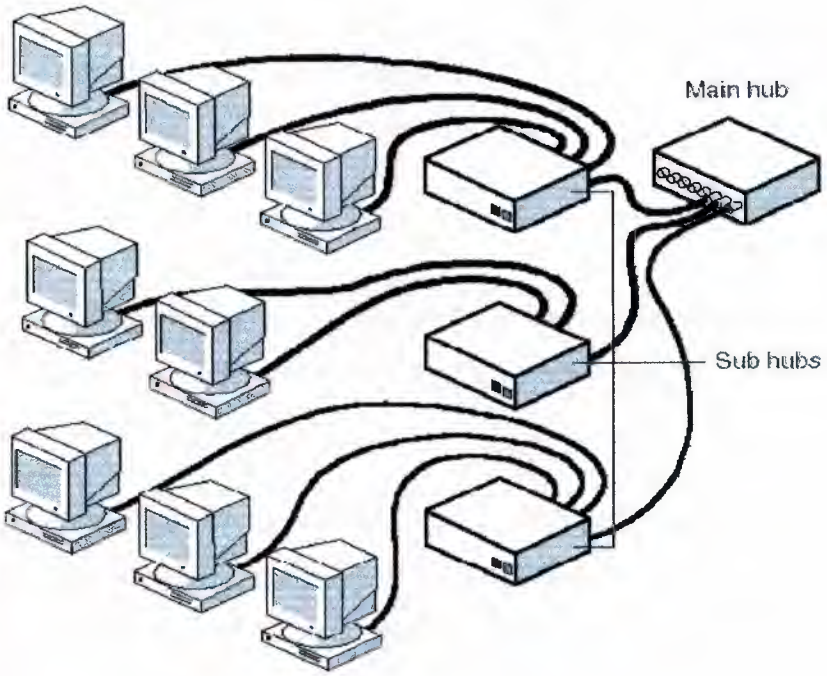

Figure 1.26 *Hybrid hub*

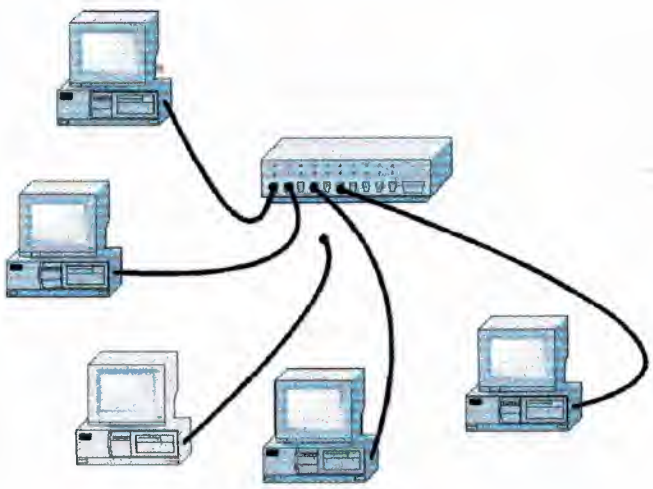

Figure 1.27 *A break or unplugged cable takes down only the unplugged computer*

Hub-based topologies include the following benefits:

- Wiring systems can be changed or expanded as needed.
- Different ports can be used to accommodate a variety of cabling types.
- Monitoring of network activity and traffic can be centralized.

1.4.4 Variations on the Standard Topologies

Many working topologies are hybrid combinations of the bus, star, ring, and mesh topologies.

- **Star Bus**

The *star bus* is a combination of the bus and star topologies. In a star-bus topology, several star topology networks are linked together with linear bus trunks. Figure 1.28 shows a typical star-bus topology.

If one computer goes down, it will not affect the rest of the network. The other computers can continue to communicate. If a hub goes down, all computers on that hub are unable to communicate. If a hub is linked to other hubs, those connections will be broken as well.

- **Star Ring**

The *star ring* (sometimes called a star-wired ring) appears similar to the star bus. Both the star ring and the star bus are centered in a hub that contains the actual ring or bus. Figure 1.29 shows a star-ring network. Linear-bus trunks connect the hubs in a star bus, while the hubs in a star ring are connected in a star pattern by the main hub.

- **Peer-to-Peer**

Many small offices use a peer-to-peer network as described earlier in this chapter before. Such a network can be configured as either a physical star or a bus topology. However, because all computers on the network are equal (each can be both client and server), the logical topology looks somewhat different. Figure 1.30 shows the logical topology of a peer-to-peer network.

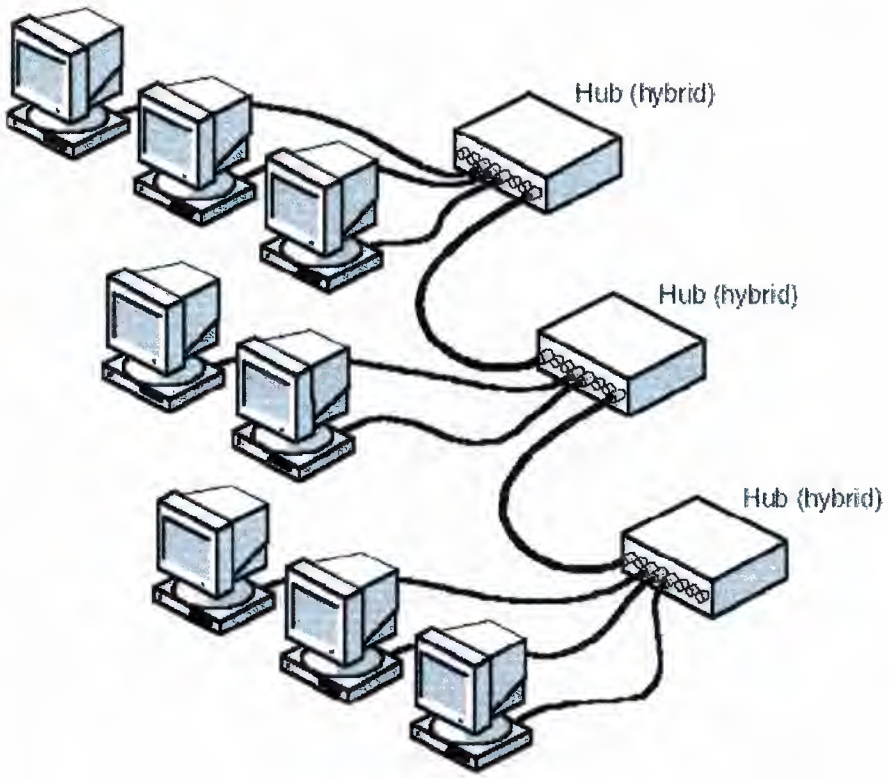

Figure 1.28 *Star-bus network*

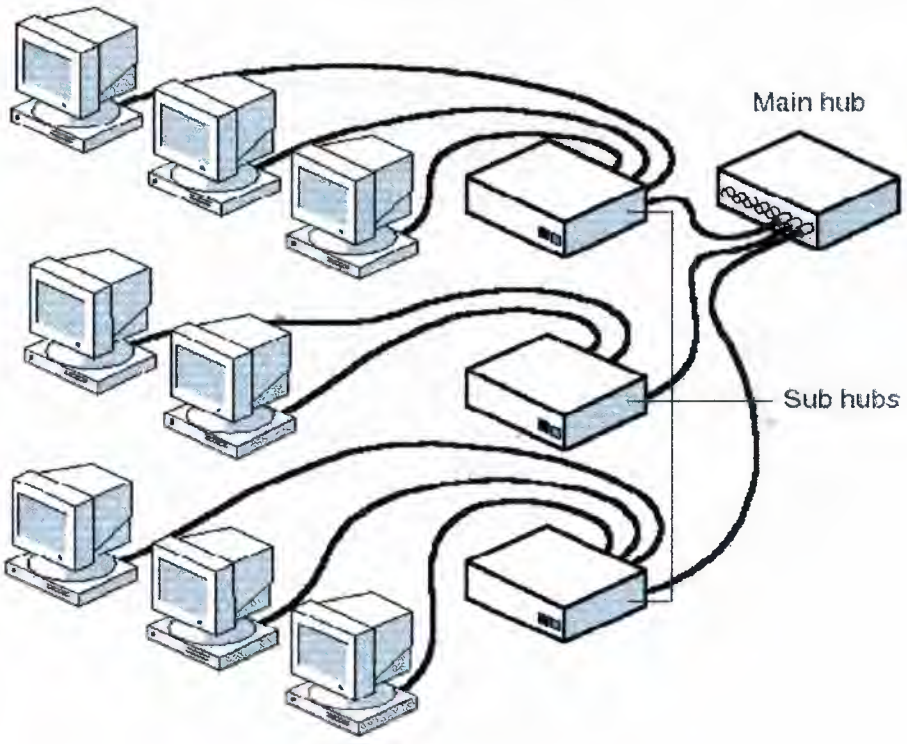

Figure 1.29 *Star-ring network*

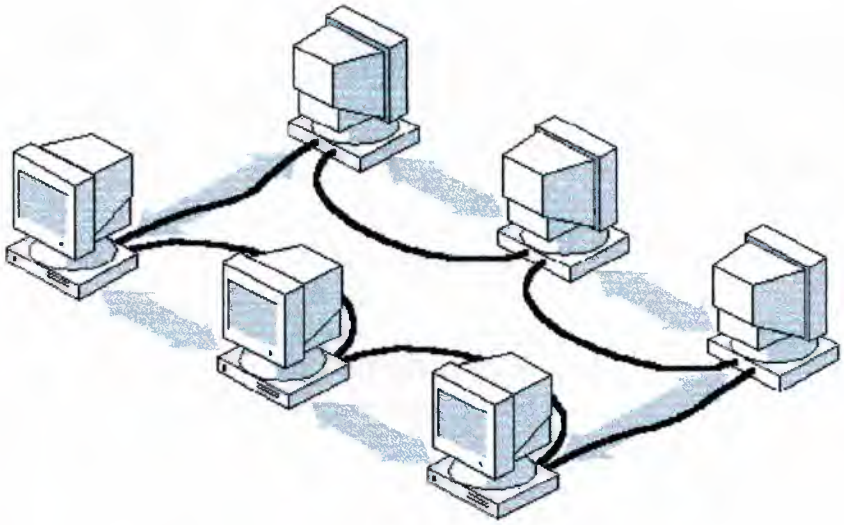

Figure 1.30 *Logical peer-to-peer topology*

1.4.5 Selecting a Topology

There are many factors to consider when deciding which topology best suits the needs of an organization. Table 1.1 provides some guidelines for selecting a topology.

Table 1.1 *Topology Advantages and Disadvantages*

Topology	*Advantages*	*Disadvantages*
Bus	• Use of cable is economical. • Media is inexpensive and easy to work with. • System is simple and reliable. • Bus is easy to extend.	• Network can slow down in heavy traffic. • Problems are difficult to isolate. • Cable break can affect many users.
Ring	• System provides equal access for all computers. • Performance is even despite many users.	• Failure of one computer can impact the rest of the network. • Problems are hard to isolate. • Network reconfiguration disrupts operation.

Topology	*Advantages*	*Disadvantages*
Star	• Modifying system and adding new computers is easy. • Centralized monitoring and management are possible. • Failure of one computer does not affect the rest of the network.	• If the centralized point fails, the network fails.
Mesh	• System provides increased redundancy and reliability as well as ease of troubleshooting.	• System is expensive to install because it uses a lot of cabling.

CHAPTER 2

NETWORK CABLING

2.1 Introduction

In Chapter 1, "Introduction to Networking," we examined the nature of a network. General terms were introduced that describe what networks are, how they are structured, and how they can benefit us. In this chapter we will focus on the cables that connect them, examining the construction, features, operation of each type of cable and the advantages and disadvantages of each.

2.2 Primary Cable Types

The vast majority of networks today are connected by some sort of wiring or cabling that acts as a network transmission medium that carries signals between computers. Many cable types are available to meet the varying needs and sizes of networks, from small to large.

Cable types can be confusing. Belden, a leading cable manufacturer, publishes a catalog that lists more than 2200 types of cabling. Fortunately, only three major groups of cabling connect the majority of networks:

- Coaxial cable
- Twisted-pair (unshielded and shielded) cable
- Fiber-optic cable

The next part of this lesson describes the features and components of these three major cable types. Understanding their differences will help you determine which type of cabling is appropriate in a given context.

2.2.1 Coaxial Cable

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial cable's wide usage: it was relatively inexpensive, and it was light, flexible, and easy to work with.

In its simplest form, *coaxial cable* consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. Figure 2.1 shows the various components that make up a coaxial cable.

The term *shielding* refers to the woven or stranded metal mesh (or other material) that surrounds some types of cabling. Shielding protects transmitted data by absorbing stray electronic signals, called *noise*, so that they do not get onto the cable and distort the data. Cable that contains one layer of foil insulation and one layer of braided metal shielding is referred to as *dual shielded.* For environments that are subject to higher interference, quad shielding is available. *Quad shielding* consists of two layers of foil insulation and two layers of braided metal shielding.

The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper.

Surrounding the core is a dielectric insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk. (*Crosstalk* is signal overflow from an adjacent wire. We will discuss this later in this chapter.

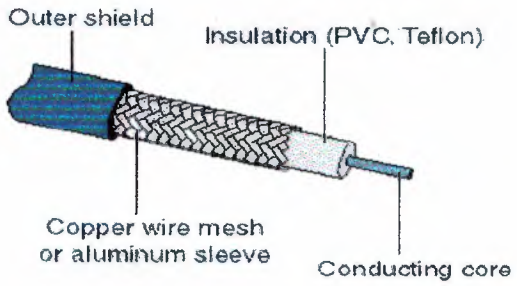

Figure 2.1 *Coaxial cable showing various layers*

The conducting core and the wire mesh must always be kept separate from each other. If they touch, the cable will experience a *short*, and noise or stray signals on the mesh will flow onto the copper wire. An electrical short occurs when any two conducting wires or a conducting wire and a ground come into contact with each other. This contact causes a direct flow of current (or data) in an unintended path. In the case of household electrical wiring, a short will cause sparking and the blowing of a fuse or circuit breaker. With electronic devices that use low voltages, the result is not as dramatic and is often undetectable. These low-voltage shorts generally cause the failure of a device; and the short, in turn, destroys the data.

A nonconducting outer shield—usually made of rubber, Teflon, or plastic—surrounds the entire cable.

Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. As shown in Figure 2.2, *attenuation* is the loss of signal strength that begins to occur as the signal travels farther along a copper cable.

Figure 2.2 *Attenuation causes signals to deteriorate*

The stranded, protective sleeve absorbs stray electronic signals so that they do not affect data being sent over the inner copper cable. For this reason, coaxial cabling is a good choice for longer distances and for reliably supporting higher data rates with less sophisticated equipment.

Types of Coaxial Cable

There are two types of coaxial cable:

- Thin (thinnet) cable
- Thick (thicknet) cable

Which type of coaxial cable you select depends on the needs of your particular network.

Thinnet Cable *Thinnet* cable is a flexible coaxial cable about 0.64 centimeters (0.25 inches) thick. Because this type of coaxial cable is flexible and easy to work with, it can be used in almost any type of network installation. Figure 2.3 shows thinnet cable connected directly to a computer's network interface card (NIC).

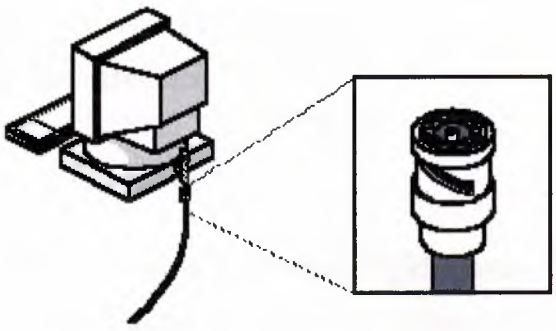

Figure 2.3 *Close-up view of thinnet cable showing where it connects to a computer*

Thinnet coaxial cable can carry a signal for a distance of up to approximately 185 meters (about 607 feet) before the signal starts to suffer from attenuation.

Cable manufacturers have agreed upon specific designations for different types of cable. (Table 2.1 lists cable types and descriptions.) Thinnet is included in a group referred to as the *RG-58* family and has 50ohm impedance. (*Impedance* is the amount of opposition shown by any circuit element against the flow of current). The principal distinguishing feature of the RG-58 family is the center core of copper. Figure 2.4 shows two examples of RG-58 cable, one with a stranded wire core and one with a solid copper core.

Figure 2.4 *RG-58 coaxial cable showing stranded wire and solid copper cores*

Table 2.1 *Cable Types*

Cable	Description
RG-58/U	Solid copper core
RG-58 A/U	Stranded wire core
RG-58 C/U	Military specification of RG-58 A/U
RG-59	Broadband transmission, such as cable television
RG-6	Larger in diameter and rated for higher frequencies than RG-59, but also used for broadband transmissions
RG-62	ArcNet networks

Thicknet Cable *Thicknet* cable is a relatively rigid coaxial cable about 1.27 centimeters (0.5 inches) in diameter. Figure 2.5 shows the difference between thinnet and thicknet cable. Thicknet cable is sometimes referred to as Standard Ethernet because it was the first type of cable used with the popular network architecture Ethernet. Thicknet cable's copper core is thicker than a thinnet cable core.

Figure 2.5 *Thicknet cable has a thicker core than thinnet cable*

The thicker the copper core, the farther the cable can carry signals. This means that thicknet can carry signals farther than thinnet cable. Thicknet cable can carry a signal for 500 meters (about 1640 feet). Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

Figure 2.6 shows a device called a transceiver. A *transceiver* connects the thinnet coaxial cable to the larger thicknet coaxial cable. A transceiver designed for thicknet

Ethernet includes a connector known as a *vampire tap,* or a piercing tap, to make the actual physical connection to the thicknet core. This connector is pierced through the insulating layer and makes direct contact with the conducting core. Connection from the transceiver to the NIC is made using a transceiver cable (drop cable) to connect to the *attachment unit interface* (AUI) port connector on the card. An AUI port connector for thicknet is also known as a *Digital Intel Xerox (DIX) connector* (named for the three companies that developed it and its related standards) or as a DB-15 connector.

Thinnet vs. Thicknet Cable As a general rule, the thicker the cable, the more difficult it is to work with. Thin cable is flexible, easy to install, and relatively inexpensive. Thick cable does not bend easily and is, therefore, harder to install. This is a consideration when an installation calls for pulling cable through tight spaces such as conduits and troughs. Thick cable is more expensive than thin cable, but will carry a signal farther.

