NETWORKS

Design and Management

Second Edition

Steven T. Karris

Includes an Introduction to Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON)

Orchard Publications
www.orchardpublications.com

NETWORKS

Design and Management

Second Edition

Steven T. Karris

Orchard Publications
www.orchardpublications.com

NETWORKS Design and Management, Second Edition

Direct all inquiries to Orchard Publications, 39510 Paseo Padre Parkway, Fremont, California 94538

Library of Congress Cataloging-in-Publication Data

Library of Congress Control Number: 2009920253

Catalog record is available from the Library of Congress

ISBN 978-1-934404-16-4

Copyright: TX 5–612–942

Disclaimer

The author has made every effort to make this text as complete and accurate as possible, but no warranty is implied. The information on hardware and software described was obtained from their respective companies through the Internet. Accordingly, the information provided is on "as is" basis. The author and publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this text.

This book was created electronically using Adobe Framemaker®.

Preface

Networks are groups of computers that communicate by either cable or wireless transmissions. By the use of computer networking, we can share data with others. Today, all businesses, small or large use some type of computers and most use computer networking to handle their daily business operations such as bookkeeping, inventory tracking, document storing, and e-mail.

Networks are growing in size and complexity and this trend has created a rapid increase for networking engineers to provide practical and efficient solutions. Networking needs vary from one network to another; there is no such thing as "one size fits all." Also, a properly designed network must allow for expansion. The management of a small company may feel that this advanced technology is of no use to them since their monetary budget is limited. However, with proper planning, small companies can start with an affordable and versatile network and later expand on the next level of affordability.

This text is the second edition and presents updated networks material. The word "design" on the title of this book implies the purchasing and installation of the essential hardware and software that one must collect to assemble an effective computer network. Basically, it means the building of a network. The word "management" is used to denote the duties and responsibilities of a network administrator. Of course, one may argue that network management should include the Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON). While this is true, a detailed treatment of those two topics are beyond the scope of this book. Chapters 8 and 9 are introductions to those two topics. SNMP and RMON are discussed in books that are devoted just to these topics.

This book is primarily intended for those student and working professionals that have the desire to become network administrators. However, all practicing engineers will find it to be a very valuable source of information on this subject. It contains very interesting topics, and with the exception of a simple example on Chapter 1, the material requires no mathematical operations.

The author makes no claim to originality of content or of treatment, but has taken care to present concepts, definitions, and statements.

A few years ago, telephone networks and computer networks were considered two separate entities. Nowadays, these two technologies are rapidly merging into one. For this reason, Chapter 1 begins with a discussion of the basic components of telephone and computer networks, and their interaction. This chapter continues with the introduction of the centralized and distributive processing networks, and outlines the differences among these networks. It concludes with a discussion of Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs).

Chapter 2 begins with a discussion on protocols to establish their relevance to the International Standards Organization (OSI) Management Model. Protocols are covered in more detail on Chapter 3. This chapter introduces several network devices and identify those that operate at different layers of the OSI model. It concludes with a discussion of the IEEE 802 Standards.

Chapter 3 introduces several protocols including X.25, TCP/IP, IPX/SPX, NetBEUI, AppleTalk, and DNA. In this chapter, we learn how these protocols combine to form a suite of protocols that work at the various layers of the OSI model.

Chapter 4 presents the various physical network connections. It begins with the different physical topologies, bus, star, ring, and mesh. Then, it introduces the network types including the ARCNet, Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). A discussion of the wiring types and methods used in each of these network types is also included.

Chapter 5 begins with a discussion of the different buses, past and present. Network adapters are discussed next. The chapter concludes with the introduction of the different components that work together to provide source-to-destination data transmissions between devices on the same network or different networks. Discussions on Bluetooth and Wi-Fi are also included.

Chapter 6 focuses on wired and wireless transmissions. No previous knowledge of data communications is required for understanding the topics of this chapter.

Chapter 7 is devoted to discussions on the various types of networks that we can use for our needs, the hardware and software required, and tasks that a network administrator must perform to maintain the network(s) he is responsible for. These tasks include security and safeguarding data from internal and external disasters.

Chapters 8 and 9 are introductions to SNMP and RMON respectively.

This text contains five appendices, A through E. Appendix A is a brief introduction to network analysis as defined in operations research which is a branch of mathematics concerned with financial and engineering economic problems. A simple and yet practical example is included. Appendix B contains a review of the binary information representation, and the standard codes used for information processing systems, communications systems, and associated equipment. It provides the basic concepts to illustrate how networking devices work and communicate with others. Appendix C is a review of the decimal, binary, octal, and hexadecimal numbers, their representation, and conversion from one base to another. The conversion procedures are illustrated with several examples. Appendix D is an introduction to RSA Encryption. Finally, Appendix E is a glossary of terms and acronyms that are used in networks and on the Internet.

Like any other new book, this text may not be completely error-free; accordingly, all feedback for errors and comments will be most welcomed and greatly appreciated. Please write us at Orchard Publications www.orchardpublications.com, e-mail info@orchardpublications.com.

Table of Contents

Chapter 1

Basic Networking Concepts

This chapter begins with a discussion of the basic components of telephone and computer networks, and their interaction. It introduces the centralized and distributive processing networks, and outlines the differences among these networks. It concludes with a discussion of Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs).

1.1 Network

A *network* can be classified either as a telephone network or computer network although this distinction is rapidly disappearing. First, we will introduce the telephone network as a separate entity, we will briefly discuss information theory, then we will describe the computer network, and finally the combined telephone and computer network.

1.1.1 Telephone Network

A *telephone network*, more commonly known as a *telecommunications network*, is a group of telephones and associated devices, such as answering machines and faxes, that are connected by communications facilities. A telephone network can involve permanent connections, such as telephone wires and trunks,* cables, or temporary connections made through telephones or other communication links. A typical local telephone network is shown in Figure 1.1.

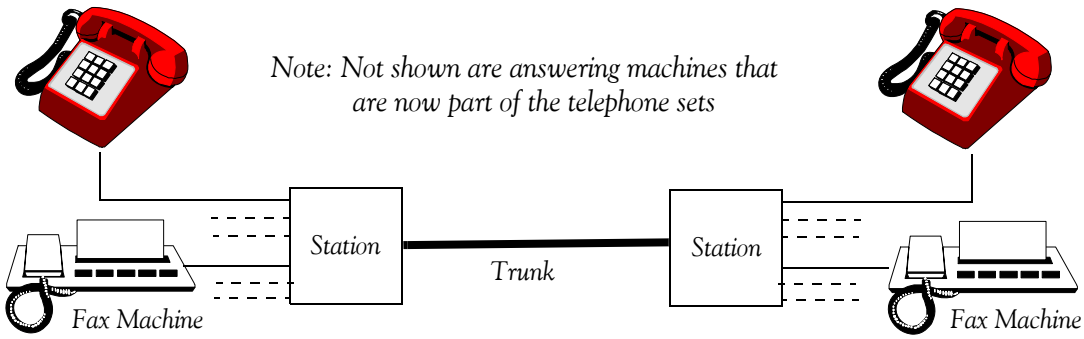


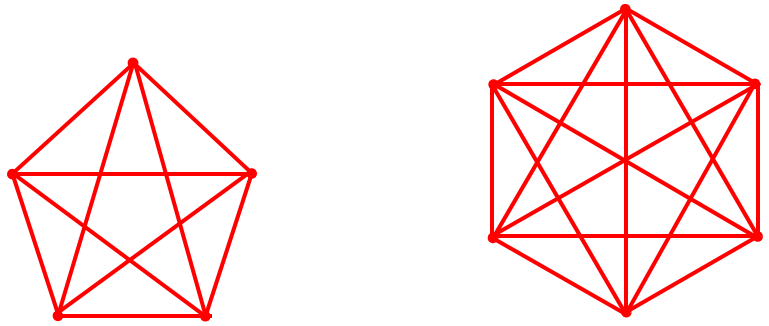
Figure 1.1. A typical local telephone network

* *In communications, a trunk is a channel connecting two switching stations. A trunk usually carries a large number of calls at the same time.*

Connecting several telephones directly would require a large number of direct lines. Figure 1.2 shows two examples of direct intercommunication of telephones. As we can see in Figure 1.2 (a), 10 lines would be required for the direct connection of 5 telephones lines. Figure 1.2 (b) shows that for 6 telephones we would require 15 direct lines. In general, for *n* lines we would require

$$\frac{n(n-1)}{2}$$

direct lines.



(a) 5 telephones – 10 lines *(b) 6 telephones – 15 lines*

Figure 1.2. Direct interconnection of telephones

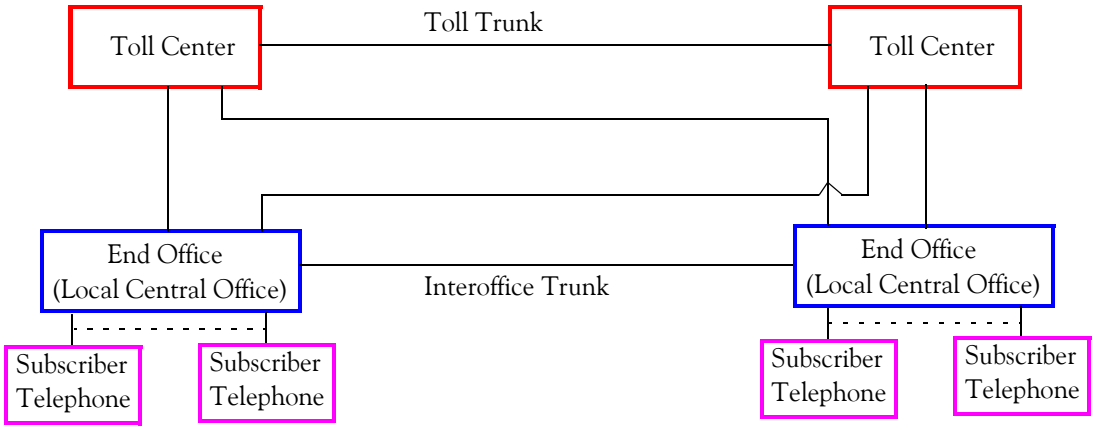
Although this arrangement assures us that there will be no blocking of calls, the number of wires becomes unrealistic as the number of telephones increases. For example, a community with 30,000 telephones would require

$$\frac{30,000 \times (30000-1)}{2} = 449985000$$

direct lines!

To make the telephone system more realistic, switching networks have been devised, and the design of a switching system assumes that not all telephones will be in operation at any particular time. Of course, in peak demand periods such as Mother's day and Christmas, switching facilities may become inadequate and some blocking may occur.

Figure 1.3 shows a two–level switched network. We observe that a call on this switching system could take one of several paths; for instance, it might be routed from one *End Office* directly to the other *End Office* via the *Interoffice trunk*, but if this trunk line is busy, it could go to the toll center which is the higher level office.



Trunk: A channel connecting two switching stations. A trunk usually carries a large number of calls at the same time.

Figure 1.3. Two–level switched network

In an actual telephone network, there are more toll centers. They are identified as *Class 1*, *Class 2*, ... , and *Class 5*. The hierarchy is shown in Figure 1.4.

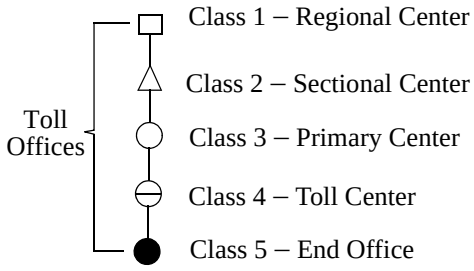


Figure 1.4. Switching center hierarchy

Figure 1.5 shows some of the many alternative routes indicated by the dotted lines.

In Figure 1.5, the actual path taken at any particular switching office is determined by the availability of the various trunks. The system should be designed so that the shortest possible route will be selected. Shown also in Figure 1.5 is a *Private Branch Exchange* (PBX). This is an automatic telephone switching system that enables users within an organization to place calls to each other without going through the public telephone network. PBX users can also place calls to outside numbers.

Each subscriber's telephone is connected to the End Office by a pair of wires enclosed by a sheath containing other wire pairs for other subscribers.

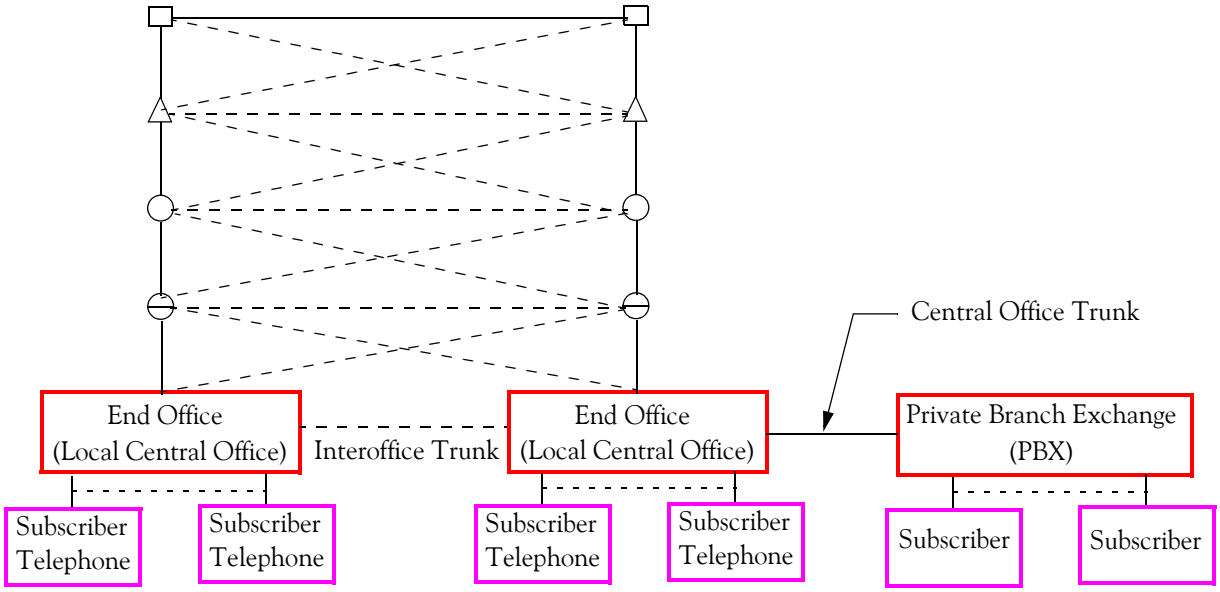


Figure 1.5. Typical routing plans available to a call made by a subscriber

In the United States, each End Office is identified by a three digit code *xyz* (for example 257) and can handle up to 10,000 telephones (0000–9999). Thus, each telephone within the End Office is identified by a 4–digit code. For long distance dialing, 3 more digits (area code) are added to identify the End Office. As an example, a long distance dial would be

1	415	257	0568
Station-to-Station	Area Code	End Office Identifier	Subscriber's Number

For international calls, the international access code 011 is dialed first; then a code assigned to a country is added. For example, an international call would be dialed as

011	49	30	2570568
International Code	Germany	Berlin	Subscriber

The telephone network is still considered to be an analog (continuous) network although in many areas have been converted to digital telephones lines.

Figure 1.6 shows how a world–wide telephone communications network is established with the use of satellites.

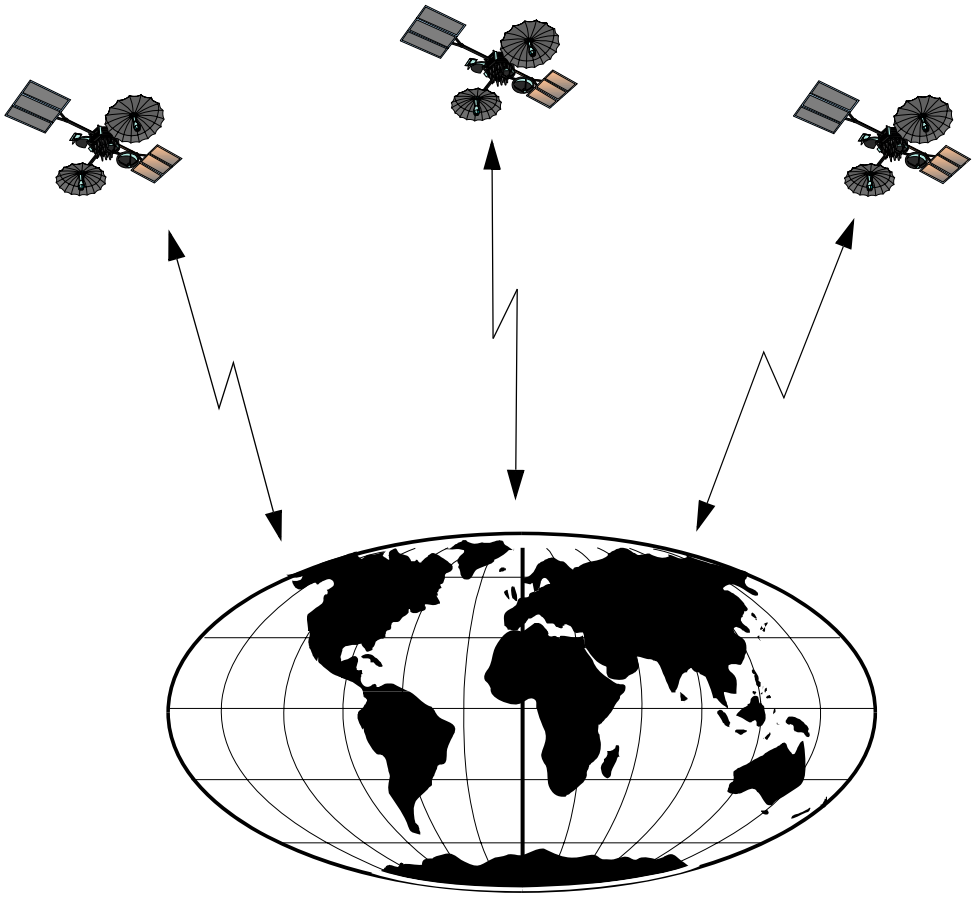


Figure 1.6. World Telecommunications Network

1.1.2 Information Theory

Information theory is concerned with the mathematical laws governing the transmission, reception, and processing of information. More specifically, information theory deals with the numerical measurement of information, the representation of information (such as encoding), and the capacity of communication systems to transmit, receive, and process information. Encoding can refer to the transformation of speech or images into electric or electromagnetic signals, or to the encoding of messages to ensure privacy.

Information theory was first developed in 1948 by the American electrical engineer Claude E. Shannon. The need for a theoretical basis for communication technology arose from the increasing complexity and crowding of communication channels such as telephone and teletype networks and radio communication systems. Information theory also encompasses all other forms of information transmission and storage, including television and the electrical pulses transmitted in computers and in magnetic and optical data recording.

When a message is transmitted through a channel, or medium, such as a wire or the atmosphere, it becomes susceptible to interference from many sources, which distorts and degrades the signals. Two of the major concerns of information theory are the reduction of noise–induced errors in communication systems and the efficient use of total channel capacity. Efficient transmission and storage of information require the reduction of the number of bits used for encoding. This is possible when processing English texts because letters are far from being completely random. The probability is extremely high, for example, that the letter following the sequence of letters *informatio* is an *n*. This redundancy enables a person to understand messages in which vowels are missing, for example, or to decipher unclear handwriting. In modern communications systems, artificial redundancy is added to the encoding of messages in order to reduce errors in message transmission.

Channel capacity is defined as the maximum rate at which information can be transmitted without error. Shannon's channel capacity theorem provides the following relationship for maximum channel capacity (bits per second) denoted as C, in terms of *bandwidth* W and *signal–to–noise ratio* S/N given by

$$\frac{C}{W} = \log_2\left(1 + \frac{S}{N}\right) \tag{1.1}$$

The S/N in *decibels* (dB) is related to S/N as a power ratio by

$$\left.\frac{S}{N}\right|_{(dB)} = 10\log_{10}\frac{S}{N} \tag{1.2}$$

Rather than working with the formulas of equations (1.1) and (1.2), it is much more convenient to plot the capacity–to–bandwidth ratio C/W versus the signal–to–noise ratio S/N in decibel (dB) units. This is easily done with the MATLAB® * script below. The generated plot is shown in Figure 1.7.

```
sndB=–20:1:30; p=0.5.*erfc(0.5.*sndB).^0.5;
cwb=2.*(1+p.*log2(p)+(1–p).*log2(1–p));
sn=10.^(0.1.*sndB); cwc=log2(1+sn);
plot(sndB,cwb,sndB,cwc);grid;xlabel('S/N in dB');ylabel('C/W in Bits/Second/Hertz')
```

* *MATLAB® (MATrix LABoratory) is a registered trademark of the MathWorks, Inc. It is a very powerful software application for performing scientific and engineering computations and generates very impressive plots. For more information, the interested reader may refer to URL www.mathworks.com. The inexpensive Student Version is available at many college bookstores. A practical introduction with numerous applications can be found on Numerical Analysis Using MATLAB® and Spreadsheets, ISBN 978–1–934404–03–4.*

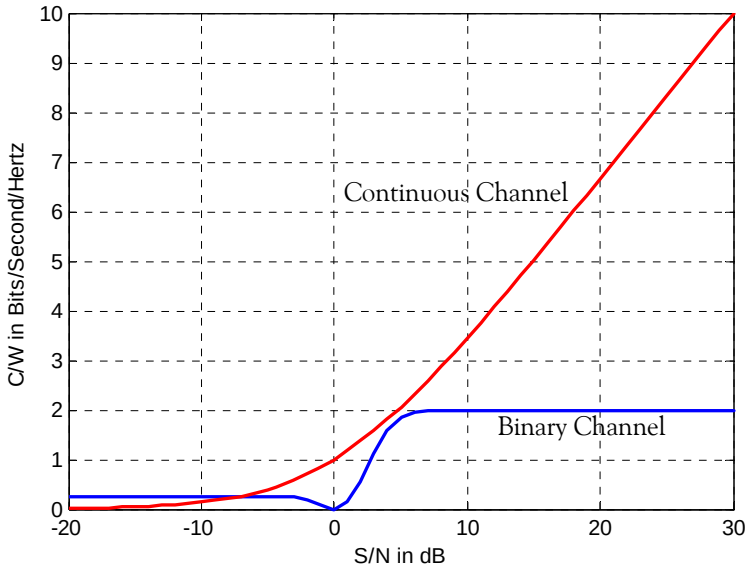


Figure 1.7. C/W versus S/N

We observe that above 5 dB, there is almost a linear relationship between C/W and S/N. The binary channel is discussed in advanced information theory textbooks.