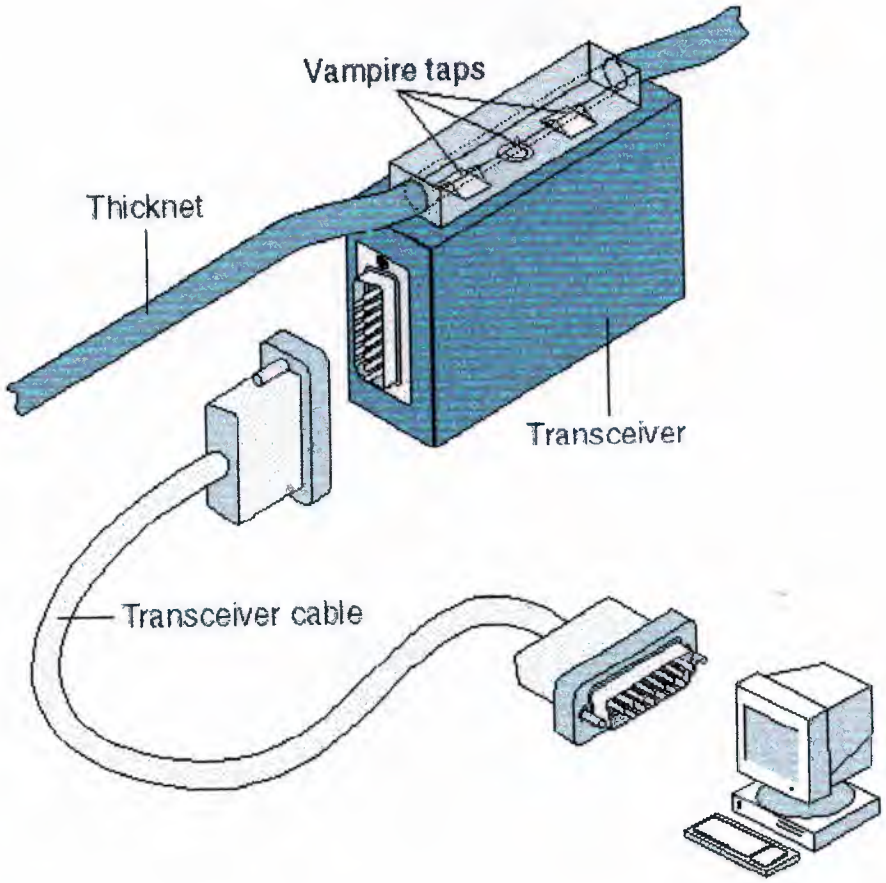

Figure 2.6 *Thicknet cable transceiver with detail of a vampire tap piercing the core*

Coaxial-Cable Connection Hardware

Both thinnet and thicknet cable use a connection component, known as a *BNC connector*, to make the connections between the cable and the computers. There are several important components in the BNC family, including the following:

- **The BNC cable connector** Figure 2.7 shows a BNC cable connector. The BNC cable connector is either soldered or crimped to the end of a cable.

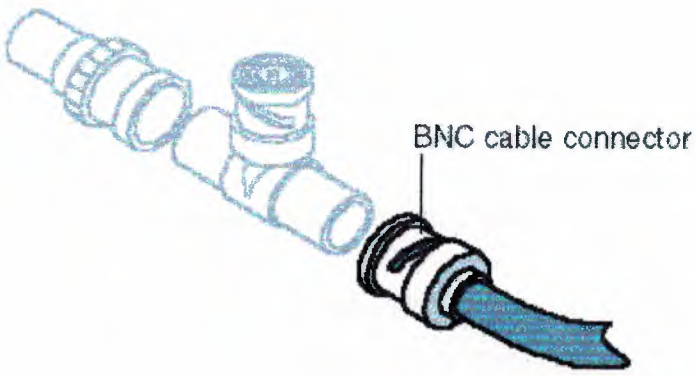

Figure 2.7 *BNC cable connector*

- **The BNC T connector** Figure 2.8 shows a BNC T connector. This connector joins the network interface card (NIC) in the computer to the network cable.

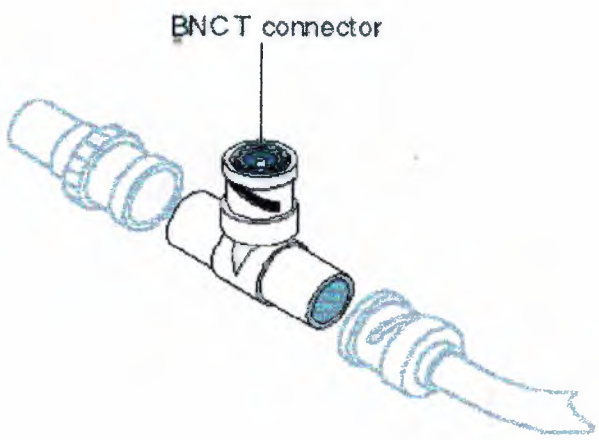

Figure 2.8 *BNC T connector*

- **The BNC barrel connector** Figure 2.9 shows a BNC barrel connector. This connector is used to join two lengths of thinnet cable to make one longer length.

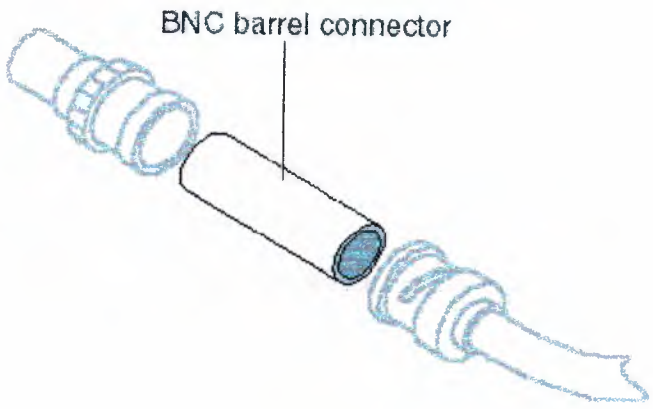

Figure 2.9 *BNC barrel connector*

- **The BNC terminator** Figure 2.10 shows a BNC terminator. A BNC terminator closes each end of the bus cable to absorb stray signals. Otherwise, as we saw in Chapter 1, "Introduction to Networking," the signal will bounce and all network activity will stop.

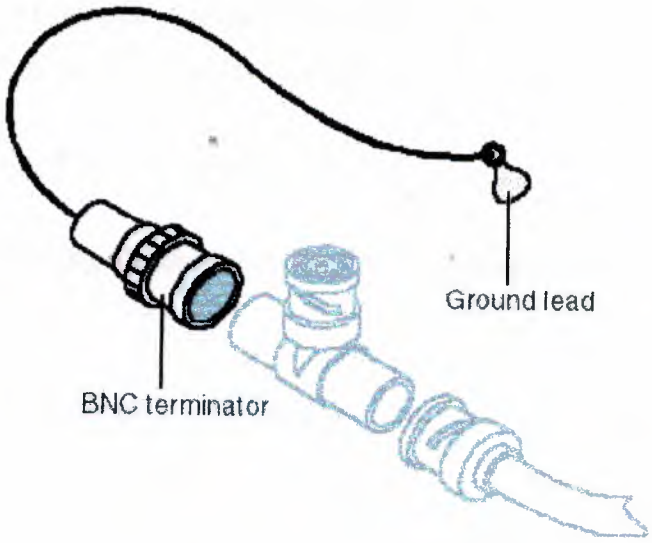

Figure 2.10 *BNC terminator*

Coaxial-Cable Grades and Fire Codes

The type of cable grade that you should use depends on where the cables will be laid in your office. Coaxial cables come in two grades:

- Polyvinyl chloride (PVC) grade
- Plenum grade

Polyvinyl chloride (PVC) is a type of plastic used to construct the insulation and cable jacket for most types of coaxial cable. PVC coaxial cable is flexible and can be easily routed through the exposed areas of an office. However, when it burns, it gives off poisonous gases.

A *plenum* is the shallow space in many buildings between the false ceiling and the floor above; it is used to circulate warm and cold air through the building. Figure 2.11 shows a typical office and where to use—or not use—PVC and plenum-grade cables. Fire codes give very specific instructions about the type of wiring that can be routed through this area, because any smoke or gas in the plenum will eventually blend with the air breathed by everyone in the building.

Plenum-grade cabling contains special materials in its insulation and cable jacket. These materials are certified to be fire resistant and produce a minimum amount of smoke; this reduces poisonous chemical fumes. Plenum cable can be used in the plenum area and in vertical runs (for example, in a wall) without conduit. However, plenum cabling is more expensive and less flexible than PVC cable.

Coaxial-Cabling Considerations

Consider the following coaxial capabilities when making a decision about which type of cabling to use.

Use coaxial cable if you need a medium that can:

- Transmit voice, video, and data.
- Transmit data for greater distances than is possible with less expensive cabling.
- Offer a familiar technology with reasonable data security.

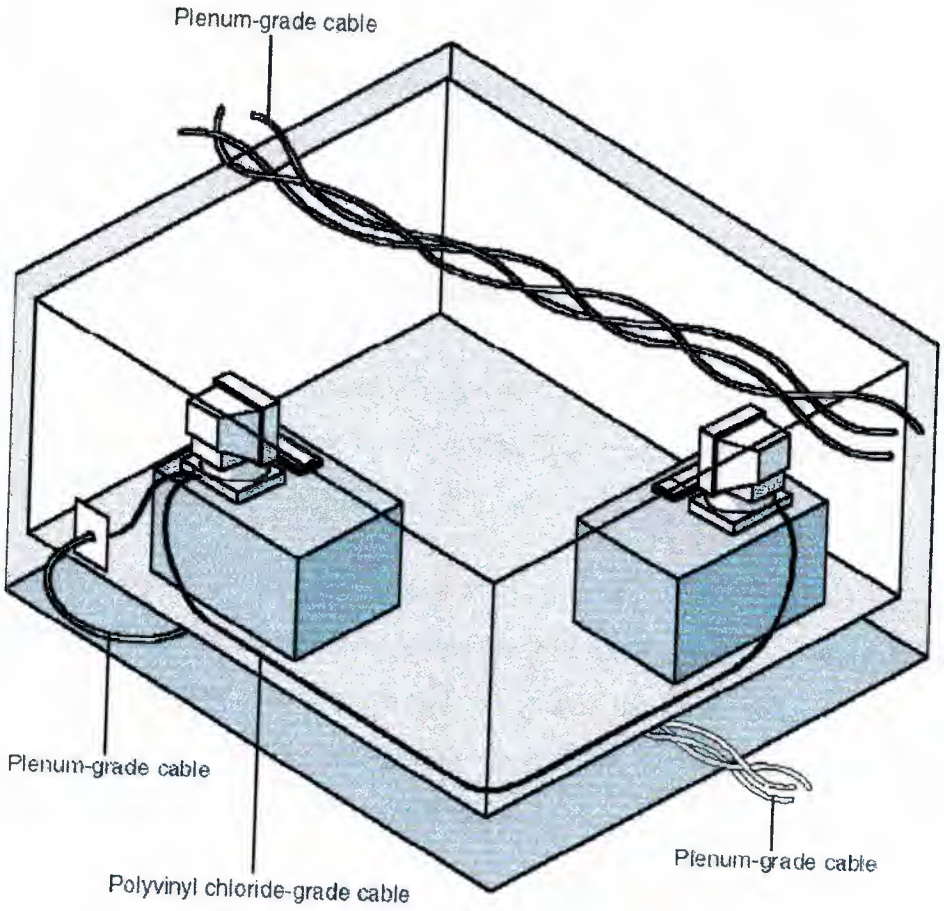

Figure 2.11 *Plenum-grade cabling is required in the plenum by fire codes*

2.2.2 Twisted-Pair Cable

In its simplest form, *twisted-pair cable* consists of two insulated strands of copper wire twisted around each other. Figure 2.12 shows the two types of twisted-pair cable: *unshielded twisted-pair (UTP)* and *shielded twisted-pair (STP)* cable.

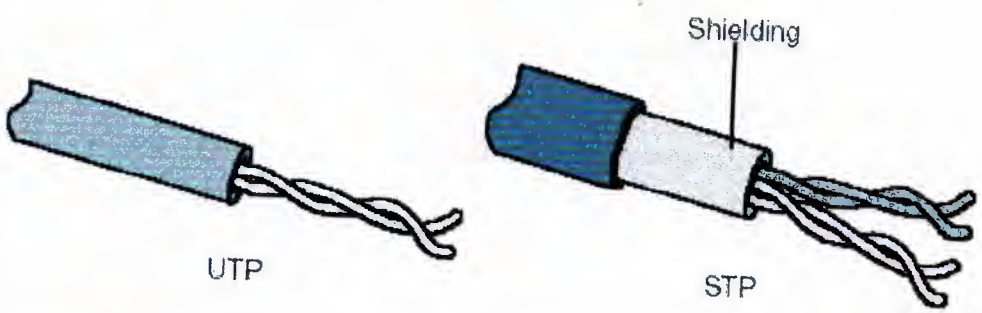

Figure 2.12 *Unshielded twisted-pair and shielded twisted-pair cables*

A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The total number of pairs in a cable varies. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays, and transformers.

1. Unshielded Twisted-Pair (UTP) Cable

UTP, using the 10BaseT specification, is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters, about 328 feet.

Traditional UTP cable, as shown in Figure 2.13, consists of two insulated copper wires. UTP specifications govern how many twists are permitted per foot of cable; the number of twists allowed depends on the purpose to which the cable will be put. In North America, UTP cable is the most commonly used cable for existing telephone systems and is already installed in many office buildings.

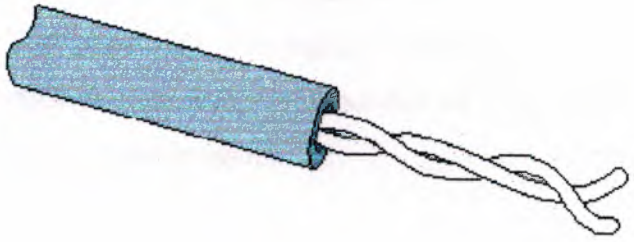

Figure 2.13 *UTP cable*

The 568A Commercial Building Wiring Standard of the Electronic Industries Association and the Telecommunications Industries Association (EIA/TIA) specifies the type of UTP cable that is to be used in a variety of building and wiring situations. The objective is to ensure consistency of products for customers. These standards include five categories of UTP:

- **Category 1** This refers to traditional UTP telephone cable that can carry voice but not data transmissions. Most telephone cable prior to 1983 was Category 1 cable.

- **Category 2** This category certifies UTP cable for data transmissions up to 4 megabits per second (Mbps). It consists of four twisted pairs of copper wire.
- **Category 3** This category certifies UTP cable for data transmissions up to 16 Mbps. It consists of four twisted pairs of copper wire with three twists per foot.
- **Category 4** This category certifies UTP cable for data transmissions up to 20 Mbps. It consists of four twisted pairs of copper wire.
- **Category 5** This category certifies UTP cable for data transmissions up to 100 Mbps. It consists of four twisted pairs of copper wire.

Most telephone systems use a type of UTP. In fact, one reason why UTP is so popular is because many buildings are prewired for twisted-pair telephone systems. As part of the prewiring process, extra UTP is often installed to meet future cabling needs. If preinstalled twisted-pair cable is of sufficient grade to support data transmission, it can be used in a computer network. Caution is required, however, because common telephone wire might not have the twisting and other electrical characteristics required for clean, secure, computer data transmission.

One potential problem with all types of cabling is crosstalk. Figure 2.14 shows crosstalk between two UTP cables. (As discussed earlier in this lesson, crosstalk is defined as signals from one line interfering with signals from another line.) UTP is particularly susceptible to crosstalk, but the greater the number of twists per foot of cable, the more effective the protection against crosstalk.

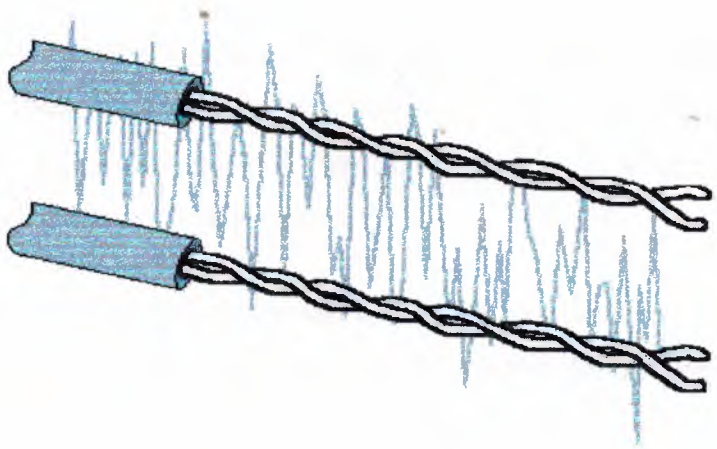

Figure 2.14 *Crosstalk occurs when signals from one line bleed into another line*

2. Shielded Twisted-Pair (STP) Cable

STP cable uses a woven copper-braid jacket that is more protective and of a higher quality than the jacket used by UTP. Figure 2.15 shows a two-twisted-pair STP cable. STP also uses a foil wrap around each of the wire pairs. This gives STP excellent shielding to protect the transmitted data from outside interference, which in turn allows it to support higher transmission rates over longer distances than UTP.

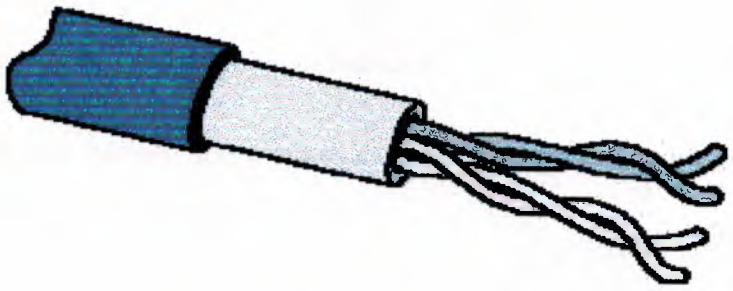

Figure 2.15 *STP cable*

Twisted-Pair Cabling Components

While we have defined twisted-pair cabling by the number of twists and its ability to transmit data, additional components are necessary to complete an installation. As it is with telephone cabling, a twisted-pair cable network requires connectors and other hardware to ensure proper installation.

Connection hardware Twisted-pair cabling uses RJ-45 telephone connectors to connect to a computer. These are similar to RJ-11 telephone connectors. An RJ-45 connector is shown in Figure 2.16. Although RJ-11 and RJ-45 connectors look alike at first glance, there are crucial differences between them.

The RJ-45 connector is slightly larger and will not fit into the RJ-11 telephone jack. The RJ-45 connector houses eight cable connections, while the RJ-11 houses only four.

Several components are available to help organize large UTP installations and make them easier to work with. Figure 2.17 shows various twisted-pair cabling components.

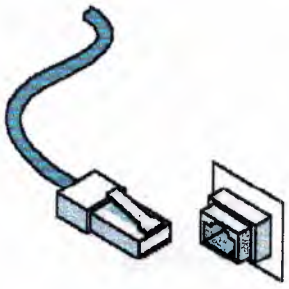

Figure 2.16 *RJ-45 connector and jack*

Distribution racks and rack shelves Distribution racks and rack shelves can create more room for cables where there isn't much floor space. Using them is a good way to organize a network that has a lot of connections.

Expandable patch panels These come in various versions that support up to 96 ports and transmission speeds of up to 100 Mbps.

Jack couplers These single or double RJ-45 jacks snap into patch panels and wall plates and support data rates of up to 100 Mbps.

Wall plates These support two or more couplers.

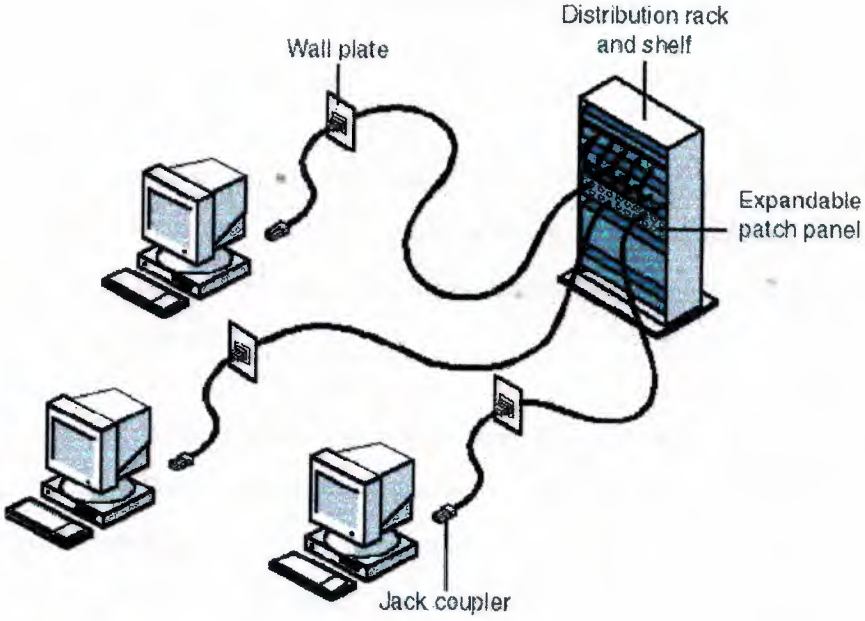

Figure 2.17 *Various twisted-pair cabling components*

Twisted-Pair Cabling Considerations

Use twisted-pair cable if:

- Your LAN is under budget constraints.
- You want a relatively easy installation in which computer connections are simple.

Do not use twisted-pair cable if:

- Your LAN requires a high level of security and you must be absolutely sure of data integrity.
- You must transmit data over long distances at high speeds.

2.2.3 Fiber-Optic Cable

In *fiber-optic cable*, optical fibers carry digital data signals in the form of modulated pulses of light. This is a relatively safe way to send data because, unlike copper-based cables that carry data in the form of electronic signals, no electrical impulses are carried over the fiber-optic cable. This means that fiberoptic cable cannot be tapped, and its data cannot be stolen.

Fiber-optic cable is good for very high-speed, high-capacity data transmission because of the purity of the signal and lack of signal attenuation.

Fiber-Optic Cable Composition

An optical fiber consists of an extremely thin cylinder of glass, called the *core*, surrounded by a concentric layer of glass, known as the *cladding*. The fibers are sometimes made of plastic. Plastic is easier to install, but cannot carry the light pulses for as long a distance as glass.

Because each glass strand passes signals in only one direction, a cable includes two strands in separate jackets. One strand transmits and one receives. A reinforcing layer of plastic surrounds each glass strand, and Kevlar fibers provide strength. See Figure 2.18 for an illustration of fiber-optic cable. The Kevlar fibers in the fiber-optic connector are placed between the two cables. Just as their counterparts (twisted-pair and coaxial) are, fiber-optic cables are encased in a plastic coating for protection.

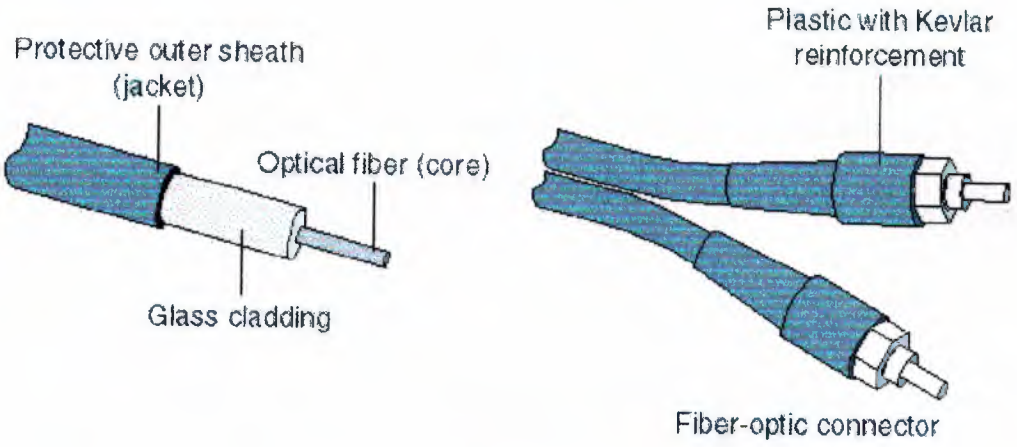

Figure 2.18 *Fiber-optic cable*

Fiber-optic cable transmissions are not subject to electrical interference and are extremely fast, currently transmitting about 100 Mbps with demonstrated rates of up to 1 gigabit per second (Gbps). They can carry a signal—the light pulse—for many miles.

Fiber-Optic Cabling Considerations

Use fiber-optic cable if you:

- Need to transmit data at very high speeds over long distances in very secure media.

Do not use fiber-optic cable if you:

- Are under a tight budget.
- Do not have the expertise available to properly install it and connect devices to it.

2.3 Signal Transmission

Two techniques can be used to transmit the encoded signals over cable: baseband and broadband transmission.

2.3.1 Baseband Transmission

Baseband systems use digital signaling over a single channel. Signals flow in the form of discrete pulses of electricity or light. Figure 2.19 shows a baseband transmission with a bidirectional digital wave. With baseband transmission, the entire communication

channel capacity is used to transmit a single data signal. The digital signal uses the complete bandwidth of the cable, which constitutes a single channel. The term *bandwidth* refers to the data transfer capacity, or speed of transmission, of a digital communications system as measured in bits per second (bps).

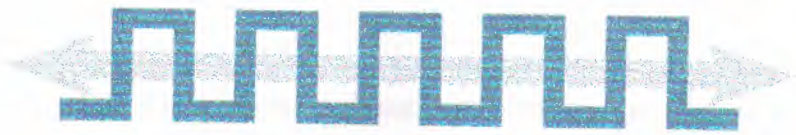

Figure 2.19 *Baseband transmission showing digital wave*

As the signal travels along the network cable, it gradually decreases in strength and can become distorted. If the cable length is too long, the received signal can be unrecognizable or misinterpreted.

As a safeguard, baseband systems sometimes use repeaters to receive incoming signals and retransmit them at their original strength and definition. This increases the practical length of a cable.

2.3.2 Broadband Transmission

Broadband systems, as shown in Figure 2.20, use analog signaling and a range of frequencies. With analog transmission, the signals are continuous and nondiscrete. Signals flow across the physical medium in the form of electromagnetic or optical waves. With broadband transmission, signal flow is unidirectional.

Figure 2.20 *Broadband transmission showing unidirectional analog wave*

If sufficient total bandwidth is available, multiple analog transmission systems, such as cable television and network transmissions, can be supported simultaneously on the same cable.

Each transmission system is allocated a part of the total bandwidth. All devices associated with a given transmission system, such as all computers using a LAN cable, must then be tuned so that they use only the frequencies that are within the allocated range.

While baseband systems use repeaters, broadband systems use amplifiers to regenerate analog signals at their original strength.

In broadband transmission, signals flow in one direction only, so there must be two paths for data flow in order for a signal to reach all devices. There are two common ways to do this:

- Through mid-split broadband configuration, the bandwidth is divided into two channels, each using a different frequency or range of frequencies. One channel transmits signals; the other receives signals.
- In dual-cable broadband configuration, each device is attached to two cables. One cable is used to send, and the other is used to receive.

2.4 Increasing Bandwidth Performance

Increasing the speed of data transmission is a priority as network sizes and data traffic increase. By maximizing the use of the data channel, we can exchange more data in less time. The most basic form of data or information transmission is called *simplex*. This means that data is sent in one direction only, from sender to receiver. A simplex transmission is shown in Figure 2.21. Examples of simplex transmission are radio and television. With simplex transmission, problems encountered during the transmission are not detected and corrected. Senders cannot even be sure that the data is received.

In the next level of data transmission, called *half-duplex transmission*, data is sent in both directions, but in only one direction at a time. Examples of technology that uses half-duplex communication are shortwave radio and walkie-talkies.

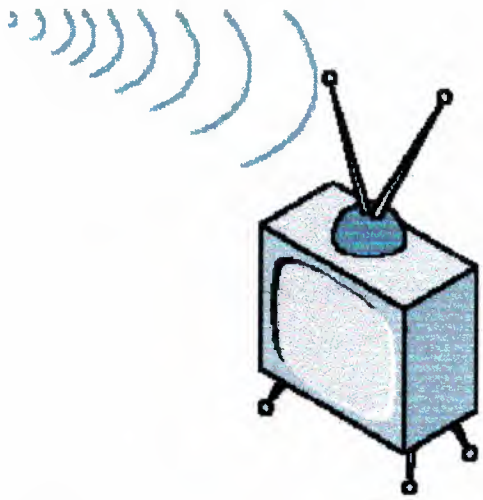

Figure 2.21 *A simplex transmission*

Figure 2.22 shows a half-duplex transmission. With half-duplex transmission, you can incorporate error detection and request that any bad data be resent. Surfing the World Wide Web is a form of half-duplex data transmission. You send a request for a Web page and then wait while it is being sent back to you. Most modem connections use half-duplex data transmission.

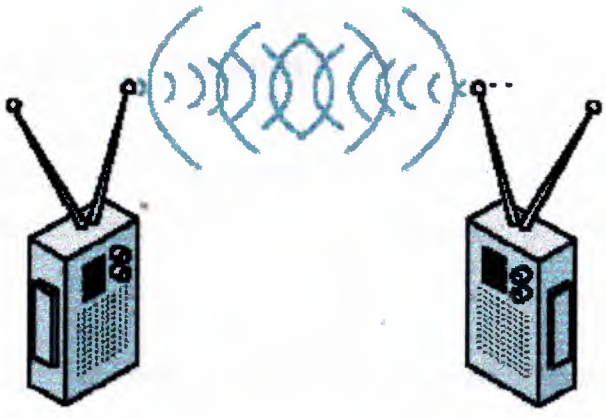

Figure 2.22 *A half-duplex transmission*

The most efficient method of transmitting data is to use a *full-duplex transmission*, in which data can be transmitted and received at the same time. A good example is a cable connection that not only allows you to receive TV channels, but also supports telephone

and Internet connection. A telephone is a full-duplex device because it allows both parties to talk at the same time. Figure 2.23 shows full-duplex communication. Modems, by design, are half-duplex devices. They either send or receive data, switching between transmission mode and receiving mode. You can create a full-duplex modem channel by using two modems and two telephone lines. The only requirement is that both computers be connected and configured to support this type of communication.

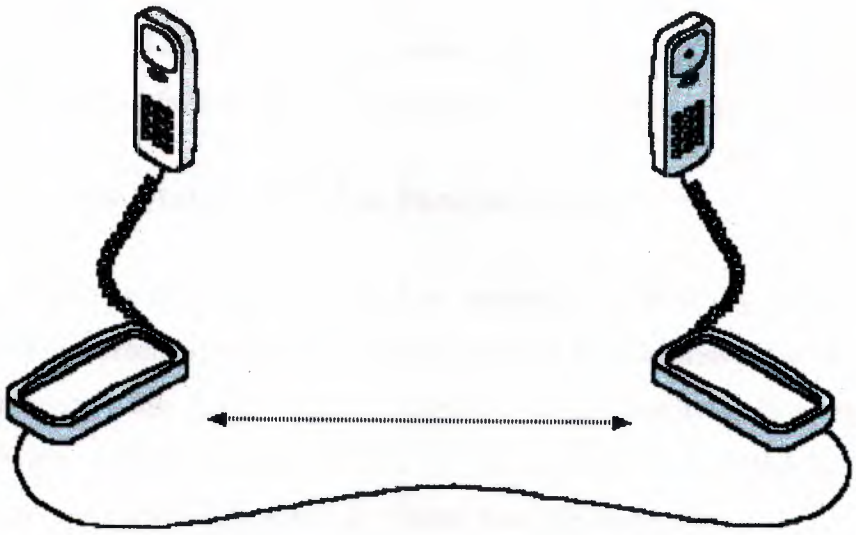

Figure 2.23 *Full-duplex communication*

2.5 The IBM Cabling System

IBM has developed its own cabling system, complete with its own numbers, standards, specifications, and designations. Many of these parameters, however, are similar to non-IBM specifications.

IBM introduced its cabling system in 1984. The purpose of this system was to ensure that the cabling and connectors would meet the specifications of their equipment. The IBM specification includes the following components:

- Cable connectors
- Face plates
- Distribution panels
- Cable types

The one IBM cabling component that is unique is the IBM connector, which is different from standard BNC or other connectors. These are IBM Type A connectors, known elsewhere as universal data connectors. They are neither male nor female; you can connect one to another by flipping either one over. These IBM connectors require special faceplates and distribution panels to accommodate their unique shape.

The IBM cabling system classifies cable into types. For example, in the IBM system, Category 3 cable (voice-grade UTP cable) is referred to as Type 3. (Table 2.2 compares the IBM cabling-system type names with standard cable type names.) The cable definitions specify which cable is appropriate for a given application or environment. The wire indicated in the system conforms to American Wire Gauge (AWG) standards.

2.5.1 AWG: The Standard Cable Measurement

Cable measurements are often expressed as numbers, followed by the initials AWG. (*AWG* is a measurement system for wire that specifies its thickness.) As the thickness of the wire increases, the AWG number decreases. Telephone wire is often used as a reference point; it has a thickness of 22 AWG. A wire of 14 AWG is thicker than telephone wire, and wire of 26 AWG is thinner than telephone wire.

2.6 Selecting Cabling

To determine which cabling is the best for a particular site you need to answer the following questions:

- How heavy will the network traffic be?
- What level of security does the network require?
- What distances must the cable cover?
- What are the cable options?
- What is the budget for cabling?

The better the cable protects against internal and external electrical noise, the farther and faster the cable will carry a clear signal. However, the better the speed, clarity, and security of the cable, the higher the cabling cost.

Table 2.2 IBM Cabling System

IBM type	Standard label	Description
Type 1	Shielded twisted-pair	Two pairs of 22 AWG wires surrounded (STP) cable by an outer braided shield; used for computers and multistation access units (MAUs)
Type 2	Voice and data cable	A voice and data shielded cable with two twisted pairs of 22 AWG wires for data, an outer braided shield, and four twisted pairs of 26 AWG wires for voice
Type 3	Voice-grade cable	Consists of four solid, unshielded twisted-pair, 22 or 24 AWG cables
Type 4	Undefined	
Type 5	Fiber-optic cable	Two 62.5/125-micron multimode optical fibers—the industry standard
Type 6	Data patch cable	Two 26 AWG twisted-pair stranded cables with a dual foil and braided shield
Type 7	Undefined	
Type 8	Carpet cable	Housed in a flat jacket for use under carpets; two shielded twisted-pair 26 AWG cables; limited to one half the distance of Type 1 cable
Type 9	Plenum-grade cable	Fire safe Two shielded twisted-pair cables

2.6.1 Cabling Considerations

As with most network components, there are trade-offs with the type of cable you purchase. If you work for a large organization and choose the least expensive cable, the accountants might initially be pleased, but you might soon notice that the LAN is inadequate in both transmission speed and data security.

Which cabling you select will depend on the needs of a particular site. The cabling you purchase to set up a LAN for a small business has different requirements from those of a larger organization, such as a major banking institution.

In the rest of this section, we examine some of the considerations that affect cabling price and performance.

Table 2.3 provides comparative information on cabling types.

Installation Logistics

How easy is the cable to install and work with? In a small installation where distances are short and security isn't a major issue, it does not make sense to choose thick, cumbersome, and expensive cable.

Shielding

The level of shielding required will affect cable cost. Almost every network uses some form of shielded cable. The noisier the area in which the cable is run, the more shielding will be required. The same shielding in a plenum-grade cable will be more expensive as well.

Crosstalk

Crosstalk and noise can cause serious problems in large networks where data integrity is crucial. Inexpensive cabling has low resistance to outside electrical fields generated by power lines, motors, relays, and radio transmitters. This makes it susceptible to both noise and crosstalk.

Transmission Rates

Transmission rates are measured in megabits per second. A standard reference point for current LAN transmission over copper cable is 100 Mbps. Fiber-optic cable transmits at more than 1 Gbps.

Cost

Higher grades of cables can carry data securely over long distances, but they are relatively expensive; lower-grade cables, which provide less data security over shorter distances, are relatively inexpensive.

Signal Attenuation

Different cable types have different rates of attenuation; therefore, cable specifications recommend specific length limits for the different types. If a signal suffers too much attenuation, the receiving computer will be unable to interpret it. Most networks have error-checking systems that will generate a retransmission if the signal is too weak to be understood. However, retransmission takes time and slows down the network

Table 2.3 *Cable Comparison Summary*

Characteristics	Thinnet coaxial (10Base2) Cable	Thicknet coaxial (10Base5) Cable	Twisted-pair (10BaseT) Cable	Fiber-optic Cable
Cable cost	More than UTP	More than thinnet	UTP: Least expensive STP: More than thinnet	More than thinnet, but less than thicknet
Usable cable length	185 meters (about 607 feet)	500 meters (about 1640 feet)	UTP and STP: 100 meters (about 328 feet)	2 kilometers (6562 feet)
Transmission rates	4-100 Mbps	4-100 Mbps	UTP: 4-100 Mbps STP: 16-500 Mbps	100 Mbps or more (> 1Gbps)
Flexibility	Fairly flexible	Less flexible than thinnet	UTP: Most flexible STP: Less flexible than UTP	Less flexible than thicknet
Ease of installation	Easy to install	Moderately easy to install	UTP: Very easy; often preinstalled STP: Moderately easy	Difficult to install
Susceptibility to interference	Good resistance to interference	Good resistance to interference	UTP: Very susceptible STP: Good resistance	Not susceptible to interference

Characteristics	Thinnet coaxial (10Base2) Cable	Thicknet coaxial (10Base5) Cable	Twisted-pair (10BaseT) Cable	Fiber-optic Cable
Preferred uses	Medium to large sites with high security needs	Linking thinnet networks	UTP: smaller sites on budget. STP: Token Ring in any size	Any size installation requiring speed and high data security and integrity
Special features	Electronic support components are less expensive than twisted-pair cable	Electronic support components are less expensive than twisted-pair cable	UTP: Same as telephone wire; often preinstalled in buildings STP: Supports higher transmission rates than UTP	Supports voice, data, and video

CHAPTER 3

NETWORK ARCHITECTURE

3.1 Introduction

In this chapter, we explore the three principal methods used to access the wires. The first method, called contention, is based on the principle of "first come, first served." The second method, token passing, is based on the principle of waiting to take turns. The third method, demand priority, is relatively new and is based on prioritizing access to the network. Last in the chapter, we continue our discussion of network architecture by examining the data itself and how it is put together before it is sent on its way.

3.2 Access Methods

3.2.1 The Function of Access Methods

The set of rules that defines how a computer puts data onto the network cable and takes data from the cable is called an *access method.* Once data is moving on the network, access methods help to regulate the flow of network traffic.

Traffic Control on the Cable

To understand traffic on a computer network, it helps to use an analogy. A network is in some ways like a railroad track, along which several trains run. The track is interspersed with occasional railway stations. When a train is on the track, all other trains must abide by a procedure that governs how and when they enter the flow of traffic. Without such a procedure, entering trains would collide with the one already on the track.

There are important differences between a railroad system and a computer network, however. On a network, all traffic appears to move simultaneously, without interruption.

Actually, this appearance of simultaneity is an illusion; in reality, the computers take turns accessing the network for brief periods of time. The more significant difference arises from the higher speed at which network traffic moves.

Multiple computers must share access to the cable that connects them. However, if two computers were to put data onto the cable at the same time, the data packets from one computer would collide with the packets from the other computer, and both sets of data packets would be destroyed. Figure 3.1 shows what happens when two computers try to access the network at the same time.