To illustrate the use of the plot for the continuous channel, let us assume that a telephone system is designed to issue an alarm whenever the S/N decreases by 3 dB. Let us suppose that the bandwidth remains fixed at 3 Kbps and an alarm is issued. We want to find the decrease in capacity C assuming that under normal operating conditions, the C/W ratio is 9. Thus, with $W = 3\ \text{Kbps}$, the capacity is $C = 27\ \text{Kbps}$.

From Figure 1.7, we observe that with $C/W = 9$ this ratio corresponds to a S/N ratio of approximately 27 dB. Therefore, with a drop of 3 dB in S/N, the value decreases to 24 dB and this corresponds to a C/W ratio of 8. Since $W = 3\ \text{Kbps}$ still, the capacity is reduced to $C = 24\ \text{Kbps}$.

1.1.3 The Computer Network

A typical *computer station* is shown in Figure 1.8. The devices shown are, in most cases, manufactured by different vendors. Also, if we need to communicate with another computer station, we must connect one end of the modem to the telephone line, and the other end to the computer.

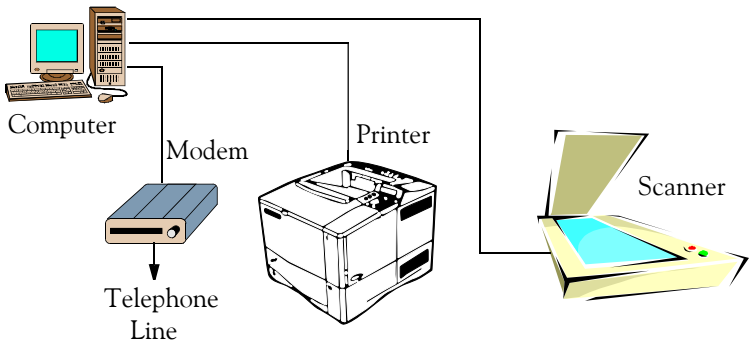


Figure 1.8. Typical computer station

Obviously, if we need to have an effective system that will provide us with world–wide telecommunications (telephone) services and data (computer) communications, we must interface the computer network with the telephone network as shown in Figure 1.9.

The services of the telecommunications network part shown in Figure 1.9 are provided by a telecommunications service provider such as AT&T, MCI, Sprint, British Telecom, etc. The Data Communications part provides communications among computers. As shown, modems transfer the information from digital to analog at the telephone terminals, and these are converted back to digital at the destination points.

Henceforth, a *network* will be understood to be a system of computers and peripherals interconnected by telephone wires or other means in order to share information. Its purpose is to process and store large amounts of information quickly and efficiently. A network is often used by both small companies and large corporations. The employees of a company assigned to a specific task in the network are referred to as *users*. While a user is normally assigned a specific task, a group of users must share resources other than files, such as printers, fax machines, and modems.

Figure 1.10 shows how several computers are interconnected to share a printer and a fax machine.

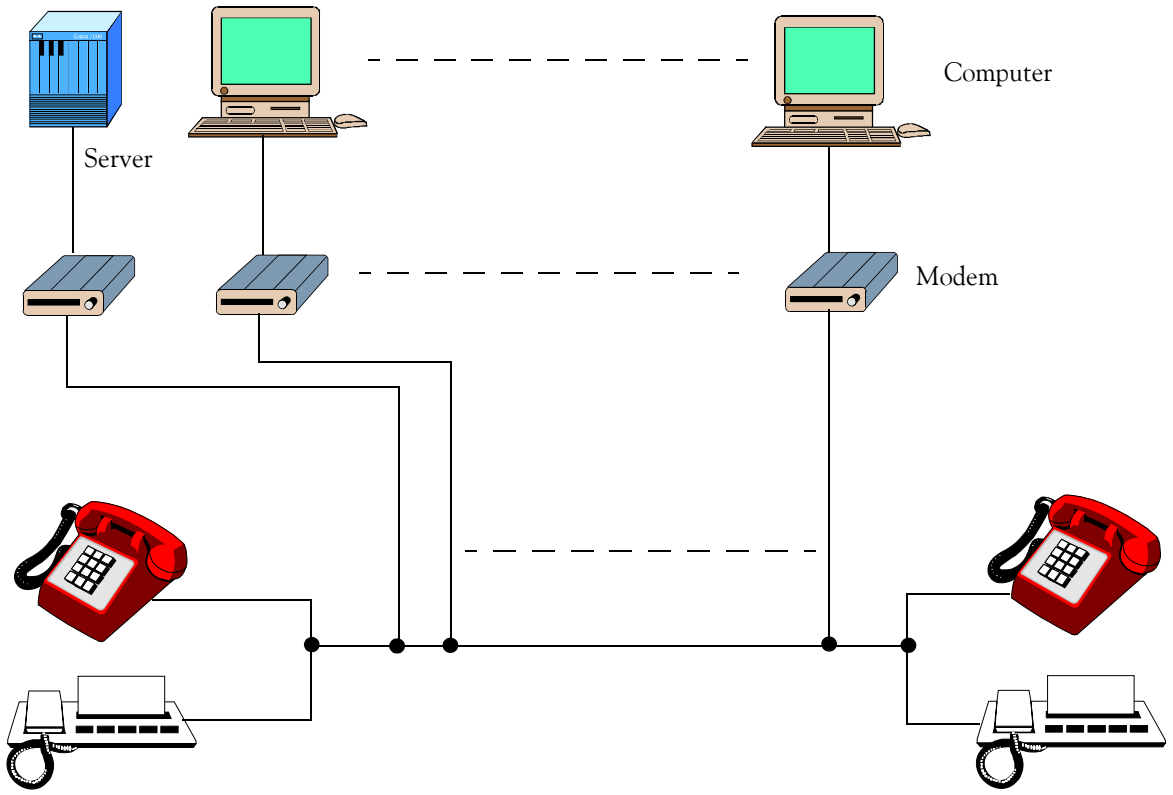


Figure 1.9. The telephone–computer network interface

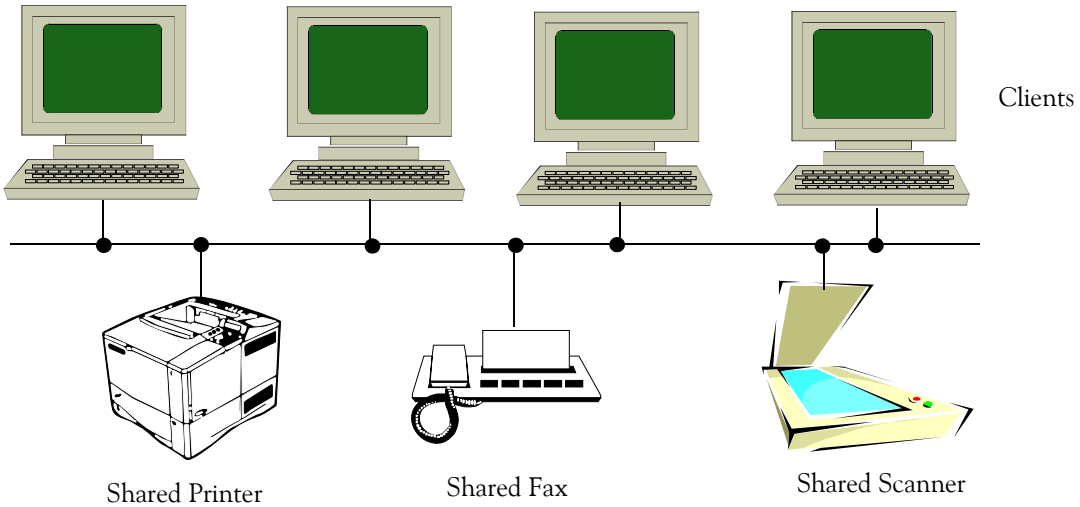


Figure 1.10. A network where several users share a printer, a fax machine, and a scanner

The person in charge of operations on a computer network is referred to as the *network administrator* or *system administrator*. The duties of a network administrator can be broad and might include such tasks as installing new *workstations*[*] and other devices, adding and removing authorized users, archiving files, overseeing password protection and other security measures, monitoring usage of shared resources, and handling malfunctioning equipment.

The network administrator must also consider fault tolerance. *Fault tolerance* is the ability of a computer or an operating system to respond to a catastrophic event or fault, such as a power outage or a hardware failure, in a way that ensures that no data is lost and any work in progress is not corrupted. This can be accomplished with a battery–backed power supply, backup hardware, provisions in the operating system, or any combination of these. In a fault–tolerant network, the system has the ability either to continue the system's operation without loss of data or to shut the system down and restart it, recovering all processing that was in progress when the fault occurred.

Tandem processors are multiple processors wired so that the failure of one processor transfers CPU operation to another processor. We use tandem processors for implementing fault–tolerant computer systems.

A typical large network consists of:

1. A *server*: A powerful computer that provides services to other computers on the network.
2. *Clients:* These are computers that use the services provided by the server.
3. *Peer:* A computer that can act as both a client and a server.
4. *Media*: The physical connection among the devices on a network.
5. *Protocols:* Written rules used for communications.
6. *Resources*: The devices that are available to a client. These are printers, fax machines, modems, etc.
7. *User:* A person using a client to access resources on the network.

1.2 Methods of Processing

In this section we will consider the *centralized* and *distributive* types of data processing.

1.2.1 Centralized Processing

With this type of networks, the location of computer processing facilities and operations in a single (centralized) place.

---

* *A powerful stand–alone computer of the sort used in computer–aided design and other applications requiring a high–end, usually expensive, machine with considerable calculating or graphics capability*

A typical example of a centralized network is the ATM banking system where all data are kept in one location, the server*, and all users have access to the same information regardless of their location.

1.2.2 Distributive Processing

With this type of networks, information is performed by separate computers linked through a communications network. Distributive processing is usually categorized as either true distributive processing or plain distributive processing.

True distributive processing has separate computers perform different tasks in such a way that each performs part of a task for the entire project. This latter type of processing requires a highly–structured environment that allows hardware and software to communicate, share resources, and exchange information freely. With this type of networks, all storage and processing is performed on a local workstation. It allows all users to share resources and services.

*Plain distributive processing*** shares the workload among computers that can communicate with one another. In other words, certain tasks are done by one computer and other tasks by others.

Table 1.1 lists the advantages and disadvantages of each of these types.

1.3 Network Architecture Types

This section discusses the *peer–to–peer network*, and the *server–based network*.

1.3.1 Peer–to–Peer Network Architecture

A *peer–to–peer network* is a network of two or more computers that use the same program or type of program to communicate and share data. Each computer, or peer, is considered equal in terms of responsibilities and each acts as a server to the others in the network. Users must share data and resources connected to the network. A typical peer–to–peer network architecture is shown in Figure 1.11.

A peer–to–peer network architecture would be appropriate for a group of people working in an office where each has a good networking knowledge, the users have full control over their data, and yet they can share their data with the other users in that office. Also, in a peer–to–peer network using Windows for Networking, accounts must be created on each client computer if different permissions are to be assigned for access to resources.

* *Another type of server is the proxy server. Proxy servers are used by many networks to do things such as monitoring the internet use by individual employees, or to block access to certain sites.*

** *Some books refer to this type of processing as collaborative or cooperative processing.*

TABLE 1.1 Advantages / Disadvantages of processing methods

Processing Method	Advantages	Disadvantages
Centralized	• Assurance that everyone obtains same information • Back up data in server only • Security required in server only • Low cost maintenance • Not very susceptible to viruses	• Slow in accessing server and processing data • Limited options
True Distributive	• Fast data access • Less expensive servers • Increased functionality • Low cost maintenance • Multiple uses • Users can be working on different versions of the same file	• More susceptible to viruses • Requires frequent backup of data to avoid the possibility that users will be working with different versions of the same file
Plain Distributive	• Fastest data access • Multiple uses	• More susceptible to viruses • Backup of data is more difficult since data can be stored in different systems of the network • Difficult file synchronization since several copies of the same file could be stored throughout the network.

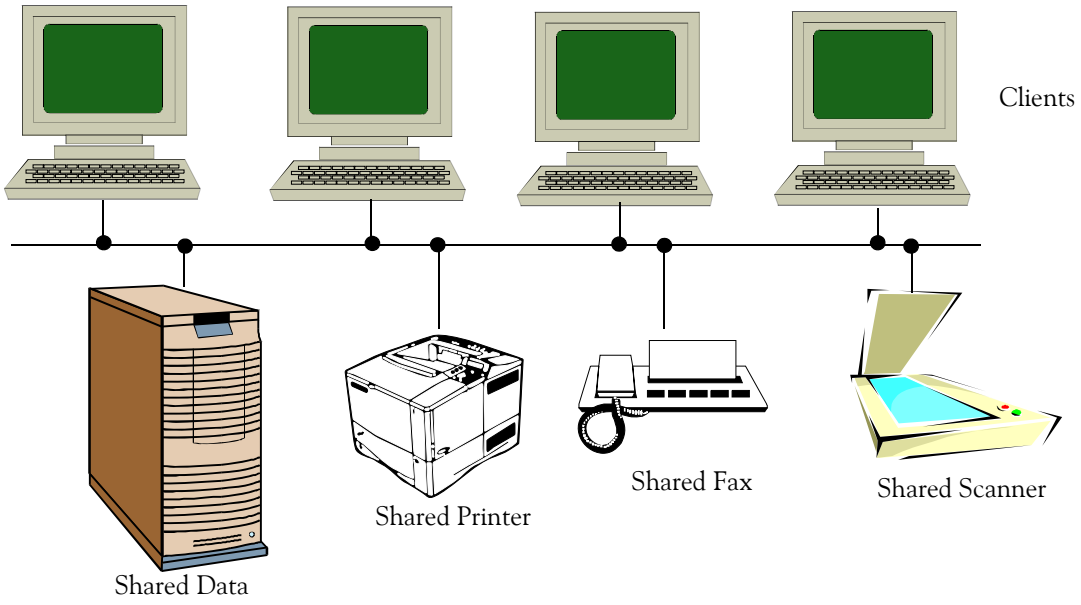


Figure 1.11. Typical peer–to–peer network architecture

1.3.2 Server–Based Network Architecture

Server–Based Network Architecture is an arrangement used on local area networks–to be defined on the next section–that makes use of distributed intelligence to treat both the server and the individual workstations as intelligent, programmable devices, thus exploiting the full computing power of each. This is done by splitting the processing of an application between two distinct components: a “front–end” client and a “back–end” server. The client component is a complete, stand–alone personal computer (not a "dumb" terminal), and it offers the user its full range of power and features for running applications.

The server component can be a personal computer, a minicomputer, or a mainframe that provides the traditional strengths offered by minicomputers and mainframes in a time–sharing environment: data management, information sharing between clients, and sophisticated network administration and security features. The client and server machines work together to accomplish the processing of the application being used. Not only does this increase the processing power available over older architectures, but it also uses that power more efficiently.

The client portion of the application is typically optimized for user interaction, whereas the server portion provides the centralized, multiuser functionality. The server controls the data and resources the clients need to access. Servers are optimized to pass on data as fast as possible. A typical server–based network architecture is shown in Figure 1.12.

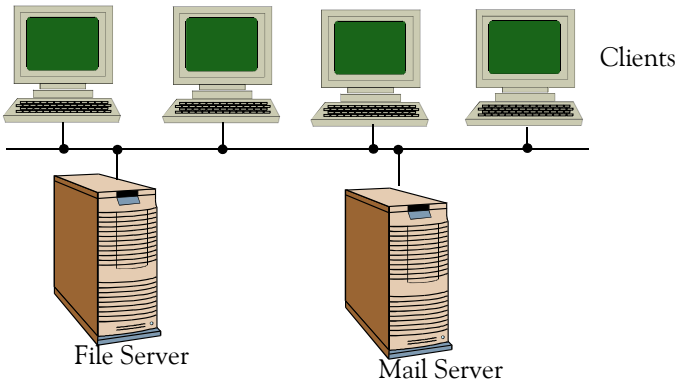


Figure 1.12. Typical server–based network architecture

Microsoft Windows includes the *Event Viewer* that enables the network administrator to view the number of logins and find out which users have logon on to the network. It also includes the *Server Manager* which can display the resources that are being used, and the for how long each user has been using them. Thus, if the network administrator wishes to know how many users are using the network at any one time, he should choose a server–based network. Windows has also built–in peer–to–peer capabilities.

Table 1.2 lists the advantages and disadvantages of each of these architectural types.

TABLE 1.2 Advantages / Disadvantages of networking architectures

Networking Architectures	Advantages	Disadvantages
Peer–to–Peer	• Less expensive • Easy to setup • Easy and low cost maintenance • Does not require a server operating system	• Requires that each user manages his/her own security • Users can easily become confused since there is no central data depository • Requires more user training • Limited to 10 or less clients
Server–based	• Since the server stores all data, large hard disk drives and extra RAM are not required on client computers. • Central security • Synchronized files • Easy backup • Easy expansion	• Requires a server • Must have an administrator • Requires a server operating system (Windows or Novell's NetWare).

1.4 Network Services

Networks provide several services. The most common are *file services*, *print services*, *message services*, *directory services*, and *application services*.

1.4.1 File Services

File services include the following tasks:

- *File transfer* – The process of moving or transmitting a file from one location to another, as between two programs or over a network. This is accomplished with the use of a a *file server* which is a file–storage device on a local area network that is accessible to all users on the network. Unlike a disk server, which appears to the user as a remote disk drive, a file server is a sophisticated device that not only stores files but manages them and maintains order as network users request files and make changes to them. To deal with the tasks of handling multiple— sometimes simultaneous— requests for files, a file server contains a processor and controlling software as well as a disk drive for storage. On local area networks, a file server is often a computer with a large hard disk that is dedicated only to the task of managing shared files.

  The most important component for a file server is the disk access speed. If the disk drive is slow, it doesn't matter how much memory we have, how fast the processor is, or how fast the network card is; the bottleneck will still be the disk drive. The only way to improve the speed would be to change the drive(s) to

faster ones or possibly add more disk controllers if we are using multiple drives. By using multiple controllers, we could potentially access two disks at the same time.

- *File storage* – The process of storing a file in different media such as floppy disks, hard disks, CD–R/Ws, and magnetic tape. *Online storage* implies that data is stored information that is readily available on a server. *Offline storage* implies that data is stored information in a resource, such as a disk, that is not currently available to the network. *Data migration* implies that data is transferred from one storage to another. *Archives* are places or collections containing records, documents, or other materials of interest. The process of backing up data in case of a hard disk failure is referred to as *archiving*.

1.4.2 Print Services

A *print server* is a workstation that is dedicated to managing the printers on a network. The print server can be any station on the network. A print spooler is software that intercepts a print job on its way to the printer and sends it to disk or memory instead, where the print job is held until the printer is ready for it. *Spooler* is an acronym created from *simultaneous print operations on line*.

Networks provide the ability to share *print services*. Thus, only a few printers can be connected to a network and can be shared among the users. Print services include also queue–based printing and fax services. Queue–based printing allows a client's application to spool the print job off to a network server so the application thinks the job has been printed and lets the user continue to work.

1.4.3 Message Services

Message services allow for e–mails with attachment files. Many people have come to rely on e–mail attachments as a way of transferring information, so message services have become a necessity on most networks. E–mail is no longer just sending text messages back and forth over a network. We can send video, sound, documents, and almost any other type of data.

Groupware* applications that use e–mail as their connection backbone are also becoming popular. These enable users to share calendars and scheduling information as well.

1.4.4 Directory Services

A *directory service* on a network is a service that returns mail addresses of other users or enables a user to locate hosts and services. Directory services let us maintain information about all of the *objects* in our network. An object is anything we can store information about, such as users, print-

* *Software intended to enable a group of users on a network to collaborate on a particular project. Groupware may provide services for communication (such as e–mail), collaborative document development, scheduling, and tracking. Documents may include text, images, or other forms of information.*

ers, shared resources, servers, and so on. Before directory services were popular, we had to keep separate configuration information about users on each file server. If a user wanted to connect to resources on multiple servers, they needed an account on each one. With directory services, we only create one user account object for that user. Each of the servers see that object, and we can then assign resource rights to that user account. The actual directory information is stored in files on the server, which are usually hidden. The network operating systems that support directory services have predefined methods to share and update this information.

1.4.5 Application Services

Application services are basically a client/server process. The server is providing the application service. Normally with application services, a small application is loaded on the client computers, and the main application and data is loaded on the server. The small application on the client is usually just a front–end to give the user an interface. It does no processing of its own. The client application sends queries to the server and lets it do the processing. The server then returns the requested information. A typical travel agent uses application services. He/she loads a small front–end application on his/her terminal to query the main database server that includes information on airlines and flight information. The database server looks up the flight number, itinerary, and price, and returns the information about it. No processing is done on the travel agent's terminal.

1.4.6 Database Services

One major consideration of a networked database is the coordination of multiple changes. All or part of the databases may also be replicated to other servers on a network to distribute the load. It can be more efficient to have portions of the database in the same regional location as the users who access it. When using distributed data, the database appears to be a single database to the users. Replicating the database to other servers can also serve as a form of backup. The database is not dependent on one particular server. Database services are responsible for updating replicated databases and keeping them current. A *database server* is a network station, dedicated to storing and providing access to a shared database.

1.5 LANs, MANs, and WANs

The sizes of networks are categorized into three groups: Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN).

1.5.1 Local Area Networks

The smallest network size is a *local area networ*k, or LAN. LANs are normally contained in a building or small group of buildings. Some characteristics of a LAN are high speed, small error counts, and inexpensive price. Figure 1.13 shows computers set up on a LAN.

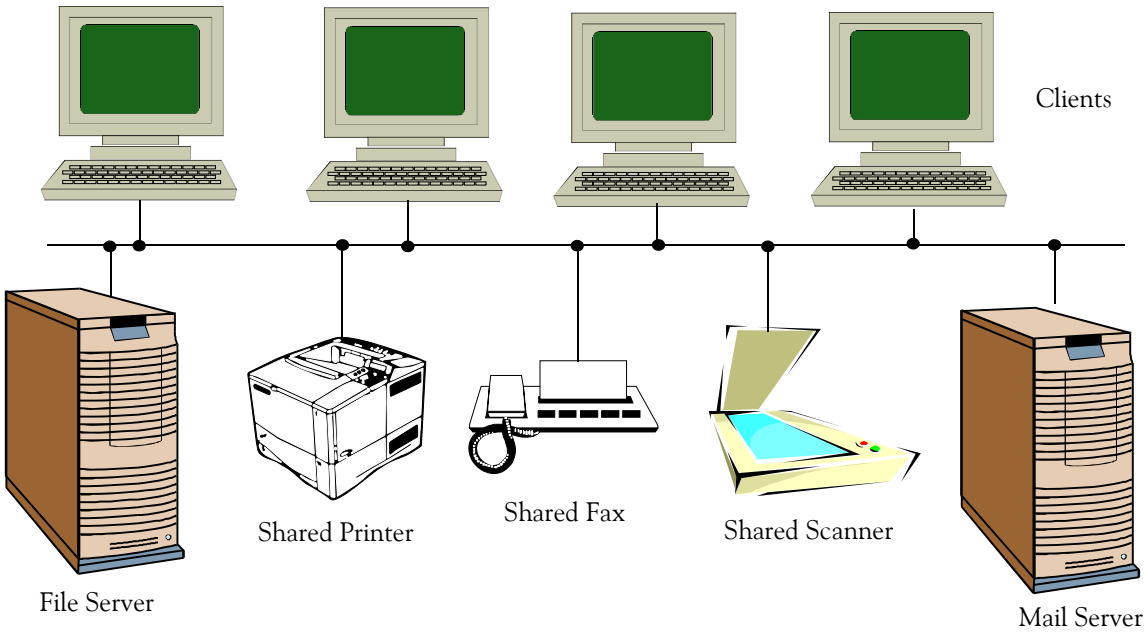


Figure 1.13. Typical LAN

Since LANs are contained in small areas, high–speed cable can be used. Also, since the installed media is usually high quality, few to no errors are generated on the network. Prices of LAN equipment are fairly cheap. Network adapters–to be discussed in a later chapter–used in LANs can be found for less than $15 each.

1.5.2 Metropolitan Area Networks

A *Metropolitan Area Network* (MAN) is a high–speed network that can carry voice, data, and images at up to 200 Mbps over distances of up to 75 km. A MAN, which can include one or more LANs as well as telecommunications equipment such as microwave and satellite relay stations, is smaller than a Wide Area Network (WAN) but generally operates at a higher speed. Figure 1.14 illustrates how several LANs can be set up as a MAN. Typical MANs are computer networks in city halls, university campuses, etc.

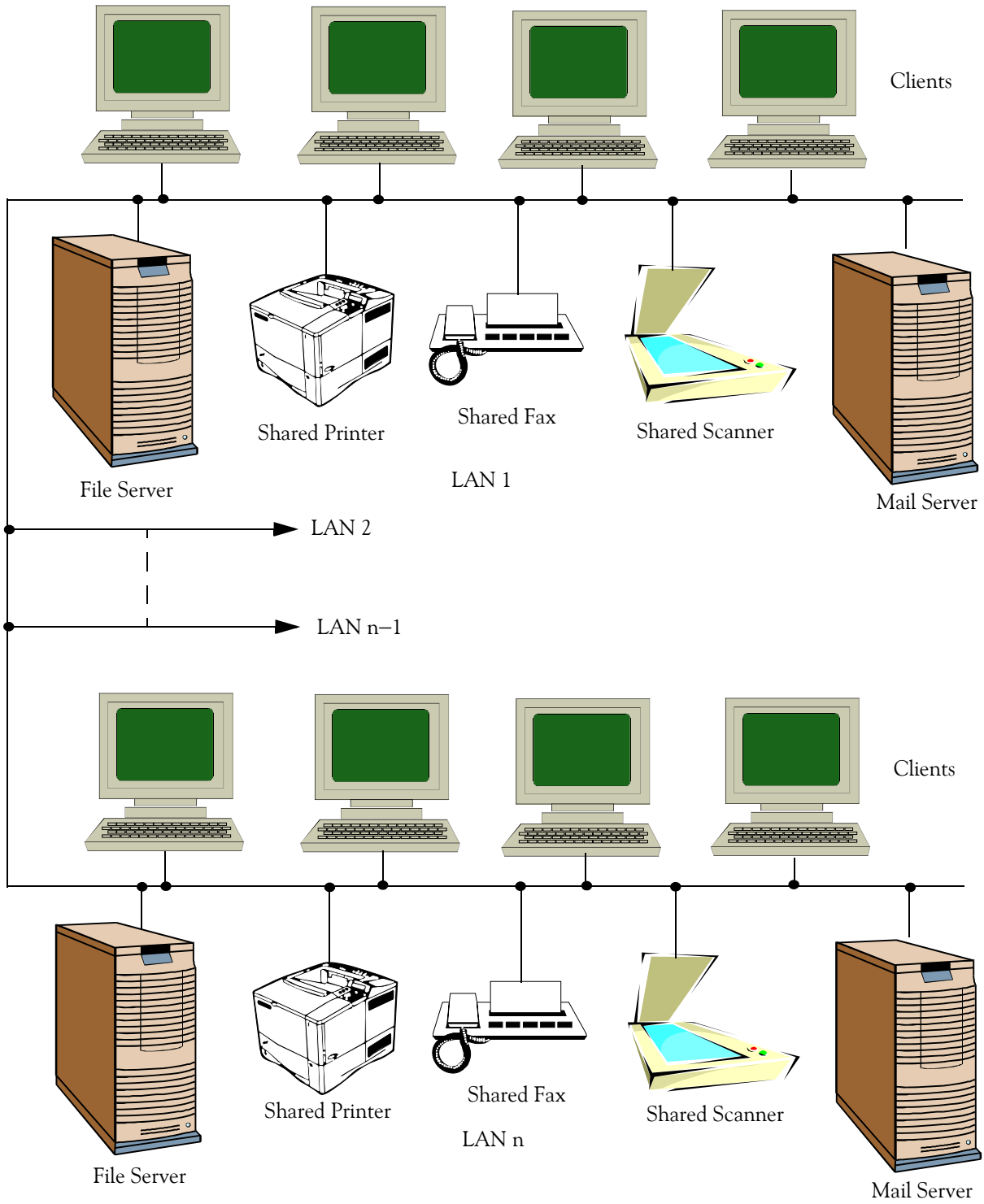


Figure 1.14. Typical MAN

1.5.3 Wide Area Networks

A *Wide Area Network* (WAN) is a communications network that connects geographically separated areas. WANs are interconnections of any number of LANs and MANs. They can connect networks across cities, states, and countries. The internet can be thought of as the largest WAN.

Table 1.3 lists the advantages and disadvantages of LANs, MANs and WANs.

TABLE 1.3 Advantages / Disadvantages of LANs, MANs, and WANs

Network Size	Advantages	Disadvantages
Local Area Network (LAN)	• Fast data access • Small space requirements • Less expensive equipment • Low error rates • Less investment for hardware and software	• Limited options
Metropolitan Area Network (MAN)	• Accommodates a large number of clients • Moderate error rates	• Large space requirements • Slower data access • More expensive equipment
Wide Area Network (WAN)	• Can grow without bounds • Multiple uses	• Large space requirements at different locations • Slower data access • Very expensive equipment • Highest error rates

1.6 Summary

In this chapter we discussed the basic components of a network and the types of resources networks can share. We learned the three methods of data processing: centralized, true distributed, and plain distributed. We explained the difference between peer–to–peer and server–based network architectures. We defined file services, print services, message services, directory services, application services, and database services. We concluded the chapter with the definitions and characteristics of LANs, MANs, and WANs. A review of concepts and definitions follows.

- A telecommunications network or telephone network, is a group of telephones and associated devices such as answering machines and faxes that are connected by communications facilities. A telephone network can involve permanent connections, such as telephone wires and trunks, cables, or temporary connection made through telephone or other communication links.
- Computer Networks are groups of computers connected together by some type of media (the physical connection among the devices on a network) to allow them to communicate and share information.
- Servers are large, powerful computers that provide services to clients.
- Clients are smaller desktop computers that users use to access network services.
- Peer computers act as both clients and servers.
- The physical connection between the computers on a network is referred to as the media.
- Resources are devices and equipment that clients can have access to. Printers, scanners, and hard disks are examples of resources.
- Users are humans that use clients and resources.
- Protocols are the written rules for communication between devices on a network.
- Centralized processing is done with a large central system with terminals as clients. All processing is done by a central computer, and the terminals are for input and output.
- Distributive Processing is a form of information processing in which work is performed by separate computers linked through a communications network. Distributed processing is usually categorized as either plain distributed processing or true distributed processing. Plain distributed processing shares the workload among computers that can communicate with one another. True distributed processing has separate computers perform different tasks in such a way that their combined work can contribute to a larger goal. This latter type of processing requires a highly–structured environment that allows hardware and software to communicate, share resources, and exchange information freely.

Summary

- Peer–to–peer architectural network is a network of two or more computers that use the same program or type of program to communicate and share data. Each computer, or peer, is considered equal in terms of responsibilities and each acts as a server to the others in the network. Unlike a client–server architecture, a dedicated file server is not required. However, network performance is generally not as good as under client–server, especially under heavy loads.
- Client/Server architectural network is an arrangement used on local area networks that makes use of distributed intelligence to treat both the server and the individual workstations as intelligent, programmable devices, thus exploiting the full computing power of each. This is done by splitting the processing of an application between two distinct components: a "front–end" client and a "back–end" server. The client component is a complete, stand–alone personal computer (not a "dumb" terminal), and it offers the user its full range of power and features for running applications. The server component can be a personal computer, a minicomputer, or a mainframe that provides the traditional strengths offered by minicomputers and mainframes in a time–sharing environment: data management, information sharing between clients, and sophisticated network administration and security features. The client and server machines work together to accomplish the processing of the application being used.
- Fault tolerance is the ability of a computer or an operating system to respond to a catastrophic event or fault, such as a power outage or a hardware failure, in a way that ensures that no data is lost and any work in progress is not corrupted.
- Tandem processors are multiple processors wired so that the failure of one processor transfers CPU operation to another processor. We can use tandem processors to implement fault–tolerant computer systems.
- File servers are file–storage devices on local area networks that is accessible to all users on the network. Unlike a disk server, which appears to the user as a remote disk drive, a file server is a sophisticated device that not only stores files but manages them and maintains order as network users request files and make changes to them. To deal with the tasks of handling multiple— sometimes simultaneous— requests for files, a file server contains a processor and controlling software as well as a disk drive for storage.
- Print servers are workstations that are dedicated to managing the printers on a network. The print server can be any station on the network. A print spooler is a computer software application that intercepts a print job on its way to the printer and sends it to disk or memory instead, where the print job is held until the printer is ready for it.
- Message services provide mail services such as e–mail.
- A directory is a listing of the files contained in a storage device, such as a magnetic disk. It contains a description of the various characteristics of a file, such as the layout of the fields in it. Directory services allow us to maintain information about every object in our network.

- Applications are programs designed to assist in the performance of a specific task, such as word processing, accounting, or inventory management. Clients can let the central network servers process data for them by using application services.
- A database is a file composed of records, each of which contains fields, together with a set of operations for searching, sorting, recombining, and other functions. Database services coordinate multiple changes to large network databases and replicate them if necessary.
- Local Area Networks (LANs) are small networks usually contained in one office or building. They have high speed, low error rates, and they are inexpensive.
- Metropolitan Area Networks (MANs) are larger networks that consist of individual LANs to interconnect large campus–type environments such as organizations spread over a city. Their characteristics fall in between LANs and WANs, in that they are relatively fast, have moderate error rates, and their equipment prices fall between LANs and WANs.
- Wide area networks can cover an entire organization's enterprise network. WANs can cover a few states or, in the case of the Internet, the entire globe. Since this is the largest network, it is the most expensive. It is also usually low speed when compared with the other network size models.

1.7 Exercises

True/False

1. A fax machine can be a telephone network or a computer network component. _____
2. Computers in a peer–to–peer network act as a client and a server. _____
3. Peer–to–peer network requires that each user manages his/her own security. _____
4. Directory services allow users to share word–processor documents. _____
5. The most powerful computer in a network is the server. _____
6. The rules that govern the communication between devices on a network are established by databases. _____
7. Clients are computers that use resources on the network._____
8. Plain Distributive Processing architecture employs a large central computer. _____
9. The True Distributive Processing architecture has clients that can process information for themselves. _____
10. Plain Distributive Processing architecture would be the appropriate choice for a network with a large number of client computers that are looking for new prime numbers._____
11. Terminals are used in Centralized Processing architecture _____
12. In an office building with thirty two client computers, a peer–to–peer architectural network would be a good choice. _____
13. A newly formed company is undecided on the architectural network to use. A server–based network would be a safe choice. _____
14. Microsoft Windows with networking capabilities would be appropriate for a peer–to–peer architectural network. _____
15. File services allow users to only log in to the network once, and access any server or resource on it. _____
16. Clients do most of the processing in a server–based network with a file server. _____
17. Users need more training in a server–based network. _____
18. Companies can realize a significant savings by installing networks to allow users to share hardware and software. _____
19. WANs require specialized, expensive equipment to connect LANs. _____
20. One of the most basic file services used on the network is the e–mail. _____

Multiple Choice

21. ABC company requires that all employees use a badge to enter the building. Which processing method does this computer network follow?

    A. Server–based
    B. Centralized
    C. Plain Distributed
    D. True Distributed

22. The main advantage of peer–to–peer architectural networks is:

    A. Ease of backup

    B. Data spread across the network

    C. Easy setup

    D. Utilization of powerful servers

23. In a fault–tolerant network, the system has the ability to

    A. continue the system's operation without loss of data

    B. shut the system down and restart it

    C. recovering all processing that was in progress when the fault occurred

    D. All of the above

24. One of the functions that filing services perform is

    A. Archiving

    B. Print spooler management

    C. E–mail

    D. All of the above

25. One of the functions that message services perform is

    A. E–mail

    B. Sound

    C. Video

    D. All of the above

Problems

26. The office of a small independent realty company has four real estate agents, an executive secretary, and two assistant secretaries. They agreed to keep all common documents in a central location to which everyone has access. They also need a place to store their individual listings so that only the agent who has the listing should have access to. The executive secretary has considerable network administration knowledge, but everyone else does not. It is expected that in the near future the office will employ ten more agents and three assistant secretaries. Would you recommend implementation of peer–to–peer or server–based architectural networking?

27. The administrator in charge of all computer users in a small office has decided on the implementation of a peer–to–peer network architecture and desires to allow access to some files on her computer station. The administrator has created user accounts for everyone else. Using Microsoft Windows for Networking, the administrator assigned the appropriate permissions for these accounts. With this arrangement, will each user have access to all files?

1.8 Answers to End–of–Chapter Exercises

Dear Reader:

The next two pages contain answers / solutions to the exercises of the previous pages.

You must, however, make an honest effort to answer the questions. It is recommended that you go through and answer those you feel that you know. For those questions that you are uncertain, review this chapter and try again. When you think that you have found the right answers, you may compare them with the answers provided. It is also recommended that you review these at a later date.

You should follow this practice with the exercises of all chapters in this book.

True/False

1. T – Review Figure 1–1, Page 1–1, and Figure 1–9, Page 1–9
2. T – Review Page 1–11
3. T – Review Table 1.2, Page 1–14
4. F – Review Pages 1–14, 1–15, and 1–16
5. T – Review Page 1–13
6. F – Review Page 1–10
7. T – Review Page 1–10
8. F – Review Page 1–11
9. T – Review Page 1–11
10. T – Review Page 1–11
11. T – Review Page 1–10
12. F – Review Table 1.2, Page 1–14
13. T – Review Table 1.2, Page 1–14
14. T – Review Page 1–13
15. F – Review Pages 1–15, 1–16
16. T – Review Page 1–14
17. F – Review Table 1.2, Page 1–14
18. T – Review Table 1.3, Page 1–19
19. T – Review Table 1.3, Page 1–19
20. F – Review Pages 1–14, 1–15, and 1–16

Multiple Choice

21. B – Review Page 1–10
22. C – Review Table 1.2, Page 1–14
23. D – Review Page 1–10
24. A – Review Page 1–15
25. D – Review Page 1–15

Problems

26. Use server–based networking architecture and setup permissions on the server to allow for the individual case needs.

27. This is a peer–to–peer network; accordingly, no central user account database exists. Therefore, for the administrator to allow each of the users in the office access to resources on his/hers computer with the correct permissions, he/she had to create accounts on his/her computer for each of them. After their accounts were created, he/she could then assign permissions to each of those accounts. If she had not created individual accounts, his/her only other option would have been to assign permissions to the "everyone" group. In that case, everyone would end up with the same permissions for each resource.

Chapter 2

The OSI Model and IEEE 802 Standards

This chapter begins with a discussion on protocols to establish their relevance to the International Standards Organization (OSI) Management Model. It introduces several network devices and identify those that operate at different layers of the OSI model. The characteristics of these devices are discussed in Chapter 5. This chapter concludes with a description of the major IEEE 802 Standards.

2.1 Terminology

Protocol: A set of rules or standards designed to enable computers to connect with one another and to exchange information with as little error as possible. Some protocols used in earlier days are listed below. Present day protocols are discussed in detail in Chapter 3.

Xmodem: A file–transfer protocol used in asynchronous communications * that transfers information in blocks of 128 bytes. It was developed in 1977, and the basic block size of 128 bytes was used on the CP/M operating system floppy disks.

Ymodem: A variation of the Xmodem file–transfer between modems protocol that included the following enhancements: the ability to transfer information in 1 kilobyte (1024 byte) blocks; the ability to send multiple files (batch–file transmission); cyclical redundancy checking (CRC); and the ability to abort transfer by transmitting two CAN (cancel) characters in a row.

Zmodem: An enhancement of the Xmodem file–transfer protocol that handles larger data transfers with less error. Zmodem includes a feature called checkpoint restart, which resumes transmission at the point of interruption, rather than at the beginning, if the communications link is broken during data transfer.

Kermit: A file transfer and management protocol and a set of communications software tools primarily used in the early years of personal computing in the 1980s. It provides a consistent approach to file transfer, terminal emulation, script programming, and character set conversion. It allows for transferring text and binary files on both full–duplex and half–duplex 8 bit and 7–bit serial connections in a system– and medium–independent fashion, and is implemented on hundreds of different computer and operating system platforms.