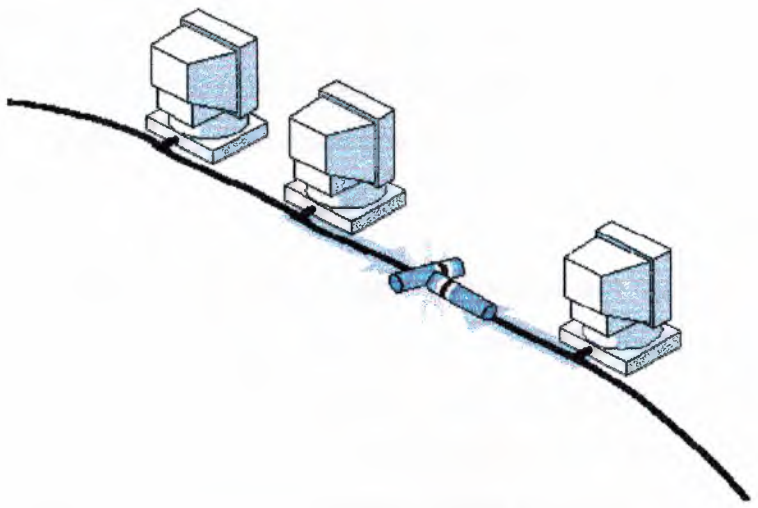

Figure 3.1 *Collision occurs if two computers put data on the cable at the same time*

If data is to be sent over the network from one user to another, or accessed from a server, there must be some way for the data to access the cable without running into other data. And the receiving computer must have reasonable assurance that the data has not been destroyed in a data collision during transmission.

Access methods need to be consistent in the way they handle data. If different computers were to use different access methods, the network would fail because some methods would dominate the cable. Access methods prevent computers from gaining simultaneous access to the cable. By making sure that only one computer at a time can put data on the network cable, access methods ensure that the sending and receiving of network data is an orderly process.

3.2.2 Major Access Methods

The three methods designed to prevent simultaneous use of the network media include:

- Carrier-sense multiple access methods (with collision detection or with collision avoidance).
- Token-passing methods that allow only a single opportunity to send data.
- Demand-priority methods.

1) a- Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Access Method

Using the method known as *carrier-sense multiple access with collision detection (CSMA/CD),* each computer on the network, including clients and servers, checks the cable for network traffic. Figure 3.2 illustrates when a computer can and cannot transmit data.

Only when a computer "senses" that the cable is free and that there is no traffic on the cable can it send data. Once the computer has transmitted data on the cable, no other computer can transmit data until the original data has reached its destination and the cable is free again. Remember, if two or more computers happen to send data at exactly the same time, there will be a data collision. When that happens, the two computers involved stop transmitting for a random period of time and then attempt to retransmit. Each computer determines its own waiting period; this reduces the chance that the computers will once again transmit simultaneously.

With these points in mind, the name of the access method—carrier-sense multiple access with collision detection (CSMA/CD)—makes sense. Computers listen to or "sense" the cable (carrier-sense). Commonly, many computers on the network attempt to transmit data (multiple access); each one first listens to detect any possible collisions. If a computer detects a possible collision, it waits for a random period of time before retransmitting (collision detection).

The collision-detection capability is the parameter that imposes a distance limitation on CSMA/CD. Due to attenuation the collision detection mechanism is not effective beyond 2500 meters (1.5 miles). Segments cannot sense signals beyond that distance and,

therefore, might not be aware that a computer at the far end of a large network is transmitting. If more than one computer transmits data on the network at the same time, a data collision will take place that will corrupt the data.

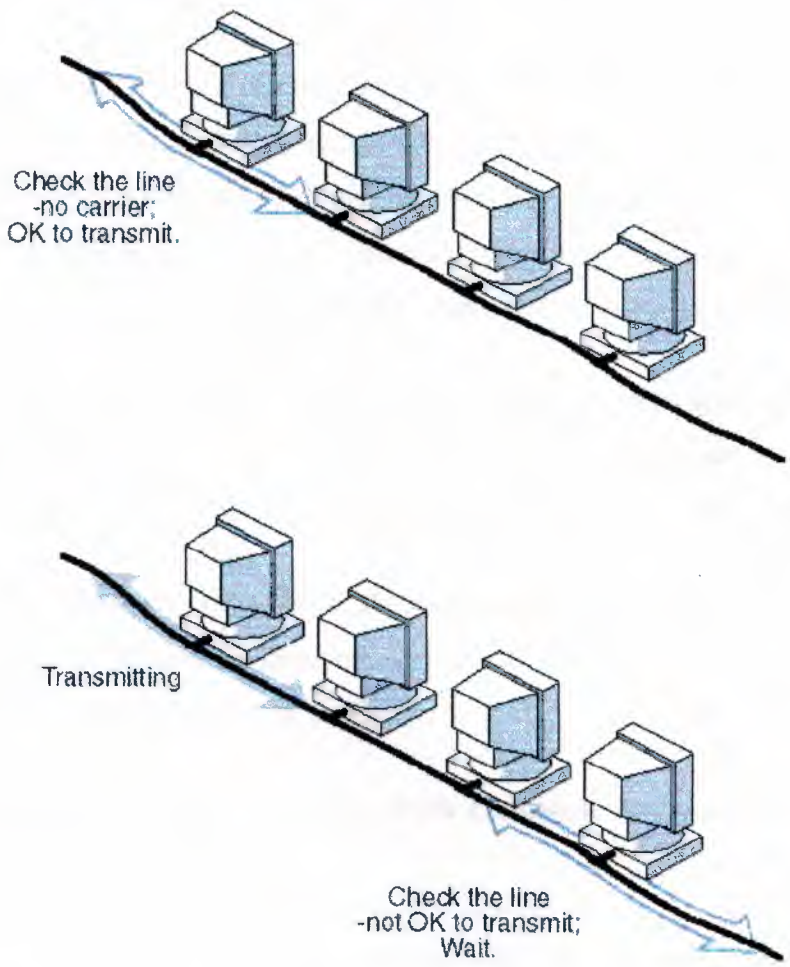

Figure 3.2 *Computers can transmit data only if the cable is free*

Contention Method

CSMA/CD is known as a *contention* method because computers on the network contend, or compete, for an opportunity to send data.

This might seem like a cumbersome way to put data on the cable, but current implementations of CSMA/CD are so fast that users are not even aware they are using a contention access method.

CSMA/CD Considerations

The more computers there are on the network, the more network traffic there will be. With more traffic, collision avoidance and collisions tend to increase, which slows the network down, so CSMA/CD can be a slow-access method.

After each collision, both computers will have to try to retransmit their data. If the network is very busy, there is a chance that the attempts by both computers will result in collisions with packets from other computers on the network. If this happens, four computers (the two original computers and the two computers whose transmitted packets collided with the original computer's retransmitted packets) will have to attempt to retransmit. These proliferating retransmissions can slow the network to a near standstill.

The occurrence of this problem depends on the number of users attempting to use the network and which applications they are using. Database applications tend to put more traffic on the network than word-processing applications do.

Depending on the hardware components, the cabling, and the networking software, using a CSMA/CD network with many users running several database applications can be very frustrating because of heavy network traffic.

1) b- Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) Access Method

Carrier-sense multiple access with collision avoidance (CSMA/CA) is the least popular of the three major access methods. In CSMA/CA, each computer signals its intent to transmit before it actually transmits data. In this way, computers sense when a collision might occur; this allows them to avoid transmission collisions. Unfortunately, broadcasting the intent to transmit data increases the amount of traffic on the cable and slows down network performance.

2) Token-Passing Access Method

In the access method known as *token passing*, a special type of packet, called a token, circulates around a cable ring from computer to computer. When any computer on the

ring needs to send data across the network, it must wait for a free token. When a free token is detected, the computer will take control of it if the computer has data to send.

The computer can now transmit data. Data is transmitted in frames, and additional information, such as addressing, is attached to the frame in the form of headers and trailers, discussed later in this chapter.

In Figure 3.3, the server is shown transmitting data. It takes control of the free token on the ring and sends data to the computer with the address 400080865402.

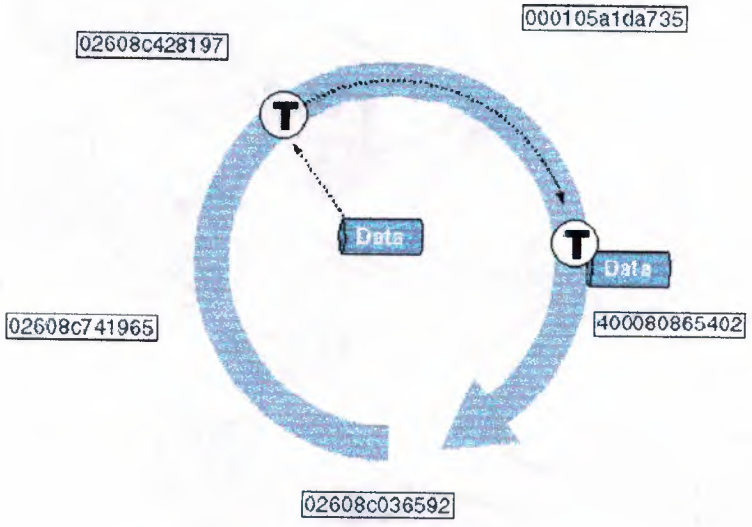

Figure 3.3 *Token-passing access method*

While the token is in use by one computer, other computers cannot transmit data. Because only one computer at a time can use the token, no contention and no collision take place, and no time is spent waiting for computers to resend tokens due to network traffic on the cable.

3) Demand Priority Access Method

Demand priority is a relatively new access method designed for the 100-Mbps Ethernet standard known as 100VG-AnyLAN. It has been sanctioned and standardized by the Institute of Electrical and Electronic Engineers (IEEE) in its 802.12 specification, which is discussed later in this chapter.

This access method is based on the fact that repeaters and end nodes are the two components that make up all 100VG-AnyLAN networks. Figure 3.4 shows a demand-priority network. The repeaters manage network access by doing round-robin searches for requests to send from all nodes on the network. The repeater, or hub, is responsible for noting all addresses, links, and end nodes and verifying that they are all functioning. According to the 100VG-AnyLAN definition, an end node can be a computer, bridge, router, or switch.

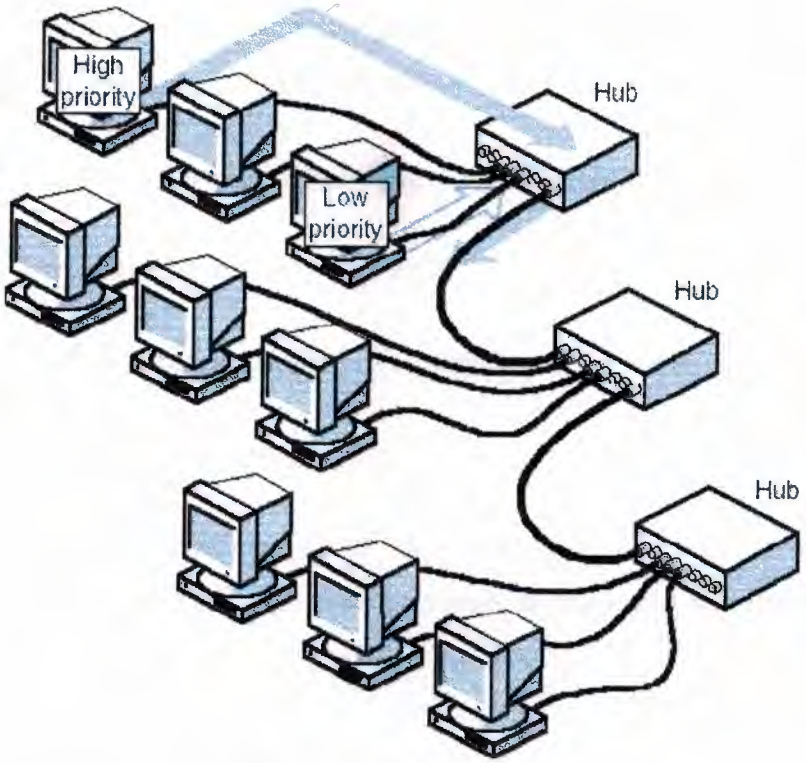

Figure 3.4 *Star-bus network access method for 100VG-AnyLAN is demand priority*

Demand-Priority Contention

As in CSMA/CD, two computers using the demand-priority access method can cause contention by transmitting at exactly the same time. However, with demand priority, it is possible to implement a scheme in which certain types of data will be given priority if there is contention. If the hub or repeater receives two requests at the same time, the highest priority request is serviced first. If the two requests are of the same priority, both requests are serviced by alternating between the two.

In a demand-priority network, computers can receive and transmit at the same time because of the cabling scheme defined for this access method. In this method, four pairs of wires are used, which enables quartet signaling, transmitting 25 MHz signals on each of the pairs of wire in the cable.

Demand-Priority Considerations

In a demand-priority network, there is communication only between the sending computer, the hub, and the destination computer. This is more efficient than CSMA/CD, which broadcasts transmissions to the entire network. In demand priority, each hub knows only about the end nodes and repeaters directly connected to it, whereas in a CSMA/CD environment, each hub knows the address of every node in the network.

Demand priority offers several advantages over CSMA/CD including:

- The use of four pairs of wires.

By using four pairs of wires, computers can transmit and receive at the same time.

- Transmissions through the hub.

Transmissions are not broadcast to all the other computers on the network. The computers do not contend on their own for access to the cable, but operate under the centralized control of the hub.

3.3 How Network Send Data

3.3.1 The Function of Packets in Network Communications

Data usually exists as rather large files. However, networks cannot operate if computers put large amounts of data on the cable at the same time. As you see in Figure 3.5, a computer sending large amounts of data causes other computers to wait (increasing the frustration of the other users) while the data is being moved. This is not called "sharing"; it is called "monopolizing the network." There are two reasons why putting large chunks of data on the cable at one time slows down the network:

- Large amounts of data sent as one large unit tie up the network and make timely interaction and communications impossible because one computer is flooding the cable with data.
- The impact of retransmitting large units of data further multiplies network traffic.

These effects are minimized when the large data units are reformatted into smaller packages for better management of error correction in transmission. This way, only a small section of data is affected, and, therefore, only a small amount of data must be retransmitted, making it relatively easy to recover from the error.

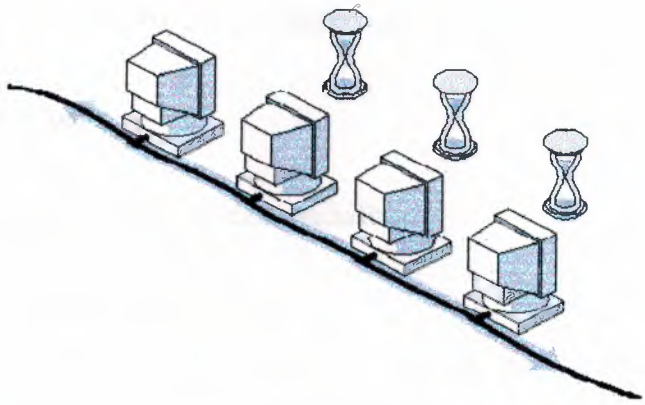

Figure 3.5 *Large continuous streams of data slow down the network*

In order for many users at once to transmit data quickly and easily across the network, the data must be broken into small, manageable chunks. This way, users each get their share of access to the network. These chunks are called *packets*, or frames. Although the terms "packet" and "frame" are often used interchangeably, there are some differences based on the type of network. we uses the term "packet," meaning "a unit of information transmitted as a whole from one device to another on a network."

When the network operating system at the sending computer breaks the data into packets (See Figure 3.6), it adds special control information to each frame. This makes it possible to:

- Send the original, disassembled data in small chunks.
- Reassemble the data in the proper order when it reaches its destination.
- Check the data for errors after it has been reassembled.

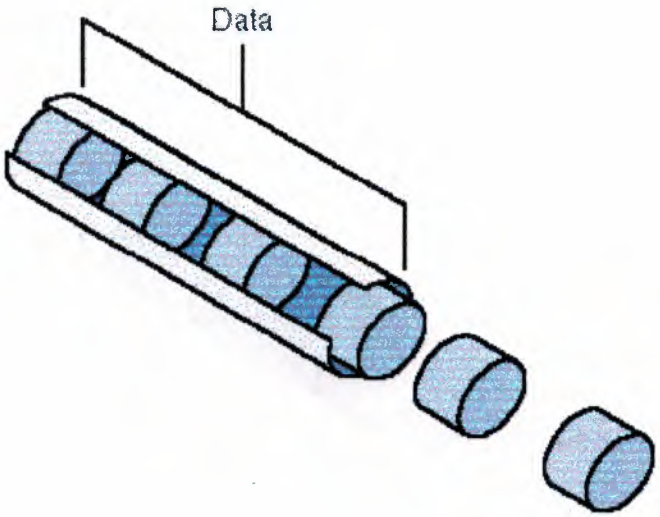

Figure 3.6 *Breaking data into packets*

3.3.2 Packet Structure

Packets can contain several types of data including:

- Information, such as messages or files.
- Certain types of computer control data and commands, such as service requests.
- Session control codes, such as error correction, that indicate the need for a retransmission.

Packet Components

All packets have certain components in common. These include:

- A source address that identifies the sending computer.
- The data that is intended for transmission.
- A destination address that identifies the recipient.
- Instructions that tell network components how to pass the data along.
- Information that tells the receiving computer how to connect the packet to other packets in order to reassemble the complete data package.
- Error-checking information to ensure that the data arrives intact.

Figure 3.7 shows these packet components grouped into three sections: header, data, and trailer.

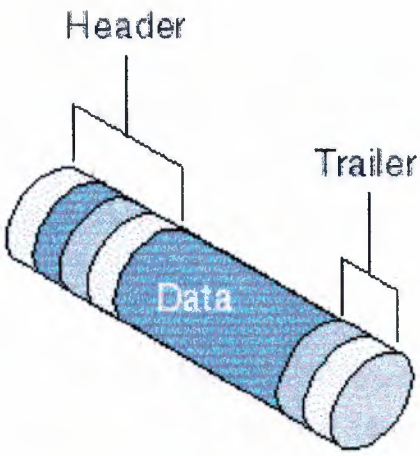

Figure 3.7 *Packet components*

- **Header**

The header includes:

- An alert signal to indicate that the packet is being transmitted.
- The source address.
- The destination address.
- Clock information to synchronize transmission.

- **Data**

This describes the actual data being sent. This part of the packet varies in size, depending on the network. The data section on most networks varies from 512 bytes—or 0.5 kilobytes (KB)—to 4 KB.

Because most original data strings are much longer than 4k, data must be broken into chunks small enough to be put into packets. It takes many packets to complete the transmission of a large file.

- **Trailer**

The exact content of the trailer varies depending on the communication method, or *protocol*. However, the trailer usually contains an error-checking component called a *cyclical redundancy check (CRC)*. The CRC is a number produced by a mathematical

calculation on the packet at its source. When the packet arrives at its destination, the calculation is made again. If the results of both calculations are the same, this indicates that the data in the packet has remained stable. If the calculation at the destination differs from the calculation at the source, this means the data has changed during the transmission. In that case, the CRC routine signals the source computer to retransmit the data.

Different networks have differing formats for the packets and allow different-sized packets. The packet-size limits determine how many packets the network operating system can create from one large piece of data.

Example: Packets in Printing

The following example illustrates, step-by-step, how packets are used in network communications.

A large print job must be sent from a computer to a print server.

1. In Figure 3.8, the sending computer establishes a connection with the print server.
2. In Figure 3.9, the computer next breaks the large print job into packets. Each packet contains the destination address, the source address, the data, and control information.