---

* ***Asynchronous communication*** *is transmission of data without the use of an external clock signal. Please refer also to Subsection 2.5.2, this chapter.*

XON/XOFF: An asynchronous communications protocol in which the receiving device or computer uses special characters to control the flow of data from the transmitting device or computer. When the receiving computer cannot continue to receive data, it transmits an XOFF control character that tells the sender to stop transmitting; when transmission can resume, the computer signals the sender with an XON character.

Handshaking: A series of signals acknowledging that communication or the transfer of information can take place between computers or other devices. A hardware handshake is an exchange of signals over specific wires (other than the data wires) in which each device indicates its readiness to send or receive data. A software handshake consists of signals transmitted over the same wires used to transfer data, as in modem–to–modem communications over telephone lines.

2.2 Protocols for Data Transmission

A protocol is standard procedure for regulating data transmission between computers. The protocol generally accepted for standardizing overall computer communications is a seven–layer set of hardware and software guidelines known as the OSI (Open Systems Interconnection) model. A somewhat different standard, widely used before the OSI model was developed, is IBM's SNA (Systems Network Architecture).*

The word protocol is often used, sometimes confusingly, in reference to a multitude of standards affecting different aspects of communication, such as file transfer (e.g., Xmodem, Zmodem), handshaking (e.g., XON/XOFF), and network transmissions (e.g., CSMA/CD).†

Some common protocols are Internetwork Packet Exchange (IPX)‡, Transmission Control Protocol/Internet Protocol (TCP/IP)**, and NetBIOS Extended User Interface (NetBEUI)††.

---

* *IBM's second–generation SNA is the Advanced Peer–to–Peer Networking (APPN). In creating APPN, IBM moved SNA from a hierarchical, mainframe–centric environment to a peer–based networking environment.*

† *CSMA/CD is discussed in Subsection 2.5.7, this chapter.*

‡ *The IPX/SPX protocol stack is supported by Novell's NetWare network operating system. Because of Netware's popularity through the late 1980s into the mid 1990s, IPX became a popular internetworking protocol. Novell derived IPX from Xerox Network Services' IDP protocol. IPX usage is in general decline as the boom of the Internet has made TCP/IP nearly universal.*

** *TCP is a messaging protocol while IP is an addressing protocol. The TCP/IP Protocol Suite is discussed in Chapter 3.*

†† *The NetBIOS allows applications on separate computers to communicate over a local area network. In present–day networks, it runs over TCP/IP (NetBIOS over TCP/IP), giving each computer in the network both a NetBIOS name and an IP address corresponding to a host name. Older operating systems ran NetBIOS over IPX/SPX or IEEE 802.2).*

Protocols can either be mandated by one company or organization, or created, used, and maintained by the entire networking industry. A de jure* standard indicates a protocol designed by one company or organization. Normally this organization maintains control of the protocol and is responsible for any additions or changes. A de facto† standard, Latin for "existing in fact," indicates a protocol controlled by the entire industry, and is thus also known as an "industry standard." Anyone can use a de facto standard free of charge. Changes to these standards are not allowed. When a company does not publish specifications for a protocol, it is considered a closed standard. If the specifications are published, then it's an open standard. De jure standards can be either open or closed standards. Most de jure standards are now open, and by definition, all de facto standards are open. TCP/IP and IPX are both open protocols. IBM's Systems Network Architecture (SNA) was once a closed protocol but are now it is open.

2.3 Protocol Stacks

Computers use protocols to talk to each other, and when information travels between computers, it moves from device to device, or layer to layer as defined by the OSI Management Model. Each layer of the model has different protocols that define how information travels. The layered functionality of the different protocols in the OSI model is called a *protocol stack*. In other words, protocol stacks are sets of protocols that work together on different levels to enable communication on a network. For example, Transmission Control Protocol / Internet Protocol (TCP/IP), the protocol stack on the Internet, incorporates more than 100 standards including File Transfer Protocol (FTP), Internet Protocol (IP), Simple Mail Transfer Protocol (SMTP), Transmission Control Protocol (TCP), and Telnet Protocol. Briefly, the functions of these protocols are described in Subsections 2.3.1 through 2.3.7 below.

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

TCP/IP is a protocol developed by the Department of Defense for communications between computers. It is built into the UNIX system and has become the de facto standard for data transmission over networks, including the Internet. The TCP/IP Protocol Suite is discussed in Chapter 3.

2.3.2 File Transfer Protocol (FTP)

This protocol is used to download files from or upload files to remote computer systems, via the Internet's File Transfer Protocol. The user needs an FTP client to transfer files to and from the remote system, which must have an FTP server. Generally, the user also needs to establish an account on the remote system to FTP files.

---

* *de jure means "according to law"*

† *de facto means "In reality or fact; actually". Here, it means "industry standard"*

Several FTP sites permit the use of anonymous FTP. *

2.3.3 Uniform Resource Locator (URL)

An address for a resource on the Internet. URLs are used by Web browsers to locate these resources. An URL specifies the protocol to be used in accessing the resource (such as http:// for a World Wide Web page or ftp:// for an FTP site), the name of the server on which the resource resides (such as www.statecapitol.gov), and, optionally, the path to a resource such as an HTML document or a file on that server.

2.3.4 Internet Protocol (IP)

URL is a protocol within TCP/IP that governs the breakup of data messages into packets, the routing of the packets from sender to destination network and station, and the reassembly of the packets into the original data messages at the destination. IP corresponds to the *Network layer* in the OSI model shown in Figure 2.1 below.

2.3.5 Simple Mail Transfer Protocol (SMTP)

SMTP is a TCP/IP protocol for sending messages from one computer to another on a network. This protocol is used on the Internet to route e–mail.

2.3.6 Transmission Control Protocol (TCP)

TCP is the protocol within TCP/IP that governs the breakup of data messages into packets to be sent via IP, and the reassembly and verification of the complete messages from packets received by IP. TCP corresponds to the *Transport layer* while IP corresponds to the *Network layer* in the OSI model as shown in Figure 2.1. These layers are discussed in more detail in Section 2.6.

2.3.7 Telnet Protocol

Telnet is a set of procedures, that enables a user of one computer on the Internet to log on to any other computer on the Internet, provided the user has a password for the distant computer or the distant computer provides publicly available files. Telnet is also the name of a computer program that uses those rules to make connections between computers on the Internet. Many computers that provide large electronic databases, like library catalogs, often allow users to Telnet in to search the databases. Because of security issues with Telnet, its use has waned as it is replaced by the use of the Secure Shell (SSH) described in Subsection 2.3.8 below.

---

* *CuteFTP®, AceFTP®, and FetchFTP® are popular software applications that allow uploading and downloading files between remote computer systems. On PC platforms, uploading and downloading files can also be done through Microsoft's Internet Explorer (IE) as follows: On the IE type ftp://hostname.com, from the Page drop menu select Open FTP Site in Windows, on the window which pops up click File>Login as, and enter id and password provided by the host station. Then, drag and drop the files to be uploaded into the blank window where the uploading is indicated by a flying page. The file names should be short.*

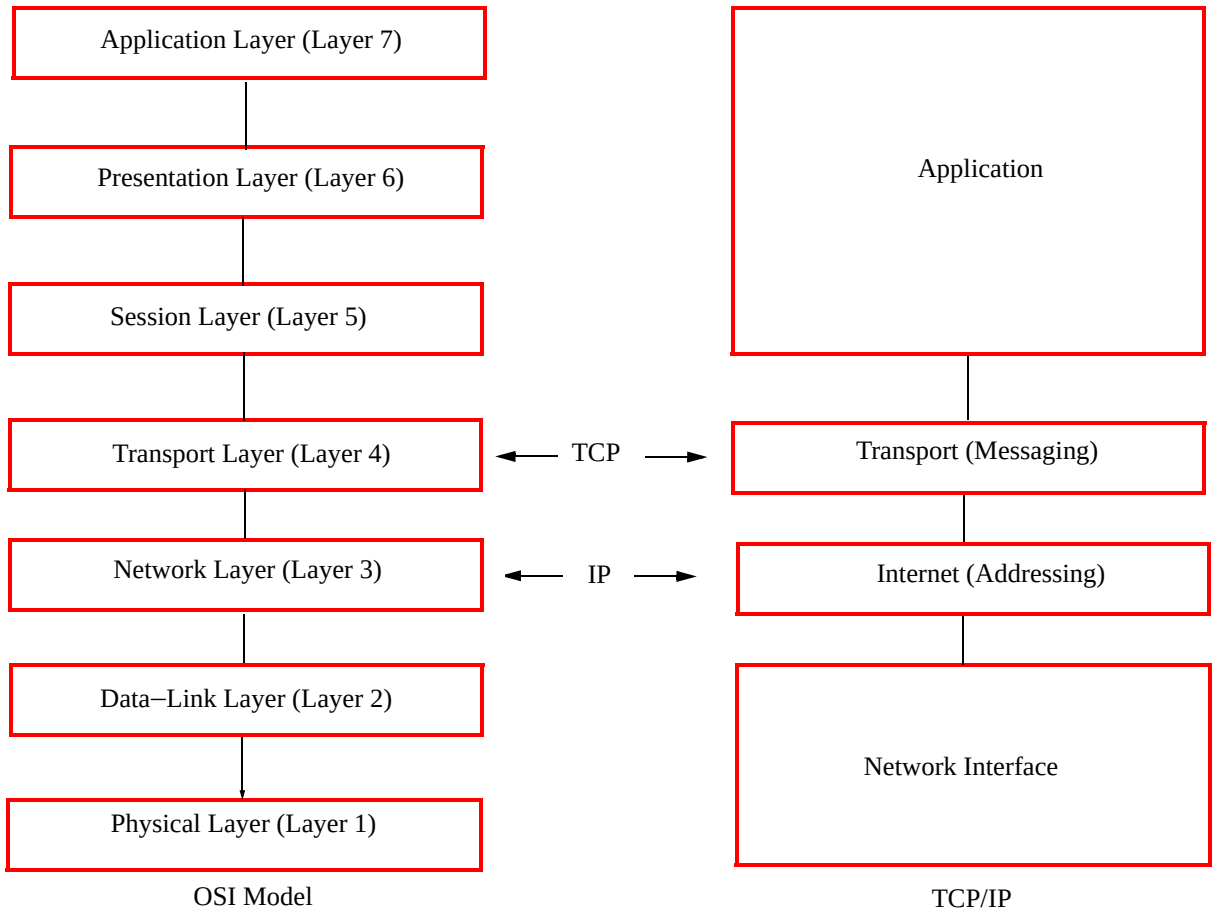


Figure 2.1. OSI and TCP/IP correspondence

2.3.8 Secure Shell (SSH) Protocol

SSH is a network protocol that allows data to be exchanged using a secure channel between two devices in a network. It was originally used on Linux and Unix based systems to access shell accounts,* and was also designed as a replacement for Telnet and other insecure remote shells, which sent information, notably passwords, in plaintext, leaving them open to interception by unauthorized persons. The encryption† used by SSH provides confidentiality and integrity of data over an insecure network, such as the unsecured items on the Internet.

2.3.9 Transport Layer Security (TLS) and Secure Socket Layer (SSL) Protocols

Transport Layer Security (TLS) and Secure Sockets Layer (SSL), are encryption protocols that provide secure communications on the Internet. They encrypt our personal information before it

* *A **shell account** is a personal account that gives a user access to a Unix shell on a remote server.*
† *Encryption is discussed in Chapter 7.*

leaves our computer ensuring that no one else can read it. We can determine that encryption is applied by observing the following two occurrences:

1. https:// .... appears in the address line where "s" stands for secure.
2. A small locked padlock appears at the lower left or right corner of our Internet Browser (Microsoft Internet Explorer and Firefox).

2.4 International Standards Organization (OSI) Management Model

The OSI Management Model is a layered architecture that standardizes levels of service and types of interaction for computers exchanging information through a communications network. The OSI model separates computer–to–computer communications into seven layers, or levels, each building upon the standards contained in the levels below it. The lowest of the seven layers deals solely with hardware links; the highest deals with software interactions at the application–program level. When data is sent from a source device down the OSI Management Model, each layer attaches its own header to that information as shown in Figure 2.2.

We will revisit the OSI Management Model after we introduce the following concepts and definitions.

2.5 Transmission and Detection

In this section we will review the types of communications, transmission, and detection.

2.5.1 Asynchronous Transmission

Asynchronous transmission is a form of data transmission in which data is sent intermittently, one character at a time, rather than in a steady stream with characters separated by fixed time intervals. Asynchronous transmission relies on the use of a start bit and stop bit(s), in addition to the bits representing the character (and an optional parity bit), to distinguish separate characters.

2.5.2 Parity

Parity is a measure of sameness or equivalence. In reference to computers, parity usually refers to an error–checking procedure in which the number of 1's must always be the same— either even or odd— for each group of bits transmitted without error. If parity is checked on a per–character basis, the method is called *Vertical Redundancy Checking* (VRC); if checked on a block–by–block basis, the method is called *Longitudinal Redundancy Checking* (LRC).

Parity is used for checking data transferred within a computer or between computers. In typical communications system, parity is one of the parameters that must be agreed upon by sending and receiving parties before transmission can take place.

The types of parity are listed in Table 2.1.

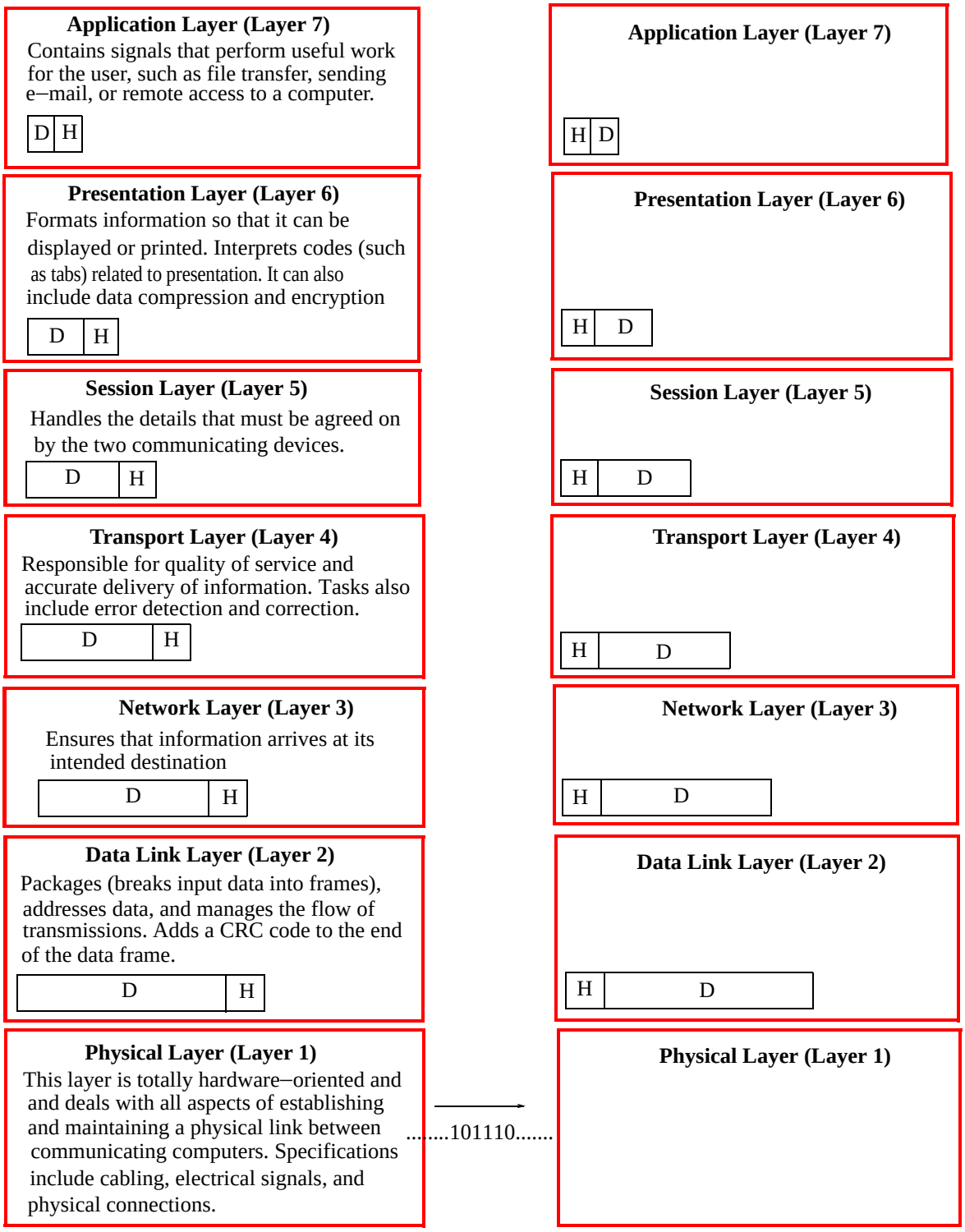


Figure 2.2. The OSI Management Model Protocol Stack

TABLE 2.1 Types of parity

Type	Description
Even parity	The number of 1's in each successfully transmitted set of bits must be an even number
Odd parity	The number of 1's in each successfully transmitted set of bits must be an odd number
No parity	No parity is used
Space parity	A parity bit is used and it is always set to 0
Mark parity	A parity bit is used and it is always set to 1

Figure 2.3 shows the coding of a typical character sent in asynchronous transmission where the parity bit is optional.

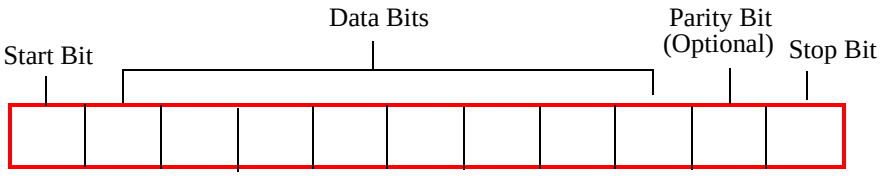


Figure 2.3. The coding of a typical character sent in asynchronous transmission

2.5.3 Synchronous Transmission

Synchronous transmission is another form of data transfer in which information is transmitted in blocks (frames) of bits separated by equal time intervals.

2.5.4 Simplex Transmission

In *simplex transmission*, communication that takes place only from sender to receiver. The speaker of a radio or a television set are examples of simplex transmission.

2.5.5 Half–Duplex Transmission

Half–duplex transmission is a two–way electronic communication that takes place in only one direction at a time. Communication between people is half–duplex when one person listens while the other talks.

2.5.6 Full–Duplex Transmission

A *full–duplex transmission* is capable of carrying information in both directions over a communications channel. A system is full–duplex if it can carry information in both directions at once.

2.5.7 CSMA/CD

CSMA/CD is an acronym for *Carrier Sense Multiple Access* with *Collision Detection*. This is a network protocol for handling situations in which two or more nodes (stations) transmit at the same

time. With CSMA/CD, each node on the network monitors the line and transmits when it senses that the line is not busy. If a collision* occurs because another node is using the same opportunity to transmit, both nodes stop transmitting. To avoid another collision, both then wait for differing random amounts of time before attempting to transmit again.

The transmission sequence on a CSMA/CD network is as follows:

1. The device inspects the media for any other transmission activity.
2. If there is no network media activity, the device proceeds with the transmission of its data.
3. After the device transmits its data, it re–inspects the network media to detect any collisions.
4. If the device detects a collision, it will send out a signal for all other devices to receive. This signal informs the other devices to refrain from sending data for a small period to clear all signals from the media.
5. The transmitting stations will then wait a random amount of time before sending their data.
6. If a second collision occurs with the same devices, they repeat the above steps, but double the random time–out before they transmit again. Once the devices have transmitted successfully, other devices are allowed to transmit again.

Collisions can still occur by devices transmitting at the exact same time, or transmitting before another device's signal reaches the other end of the physical media.

The CSMA/CD protocol was used in earlier Ethernet† designs. However, CSMA/CD is not used in the 10 Gigabit Ethernet which uses a switched full duplex system offering higher performance.

2.5.8 CSMA/CA

CSMA/CA is an acronym for *Carrier Sense Multiple Access with Collision Avoidance*. This network protocol uses a different method of avoiding collisions.

The transmission sequence on a CSMA/CA network is as follows:

1. The device wanting to send checks the media for any active transmissions.
2. If the media is clear, the device sends a Request to Send message.
3. If it is OK to transmit, the network server responds with a Clear to Send signal.
4. When the device receives the Clear to Send signal, it transmits its data.

---

* *Collision is a situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant. Also, a situation that occurs when an attempt is made to store simultaneously two different data items at a given memory address that can hold only one of the items.*

† *Ethernet is a Local Area Network (LAN) and it is described in Chapter 3. Ethernet is standardized as IEEE 802.3*

5. After the transmission is completed, the device sends out an abort sequence to signal that it is finished.

CSMA/CA is used by Apple's LocalTalk network, and Wireless Personal Area Network (WPAN).*

2.5.9 CRC

CRC is an acronym for *cyclical (or cyclic) redundancy check*. This procedure is used in checking for errors in data transmission. CRC error checking uses a math calculation to generate a number based on the data transmitted. The sending device performs the calculation before transmission and sends its result to the receiving device. The receiving device repeats the same calculation after transmission. If both devices obtain the same result, it is assumed that the transmission was error–free. The procedure is known as a redundancy check because each transmission includes not only data but extra (redundant) error–checking values. Communications protocols such as Xmodem and Kermit† use cyclical redundancy checking. CRCs do not correct errors.

Errors occur in telecommunications systems primarily from disturbances (noise) that are relatively long in time duration. Thus, a noise burst of 0.01 second is not uncommon, and if it occurs during a 1,200 bit per second data transmission, we would expect (at worst case) to receive 12 erroneous data bits known as an error burst of 12 bits long. A cyclic redundancy check code known as CRC–12 has a 99.955% chance of detecting error bursts of 12 bits in length.

CRCs add several bits (up to about 25) to the message to be transmitted. The total data block (message plus added bits) to be transmitted, is considered as one lengthy binary polynomial‡ denoted as $T(x)$. At the *transmitting end* the message block (the actual message without the added bits) expressed as a polynomial in powers of x. It is referred to as the *message polynomial* and it is denoted as $M(x)$. The message polynomial $M(x)$ is divided by a fixed polynomial referred to as the *generator polynomial* and denoted as $G(x)$. This division produces a *quotient polynomial* denoted as $Q(x)$ and a *remainder polynomial* denoted as $R(x)$.

The remainder polynomial $R(x)$ also known as the *checksum*, is added to the message polynomial to form the encoded transmitted polynomial $T(x)$

---

* *A WPAN (wireless personal area network) is a personal area network for interconnecting wireless devices. It uses a technology that permits communication within approximately 10 meters. One application is Bluetooth, which is based on the IEEE 802.15 standard.*

† *Xmodem and Kermit are described on Page 1, this chapter.*

‡ *The serial data bits of the various code words in CRCs are usually represented as polynomials in the form* $x^n + x^{n-1} + \ldots + x^2 + x + 1$ *where* x^n *represents the most significant bit (msb) and* x^0 *the least significant bit (lsd). Missing terms represent zeros; for instance the binary word* 10101 *is represented by the polynomial* $x^4 + x^2 + 1$. *We observe that the degree of the polynomial is one less than the number of bits in the code word.*

At the *receiving end* the received data block is divided by the same generator polynomial $G(x)$. If it is found that there is no remainder. i.e., remainder is zero, the message was transmitted correctly. However, if the remainder is non–zero, an error has occurred. In this case either retransmission is requested, or error correction needs to be performed. The non–zero polynomial at the receiving end is referred to as the error polynomial and it is denoted as $E(x)$.

The addition or subtraction operation when calculating polynomials in CRCs is the modulo–2 addition and it is performed by Exclusive–OR gates. Thus,

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

and subtraction is identical to addition.

Let us review the definitions of the polynomials mentioned above.

$M(x)$ = message polynomial consisting of m bits to be transmitted
$G(x)$ = generator polynomial of fixed length known by transmitter and receiver
$T(x)$ = polynomial consisting of t bits to be transmitted
$Q(x)$ = quotient polynomial
$R(x)$ = remainder polynomial
$E(x)$ = error polynomial

The transmitted polynomial $T(x)$ is obtained as follows:

1. The message polynomial $M(x)$ is shifted c bits to the left where c is the highest degree of the generator polynomial $G(x)$. The shifted data block is thus expressed as $M(x)x^c$.

2. The new polynomial $M(x)x^c$ is now divided by the generator polynomial $G(x)$, and the remainder (checksum) of this division is added to $M(x)x^c$ to form the transmitted polynomial $T(x)$. The transmitted polynomial $T(x)$ obtained by this procedure can always be divided by the polynomial $G(x)$ as proved below.

Proof:

$$\frac{M(x)x^c}{G(x)} = Q(x) + \frac{R(x)}{G(x)} \qquad (2.1)$$

Multiplication of (2.1) by $G(x)$ yields

$$M(x)x^c = Q(x)G(x) + R(x) \tag{2.2}$$

or

$$M(x)x^c - R(x) = Q(x)G(x) \tag{2.3}$$

Since subtraction is identical to addition, (2.3) can be expressed as

$$T(x) = M(x)x^c + R(x) = Q(x)G(x) \tag{2.4}$$

or

$$\boxed{\frac{T(x)}{G(x)} = Q(x) + \text{Zero Remainder}} \tag{2.5}$$

Example 2.1

Let the message and generator polynomials be

$$M(x) = 101101 \rightarrow x^5 + x^3 + x^2 + 1$$

and

$$G(x) = 11001 \rightarrow x^4 + x^3 + 1$$

Since the highest degree of $G(x)$ is 4, we shift $M(x)$ four bits to the left. In polynomial form, this is done by forming the product $M(x)x^c$. For this example,

$$M(x)x^4 = (x^5 + x^3 + x^2 + 1)(x^4 + x^3 + 1) = x^9 + x^7 + x^6 + x^4 \rightarrow 1011010000$$

Next, we divide this product by $G(x)$

Divisor: $x^4 + x^3 + 1$ | Quotient: $x^5 + x^4 + x^2$

Dividend: $x^9 + x^7 + x^6 + x^4$

$x^9 + x^8 + x^5$

$x^8 + x^7 + x^6 + x^5 + x^4$

$x^8 + x^7 + x^4$

$x^6 + x^5$

$x^6 + x^5 + x^2$

Remainder $R(x) \rightarrow x^2$

Now, we add $R(x)$ to $M(x)x^4$ to get the transmitted polynomial

$$T(x) = M(x)x^4 + R(x) = x^9 + x^7 + x^6 + x^4 + x^2 \rightarrow 1011010100$$

If there is no error at the receiver, this message will produce no remainder when divided by $G(x)$.

A check procedure is shown below.

Divisor: $x^4 + x^3 + 1$

Quotient: $x^5 + x^4 + x^2$

Dividend: $x^9 + x^7 + x^6 + x^4 + x^2$

$x^9 + x^8 + x^5$

$x^8 + x^7 + x^6 + x^5 + x^4 + x^2$

$x^8 + x^7 + x^4$

$x^6 + x^5 + x^2$

$x^6 + x^5 + x^2$

Remainder $R(x) \rightarrow 0$

2.5.10 American Standard Code for Information Interchange (ASCII)

ASCII is a standard* for defining codes for information exchange. It uses seven bits for 128 different characters. Another bit is added at the end for parity checking. For instance, the letter *X* is represented as 1011000. With odd parity, it is represented as 10110000 (odd number of ones) and with even parity is represented as 10110001 (even number of ones).

2.5.11 Error Detecting and Correcting Codes

Error detecting and correcting codes are topics discussed in Information Theory textbooks. Here, we will present an example of a simple systematic code in which a single check digit is added as a means of detecting an odd number of errors in a code word. The information digits are arranged in a two dimensional array as shown below where an even– parity–check digit has been added to each row and each column. In addition, checks are also carried out on check digits.

* *For a detailed discussion, please refer to Appendix B*

Information Bits

Information Bits							Row Checks
1	0	1	1	0	1	0	
0	1	1	1	0	1	0	
1	0	1	0	0	1	1	
1	0	0	0	1	1	1	
0	0	1	1	0	1	1	
1	0	1	1	1	0	0	
0	1	1	0	0	1	1	

Column Checks

In the table above, the position of an error is located as the common element of the row and the column whose parity checks fail.

2.5.12 EBCDIC

EBCDIC is an acronym for *Extended Binary Code Decimal Interchange Code*. It is a standard code that uses 8 bits to represent each of up to 256 alphanumeric characters.

2.5.13 Repeater

A repeater is a device used on communications circuits that decreases distortion by amplifying or regenerating a signal so that it can be transmitted onward in its original strength and form. On a network, a repeater connects two networks or two network segments at the physical layer of the OSI model and regenerates the signal.

2.5.14 Hub

A network hub or simply hub, is a device joining communication lines at a central location, providing a common connection to all devices on the network. Hubs operate at the physical layer (layer 1) of the OSI model.

2.5.15 Concentrator

A concentrator is a communications device that combines signals from multiple sources, such as terminals on a network, into one or more signals before sending them to their destination. Concentrators have been used by Internet Service Providers (ISPs) to initiate modem dialing.

2.5.16 Gateway

A gateway is a device that connects networks using different communications protocols so that information can be passed from one to the other. A gateway both transfers information and converts it to a form compatible with the protocols used by the receiving network.

2.5.17 Router

A router is an intermediary device on a communications network that expedites message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over the most efficient available route. On an interconnected set of local area networks (LANs) using the same communications protocols, a router serves the somewhat different function of acting as a link between LANs, enabling messages to be sent from one to another.

In packet–switched networks such as the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each point–of–presence on the Internet. A router is often included as part of a network switch.

2.5.18 Bridge

A bridge is a device that connects networks using the same communications protocols so that information can be passed from one to the other.

2.5.19 Brouter

A brouter is a device that is a combination od a bridge and a router, providing both types of services. Brouters operate at both the network layer for routable protocols* and at the data link layer for non–routable protocols.†

2.5.20 Backbone

A backbone is the main part of a network that handles the heaviest traffic and runs the longest distance, supporting smaller networks attached to it.

2.5.21 Firewall

A firewall is a security system intended to protect a network against external threats, such as hackers, coming from another network. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

---

* *A communications protocol that contains a network address as well as a device address. It allows packets to be forwarded from one network to another. Examples of routable protocols are TCP/IP, IPX, AppleTalk, SNA, XNS and DECnet.*

† *A communications protocol that contains only a device address and not a network address. It does not incorporate an addressing scheme for sending data from one network to another. Examples of non–routable protocols are NetBIOS and DEC's LAT protocols.*

2.5.22 Node

A network node or simply node, is a junction. In local area networks, it is a device that is connected to the network and is capable of providing communications with other network devices. If the network in question is a LAN or WAN, every node must have a MAC address if it is at least a data link layer device, as defined in the OSI model. In the Internet, many network nodes are host computers, identified by an IP address, and all hosts are nodes. However, datalink layer devices such as switches and bridges have an IP host address, but are considered as network nodes.

2.5.23 Port

A port is an Input/Output port. In computer networking, a port number is an application–specific or *process–specific* communications endpoint used by Transport Layer protocols in the OSI model, such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) of the Internet Protocol Suite. UDP is discussed in Chapter 3.

A port number* enables IP packets to be sent to a particular process on a computer connected to the Internet. Thus, e–mail data under SMTP† "talks" to port number 25, while POP3‡ "listens" on port 110. Likewise port number 21 is used with FTPs. A total of $2^{16} = 65,535$ port numbers are available for use with TCP, and the same numbers are available for User Datagram Protocol (UDP).

Typically, one server used for sending and receiving e–mail by providing both an SMTP (for sending) and a POP3 (for receiving) service; these are handled by different server processes, and the port number will be used to determine which data is associated with which process.

2.5.24 Packet

A packet is a piece of data transferred over a network. Also called *data packet*.

---

* *As an analogy, we can think IP as being a street where a letter can be delivered by the post office, and port number the number on that street.*

† ***The Simple Mail Transfer Protocol (SMTP)*** *is a de facto standard for electronic mail (e–mail) transmissions across the Internet. The protocol in widespread use today is also known as extended SMTP (ESMTP) and An update of this standard is currently (2008) pending approval in the Internet Engineering Task Force (IETF).*

‡ *The* ***Post Office Protocol version 3 (POP3)****, an application–layer Internet standard protocol, to retrieve e–mail from a remote server over a TCP/IP connection. POP3 and IMAP4 (Internet Message Access Protocol) are the two most prevalent Internet standard protocols for e–mail retrieval. Virtually all modern e–mail clients and servers support both.*

2.5.25 Cell

A cell is a fixed length message unit. Like packets, cells are pieces of a message.

2.5.26 Frame

In asynchronous serial communications, a frame is a unit of transmission that is sometimes measured in elapsed time and begins with the start bit that precedes a character and ends with the last stop bit that follows the character. In synchronous communications, it is a package of information transmitted as a single unit. Every frame follows the same basic organization and contains control information, such as synchronizing characters, station address, and an error–checking value, as well as a variable amount of data.

2.5.27 Switch

A switch is a network device that connects PCs with dedicated bandwidth, full duplex data transfer, and forwards data to the correct network destination. It operates at the Data Link layer of the OSI model.

2.5.28 Plug–and–Play

Plug–and–Play is a standard that enables a PC to recognize a device when it is connected to it.

2.5.29 Universal Serial Bus (USB)

A Universal Serial Bus (USB) is a serial bus with maximum speed at 12 Mbps for connecting peripherals to a PC. A USB can connect many peripherals, such as external CD–ROM drives, printers, modems, mice, and keyboards, to the system through a single, general–purpose port. This is accomplished by daisy chaining* peripherals together. USB supports hot plugging and multiple data streams. It was developed by Intel. The USB 2.0 has maximum speed at 480 Mbps.

2.5.30 Converter

A converter is any device that changes electrical signals or computer data from one form to another. For example, an analog–to–digital converter translates analog signals to digital signals.

2.5.31 Circuit Switching

Circuit switching is a method of opening communications lines, as through the telephone system, by creating a physical link between the initiating and receiving parties. In circuit switching, the connection is made at a switching center, which physically connects the two parties and maintains an open line between them for as long as needed. Circuit switching is typically used on the dial–up telephone network, and it is also used on a smaller scale in privately–maintained commu-

* *A daisy chain is a set of devices connected in series. In order to eliminate conflicting requests to use the channel (bus) to which all the devices are connected, each device is given a different priority, or, as in the Apple Desktop Bus, each device monitors the channel and transmits only when the line is clear.*

nications networks. A circuit switching network is shown in Figure 2.4 where terminal T2 is connected through junctions J1 and J2 to terminal T3.

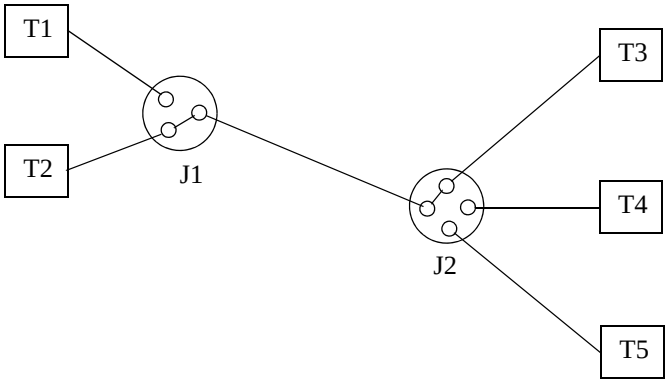


Figure 2.4. Typical circuit switching network

2.5.32 Message Switching Network

Message switching is a technique used on some communications networks in which a message, with appropriate address information, is routed through one or more intermediate switching stations before being sent to its destination. On a typical message–switching network, a central computer receives messages, stores them, usually briefly, determines their destination addresses, and then delivers them. Message switching enables a network both to regulate traffic and to use communications lines efficiently. A message switching network is shown in Figure 2.5 where the message is transmitted from terminal T1 to terminal T2 via junctions J1 and J2.

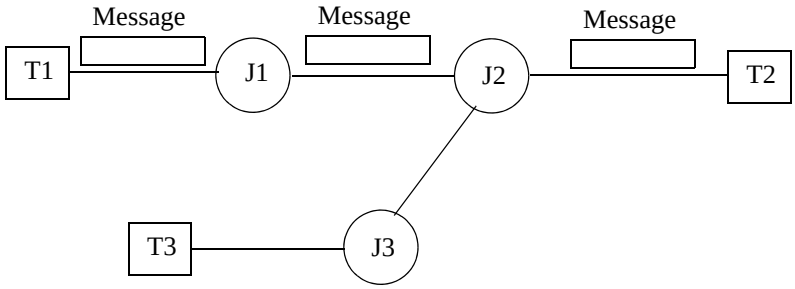


Figure 2.5. Typical message switching network

2.5.33 Packet Switching

Packet switching is a message–delivery technique in which small units of information (packets) are relayed through stations in a computer network along the best route available between the source and the destination. A packet–switching network handles information in small units, breaking long messages into multiple packets before routing. Although each packet may travel

along a different path, and the packets composing a message may arrive at different times or out of sequence, the receiving computer reassembles the original message. Packet–switching networks are considered to be fast and efficient. To manage the tasks of routing traffic and assembling/disassembling packets, such a network requires some "intelligence" from the computers and software that control delivery. The Internet is an example of a packet–switching network. Standards for packet switching on networks are documented in the CCIT recommendation X.25. A packet switching network is shown in Figure 2.6 where the message is split in packets P1, P2, and P3. At the junction J1 the packets P1 and P3 are routed to junction J2 whereas P2 is routed to junction J3 and then to J2. The three packets are then transmitted to terminal T2 in the P1, P3 and P2 sequence. They are reassembled to their original sequence at terminal T2.

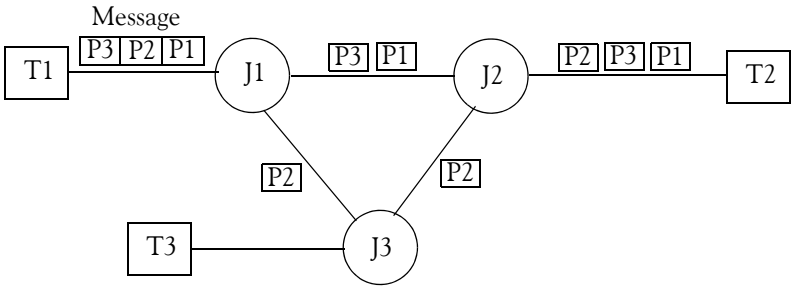


Figure 2.6. Typical packet switching network

2.5.34 Hop

In a packet–switching network, a hop is the trip a data packet takes from one router or intermediate point to another in the network. On the Internet (or a network that uses TCP/IP), the number of hops a packet has taken toward its destination (called the "hop count") is kept in the packet header. A packet with an exceedingly large hop count is discarded.

2.5.35 Datagram

A *datagram* is one packet, or unit, of information, along with relevant delivery information, such as the destination address, that is sent through a packet–switching network.

2.5.36 Byte

A *byte* is unit of data consisting of eight bits. A byte can represent a single character, such as a letter, a digit, or a punctuation mark. Because a byte represents only a small amount of information, amounts of computer memory and storage are usually given in kilobytes (1024 bytes), megabytes (1,048,576 bytes), or gigabytes (1,073,741,824 bytes).

2.5.37 Asynchronous Transmission

This is a form of data transmission in which data is sent intermittently, one character at a time, rather than in a steady stream with characters separated by fixed time intervals. Asynchronous

transmission relies on the use of a start bit and stop bit(s), in addition to the bits representing the character (and an optional parity bit), to distinguish separate characters as shown in Figure 2.7.

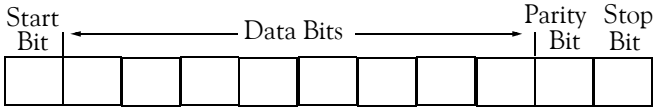


Figure 2.7. Asynchronous serial transmission

2.5.38 Integrated Services Digital Network (ISDN)

ISDN is a worldwide digital communications network evolving from existing telephone services. The goal of ISDN is to replace the current telephone network, which requires digital–to–analog conversions, with facilities totally devoted to digital switching and transmission, yet advanced enough to replace traditionally analog forms of data, ranging from voice to computer transmissions, music, and video. ISDN is built on two main types of communications channels: a B channel, which carries data at a rate of 64 Kbps (kilobits per second), and a D channel, which carries control information at either 16 or 64 Kbps. Computers and other devices connect to ISDN lines through simple, standardized interfaces. It provides users with faster, more extensive communications services. Most recently, ISDN service has largely been displaced by broadband internet service, such as xDSL and Cable Modem service. These services are faster, less expensive, and easier to set up and maintain than ISDN. Still, ISDN has its place, as backup to dedicated lines, and in locations where broadband service is not yet available.

2.5.39 Asynchronous Transfer Mode (ATM)

ATM is a network technology capable of transmitting data, voice, video, and frame relay traffic in real time. Data, including frame relay data, is broken into packets containing 53 bytes each, which are switched between any two nodes in the system at rates ranging from 1.5 Mbps to 622 Mbps. It is currently used in local area networks involving workstations and personal computers, but it is expected to be adopted by the telephone companies, who will be able to charge customers for the data they transmit rather than for their connect time.

2.5.40 Frame – Asynchronous communications

In asynchronous serial communications, a frame is a unit of transmission that is sometimes measured in elapsed time and begins with the start bit that precedes a character and ends with the last stop bit that follows the character.

2.5.41 High–level Data Link Control (HDLC)

HDLC is a protocol for information transfer and was developed by the ISO. HDLC is a bit–oriented, synchronous protocol that applies to the data–link (message–packaging) layer of the ISO Open Systems Interconnection (OSI) model for computer–microcomputer communications. Messages are transmitted in units called frames, which can contain different amounts of data but which must be organized in a particular way.