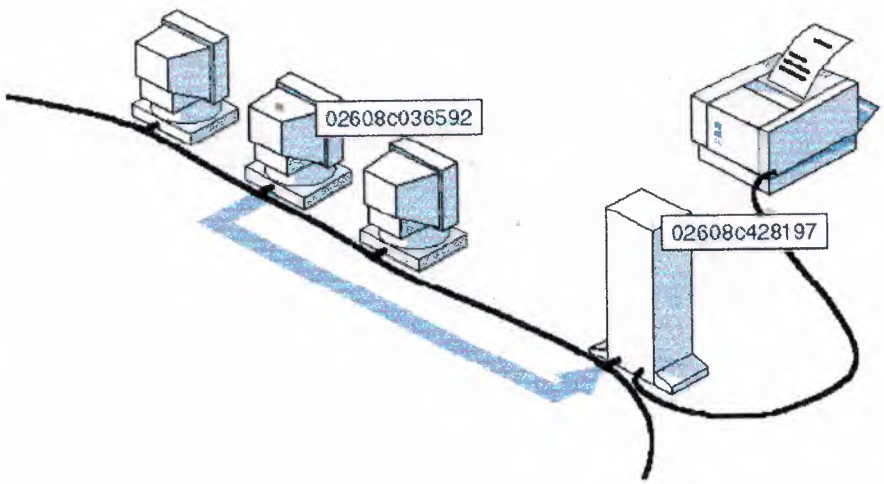

Figure 3.8 *Establishing a connection with a print server*

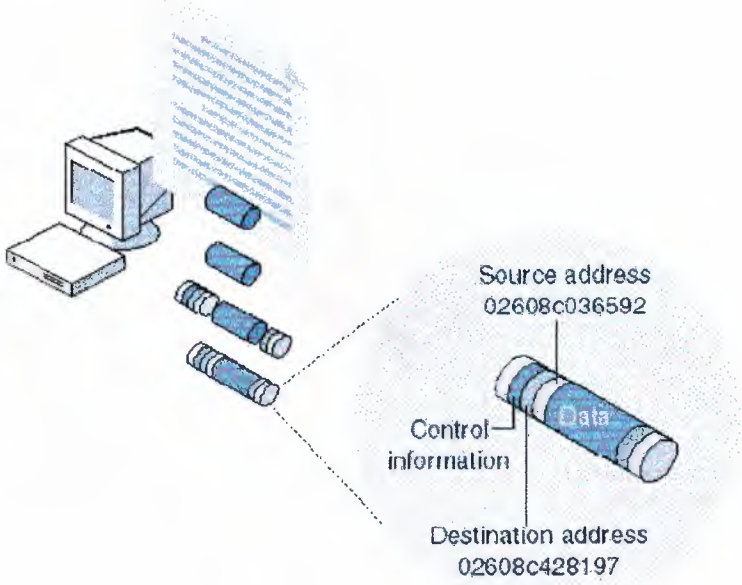

Figure 3.9 *Creating packets*

3. In Figure 3.10, the network interface card (NIC) in each computer examines the receiver's address on all frames sent on its segment of the network. However, because each NIC has its own address, the card does not interrupt the computer until it detects a frame addressed specifically to it.
4. In Figure 3.11, the destination computer is the print server. The packets enter through the cable into the NIC.

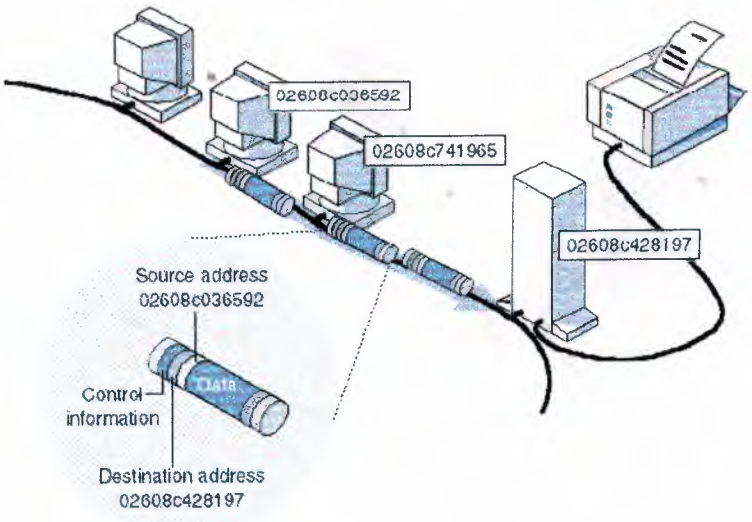

Figure 3.10 *Examining the receiver's address*

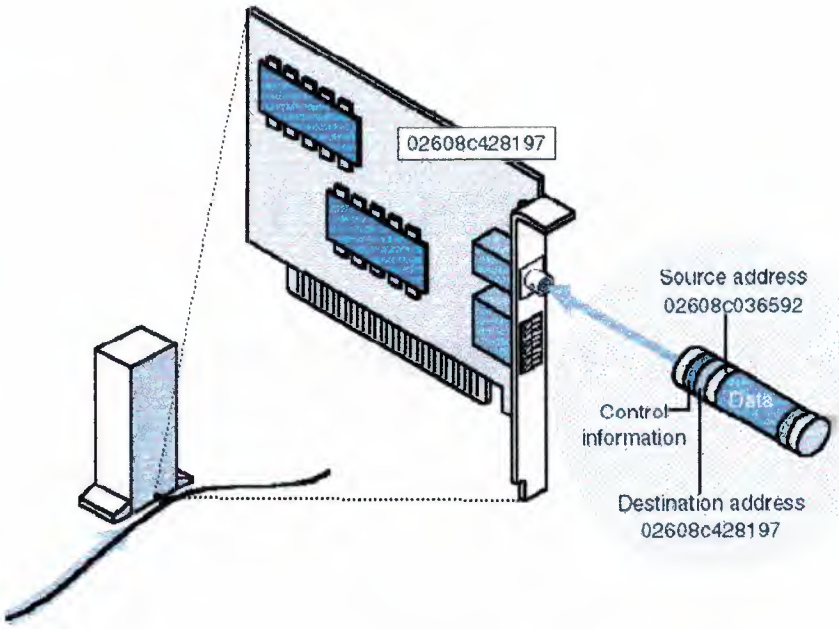

Figure 3.11 *Network interface card (NIC) accepts packets addressed to the print server*

5. The network software processes the frame stored in the NIC's receive buffer. Sufficient processing power to receive and examine each incoming frame is built into the NIC. This means that no computer resources are used until the NIC identifies a frame addressed to itself.
6. In Figure 3.12, the network operating system in the receiving computer reassembles the packets back into the original text file and moves the file into the computer's memory. From there the file is sent to the printer.

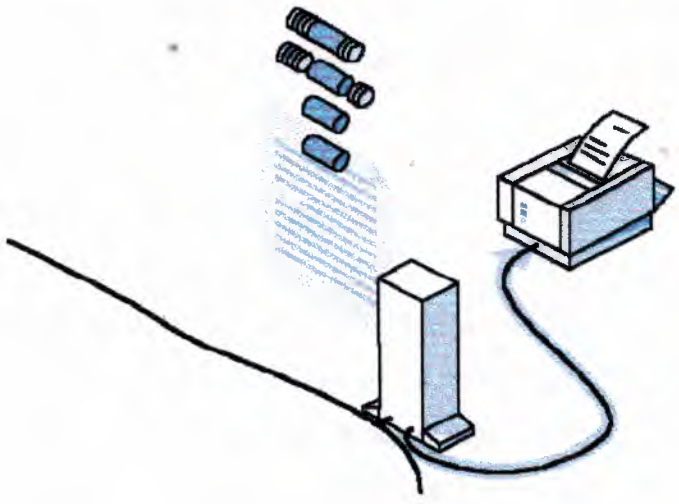

Figure 3.12 *Reassembled packets sent to the printer*

CHAPTER 4

NETWORK PROTOCOLS

4.1 Introduction

In the previous chapters, we talked about the physical parts of the networks, in this chapter we'll talk about the way in which the data carried through. To ensure that computers in a network are able to communicate, they must share a common language known as a protocol. A protocol is a set of rules or standards that enables communication between computers in a network. A number of protocols are available today, each having its own set of characteristics and capabilities. However, not every protocol is compatible with all computers and operating systems. To determine if a client computer a network can communicate with other computers in the network, you must be familiar with the protocols supported by the operating system in use.

Windows operating system supports many of the common network protocols available today, as well as other communication protocols, including protocols for remote access. The compatibility of Windows operating system with different types of protocols enhances the usability of Windows in different network environments, this feature is only available in windows systems, most of other operating systems, are supported in only one or two protocols.

4.2 Introduction to Protocols

Protocols are software and must he installed on network components that need them. Computers can communicate with each other only if they use the same protocol. If the protocol used by a computer in a network is not compatible with the protocol used by another computer, the two computers cannot exchange information. A variety of protocols are available for use in specific network environments. Although each protocol

facilitates basic network communication, each has a different function and accomplishes different tasks.

You can understand the function of different protocols by examining the standard model for networks—the Open Systems Interconnection (OSI) reference model. This model is built around a set of seven protocol layers, and each layer is responsible for some function that assists in the transmission of data over the network.

According to the OSI conceptual model, several protocols must work together to ensure the proper transmission of data. In reality, this is achieved with the help of a protocol stack. A protocol stack is a collection of protocols that function together to transmit data across a network of computers.

4.2.1 Types of Protocols

Two types of protocols are available today: open and vendor-specific.

Open Protocols

Open protocols are protocols that are written to publicly known industry standards. A protocol that adheres to these industry standards is compatible with other protocols written to the same standards. Open protocols are nonproprietary (not privately owned). A common example of an open protocol is Transmission Control Protocol/Internet Protocol (TCP/IP), which is used as the standard for communication over the Internet. Figure 4.1 shows the two types of protocols available today.

Vendor-Specific Protocols

Vendor-specific protocols are proprietary and have been developed by different vendors for use in specific environments. For example, Novell provides a set of protocols, such as Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX), developed specifically for its NetWare architecture. (See Figure 4.1)

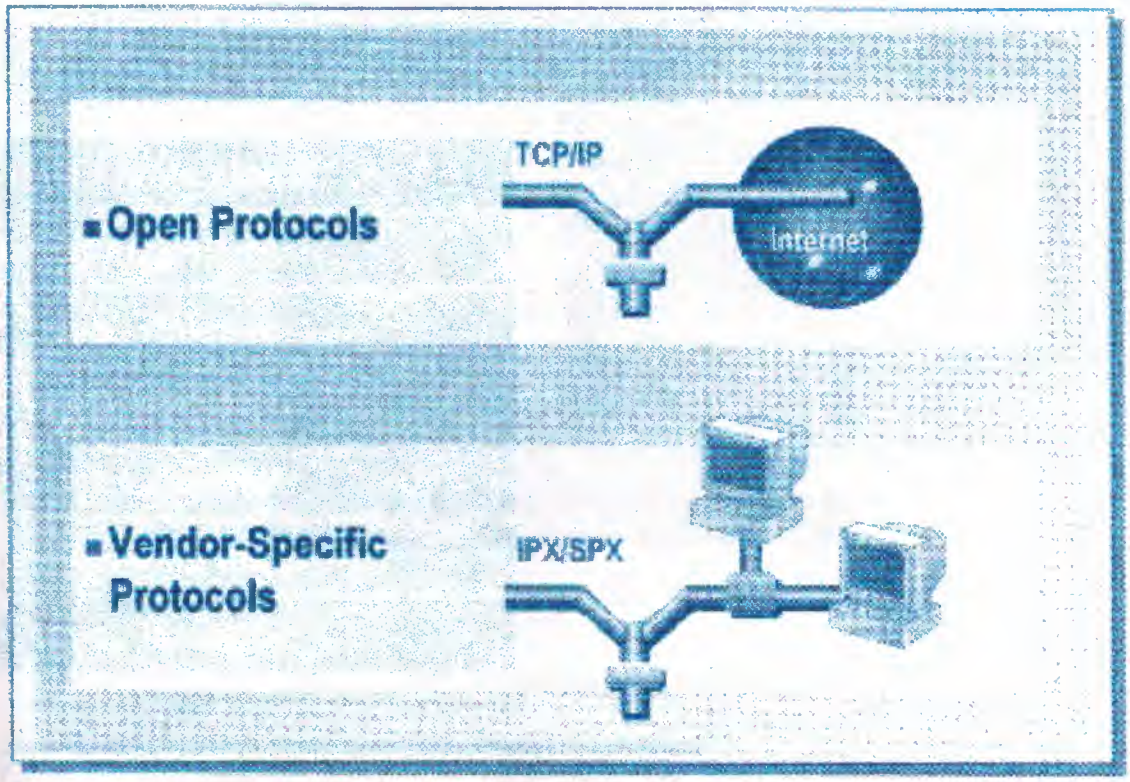

Figure 4.1 *the two types of protocols*

4.2.2 Open Systems Interconnection (OSI) Reference Model

The need for worldwide standardization of technologies led to the creation of the International Organization for Standardization (ISO). ISO is responsible for standardizing the methods by which computers communicate worldwide. To do so, ISO created a model for network communication, called the Open Systems Interconnection (OSI) reference model, or the OSI model.

OSI Model

The OSI model divides network communications into seven layers as shown in Figure 4.2. Each layer carries out specific functions in transmitting data on the network.

Before data is moved through the layers of the OSI model, it must be divided into packets. A packet is a unit of information that is transmitted as a whole from one computer to another on a network. The network passes a packet from layer to layer, and at each layer some additional formatting is added to the packet.

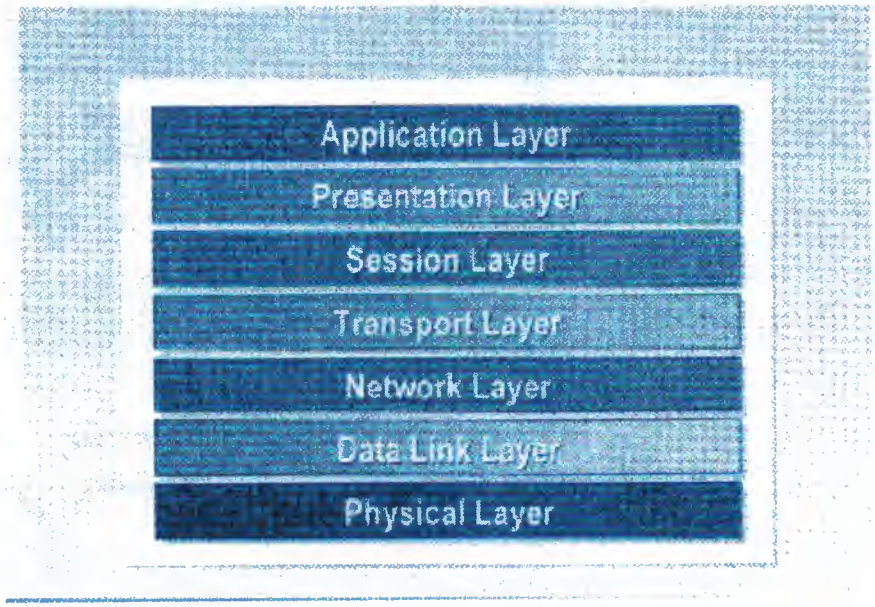

Figure 4.2 *The Seven layers of the OSI Model*

Table 4.1 describes the function of each layer. The layer at which a protocol works describes the function of the protocol. Some protocols work only at particular layers of the OSI model.

Table 4.1 *the function of each layer in the OSI model*

OSI layer	*Function*
Application Layer	Defines how applications interact with each other
Presentation Layer	Adds common formatting for data representation
Session Layer	Establishes and maintains communications channels
Transport Layer	Ensures error-free delivery of data
Network Layer	Addresses messages both within and between networks
Data Link Layer	Defines access methods for the physical medium, such as the network cable
Physical Layer	Puts the data on the physical medium

4.2.3 Protocol Stacks

The OSI model defines distinct layers related to packaging, sending, and receiving data transmissions in a network. A layered set of related protocols actually carries out these

services. This layered set of protocols running on a network is called a protocol stack. Together, the protocols in the stack handle all tasks required in packaging, sending, and receiving transmissions.

Several protocol stacks are designated as standard protocol models. Some of the common protocol stacks are TCP/IP, IPX/SPX, and AppleTalk. Protocols exist at each layer of these stacks, performing the tasks specified by that layer. Generally, however, the responsibility for performing specific communication tasks in the network is assigned to protocols working as one of three types: application protocols, transport protocols, and network protocols.

Application Protocols

Application protocols provide data exchange between applications in a network. Examples of common application protocols include File Transfer Protocol (FI'P) and Simple Mail Transfer Pr (SMTP).

Transport Protocols

Transport protocols provide for communication sessions between computers and ensure that data moves reliably between computers. A common transport protocol is Transmission Control Protocol (TCP).

Network Protocols

Network protocols provide what are called link services. These protocols define the rules for communicating in a particular network environment. A common protocol that provides network services is Internet Protocol (IP).

4.3 Protocols and Data Transmissions

In a large network, it is difficult to manage communication efficiently because of the large volume of network traffic. Network administrators can bypass this problem by dividing large networks into network segments. Network segments are smaller networks, which, when combined, form a large network.

Within a network, data may be transmitted from one network segment to another along any of several available paths. The transmission of data between network segments is called routing. However, not every protocol supports routing. Protocols are categorized as routable or non-routable based on their ability or inability to support routing.

The ability of protocols to support routing enables data transmission between computers in different network segments. There are different types of data transmissions. Each transmission type determines which computers in a network receive the transmitted data. Because not all computers on the network may need to receive the transmitted data, you can control to a certain degree which computers receive and process the transmitted data by controlling the type of transmission.

4.3.1 Routable/Non-Routable Protocols

Based on whether or not protocols support routing, they can be categorized as routable or non-routable protocols.