2.5.42 Synchronous Data Link Control (SDLC)

SDLC is a data transmission protocol most widely used by networks conforming to IBM's *Systems Network Architecture* (SNA). SDLC is similar to the HDLC (High–level Data Link Control) protocol developed by the International Organization for Standardization (ISO).

2.5.43 Frame – Synchronous communications

In synchronous communications, a frame is a package of information transmitted as a single unit. Every frame follows the same basic organization and contains control information, such as synchronizing characters, station address, and an error–checking value, as well as a variable amount of data as shown in Figure 2.8. For example, a frame used in the widely accepted HDLC and related SDLC protocols begins and ends with a unique flag (01111110).

Figure 2.8. Fields of HDLC – SDLC frame

2.5.44 Broadband

Broadband is a form of communications systems in which the medium of transmission (such as a wire or fiber optic cable) carries multiple messages at a time, each message modulated on its own carrier frequency by means of modems. Broadband communication is found in wide area networks.

2.5.45 Baseband

This is a form of communications systems in which the medium of transmission (such as a wire or fiber–optic cable) carries a single message at a time in digital form. Baseband communication is found in local area networks such as Ethernet and Token Ring.

2.6 The OSI Management Model Revisited

The OSI Management Model was introduced in the previous section, and the function of each layer was given in the block diagram of Figure 2.1. In this section, we will review the OSI Management Model and provide more detailed explanations. It consists of the following seven layers.

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

The OSI Management Model depicts the stream of information down the seven layers of the model on the source device, across intermediate devices, and up through the seven layers on the destination device. These devices can be any type of network equipment. Networked computers, printers, and faxes, as well as internet working devices such as routers and switches, are all examples of these devices. The model is a theoretical object, most often followed loosely and not to the letter, that breaks down the functions of a network into seven layers. Most protocol standards can be placed into one of the seven layers. If we know the layer or layers that a protocol fits into in the model, we have some idea of its purpose and function.

It is often referred to as the IOS/OSI model which is an acronym for *International Organization for Standardization Open Systems Interconnection* model. It was established by the International Standards Organization (ISO)* in 1984 model to be used as a guide for future network protocols.

2.6.1 Physical Layer

The first layer of the OSI model is the Physical layer. Its function is the transmission of bits over the network media. In other words, it provides a physical connection for the transmission of data among the network devices. The Physical layer is responsible for making sure that data is read the same way on the destination device as it was sent from the source device.

The Physical layer works binary numbers regardless of code. Network devices that operate at this layer are repeaters and converters. As we recall, repeaters are used to improve the signal quality and also permit the wiring to span greater lengths that would otherwise be possible. On the negative side, repeaters introduce some small delay. For this reason, standards such as the coaxial 10Base–2 Ethernet (Thin Ethernet) use a thin coaxial cable up to 200 meters long and carrying 10 Mbps in a bus topology. Thus, if it is necessary to transmit a signal over a wire length of 350 meters, we could insert a repeater in the middle of it. But because a repeater adds a delay, it is recommended that one never places more than 3 repeaters on the same wire link.

Another device that operates at the Physical layer is a converter that it is used to transform a signal from one medium to another.

A typical Physical layer transmission is shown in Figure 2.9.

---

* *The International Standards Organization is a voluntary, non–treaty organization that produces international standards. It was founded in 1946. The members of ISO are actually other organizations from eighty–nine member countries. The United States representative in ISO is the American National Standards Institute (ANSI). ISO standards are sometimes coordinated with International Telecommunications Union, Telecommunication Standards Sector (ITU–T) recommendations to avoid two incompatible international standards. ITU–T, headquartered in Geneva, Switzerland, is an international organization within which governments and the private sector coordinate global telecommunications networks and services. ITU–T activities include the coordination, development, regulation, and standardization of telecommunications. (ITU–T was formerly known as the Consultative Committee for International Telegraphy and Telephony.) The ISO issues standards on a large number of subjects, ranging from data communications protocols to telephone pole coatings. The ISO has almost 200 technical committees, each dealing with a specific subject. Each committee has subcommittees that are themselves divided into working groups. Working groups are where most of the real work is done. Over 100,000 volunteers are part of the working groups. These volunteers are usually assigned to work on ISO matters by companies whose products are affected by the standards being created.*

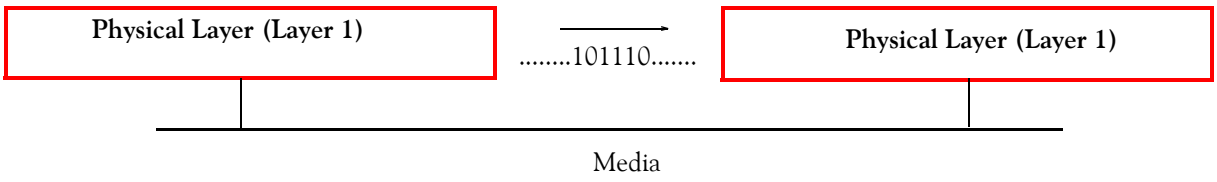


Figure 2.9. The Physical layer

2.6.2 Data–Link Layer

The second layer of the OSI model is the Data–Link layer. Its function is to provide a reliable method of transmitting data across the physical media. This layer deals with both hardware and software. Bridges are the hardware used on this layer. A Data–Link layer transmission is shown in Figure 2.10.

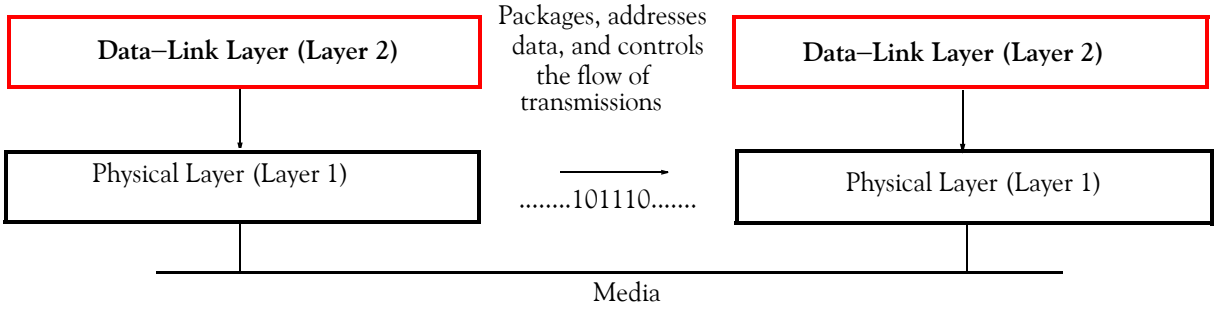


Figure 2.10. The Data–link layer

This layer breaks the input data into frames, transmits the frames sequentially, and processes the acknowledged frames sent back by the receiver. It adds a header and trailer to the frames it creates. These allow the destination device to see when a frame begins or ends on the physical media.

The IEEE 802 team enhanced the OSI model by dividing the Data Link Layer to two sublayers instead of adding an eighth layer to the seven–layer mode. These sublayers are the *Media Access Control* (MAC) *Sublayer* and the *Logical Link Control* (LLC) *Sublayer* shown in Figure 2.11.

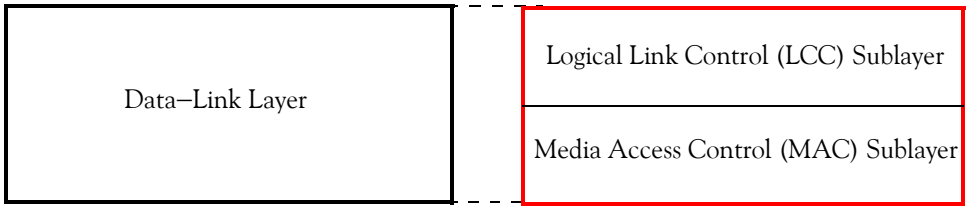


Figure 2.11. The Data–link sublayers

Briefly, the Media Access Control (MAC) sublayer is concerned with network access and collision detection. The Logical Link Control (LCC) is responsible for station–to–station connections,

generation of message frames, and error control. These sublayers are discussed below in more detail.

Media Access Control (MAC)

The MAC sublayer ensures that only one device can transmit on any type of media at any time. If two or more devices attempt to transmit at the same time on the same media, a collision of signals will occur. Currently, there are three ways to control access to media. These are:

- *Addressing* – Generally, addressing refers to the process of assigning or referring to an address. Thus, in programming, the address is typically a value specifying a memory location. But on a network, every device has a physical address attached to it. This address is a serial number–like address and it is referred to as the MAC address. The MAC sublayer handles the physical addresses of devices on the network. An example of this address for an Ethernet card could be 00–E0–18–90–1E–CB. Although every client in a network can be assigned a name by the software, the Physical layer does not recognized it. Therefore, for messages to be sent to the proper destination, the Physical layer must have a unique address which it can recognize; this is the MAC address.

- *Contention* – On a network, contention refers to the competition among network devices for the opportunity to use a media or network resource. In one sense, contention applies to a situation in which two or more devices attempt to transmit at the same time, thus causing a collision on the line. In a somewhat different sense, contention also applies to a free–for–all method of controlling access to a communications line, in which the right to transmit is awarded to the station that wins control of the line.

  With recent design improvements, contention–based networks devices listen for other signals on the media before transmitting. Although collisions are not totally eliminated, but they are kept down to a minimum. This is known as Carrier Sense Multiple Access, or CSMA. As stated earlier, the two types of CSMA are CSMA/CD and CSMA/CA. CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection. The transmission sequences on CSMA/CD and CSMA/CA networks were discussed earlier, but are repeated here for convenience.

  A. With CSMA/CD:

  1. The device "checks" the media to see if other transmissions are taking place.
  2. If there is no "traffic" on the network media, the device proceeds with the transmission of its data.
  3. While transmission takes place, the device "checks" the media for possible any collisions.

4. If the device detects a collision, it sends out a signal to the other devices This signal requests that the other devices refrain from sending data until the media is clear.

5. The devices that wish to transmit, will wait a random amount of time before sending their data.

6. If another collision occurs with the same devices, the above steps are repeated, but they increase the random time–out before they transmit again. Once the devices have transmitted successfully, other devices are allowed to transmit again.

The CSMA/CD method which is used by the Ethernet, is based on the belief that most collisions can be avoided by simply checking the media to see if it is clear before transmitting. Of course, collisions will occur by devices transmitting at the exact same time, or transmitting before another device's signal reaches the other end of the media.

B. With CSMA/CA:

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) networks use a more conservative method of avoiding collisions. The Apple's LocalTalk network uses this method. The CSMA/CA method uses the following procedure:

1. The device that has a need to transmit "checks" the media for any active transmissions.

2. If the media is clear, the device sends a Request to Send message.

3. If the media is cleat, the network server responds with a Clear to Send signal.

4. When the device receives the Clear to Send signal, it transmits its data.

5. After the transmission is completed, the device sends out a signal to inform the network server that transmission was successfully completed.

While contention–based systems are relatively simple, they do not assign priorities to special devices. Also, immediate media access is not guaranteed.

• *Deterministic* – A deterministic network dictates that the network must follow certain rules and procedures before transmitting. The two types of deterministic networks are *token passing* and *polling*.

A. Token passing

Token passing is a method of controlling access on local area networks through the use of a special signal, called a *token*, that determines which station is allowed to transmit. The token, which is actually a short message, is passed from station to station around the network. Only the station with the

token can transmit information. Thus, in a token–passing system, a small data frame is passed from device to device across the network in a predetermined order. The device that has control of the token frame has the ability to transmit data across the network. Even on large networks where contention would start to break down due to increased levels of collisions, token passing maintains an orderly network.

Token passing networks are more expensive and they are slower than contention–based networks. However, they have the advantages that special devices can be assigned highest priorities, and the network can operate more efficiently.

B. Polling system

Polling is the process of periodically determining the status of each device in a set so that the active program can process the events generated by each device, such as whether a mouse button was pressed or whether new data is available at a serial port. This can be contrasted with event–driven processing, in which the operating system alerts a program or routine to the occurrence of an event by means of an interrupt or message rather than having to check each device in turn. Thus, in a polling system a master device checks the other secondary devices on the network to see if they need to transmit. The order of the devices polled and their priority can be set by the administrator. Most networks that use this configuration operate in a multipoint configuration, where each secondary device is directly connected to the primary.

Logical Link Control

The logical link control (LLC) sublayer covers station–to–station connections, generation of message frames, and error control. To ensure that the data frames are received properly, the LLC sublayer adds the CRC code to provide error detection and verification information.

Bridges operate at the Data Link layer. A special type of bridges known as transparent bridges* can use MAC addresses to filter traffic between segments. They may be used to connect two segments with different cable types, assuming the network type (for example, Ethernet, Token Ring) is the same.

2.6.3 Network Layer

The third layer of the OSI model is the Network layer. This layer manages the movement of data between networks. Protocols such as IP, IPX, and AppleTalk at this layer are responsible for find-

* *We will discuss transparent bridges in Chapter 5. Briefly, a transparent bridge has knowledge only of its neighbor and is transparent (invisible) to other devices.*

ing the device for which the data are destined. Figure 2.12 shows data being sent between the Network layer of two devices.

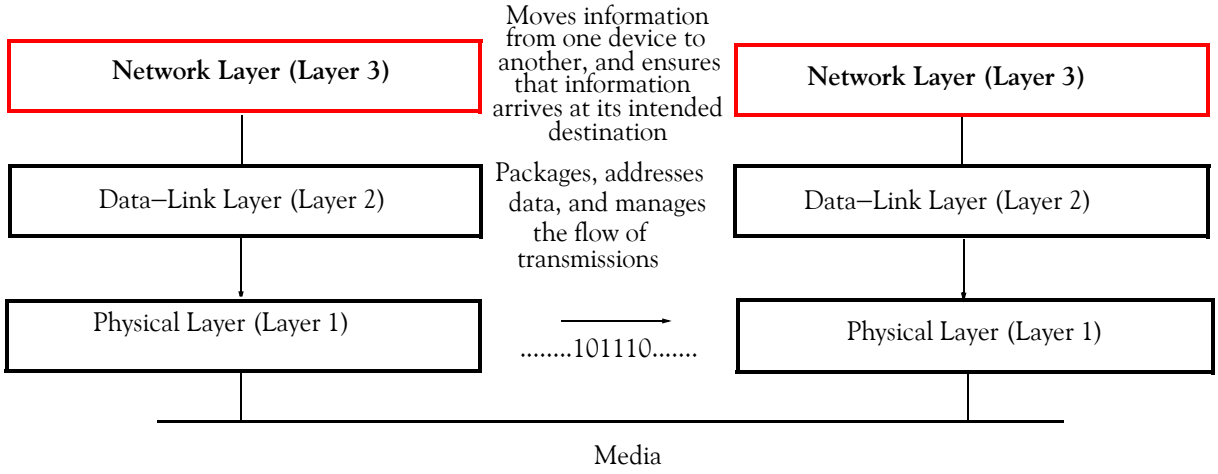


Figure 2.12. The Network layer

The Network Layer handles the delivery of datagrams in a media–independent manner. As mentioned earlier, datagrams are a group of data that travel as a single package from a sending computer's operating system to a receiving computer's operating system.

Datagrams also contain addressing information. A Network layer protocol will assign an address to each Network layer device. The receiver's address needs to be attached to the datagrarn and the sender's address is also typically required to be present. The Network layer addresses may or may not be related to any Data Link layer address in any direct way. The addressing information is typically contained in a datagram header separate from the message data being delivered from one computer to another.

Sending and receiving computers might not be directly connected by a communication link. In that case, they would depend on the services of a router. We recall that a router is a device which connects to more than one network and offers its services to computers on those networks as a means to forward datagrams from one network to another network, The joining of two or more networks in this way is called *internetworking* and the networks formed in this way are called *internets*.

A datagram may travel from sender to receiver via a router, as shown in Figure 2.13. In this case, the router may use different Layer 1 and Layer 2 devices and media may differ in type from each other.

The Network layer decides what path data will take if the destination device is located on another network. Data passes through the network by devices called intermediate devices. The source and destination devices are end systems. The Network layer accepts messages from the source host, converts them to packets, and makes sure that the packets are directed toward the destination.

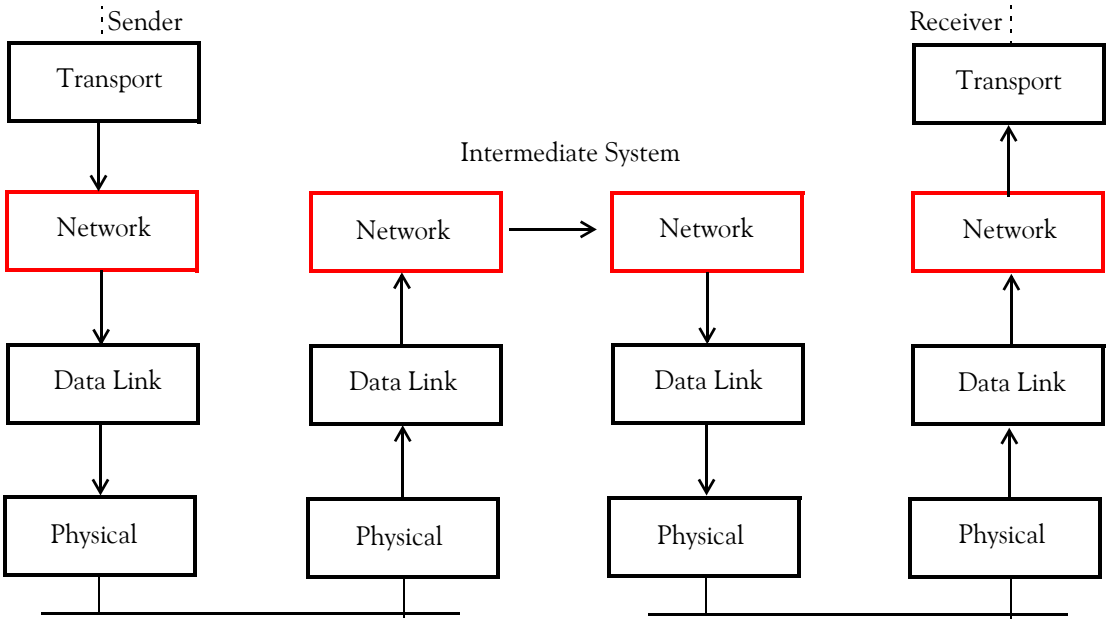


Figure 2.13. Datagram path from sending computer to receiving computer via a router

The Network layer is also responsible for deciding on the best route the packet should take through the network. It does this by checking to see if the destination device is on another network. If it is, then the Network layer must decide where to send the datagram to so it will reach the final destination. In addition, if too many datagrams are present in the network at the same time, they will interfere with each other. The Network layer is responsible for avoiding such interferences.

Connections between devices at the Network layer are through the so–called *Unacknowledged Connectionless Service*, or simply referred to as *connectionless*.* No verification that the data were transmitted and received correctly is required. If it does not arrive or is incorrect, then the destination device must request a retransmit. The job of the Network layer is to get data through the network in the best possible way. By using the processes of switching, routing, and addressing, it finds the most efficient route through the network.

Switching

We recall that a datagram is one packet, or unit, of information, along with relevant delivery information, such as the destination address, that is sent through a packet–switching network. Datagram switching describes how data is forwarded across an internetwork. The type of datagram switching that a service or application may use depends on how fast the data needs to be

* *A connectionless service provides the fastest means of transferring data at the LLC sublayer of the Data Link Layer of the OSI Model. Although it is the most unreliable way to handle data transfers, it is commonly used as most upper layer protocols of the OSI Model handle their own error checking.*

delivered. For example, e–mail does not need to be delivered in real time, so it does not have to go directly to the destination device. The three switching methods, i.e., circuit switching, message switching, and packet switching were described earlier in this chapter.

Routing

Since the Network Layer is responsible for routing datagrams across a network, a table must be created to indicate the shortest routes between two networks. These tables can either be dynamic or static. These are defined below.

- *Static Routing* – A static route is a fixed–path that has been programmed by a network administrator. Static routes cannot make use of routing protocols and don't self–update after receipt of routing update messages; they must be updated manually. Since a router can't possibly know routes to all destinations, it is configured with a default gateway path to which datagrams with unknown destinations are sent. Default gateways are entered as static routes to make sure undeliverable traffic is forwarded to a router that has routing table entries leading outside the internetwork. Figure 2.14 shows how a datagram with unknown destination can reach the proper destination via a default gateway and a router with routing table.

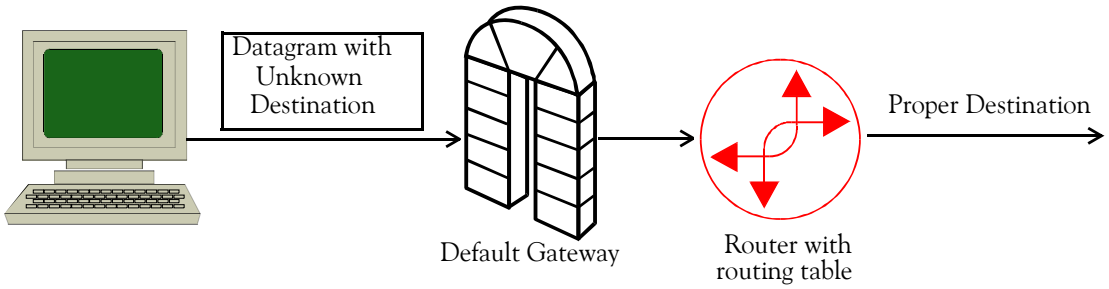


Figure 2.14. Using default gateway to reach an unknown destination

- *Dynamic Routing* –This is the type of muting made possible by routing protocols, which automatically calculate routes based on routing update messages. The majority of all internetwork routes are dynamic.