Routable Protocols

Routable protocols support communication between LANs or network segments that may be spread throughout a building, across a small geographic area, such as a college campus, or across the globe, such us the Internet. Routable protocols support the transmission of data from one network segment to another along any of several paths connecting the two network segments. Examples of routable protocols are TCP/IP and IPXISPX. (See Figure 4.3)

Non-Routable Protocols

Non-routable protocols, unlike routable protocols, do not support the transmission of data from one network segment to another. Computers that use non-routable protocols can communicate only with other computers in the same network segment. NetBEUI and Data Link control (DLC) are examples of non routable protocols. (See Figure 4.4)

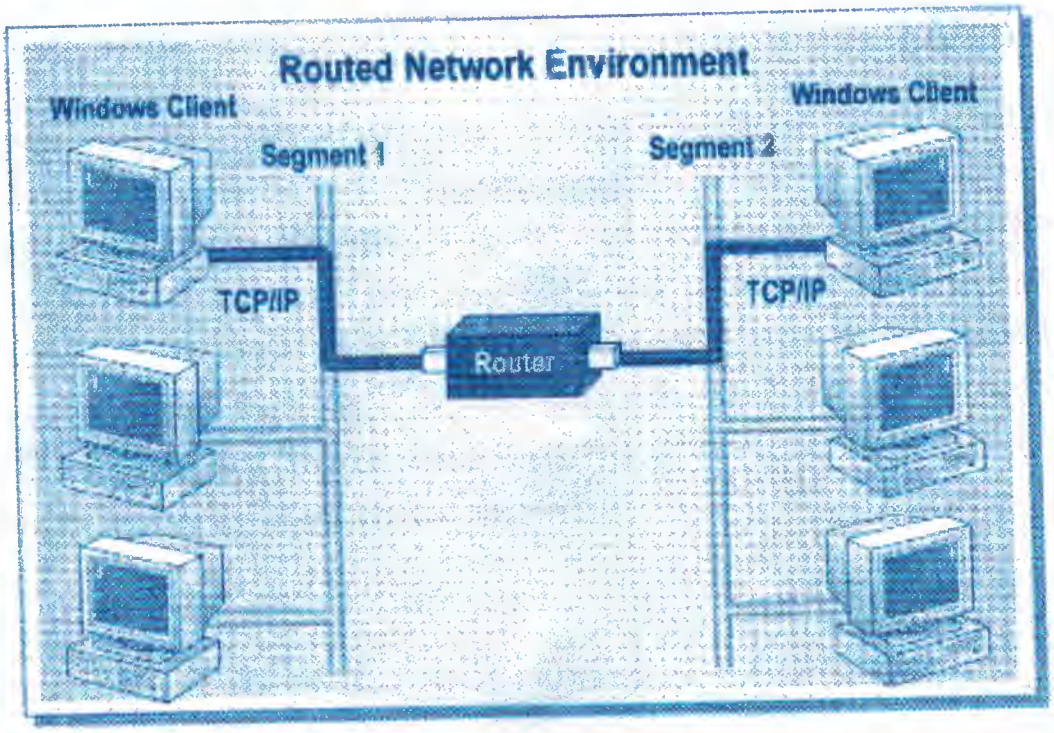

Figure 4.3 *an example of a routable protocol*

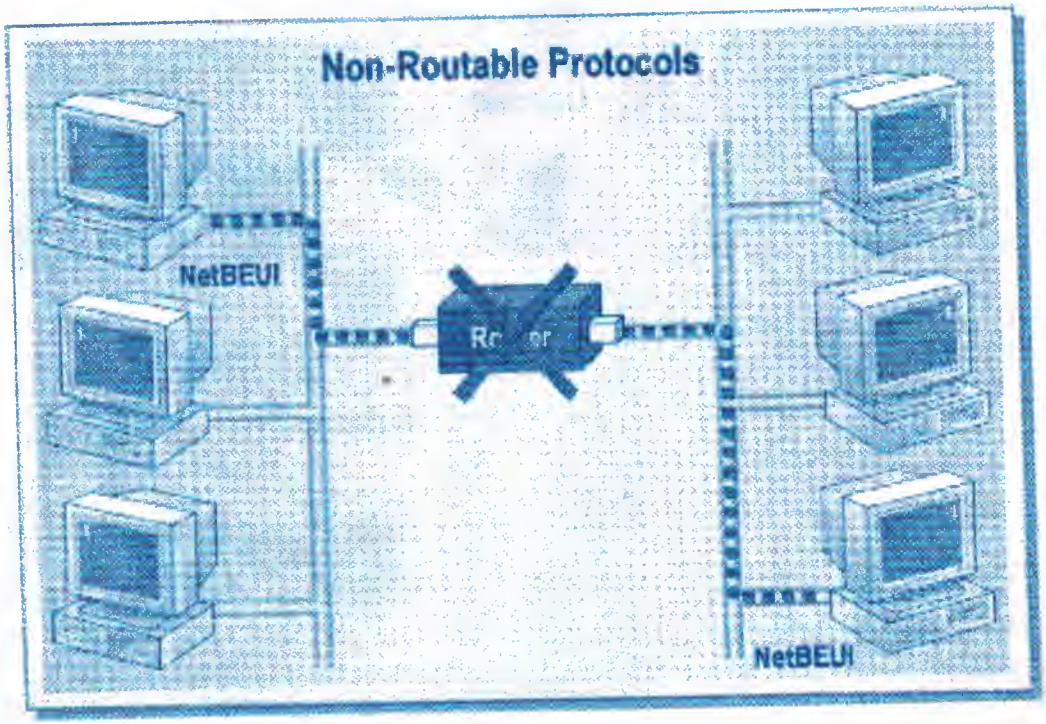

Figure 4.4 *an example of a non-routable protocol*

4.3.2 Types of Data Transmissions

Routable protocols enable the transmission of data between computers in different segments of a network. However, high volumes of certain kinds of network traffic, such as the deployment of multimedia applications, can affect network efficiency because it slows down transmission speed. The amount of network traffic generated varies with the three types of data transmissions: unicast, broadcast, or multicast. To understand how each transmission type affects network traffic, you must be familiar with the characteristics of each type of transmission. Figure 4.5 shows the graphically the difference between the 3 types of data transmission.

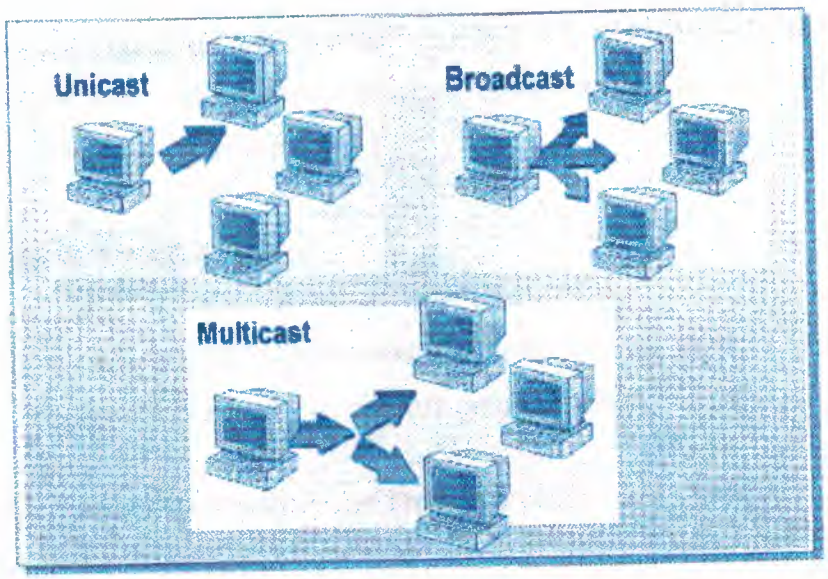

Figure 4.5 *the difference between the tree types of data transmission*

Unicast

In a unicast transmission, a separate copy of the data is sent from the source to each client computer requesting it. No other computer on the network needs to process the traffic. However, unicast transmission is not as efficient when multiple computers request the same data because the source transmits multiple copies of the data. Unicast transmission works best when just a small number of client computers request the data. Unicast transmission is also referred to as directed transmission. Most traffic on networks today is unicast.

Broadcast

When data is broadcast, a single copy of the data is sent to all clients on the same network segment as the sending computer. However, if that data must be sent to only a portion of the network segment, broadcast transmission is not an efficient transmission method because data is sent to the whole segment irrespective of whether it is required. This needlessly slows the performance of the network because each client must process the broadcast data.

Multicast

In a multicast transmission, a single copy of the data is sent only to client computers requesting it. Multiple copies of data are not sent across the network. This minimizes the network traffic and enables the deployment of multimedia applications on the network without overburdening the network. Many Internet services use multicasting to communicate with client computers.

4.4 Common Protocols

Different protocols are needed for communication with systems, devices, and computers in various environments. The common network protocols that you can use are:

- Transmission Control Protocol/Internet Protocol (TCP/IP).
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).
- NetBIOS Enhanced User Interface (NetBEUI).
- AppleTalk.

4.4.1 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP is an industry-standard protocol stack (a layered set of protocols) that enables communication in different networking environments. Because of the interoperability of TCP/IP among different types of computers, most networks support TCP/IP.

TCP/IP supports routing and enables computers to communicate across network segments. Because of this feature, TCP/IP is the standard protocol for communications over the Internet. Its reliable delivery and global use have made TCP/IP a necessity for

accessing worldwide information networks, such as the Internet. However, you must configure TCP/IP on all computers with which you want to use the protocol to communicate.

TCP/IP offers the following advantages:

- It is an industry standard. As an industry standard, it is an open protocol that is not controlled by a single organization.
- It contains a set of utilities for connecting dissimilar operating systems. Connectivity between two computers does not depend on the network operating system of either computer.
- It uses scalable, cross-platform, client-server architecture. TCP/IP can expand or shrink to meet the future needs of a network.

4.4.2 Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a protocol stack developed specifically for NetWare architecture. The 1PX/SPX stack includes IPX and SPX. IPX defines the addressing schemes used on a NetWare network, and SPX provides security and reliability to the IPX protocol. IPX is a network-layer protocol that is equivalent to the IP of the TCP/IP protocol stack. SPX provides reliable service at the transport layer.

IPXISPX has the following characteristics:

- It is used on networks with NetWare servers.
- It is routable. IPX/SPX enables computers in a routed networking environment to exchange information across segments.

4.4.3 NetBIOS Enhanced User Interface (NetBEUI)

NetBIOS Enhanced User Interface (NetBEUI) was one of the earliest protocols available for use on networks composed of personal computers. It was designed around the Network Basic Input/Output System (NetBIOS) interface to be a small, efficient

protocol for use in department-sized LANs of 20 to 200 computers, which would not need to be routed to other subnets.

At present, NetBEUI is used almost exclusively on small, non-routed networks consisting of computers running a variety of operating systems.

Windows 2000-based NetBEUI, known as NetBIOS Frame (NBF), is the underlying implementation of the NetBEUI protocol and is installed on computers running Windows 2000. It provides compatibility with existing LANs that use the NetBEUI protocol.

The advantages of NetBEUI include:

- Small stack size.
- No configuration requirement.
- High speed of data transfer on the network.
- Compatibility with all Microsoft-based operating systems, including Windows 2000.

The major disadvantage of NetBEUI is that it does not support routing. Because of this, computers running NetBEUI can communicate only with other computers in the same network segment.

4.4.4 AppleTalk

AppleTalk is Apple Computer's proprietary protocol stack designed to enable Apple Macintosh computers to share files and printers in a network environment.

Some of the characteristics of the AppleTalk protocol are:

- It enables Macintosh clients to access a server running Windows 2000.
- It is routable. Computers running AppleTalk can communicate across segments in a routed network environment.
- It enables Macintosh clients to access print services provided by a server running Windows 2000 if Print Server for Macintosh is installed on the server.

4.5 Other Communication Protocols

In addition of the commonly used networking protocols, there are other communication protocols for special needs, such as:

- Asynchronous transfer mode (ATM).
- Infrared Data Association (IrDA).

ATM and IrDA are both international standards for communication technologies. ATM was developed for the high-speed transmission of multimedia content, and IrDA was developed for wireless connectivity.

4.5.1 Asynchronous Transfer Mode (ATM)

Asynchronous transfer mode (ATM) is a high-speed protocol that transports multiple types of traffic across a network. The ATM technology was developed from international standards for the simultaneous transmission of data, voice, and video over a network at high speed. A device called an ATM switch is used to enable network communication by using the ATM protocol. Client computers communicate with each other by means of a network of ATM switches. (See Figure 4.6)

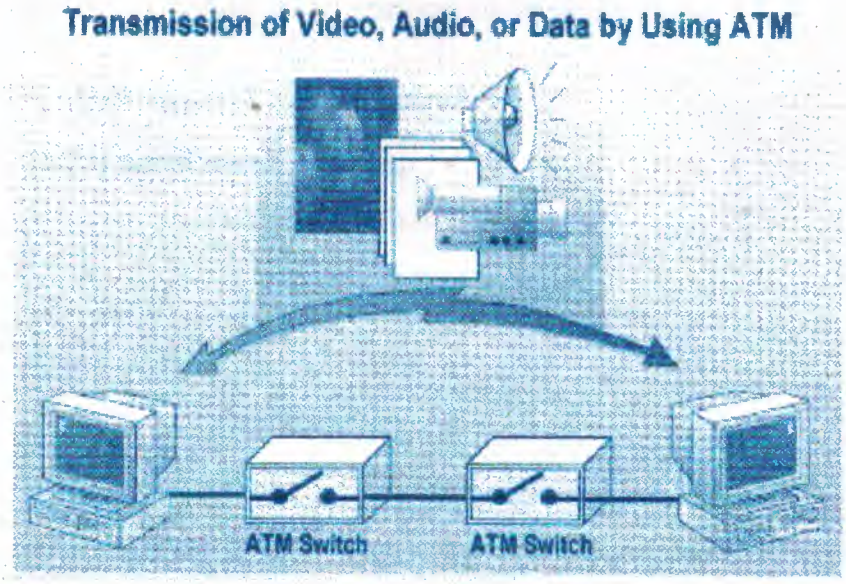

Figure 4.6 characteristics *of ATM*

Some of the characteristics of ATM are:

- It provides a single network connection that can reliably mix voice, video, and data. ATM can simultaneously transport such electronic communication as telephone calls, movies, and the e-mail and files contained on a Web server.
- It provides high-speed communication.
- It assures that no single type of data overuses the line. It efficiently allocates network bandwidth, thereby guaranteeing the reliability of the connection.

4.5.2 Infrared Data Association (IrDA)

The Infrared Data Association (IrDA) is an association that defined the group of short-range, high speed, bidirectional wireless infrared protocols, generically referred to as IrDA. The IrDA protocol stack enables computers to connect easily to peripheral devices or other computers without the use of connecting cables. For example, Windows automatically detects infrared devices, such as other computers or cameras, which are within range of each other. IrDA enables users to transfer information and share resources, such as printers, cameras, portable computers, desktop computers, and personal digital assistants (PDA5). (See Figure 4.7)

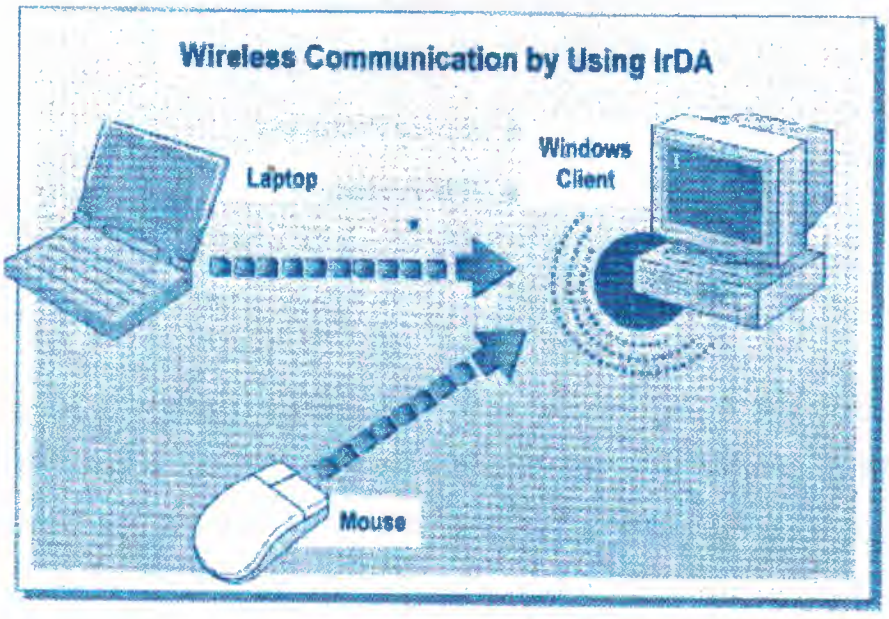

Figure 4.7 *the sensitive detection of windows client to other computers or devices*

IrDA enables wireless communication between any two infrared devices within range of each other. For example, two users traveling with laptop computers can transfer files by setting up an IrDA connection, instead of by using cables or floppy disks. IrDA automatically configures the connection when the portable computers are placed within close proximity. In addition, IrDA enables a computer to access resources that are attached to another computer. For example, if a user with a laptop computer needs to print a document, the user can create an IrDA connection with a computer that is connected to a printer, either locally or on a network. When that connection is established, the user, with appropriate permissions, can print over the IrDA connection.

The characteristics of IrDA wireless communication include:

- A worldwide standard for wireless infrared connectivity.
- Ease of implementation and use.
- No risk of radiation from infrared rays.
- No electromagnetic noise.
- No government regulatory issues.
- Minimum crosstalk (signal overflow from adjacent cable).

4.6 Remote Access Protocols

In Windows environment, you can establish a remote connection by using either dial- up remote access or a virtual private network (VPN). To establish a remote access connection to a Windows network, you can select from the following remote access protocols:

- Dial-up protocols
- VPN protocols

These remote access protocols are supported by Windows and provide interoperability with third party remote access components. Understanding the features of each protocol will help you decide which protocol is appropriate for your network.

4.6.1 Dial-Up Protocols

A dial-up remote access protocol -such as Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) - provides clients with access to a variety of remote access servers. (See Figure 4.8)

SLIP

SLIP allows remote access clients to connect to a remote access server through a modem. This allows client computers running Windows to connect to SLIP servers. A SLIP server is a remote access protocol component on the remote access server that services connection requests from SLIP clients. Although client computers running Windows can connect to SLIP servers, Routing and Remote Access does not itself include a SLIP server component. Therefore, you cannot use a computer running Windows as a SLIP server. Instead, you can use a server running UNIX as a SLIP server.

SLIP is an industry standard protocol that addresses TCP/IP connections made over serial lines. SLIP is supported by Routing and Remote Access and gives clients running Windows 2000 access to Internet services. SLIP has several limitations:

- Support is limited to TCP/IP. You cannot use SLIP to directly transfer other network protocols, such as IPX/SPX or NetBEUI.
- A static IP address is required. SLIP requires the client to configure all of the TCP/IP configuration parameters, such as the IP address, prior to establishing a connection to the server.
- It typically relies on text-based logon authentication sessions and usually requires a scripting system to automate the logon process.
- It transmits authentication passwords as clear text. This might result in a security compromise because passwords are not encrypted during user authentication.

PPP

PPP is a set of industry-standard protocols that enable remote access clients and servers to operate in a network consisting of components manufactured by multiple vendors.

PPP supports encrypted password authentication. PPP is an enhancement to the original SLIP specification and provides a standard method for sending network data over a point-to-point link.

PPP support enables computers running Windows to connect to remote networks through any server that complies with PPP standards. PPP compliance also enables a server to receive calls from, and provide access to, other vendors' remote access software.

The PPP architecture enables clients to use any combination of NetBEUI, TCP/IP, and IPX/SPX network transport protocols. You can run applications written to the IPX/SPX, NetBIOS, or Windows Sockets (WinSock) interface on a remote computer running Windows. The PPP architecture enables a server to download and configure TCP/IP parameters.

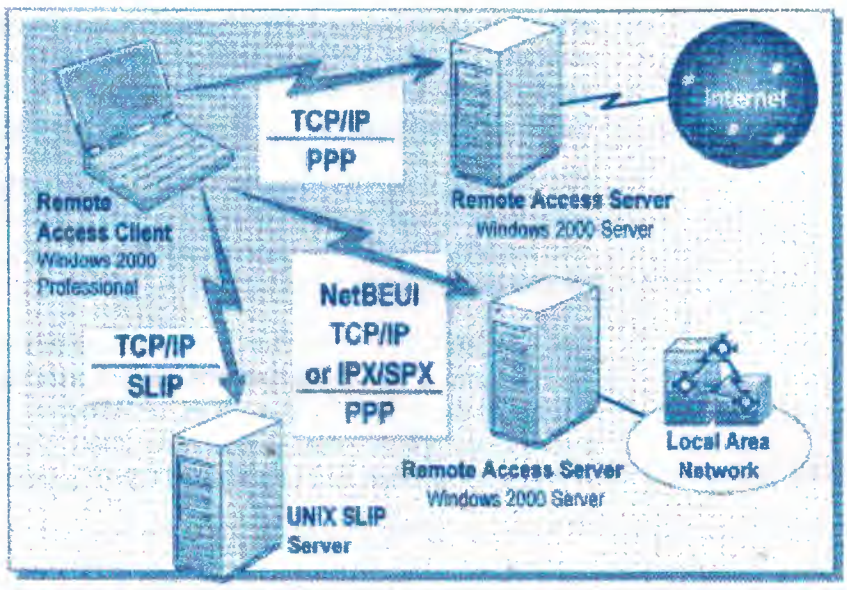

Figure 4.8 *Dial-Up Protocols*

4.6.2 VPN Protocols

You can use virtual private networks (VPNs) to provide remote access without having to rely on dial-up networking hardware, such as modems, on the remote access servers. VPNs use an additional protocol that allows users to connect to LANs over their existing

Internet or dial-up connections. These connections can be secure even though the connection may use public Internet hardware.

VPN protocols encapsulate TCP/IP, IPX/SPX, or NetBEUI data packets inside PPP data packets. The remote access server, with the help of the client, performs all security checks and validations and enables data encryption, making it safe to send data over non-secure networks, such as the Internet. Typically, users connect to the VPN by first connecting to an Internet service provider (ISP) and then connecting to the VPN ports through that Internet connection.