  Dynamic routing uses protocols. One such protocol is the *Distance Vector Multicast** *Routing Protocol* (DVMRP). This is an Internet routing protocol that provides an efficient mechanism for connectionless datagram delivery to a group of hosts across an Internet network. It is a distributed protocol that dynamically generates IP multicast delivery trees using a technique called *Reverse Path Multicasting* (RPM).

* *Multicasting is the process of sending a message simultaneously to more than one destination on a network.*

Dynamic routing uses three types of routing protocols. These are distance vector, link state, and hybrid.

- *Distance vector* – Distance is the number of router hops to the destination. With this routing method routers use the so–called distance metric where each router adds its hop to the metric to calculate the best route to the destination. Routers pass routing tables to their nearest neighbors in all directions. At each exchange, the router increments the distance value received for a route, thereby applying its own distance value to that route as shown in Figure 2.15.

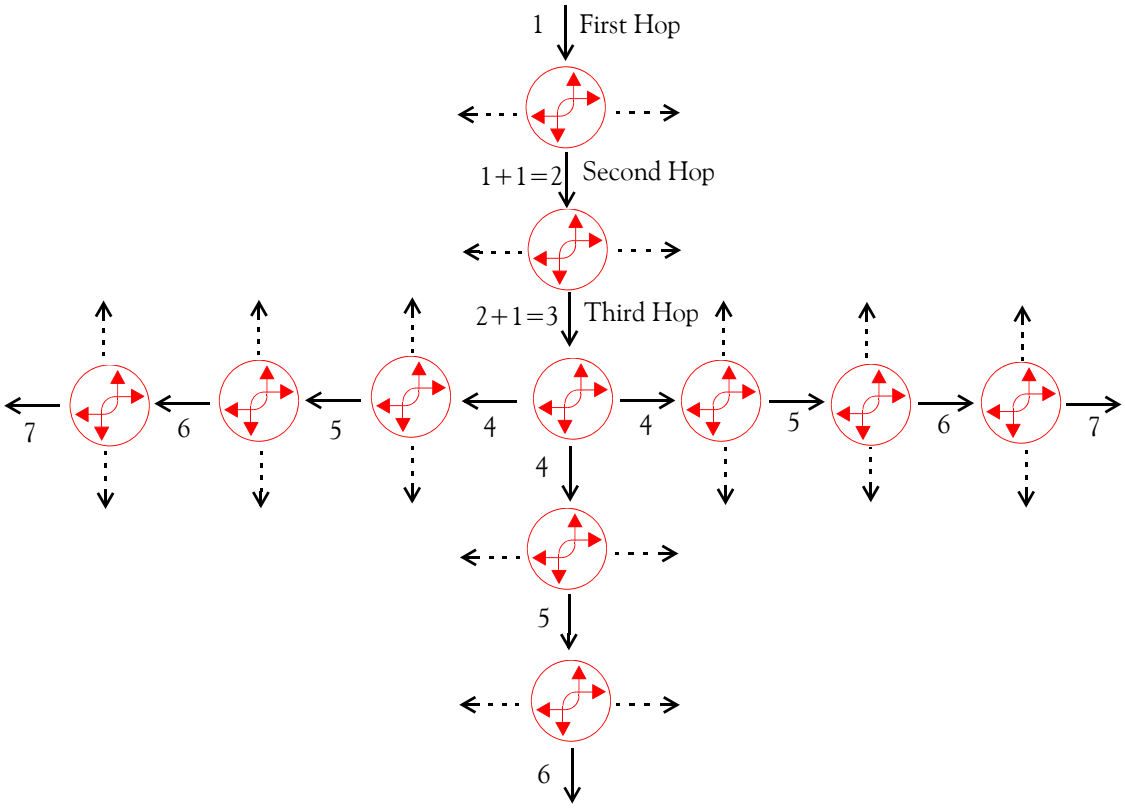


Figure 2.15. Distance vector routing

Generally, distance–vector protocols are limited to 16 hops and are used in internetworks with less that 50 routers. But because they are simple and easy to configure, they are the most widely used.

- *Link state routing* – Link state routing is event–driven.* It is also known as Shortest Path First (SPF). The link–state routing protocols are concerned with the state of the internetwork links that form routes. Thus, whenever the state of a link changes, a routing update called Link–State Advertisement (LSA) is exchanged between routers. When a router receives an LSA routing update, a link–state algorithm is used to recalculate the shortest path to affected destinations. Also, link–state considers link speed, latency (the time required for a signal to travel from one point on a network to another), and congestion.

- *Hybrid routing* – Hybrid routing protocols use more accurate distance–vector metrics† designed to converge more rapidly.

Addressing

Since the Network layer is concerned with getting data from one computer to another, even if they are on a different network, it uses network addresses. A device on a network has not only a device address but also a network address that tells other computers where to locate that device. By using this address, the sending device can tell whether the destination device is on the same network segment (local) or on another network segment (remote).

2.6.4 Transport Layer

The Transport layer provides a transport service between the Session layer and the Network layer. It ensures that packets are sent error–free and repackages messages. If a package is too large, it divides the message into a number of smaller packages before it is sent. The receiving station gathers and reassembles them. Then, it ensures that data reach their destination intact and in the proper order.

The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) in the TCP/IP suite and the Sequence Packet Exchange (SPX) of the NetWare IPX/SPX suite operate at this layer. The Transport layer communications are shown in Figure 2.16

The Transport layer is a true source–to–destination layer. This means that a program on the source device carries on a dialogue with another program on the destination device by using message headers and control messages. These message headers and control messages are used for error detection, sequencing, and flow control.

---

* *This term applies to computer programming. Thus, event–driven programming is a type of programming in which the program constantly evaluates and responds to sets of events, such as key presses or mouse movements. Event–driven programs are typical of Apple Macintosh computers, although most graphical interfaces, such as Microsoft Windows or the X Window System, also use such an approach.*

† *Metric refers to a standard of measurement. In mathematics is a geometric function defined for a coordinate system such that the distance between any two points in that system may be determined from their coordinates.*

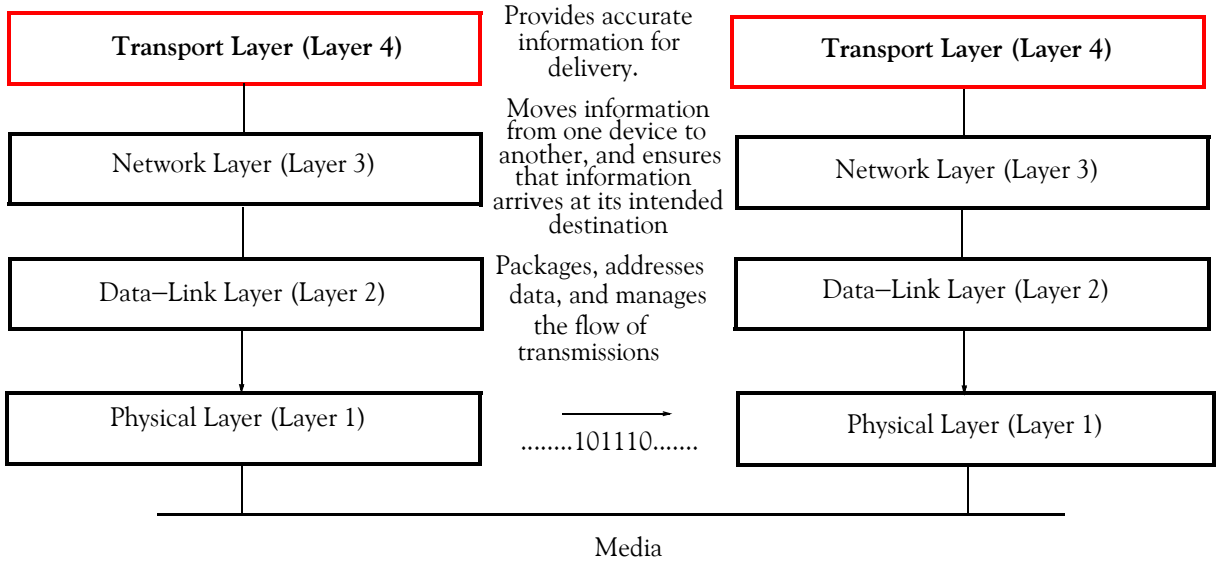


Figure 2.16. The Transport layer

Unlike the Network layer, the connections at the Transport layer are considered *connection oriented*.* Data passed through this layer will be acknowledged by the destination device. If an acknowledgment is not received in a specified time–out period, the data is re–sent.

2.6.5 Session Layer

The fifth layer of the OSI model is the Session layer. This layer lets users establish a connection — called a session — between devices. A network session is analogous to a computer terminal session where a user logs in, performs a task by sending keystrokes, receives text characters on his monitor, and then logs out. Once the connection has been established, the Session layer can manage the dialogue. Figure 2.17 shows the Session layer communications.

The Session layer attempts to establish a session between two stations. Security and name recognition are performed at this layer before data is transmitted back and forth. As the data is transmitted, this layer inserts checkpoints to indicate where receipt of data has been acknowledged. If connection between two stations is lost, only the data from the last checkpoint need to be re–transmitted.

* *Connection–oriented communication uses a procedure to ascertain that each recipient receives all the data that were transmitted. If the transmitting station does not receive an acknowledgement of the data being received within a certain period of time, it re–transmits the data and doubles the amount of time that it should take to be received. Of course, when this is done, the transmission becomes slower but it is guaranteed. This process takes place no matter what type of links are used or the distance between the transmitting and receiving stations.*

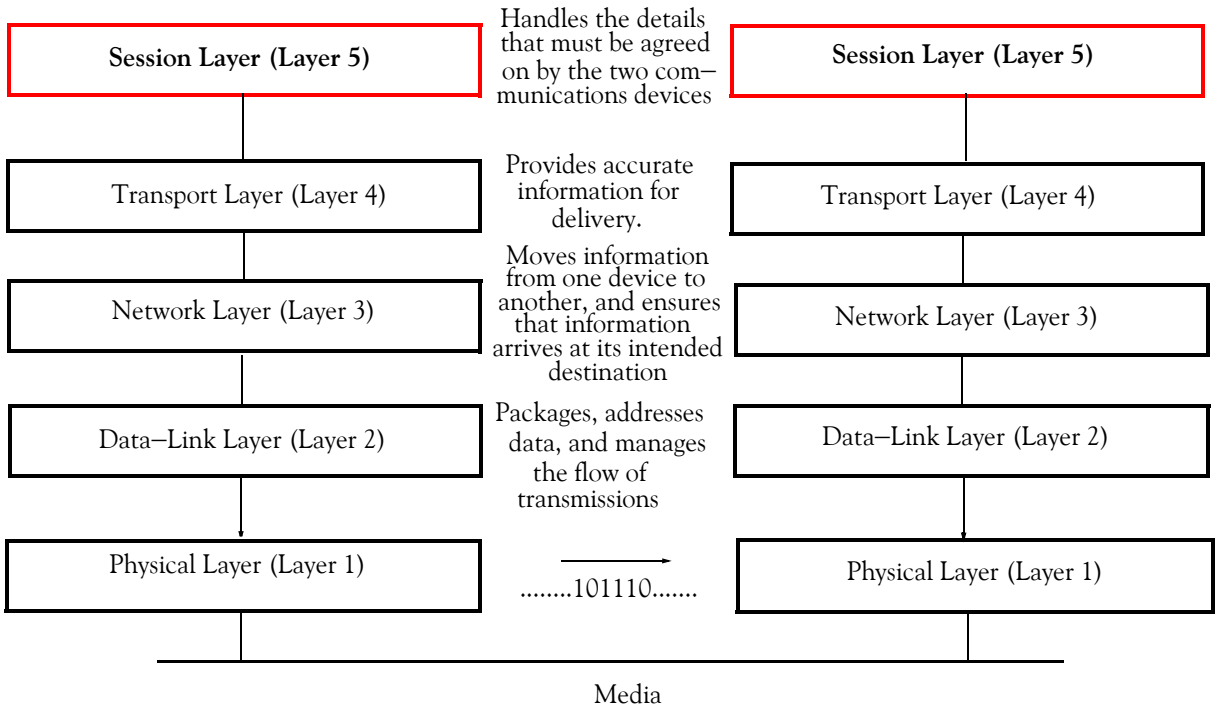


Figure 2.17. The Session layer

The Session layer establishes the communication at the beginning of a session, monitors, synchronizes, performs error–correction on the information exchanged during the session, and releases the logical link at the end of the session.

To establish a session, the user must provide the remote address to which they want to connect. These addresses are not like MAC or network addresses; they are intended for users and are easier to remember. Examples are DNS names such as www.websitename.com or computer names such as MAILSERVER01.

2.6.6 Presentation Layer

The sixth layer of the OSI model, the Presentation layer, negotiates and establishes the format in which data is exchanged. This layer is responsible for any character set or numeric translations needed between devices. It is also responsible for data compression to reduce the amount of data transmitted, as well as encryption. Figure 2.18 shows the Presentation layer communications.

As the packets come up the stack, the Presentation layer translates the intermediary format that was used for transporting the packet back into a format that the Application layer can use. This layer also encrypts data, converts character sets, expands graphic commands, and manages data compression.

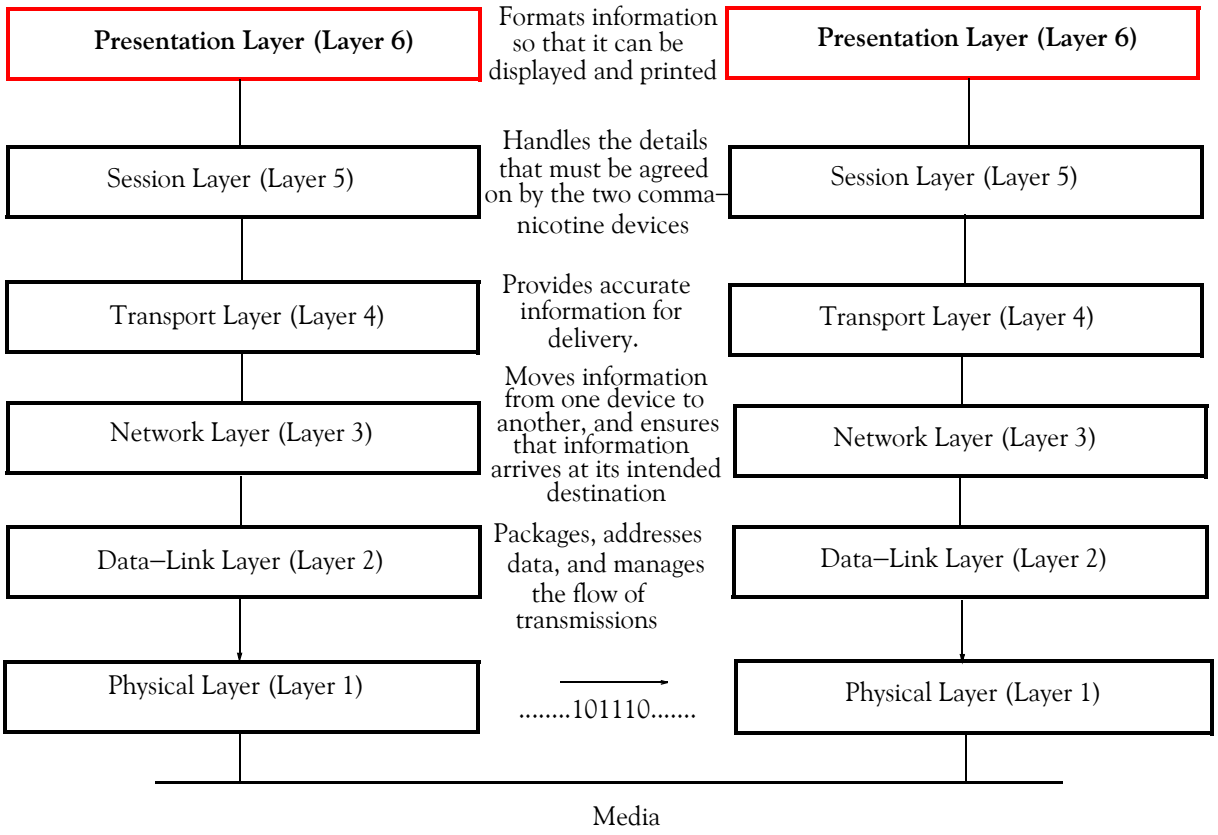


Figure 2.18. The Presentation layer

The Presentation layer is a context–sensitive layer. It can be thought of as the common language and image that the users at both ends use and understand. The Presentation layer also formats data for screen display or for printing.

The Presentation layer takes care of the job of sending the bits in the correct order. Should the destination device receive the information out of order, the data would be extremely garbled. As with bit order, different computers read the order of bytes in different ways. Some computers designate the least significant byte first; others use the most significant byte first.

Within the internal construction of computers, there are no such things as letters and punctuation marks – computers use numbers to represent everything. Since they can only use numbers, they need some way to correspond letters to some sort of numeric convention. Computers use character codes to represent the numbers and letters that users see. The codes are normally binary numbers that directly relate to a physical character. For example, on an IBM compatible the letter A is decimal number 65, which relates to binary 01000001. The ASCII and EBCDIC codes are discussed in Appendix B.

2.6.7 Application Layer

The top layer of the OSI model is the Application layer. This layer is the interface between the user's application and the network. It allows the application that the user sees to transfer files, send e–mail, and do anything else it needs to on the network. This should not be confused with the actual application that the user is running. Figure 2.19 shows Application layer communication.

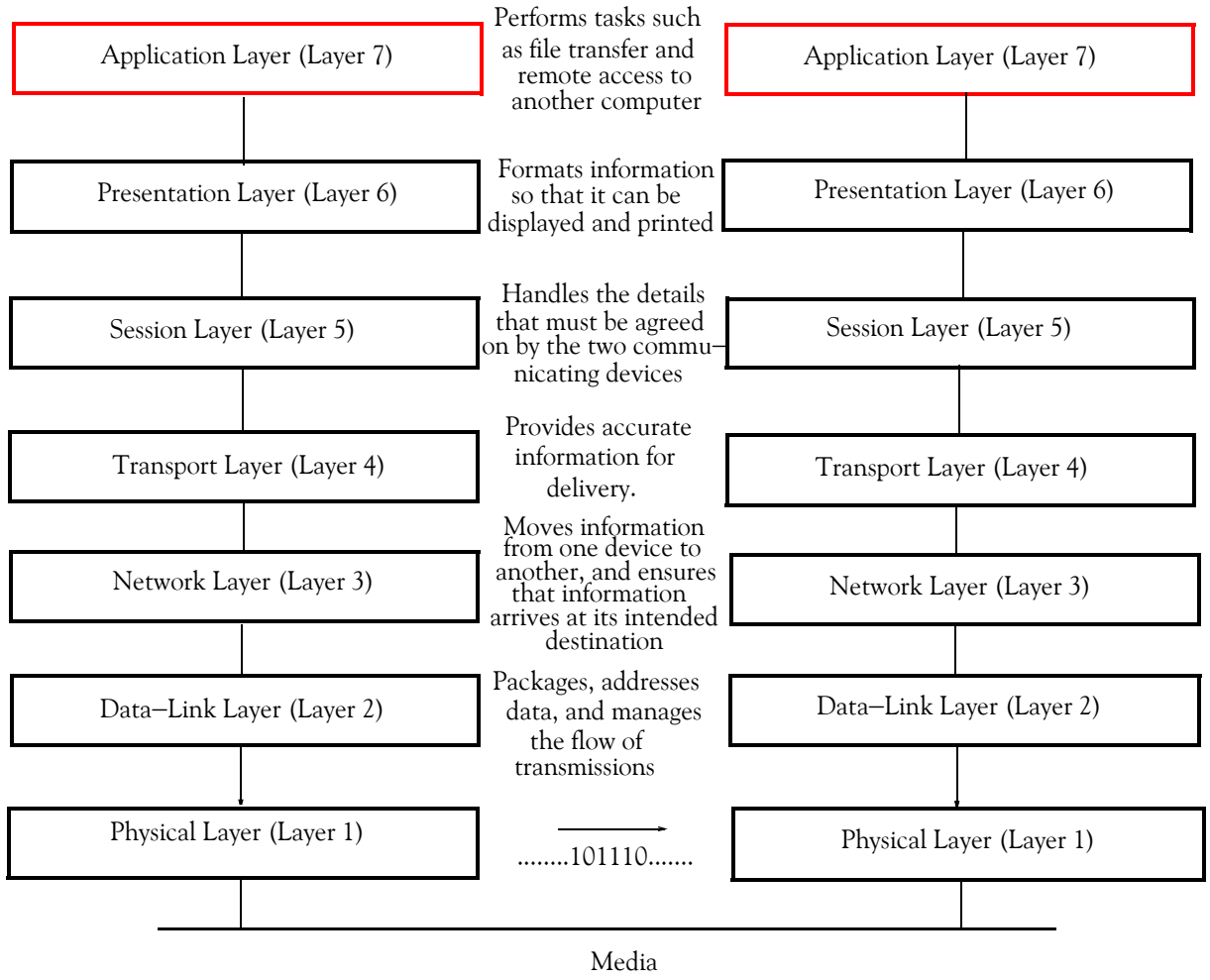


Figure 2.19. The Application layer

The Application layer runs network applications such as e–mail, Web browsing (HTTP), FTP, and other network tasks. It does not run applications such as word–processing and spreadsheets. When the user makes a request that requires access to the network, the Application layer presents a collection of functions that allows programs to access an internal environment known as Application Program Interfaces (APIs) from which the user can choose. An example of an API is Microsoft's DirectX which is a collection of application programming interfaces (APIs) for

handling tasks related to multimedia, especially game programming and video, on Microsoft platforms. This layer handles error recovery and network access.