VPNs use either Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) to establish connections. (See Figure 4.9)

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) enables the secure transfer of encapsulated data from a PPTP client to a PPTP server across a TCP/IP Internetwork, such as the Internet. PPTP encapsulates PPP frames in TCP/IP packets for transmission over an Internetwork. Because of this encapsulation, you can use all features of PPP, including TCP/IP, IPX/SPX, NetBEUI, and Microsoft Point-to-Point Encryption (MPPE), in a PPTP virtual private network.

Windows supports PPTP, which you can use in private LAN-to-LAN networking.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an industry standard tunneling protocol. Like PPTP, L2TP uses the authentication and compression mechanisms of PPP. Unlike PPTP, L2TP does not utilize MPPE to encrypt PPP frames. Instead, L2TP relies on Internet Protocol Security (IPSec) for encryption services. The result is that L2TP-based virtual private network connections are typically a combination of L2TP and IPSec. For an encrypted L2TP virtual private network, both the client and the server must support L2TP and IPSec. L2TP allows any combination of TCP/IP, IPX/SPX, or NetBEUI traffic to be encrypted and then sent over any medium that supports point-to-point packet delivery, such as Ethernet, X.25, frame relay, or asynchronous transfer mode (ATM).

IPSec

Internet Protocol Security (IPSec) ensures data security in TCP/IP-based communications by providing an additional layer of network security. IPSec integrates with the security inherent in Windows 2000 to safeguard intranet and Internet communications. The VPN protocols, PPTP and L2TP, can he combined with the security provided by IPSec to provide data security.

IPSec provides data integrity and encryption. It is superior to PPTP, which uses MPPE encryption. Using IPSec, results in both increased demands on the CPU resources of the client and the server and an increased network payload.

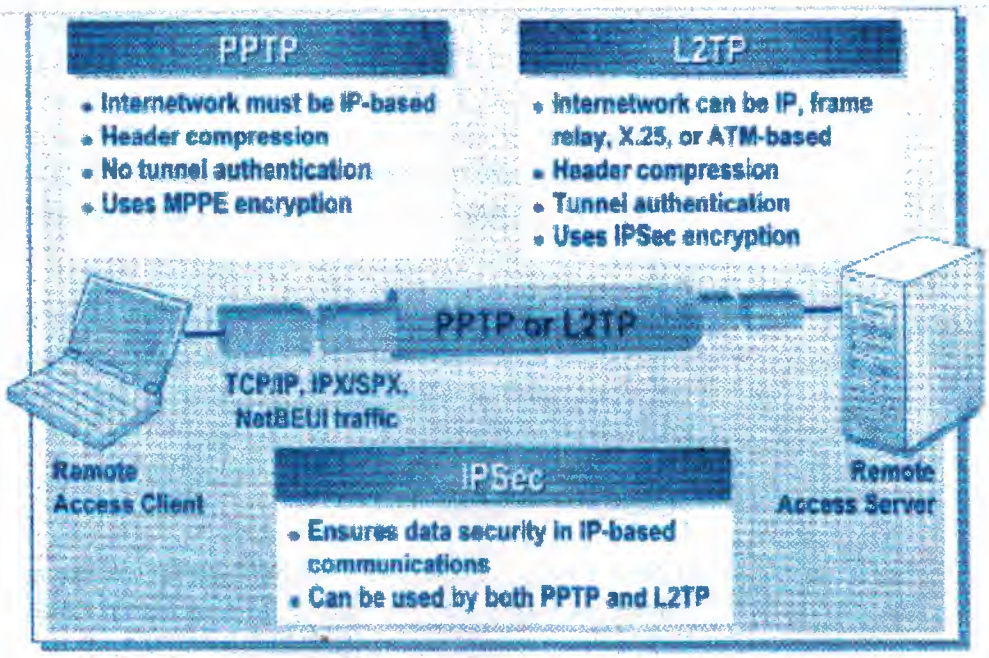

Figure 4.9 *VPN Protocols*

4.7 Introduction to TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry- standard protocol stack that is used mainly for communication between Windows based computers. TCP/IP is designed for communication across large-scale networks.

The tasks involved in using TCP/IP in the communication process are distributed between protocols that are organized into four distinct layers of the TCP/IP stack. Each protocol in the TCP/IP stack has a distinct role in the communication process.

During the communication process, many applications may he in communication at the same time. TCP/IP has the ability to differentiate one application from another. TCP/IP identifies an application on one computer and then moves the data from that application to an application on another computer.

4.7.1 The Communication Process

The process by which TCP/IP transmits data between two locations is analogous to the procedure used to send a letter from one city to another by postal mail. Figure 4.10 illustrate this process.

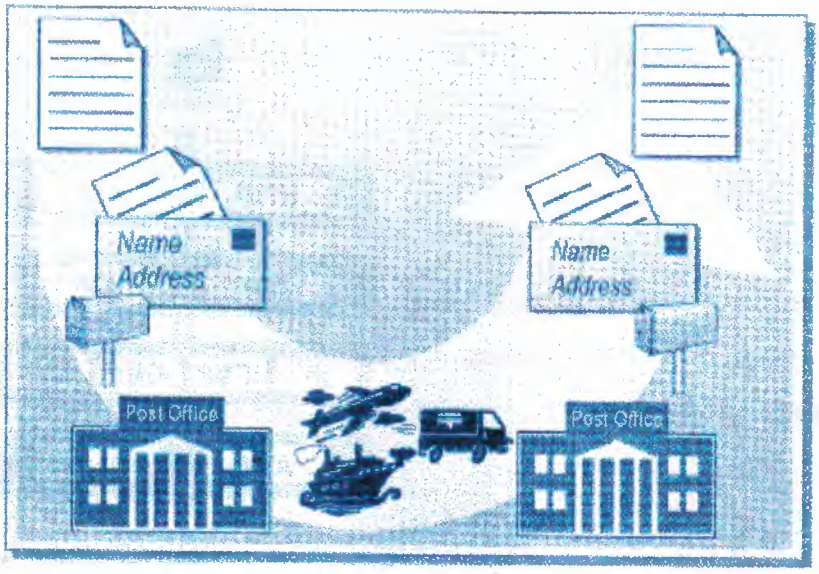

Figure 4.10 *the communication process*

TCP/IP Activities

The TCP/IP communication process is initiated using an application on the source computer that prepares the data to be transmitted in a format that an application on the destination computer can read. This is similar to writing a letter in a language that the

recipient can understand. Then the data is associated with the destination application and computer, much like how you address a letter to a recipient and household. The address of the destination computer is then added to the data, just as the address of the recipient is specified on the letter.

After these activities are performed, the data and additional information, including a request for confirmation of its delivery, are sent over the network to the destination. The network medium used for transmitting the data is independent of the above activities, just as the means of transport that transfers the letter from one post office to another is independent of the letter's content or address.

TCP/IP Protocols and Layers

TCP/IP organizes the communication process outlined here by assigning these activities to various protocols in the TCP/IP stack. To increase the efficiency of the communication process, the protocols are arranged in layers. The addressing information is placed last, so that the computers on a network can quickly check whether the data is meant for them. Only the computer that is the destination computer opens and processes all of the data.

4.7.2 TCP/IP Layers

TCP/IP uses a four-layer communication model to transmit data from one location to another. The four layers in this model are application, transport, Internet, and network interface. All protocols that belong to the TCP/IP protocol stack are located in these layers of the model. (See Figure 4.11)

Application Layer

The application layer is the topmost layer in the TCP/IP stack. All applications and utilities are contained in this layer and use this layer to gain access to the network. The protocols in this layer are used for the formatting and exchange of user information. They include:

- Hypertext Transfer Protocol (HTTP)

HTTP is used to transfer files that make up the Web pages of the World Wide Web.

- File Transfer Protocol (FTP)

  FFP is used for interactive file transfer.

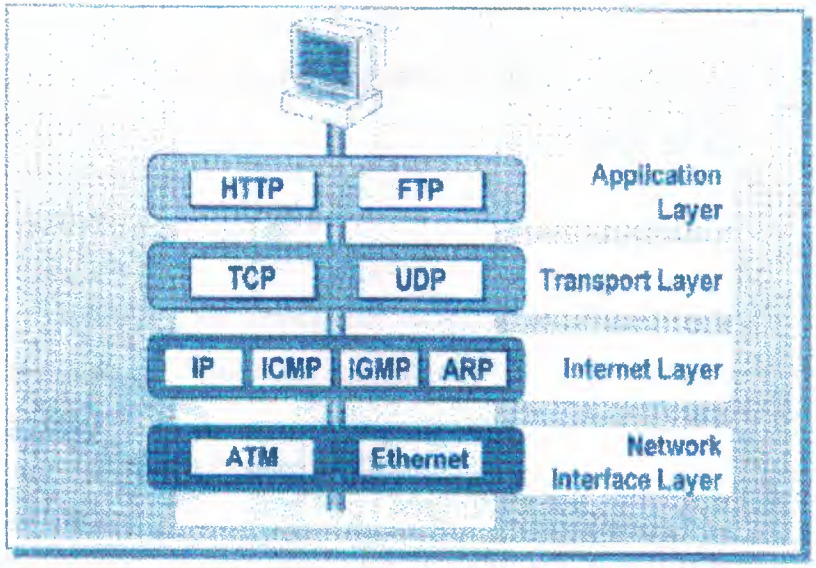

Figure 4.11 *TCP/IP Layer*

Transport Layer

The transport layer provides the ability to order and guarantee communication between computers and passes the data up to the application layer or down to the Internet layer. The transport layer also specifies the unique identifier of the application to which data is to be delivered.

The transport layer has two core protocols that control the method by which data is delivered. They are:

- Transmission Control Protocol (TCP)

  TCP guarantees the delivery of data through an acknowledgement.

- User Datagram Protocol (UDP)

UDP provides fast delivery of data hut does not guarantee data delivery.

Internet Layer

The Internet layer is responsible for addressing, packaging, and routing the data that is to he transmitted. This layer contains four core protocols:

- Internet Protocol (IP)

  IP is responsible for addressing the data to he transmitted and getting it to its destination.

- Address Resolution Protocol (ARP)

  ARP is responsible for identifying the media access control (MAC) address of the network adapter on the destination computer.

- Internet Control Message Protocol (ICMP)

  ICMP is responsible for providing diagnostic functions and reporting errors due to unsuccessful delivery of data.

- Internet Group Management Protocol (IGMP)

  IGMP is responsible for the management of multicasting within TCP/IP.

Network Interface Layer

The network interface layer is responsible for placing data on the network medium and receiving data off the network medium. This layer contains such physical devices as network cables and network adapters. The network adapter has a unique I 2-character hexadecimal number, such as B5-50-04-22-D4-65, which is known as the media access control (MAC) address. The network interface layer does not contain the type of software-based protocols that are included in the other three layers, hut it does contain such protocols as Ethernet and asynchronous transfer mode (ATM), which define how data is transmitted on the network.

4.7.3 Identifying Application

In a network, many applications are in communication at the same time. When multiple applications are active on a single computer, TCP/IP requires a method for differentiating one application from another. For this purpose, TCP/IP uses a socket, also known as an end point in network communication, to identify a specific application.

IP Address

To start a network communication, the location of the source and destination computers in the network must be known. The location is identified by a unique number, known as an IP address, which is assigned to each computer on the network. An example of an IP address is 192.168.2.200.

TCP/UDP Port

A port is an identifier for an application within a computer. A port is associated with either TCP or UDP transport layer protocols and is referred to as a TCP port or UDP port. A port can be any number between 0 and 65,535. Ports for common server-side TCP/IP applications, referred to as well-known port numbers, are reserved to numbers below 1,024 in order to avoid confusion with other applications. For example, the FTP Server application uses the TCP port numbers 20 and 21. (See Figure 4.12)

Socket

A socket is the combination of an IP address and the TCP port or UDP port. An application creates a socket by specifying the IP address of the computer, the type of service (TCP for guarantee of data delivery, otherwise UDP), and the port that the application monitors. The IP address component of the socket helps to identify and locate the destination computer, and the port determines the specific application to which the data is to he sent. (Figure 4.12)

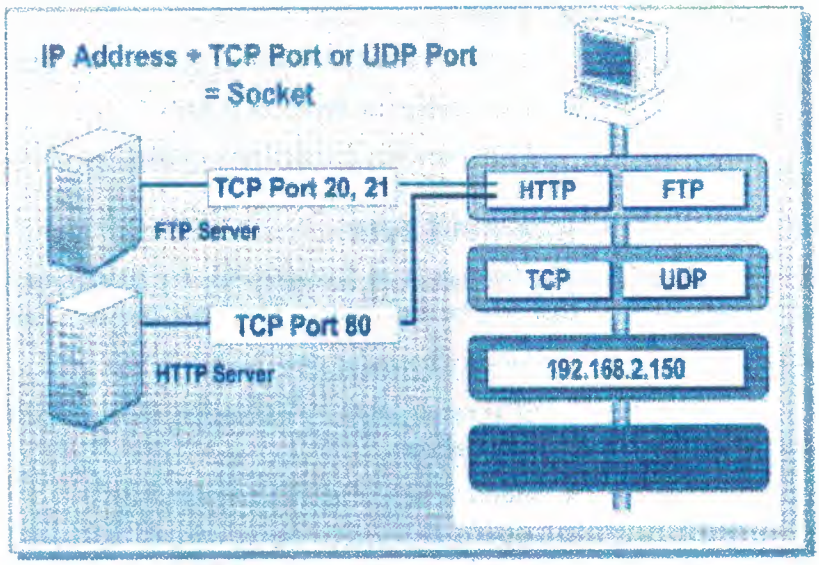

Figure 4.12 *Identifying Application*

4.8 TCP/IP Protocol Suite

The Microsoft TCP/IP protocol suite enables enterprise networking and connectivity on Windows-based computers. A suite is created by a vendor or organization to customize a protocol stack for its requirements. Therefore, a protocol suite is a set of protocols designed and built as complementary parts of a complete, smoothly functioning set.

The TCP/IP protocol suite includes six core protocols and a set of utilities. The six core protocols—TCP, UDP, IP, ICMP, IGMP, and ARP—provide a set of standards for communications between computers and for connections between networks. All applications and other protocols in the TCP/IP protocol suite rely on the basic services provided by these core protocols.

4.8.1 Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) is a required TCP/IP standard protocol that provides a reliable, connection-oriented data delivery service between only two computers. Such a communication is known as a unicast. In connection- oriented communication, the connection must be established before data can be transmitted between the two computers.

After the connection is established, data is transmitted over this single connection only. Connection-oriented communication is also referred to as reliable communication because it guarantees the delivery of the data at the destination.

On the source computer, TCP organizes the data to be transmitted into packets. On the destination computer, TCP reorganizes the packets to recreate the original data. (See Figure 4.13)

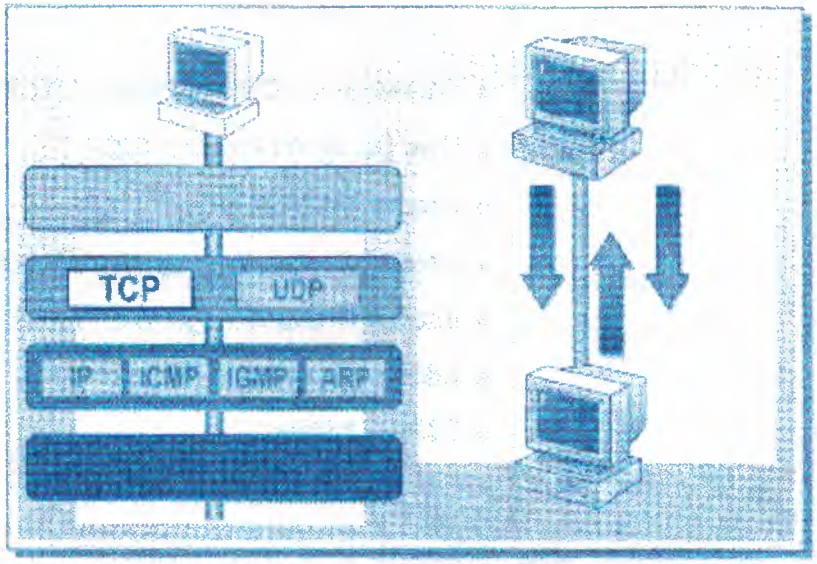

Figure 4.13 *Transmission Control Protocol (TCP)*

Data Transmission Using TCP

TCP transmits packets in groups to increase efficiency. It assigns a sequence number to each packet and uses an acknowledgment to verify that the destination computer has received a group of packets. If the destination computer does not return an acknowledgment for each group of packets sent within a specified period of time, the source computer retransmits the data.

In addition to adding the sequencing and acknowledgement information to the packet, TCP also adds the port information for both the source and the destination applications. The source computer uses the destination port to direct the packet to the proper

application at the destination computer, and the destination computer uses the source port to return information to the correct source application.

Three-Way Handshake

Because TCP is a reliable protocol, two computers using TCP for communication must establish a connection before exchanging data. This connection is a virtual connection and is known as a session. Two computers using TCP establish a connection, or TCP session, through a process known as a three-way handshake. This process synchronizes sequence numbers and provides other information needed to establish the session.

The three-way handshake is a three-step process:

1. The source computer initiates the connection by transmitting the session information, including the sequence number and size of the packet.
2. The destination computer responds with its session information.
3. The source computer agrees with and acknowledges the received information

4.8.2 User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is a transport layer protocol that identifies the destination application in network communications. UDP provides a connectionless packet delivery service that offers fast but unreliable, best-effort delivery of the data. UDP does not require an acknowledgment for the data received and does not attempt to retransmit data that is lost or corrupted. This means that less data is sent, but neither the arrival of packets nor the correct sequencing of delivered packets is acknowledged or guaranteed.

UDP is used by applications that transmit data to multiple computers by using broadcast or multicast transmissions. It is also used for transmitting small amounts of data or data that is not of high importance. Example uses of UDP include multicasting streaming media, such as during a live videoconference, and broadcasting a list of computer names, which are maintained for local communication. (See Figure 4.14)

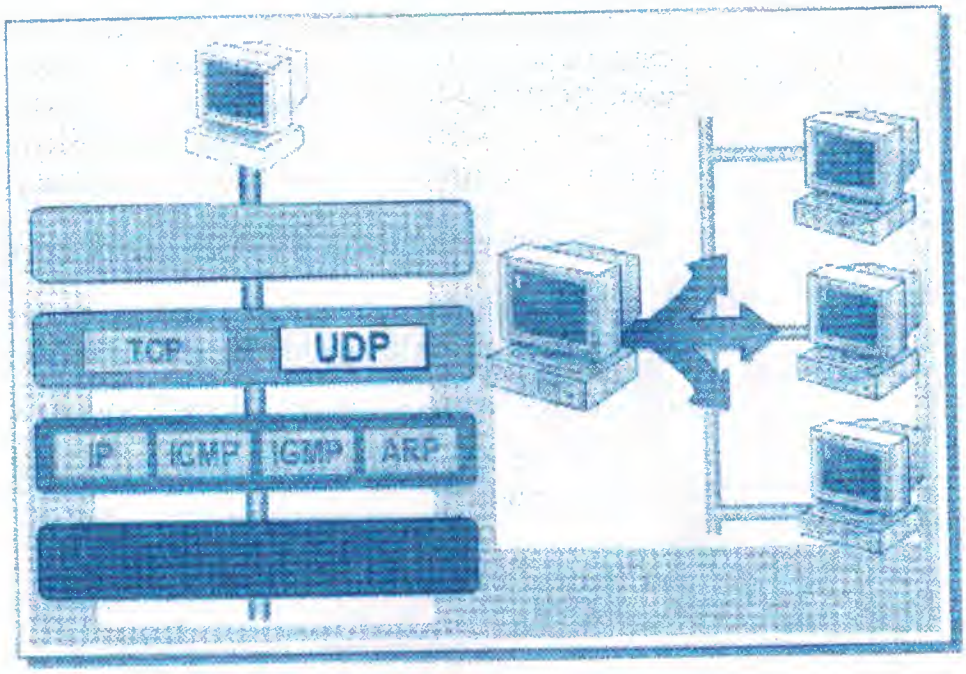

Figure 4.14 *User Datagram protocol (UDP)*

To use UDP, the source application must supply its UDP port number as well as that of the destination application. It is important to note that UDP ports are distinct and separate from TCP ports, even though some of them use the same numbers.

4.8.3 Internet Protocol (IP)

Internet Protocol (IP) helps to identify the location of the destination computer in a network communication. IP is a connectionless, unreliable protocol that is primarily responsible for addressing packets and routing them between networked computers. Although IP always attempts to deliver a packet, a packet may be lost, corrupted, delivered out of sequence, duplicated, or delayed. However, IP does not attempt to recover from these types of errors by requesting retransmission of the data. Acknowledging the delivery of packets and recovering lost packets is the responsibility of a higher-layer protocol, such as TCP, or of the application itself. (See Figure 4.15)

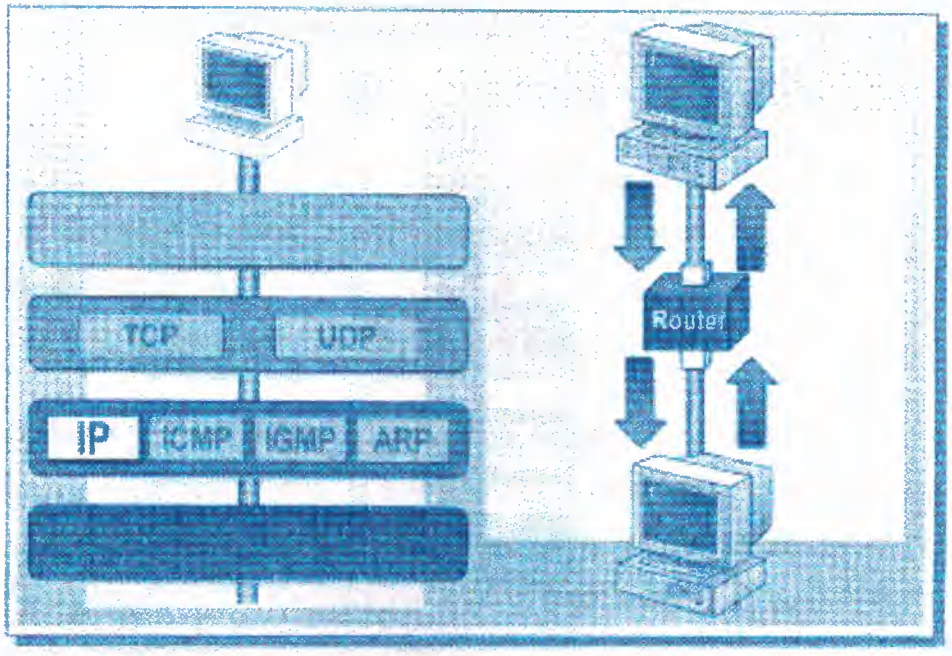

Figure 4.15 *Internet Protocol (IP)*

Activities Performed by IP

You can visualize IP as the mailroom of the TCP/IP stack, where packet sorting and delivery take place. The packets are passed down to IP by UDP or TCP from the transport layer or passed up from the network interface layer. The primary function of IP is to route the packets until they reach their destination.

Each packet includes the source IP address of the sender and the destination IP address of the intended recipient. These IP addresses in a packet remain the same throughout the packet's journey across a network.

If IP identifies a destination address as an address from the same segment, it transmits the packet directly to that computer. If the destination IP address is not on the same segment, IP must use a router to send the information.

IP is also responsible for ensuring that a packet does not remain on the network forever by limiting the number of networks across which the packet can travel. This is done by assigning a Time to Live (TTL) number to every packet. A TTL specifies the maximum length of time that the packet can travel on the network before being discarded.

4.8.4 Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) provides troubleshooting facilities and error reporting for undeliverable packets. With ICMP, computers and routers that use IP communication can report errors and exchange limited control and status information. For example, if IP is unable to deliver a packet to a destination computer, ICMP sends a Destination Unreachable message to the source computer.

Although the IP protocol is used to move data across routers, ICMP reports errors and control messages on behalf of IP. ICMP does not attempt to make IP a reliable protocol, because ICMP messages are unacknowledged and therefore unreliable. It only attempts to report errors and provide feedback on specific conditions. Although this may not seem effective, it is much more efficient than using bandwidth to acknowledge each ICMP message. (See Figure 4.16)

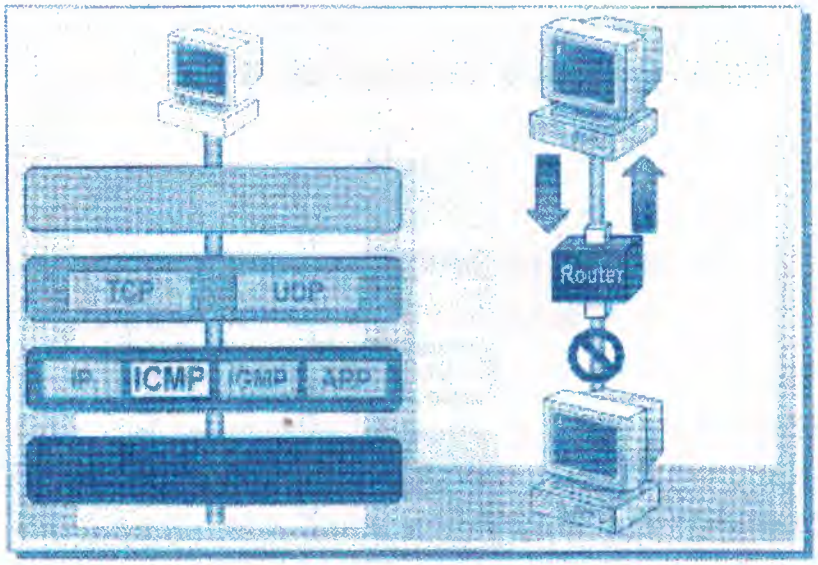

Figure 4.16 *Internet Control Message Protocol (ICMP)*

4.8.5 Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is a protocol that manages the membership lists for IP multicasting in a TCP/IP network. IP multicasting is a process by which a message is transmitted to a select group of recipients, known as a multicast

group. IGMP maintains the list of members who subscribe to each multicast group. (See Figure 4.17)

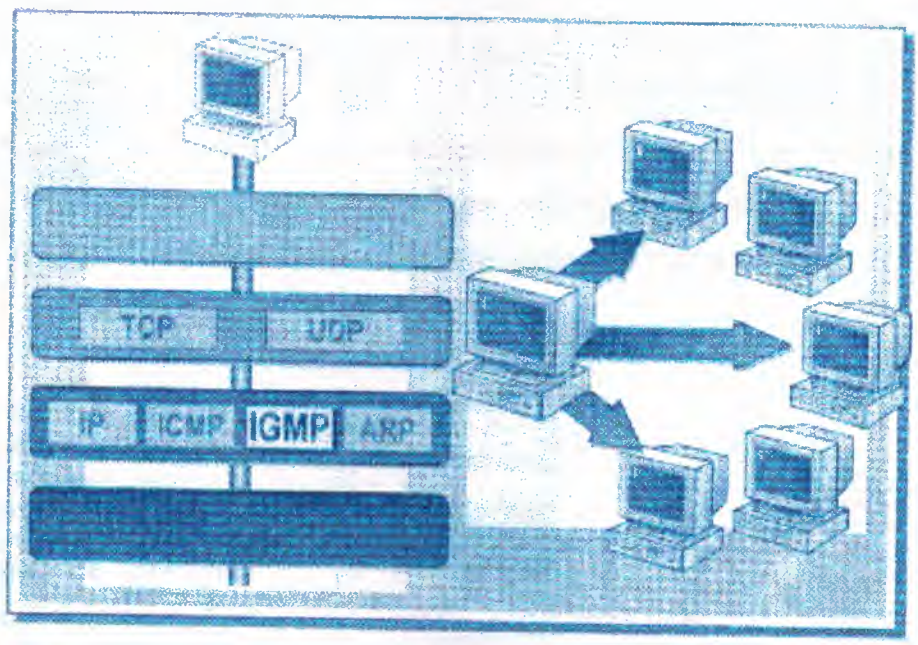

Figure 4.17 *Internet Group Management Protocol (IGMP)*

Managing IP Multicasting

All of the members of a multicast group listen for IP traffic directed to a specific multicast IP address and receive the packets sent to that IP address. However, because multicasting involves multiple computers, the packets are sent using the unreliable UDP protocol, which does not guarantee the delivery of the packets to the multicast group.

When multiple computers need to access information, such as streaming media, an IP address reserved for multicasting is used. Routers that are configured to process multicast IP addresses pick up this information and forward it to all subscribers of the multicast group associated with the multicast IP address.

For multicast information to reach its recipients, it is important that each router in the path of communication supports multicasting. Windows -based computers can both send and receive IP multicast traffic.

4.8.6 Address Resolution Protocol (ARP)

Located in the Internet layer of the TCPIIP suite, Address Resolution Protocol (ARP) performs address resolution for outgoing packets. Address resolution is the process by which IP addresses are mapped to MAC addresses. The network adapters use the MAC address to determine if a packet is meant for that computer.

Without the MAC address, the network adapters do not know if they are to pass the data to a higher layer for further processing. As the outgoing packets in the IP layer are being readied for transmission on the network, the source and destination MAC addresses must be added. (See Figure 4.18)

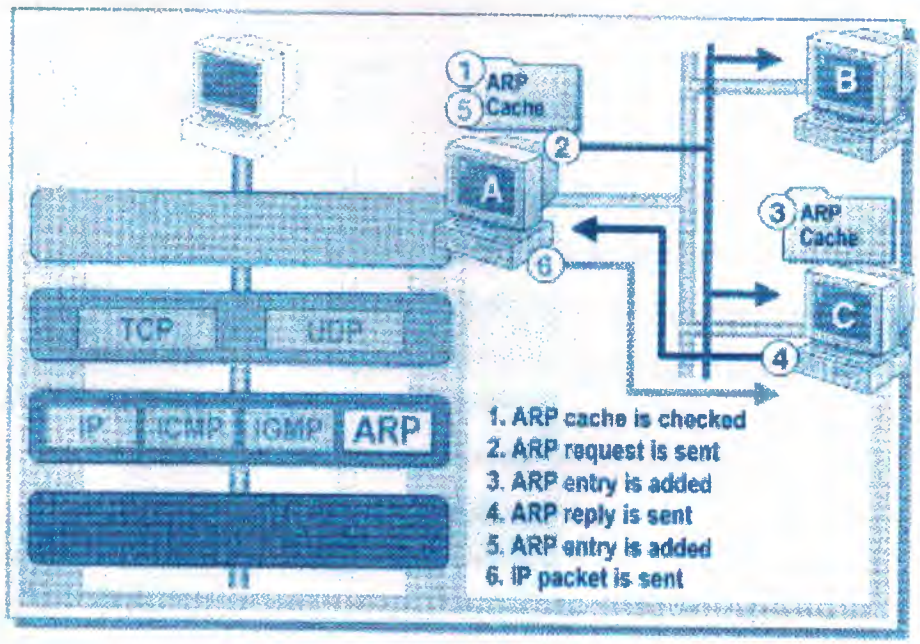

Figure 4.18 *Address Resolution Protocol (ARP)*

ARP Cache

ARP stores a table containing IP addresses and their corresponding MAC addresses. The area of memory where this table is stored is referred to as the ARP cache. The ARP cache for any computer contains the mappings for only computers and routers that reside on the same segment.

Physical Address Resolution

ARP compares every outbound packet's destination IP address with the ARP cache to determine the MAC address to which the packet will be sent. If there is a matching entry, the MAC address is retrieved from the cache. If not, ARP broadcasts a request for the computer owning the IP address in question to reply with its MAC address. Next, the computer with the corresponding IP address adds the initial computer's MAC address to its cache and then replies with its own MAC address. When an ARP reply is received, the ARP cache is updated with the new information and the packet can then be sent.

If the packet is going to another segment, ARP resolves the MAC address for the router responsible for that segment, rather than resolving the address for the final destination computer. The router is then responsible for either finding the MAC address of the destination or forwarding the packet to another router.

4.8.7 TCP/IP Utilities

The Microsoft TCP/IP suite provides basic TCP/IP utilities that enable a computer running Windows to access a wide variety of information on the network. Their capabilities range from determining if a specific computer on the network is accessible to downloading multimedia documents from the Internet. (See Figure 4.19)

Windows operating systems includes three types of TCP/IP-based utilities: diagnostic utilities, connectivity utilities, and server-based software.

Diagnostic Utilities

Diagnostic utilities allow users to detect and resolve networking problems.

Some of the common diagnostic utilities are:

- Arp: This utility displays and modifies the Address Resolution Protocol (ARP) cache.
- Hostname: This utility displays the host name of your computer.
- Ipconfig: This utility displays and updates the current TCP/IP configuration, including the IP address.

- Nbstat: This utility displays the local NetBIOS name table, which is a table of user-friendly computer names mapped to IP addresses.
- Netstat: This utility displays the TCP/IP protocol session information.
- Ping: This utility verifies configurations and tests IP connectivity between two computers. Ping sends an ICMP request from the source computer, and the destination computer responds with an ICMP reply.
- Tracert: This utility traces the route that a packet takes to a destination

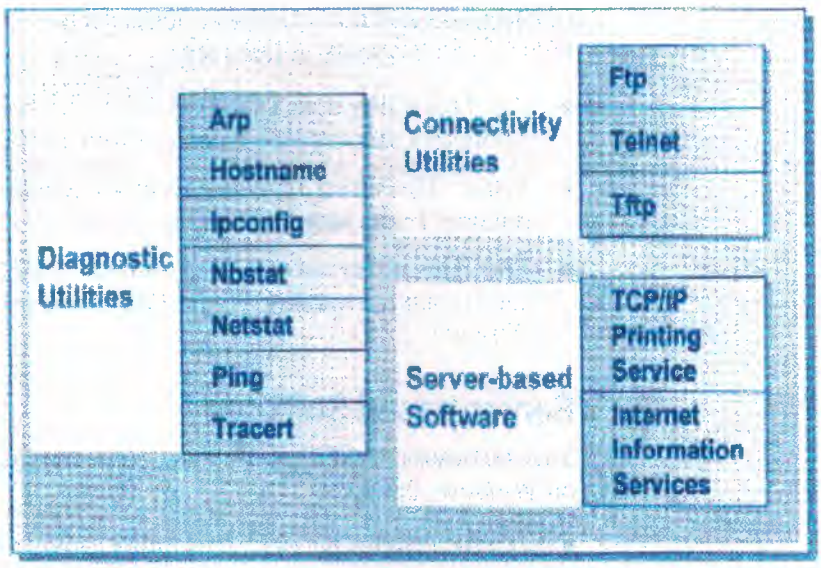

Figure 4.19 *TCP/IP Utilities*

Connectivity Utilities

Connectivity utilities allow users to interact with and use resources on a variety of Microsoft and non-Microsoft hosts, such as UNIX systems. Some of the common connectivity utilities are:

- Ftp: This utility uses TCP to transfer files between Windows and computers running File Transfer Protocol (FTP) server software.
- Telnet: This utility remotely accesses network resources on computers running Telnet server software.
- Tftp: This utility uses UDP to transfer small files between Windows and computers running Trivial File Transfer Protocol (TFTP) server software.

Server-based Software

This software provides printing and publishing services to TCP/IP-based clients on Windows operating system family.

- TCP/IP Printing service: This utility provides standard TCP/IP printing services. It allows computers running operating systems other than Windows to print to a printer attached to a Windows -based computer.
- Internet Information Services: Internet Information Services (IIS) offers Web, news, e-mail, and file transfer server software for TCP/IP-based publishing services.

Examples of Common Utilities

Hostname, Arp, and Ping are three common TCP/IP utilities. Because they are frequently used, it is recommended that you know how to access them.

Hostname

The syntax to use this utility is *hostname*. To access this utility, type **hostname** at the command prompt. The system displays the host name of your computer.

Arp

The syntax to access information from the ARP cache is Arp -a. Type **Arp –a** at the command prompt to display the information in your ARP cache.

Ping

The syntax to test connectivity is ping. To test connectivity by using an IP address or computer name, type **ping** *[IP _address or computer _name]*

To test the TCP/IP configuration of your own computer, you use *local loopback.* Local loopback is the IP address 127.0.0.1. To test system configuration by using local loopback, type **ping 127.0.0.1**

CONCLUSION

The primary reasons for networking computers are to share information, to share hardware and software, and to centralize administration and support. A local area network (LAN) is the smallest form of a network and is the building block for larger networks. A wide area network (WAN) is a collection of LANs and has no geographical limitation.

Networks are classified into two principal groups based on how they share information: peer-to-peer networks and server-based networks.

The physical layout of computers on a network is called a topology. There are four primary topologies: star, bus, ring, and mesh. Topologies can be physical (actual wiring) or logical (the way they work). Hubs are used to centralize the data traffic and localize failures. If one cable breaks, it will not shut down the entire network.

Three primary types of cables are used with networks: coaxial, twisted-pair, and fiber-optic. Coaxial cable comes in two varieties: thinnet and thicknet. Twisted-pair cable can be either shielded (STP) or unshielded (UTP). Fiber-optic cables use light to carry digital signals. Fiber-optic cables provide the greatest protection from noise and intrusion. IBM uses its own system of cabling and standards, but follows the same basic technology as other cables.

Managing data on a network is a form of traffic control. The set of rules that governs how network traffic is controlled is called the access method. There are four accessing methods: CSMA/CD, CSMA/CA, token-ring, demand-priority. Data on a network is not sent in one continuous stream. It is divided up into smaller, more manageable packets.

Protocols in a networking environment define the rules and procedures for transmitting data. To send data over a network successfully requires a series of separate steps that must be carried out in a prescribed order.

Several stacks are used as standard protocols; the most prominent standard protocols are based on the OSI reference model layers.

REFERENCES

[1] *MCSE Training kit Networking Essentials Plus*, third edition. Copyright© 1999 by Microsoft Corporation, Microsoft Press.

[2] R. Johnston., *Microsoft windows 2000 networking and operating system essentials*, Microsoft press, revised 11.15.1999

[3] "Intranet /Web Design Tutorials" *"http://www.comedition.com/Business/Intranets/intranettutorials.htm"* Revised: August 11, 2001 Copyright © 1996-2001 EDA, Inc... All rights reserved.

[4] N. Bader master of science degree in computer engineer/ London/England "Networking Books". *"http://www.nehadbader.com/books.html"*

[5] "Protocol Directory". *"http://www.protocols.com/protoc.shtml"*

[6] "CEN Training guide Netware 4.1 Administration" *"http://docs.rinet.ru:8080/NetWare/"*

[7] "Intranetworking Technology Overview". All contents are copyright © 1992--2001 Cisco Systems, Inc. All rights reserved. *"http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm"*

[8] "Client –server computing". *"http://hackersincorporated.org/complete-books/client-server-computing/"*

[9] "Tcp/ip illustrating". *"http://hackersincorporated.org/complete-books/Tcp-ip-illustrated/"*

[10] J. Helmig "World of windows networking". *"http://www.wown.com"*