2.7 The IEEE 802 Standards

A set of standards developed by the IEEE to define methods of access and control on local area networks. Unlike the theoretical OSI model, the 802 standards are documented, real–world standards that define different technologies, such as Ethernet. The IEEE 802 standards correspond to the physical and data–link layers of the ISO Open Systems Interconnection model, but they divide the data–link layer into two sublayers. The logical link control (LLC) sublayer applies to all IEEE 802 standards and covers station–to–station connections, generation of message frames, and error control. The media access control (MAC) sublayer, dealing with network access and collision detection, differs from one IEEE 802 standard to another: IEEE 802.3 is used for bus networks that use CSMA/CD, both broadband and baseband, and the baseband version is based on the Ethernet standard. IEEE 802.4 is used for bus networks that use token passing; and IEEE 802.5 is used for ring networks that use token passing (token ring networks). In addition, IEEE 802.6 is an emerging standard for Metropolitan Area Networks, which transmit data, voice, and video over distances of more than five kilometers.

The major 802 standards are listed below. Others can be found on the Internet.

802.1d This standard created what is now known as the *spanning tree algorithm.*[*] The spanning tree algorithm is used by transparent bridges[†] (we will discuss these in Chapter 5). They use this algorithm to detect other bridges on the network, remove loops, and to detect when another bridge fails.

802.2 This standard defines the standards for the LLC sublayer of the Data Link layer. We recall that the Data Link layer of the OSI model is made up of two parts. The two parts are the LLC sublayer and the MAC sublayer. The MAC sublayer varies for different network types and is defined by standards IEEE 802.3 through IEEE 802.5.

802.3 This is a collection of IEEE standards defining the physical layer, and the media access control (MAC) sublayer of the data link layer for bus networks that use CSMA/CD in a wired Ethernet. Physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper wire or fiber cable.

802.3u This defines the standard of the 100 Mbps Ethernet known as *Fast Ethernet.*

---

* *A spanning tree algorithm builds and stores a table of ports associated with destination addresses. The algorithm is specifically constructed to avoid bridge loops (multiple paths linking one segment to another, resulting in an infinite loop situation). The algorithm is responsible for a bridge using only the most efficient path when faced with multiple paths. If the best path fails, the algorithm recalculates the network and finds the next best route.*

† *These are networking devices that use hardware network adapters (cards) that contain addresses so that the network will know which data to pass and which should be filtered out.*

802.3z This defines the standard of the1000 Mbps Ethernet known as *Gigabit Ethernet.*

802.4 This standard defines the medium access control (MAC) sublayer for bus networks that use a token–passing mechanism (token bus networks). These types of networks will be discussed in Chapter 4. The IEEE 802.4 Working Group has been disbanded.

802.5 This standard defines IBM's Token Ring network standard. This standard uses a logical ring topology (discussed in Chapter 4) running at 4 or 16 megabits.

802.6 This standard defines standards for MANs. The main purpose of this standard is to define Distributed Queue Dual Bus (DQDB), a distributed multi–access network that supports communications using a dual bus and distributed queuing.

802.7 This standard defines broadband local area networks (LANs) using coaxial cable. This standard was developed for cable Internet companies. It is presently inactive.

802.8 This standard defines a LAN standard for fiber optic media used in token passing computer networks like FDDI,* and was created by the Fiber Optic Technical Advisory.

802.9 This standard defines standards for integrated voice and data access over existing Category 3 twisted–pair network cable installations. Its major standard was usually known as *isoEthernet*.†

802.10 This standard defines Network security issues. It provides a method for secure bridging of data across a shared backbone. It defines a single frame type known as the Secure Data Exchange (SDE), a MAC–layer frame with an IEEE 802.10 header inserted between the MAC header and the frame data. A well–known Logical Link Control Service Access Point notifies the switch of an incoming IEEE 802.10 frame.

802.11r This standard, commonly referred to as Wi–Fi, allows continuous connectivity aboard wireless devices in motion, with fast and secure transfers from one base station to another managed in a seamless manner. It operates in the 2.4 GHz and 5 GHz public spectrum frequencies.

802.12 This standard defines a variety of 100 Mbit/s plus technologies, including 100BaseVG–AnyLAN. 100BaseVG is a 100 Mbit/s Ethernet standard specified to run over four pairs of category 3 UTP wires (known as voice grade, hence the "VG"). It is also called 100VG–AnyLAN because it was defined to carry both Ethernet and token ring frame types. 100BaseVG was originally proposed by Hewlett–Packard but it is now extinct.

---

* *Fiber distributed data interface (FDDI) provides a standard for data transmission in a local area network that can extend in range up to 200 kilometers (124 miles). It is discussed in Chapter 4.*

† *The isoEthernet, lost its marketplace to the rapid adoption of Fast Ethernet and the isoEthernet working group was disbanded.*

2.8 Summary

In this chapter we briefly discussed some protocols, in order to establish their relationship with the OSI model. These and other protocols are discussed in more detail in Chapter 3. We also introduced several network devices and identified those that operate at different layers of the OSI model. The characteristics of these devices are discussed in Chapter 5.

Protocol suites are the real–world implementation of the OSI model. The OSI model has seven layers, each of which outlines tasks that allow different devices on the network to communicate.

- The Physical layer specifies transmission of bits across the network media.
- The Data Link layer packages data into frames and provides for reliable transmission of data. This layer contains the Media Access Control and Logical Link Control sublayers.
- The Media Access Control sublayer is responsible for access to the network media. Access can be provided using a contention or deterministic system. In a contention–based system, any device can transmit when it needs to. Deterministic systems require that a device first possess the right to transmit. Ethernet is a contention system, while Token Ring is deterministic.
- The Logical Link Control sublayer establishes and maintains network connections and performs flow control and error checking.
- The Network layer is responsible for routing data across the network. Data is converted to datagrams at this layer, which are sent using connectionless transmission to a specific network address.
- The Transport layer provides end–to–end reliability using connection–oriented transmissions. Data at the Transport layer is packaged in segments and sent using connection–oriented transmissions, in which an acknowledgment is sent after data is received. If the sender receives no acknowledgment, the data is then re–sent.
- The Session layer allows users to establish communications between devices using easily remembered computer names. Dialogue between devices is managed at this layer. At the Session layer, data is packaged as packets.
- The Presentation layer negotiates and establishes the format for data exchange. Data compression and translation are handled at this layer.
- The Application layer is the final layer of the OSI model. At this layer all of the interaction between the user's application and the network is handled.
- 802.3 is the standard that describes CSMA/CD, used in Ethernet.
- 802.5 defines the logical ring topology used in Token Ring.
- 802.11 defines wireless networks.

2.9 Exercises

True/False

1. The Application layer of the OSI model runs applications such as databases such as MS Access, spreadsheets such MS Excel, and word–processing such as MS Word. _____
2. The Physical layer of the OSI model will transmit data only if these are in ASCII format. _____
3. The Physical layer of the OSI model will transmit data only if a parity bit is present. _____
4. CSMA/CA is a more reliable method of collision detection than CSMA/CD. _____
5. Distance–vector routing protocols are used in static routing methods. _____
6. CRCs can perform both error detection and error correction. _____
7. Datagrams are groups of data that contain addressing information also. _____
8. Repeaters operate exclusively at the Network layer of the OSI model. _____
9. Routers are normally operated at the Physical layer of the OSI model. _____
10. Brouters and switches can operate at any of the seven layers of the OSI model. _____

Multiple Choice

11. Access to the network media is provided by the _____ layer of the OSI model.

    A. Transport
    B. Network
    C. Physical
    D. Data Link

12. The _____ layer of the OSI model does not recognize data frames.

    A. Physical
    B. Network
    C. Presentation
    D. Session

13. The _____ layer of the OSI model breaks large messages into packets.

    A. Network
    B. Session
    C. Transport
    D. Data Link.

14. The _____ layer of the OSI model establishes connection between two devices.

    A. Transport
    B. Session

C. Network
D. Application

15. The _____ layer of the OSI model addresses messages and translates names and logical addresses into physical addresses.

A. Transport
B. Data Link
C. Network
D. Presentation

16. The _____ layer of the OSI model provides CRC to detect data errors.

A. Data Link
B. Transport
C. Network
D. Session

17. The User Datagram Protocol (UDP) in the TCP/IP suite operates at the _____ layer of the OSI model.

A. Network
B. Data Link
C. Session
D Transport

18. The Internet Protocol (IP) in the TCP/IP suite operates at the _____ layer of the OSI model.

A. Session
B. Transport
C. Network
D. Data Link

19. The IEEE 802.5 standard implements a way for preventing collisions on the media of a network using a method known as

A. CSMA/CD
B. CSMA/CA
C. Token Passing
D. None of the above

20. The IEEE standard that defines how Ethernet operates is known as

A. IEEE 802.1
B. IEEE 802.3
C. IEEE 802.11
D. IEEE 802.12

Problems

21. As a network administrator, you are preparing for a presentation to explain the functions of each of the seven layers of the OSI model. You may use a brief sentence in explaining the function of each layer. You may also use a metaphor by comparing each layer to the postal service.

22. After you took over the position of the previous network administrator who left the company, everything seemed to be working OK. Ten days later a segment of the network failed and the data were not re–routed properly as they should. You suspected that the problem would be with a router in the network. What would you check before replacing the router?

2.10 Answers to End–of–Chapter Exercises

True/False

1. F – Review Page 2–35

2. F – Review Page 2–22

3. F – Review Page 2–22

4. T – Review Page 2–9

5. F – Review Page 2–30

6. F – Review Page 2–10

7. T – Review Page 2–19

8. F – Review Page 2–22

9. F – Review Page 2–27

10. F – Review Pages 2–15, 2–17

Multiple Choice

11. D. Data Link. The Media Access Control sublayer of the Data Link layer provides access to the media using addressing, contention, or deterministic methods.

12. A. Physical. This layer just transmits bits of data across the network media. The other layers recognize and handle frames of data between clients.

13. C. Transport. If a message is too large, this layer divides the message into smaller pieces before transmission. These pieces are gathered and reassembled at the receiving station.

14. B. Session. The Session layer establishes communications between devices. This layer also verifies the identity of the party at the other end of the communication path.

15. C. Network. This layer translates and routes data across the network. Data is converted to datagrams and using connectionless transmission, the data are sent to a specific network address.

16. A. Data Link. This layer adds the CRC code to the end of the data frame to provide error detection.

17. D. Transport. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) in the TCP/IP suite and the Sequence Packet Exchange (SPX) of the NetWare IPX/SPX suite operate at this layer.

18. C. Network. IP is an addressing protocol and as we know, the Network layer translates a logical address into a physical address.

19. C. Token Passing. This is a method that token–ring networks use to avoid collisions using a token. With this method, the only device that can transmit data packets is the one that has the token. When this device is finished with the transmission of data, it passes the token to the next device.

20. B. IEEE 802.3. This standard is also known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Problems

21. Let us assume that a user is running some sort of chat application on their computer that enables them to connect to another person's computer and talk to that person over a network. The user types the message "Hello Everybody" into the chat application. The Application layer passes the data from the user's application to the Presentation layer. At the Presentation layer the data is translated and encrypted. The data is then passed to the Session layer, where the dialogue is set for full–duplex communication. The Transport layer packages the data as segments. The recipient's name is found by the corresponding Internet Protocol (IP) address. CRCs are added for error checking.

Next, the Network layer packages the data as datagrams. After examining the IP address, the destination device is discovered to be on a remote network. The IP address for the intermediate device is then added as the next destination. Data is sent to the Data Link layer, where it is packaged as frames. The physical address of the device is resolved. This is the address belonging to the intermediate device, which will forward the data on to its destination. The access type for the network is determined to be Ethernet.

The data is then passed on to the Physical layer on the left side, where it is packaged as bits and sent from the network adapter across the transmission media. The intermediate device reads the bits off the network media at the Physical layer on the right side. The Data Link layer packages the data as frames. The physical address of the destination device is resolved to its IP address. The Network layer packages the data as datagrams. After examining the IP address of the destination device, the location of this device on the network is determined. The data is passed back to the Data Link layer, where it is again packaged as frames. The IP address is resolved to the MAC address. The access type for the network is determined to be Ethernet.

It is then passed on to the Transport layer. Data is compiled into segments, and error checking is performed. CRCs are performed to determine that the data is error free. The Session layer acknowledges that the data has been received. At the Presentation layer the data is translated and unencrypted. The Application layer then passes the data from the Presentation layer on to the user's chat application. The message "Hello Everybody" then appears on the recipient user's screen.

The metaphor, using the US Postal Service would be as follows:

Physical layer – The postal service dispatching method (trucks, trains, airplanes

Data Link layer – The recipient's address with the ZIP code written on a letter or package

Network layer – The post office physical location

Transport layer – The mailman picking up a letter or a package from a post office box to take it to the post office, or delivering to a designated address

Session layer – The packaging, envelope or package

Presentation layer – The contents of a letter or package

Application layer – The sender or recipient

Let us begin with the Application layer. The sender (Application layer) puts a letter or a gift (Presentation layer) in an envelope or a box (Session layer), writes the address of the recipient on the letter or package, and places it in a mail box.* The mailman (Transport layer) takes it to the post office (Network layer). The post office workers read the address (Data Link layer), and decide how to deliver it (Physical layer).

At the destination post office, the process is reversed, that is, the postal workers unload the truck or train or airplane, take all mail inside the post office building where it is sorted out for each mailman who in turn delivers it to the recipient.

22. The network administrator should check to find out if the routing was set to be static or dynamic. If static, it cannot establish a new route. Recall a static routing must be changed manually. However, if the routing was configured to be dynamic, it should have automatically update itself.

* *Special deliveries and certified mail correspond to the function of the MAC sublayer.*

Chapter 3

Protocols, Services, and Interfaces

This chapter discusses several protocols including X.25, TCP/IP, IPX/SPX, NetBEUI, and DNA. We learn how these protocols combine to form a suite of protocols that work at the various layers of the OSI model which were discussed in the previous chapter. It concludes with a brief discussion of popular WAN protocols.

3.1 Definitions

The word *protocol* has different meaning in different areas. It denotes the forms of ceremony and etiquette observed by the military, diplomats and heads of state. Also, it is a code of correct conduct. For instance, we may hear the expressions a "violation of safety protocols" or we must "observe academic protocols". In computer science language protocol implies a standard procedure for regulating data transmission between computers. As such, they specify packet size, information in the headers, how data are stored in the packet, and so on.

Most protocols are grouped together in a suite. One protocol usually covers only one aspect of communications between devices. For example, the TCP/IP suite has multiple protocols, including one for file transfer, another for e–mail, and a third for routing information.

3.2 The X.25 Protocol

The X.25 protocol was one of the first protocols of world–wide acceptance. It was introduced in 1974 by the International Consultative Committee for Telephony and Telegraphy (CCITT) to define the rules governing the use of a common packet switching network. It was developed jointly by US, England, Canada, France and Japan. It was adopted by the European Common Market for the EURONET network which is a packet switching network.

Basically, X.25 is a data communications interface protocol that was developed to describe how data passes into and out of public data communications networks. It operates at ISO model layers 1 through 3, that is, the Physical, Data Link, and Network layers. Although in the United States and other developed countries it has been superseded by newer protocols, it may be suitable for connection services to other less developed countries in Africa, South America, and Asia. A brief discussion of X.25 will serve as a good introduction to protocols.

X.25, when used, it is implemented in WANs throughout the world where no other services are available and around relatively unreliable telephone line communications. Although X.25 networks are implemented with speeds up to 64 Kbps, error checking and flow control slow down X.25 considerably. Accordingly, it is not suitable for LANs which typically require speeds of at

least 1 Mbps. Other technologies such as Asynchronous Transfer Mode (ATM) and frame relay are now more suitable for internetworking. More details are discussed later in this chapter.

Figure 3.1 shows the so–called *Public Packet Switching Network* (PPSN) and the processors within PPSN are referred to as *Data Circuit Equipment* (DCE). The compatible equipment used with the X.25 were referred to as *Data Terminal Equipment* (DTE). Accordingly, the X.25 protocol defined the communications interface between DCEs and DTEs.

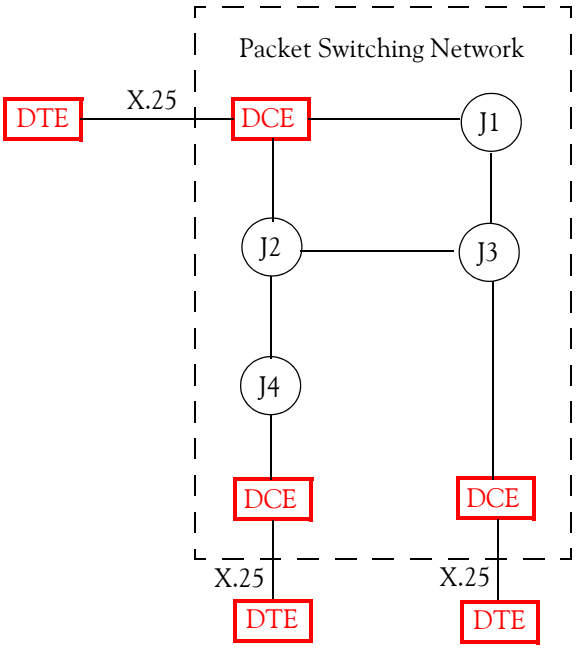


Figure 3.1. Public Packet Switching Network (PPSN)

The levels of the X.25 protocol are shown in Figure 3.2.

The Physical level shown in Figure 3.2 specifies the media used for linking the transmitter and receiver terminals. These can be wired or wireless.

The *Data Link* specifies the procedures of data transfer between the network and the sending or receiving station. Thus, in Figure 3.1 the data link controls the transfer of data between the user (DTE) and the network (DCE). This transfer includes control transmissions for initiating, sequencing, checking, and terminating the exchange of user information. The data link procedures are defined in terms of commands and responses, and may be thought of as two independent but complementary transmission paths that are superimposed on a single physical circuit. Thus, the DTE controls its transmissions to the DCE, and the DCE controls its transmissions to the DTE.

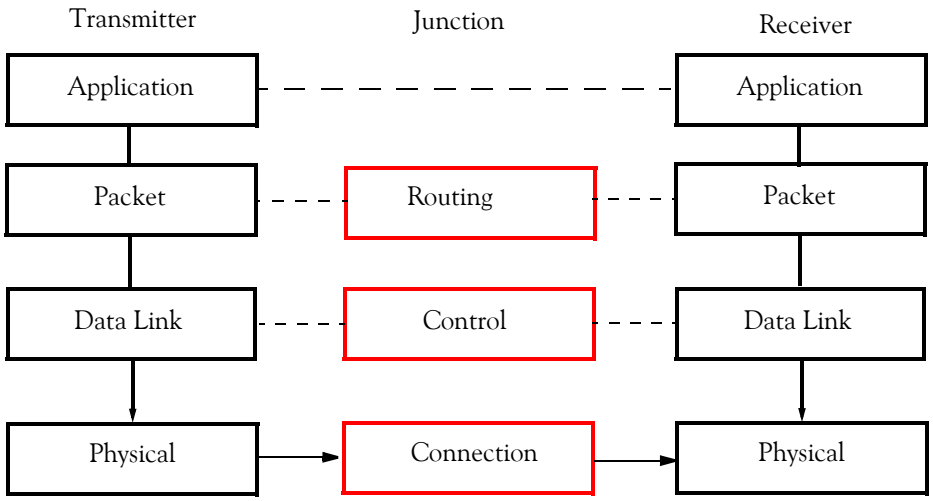


Figure 3.2. The levels of the X.25 protocol

3.2.1 Synchronization

To transmit information through the Data Link, the link must first be synchronized. This is accomplished by enclosing each frame* with unique bit patterns called *flags* as shown in Figure 3.3.

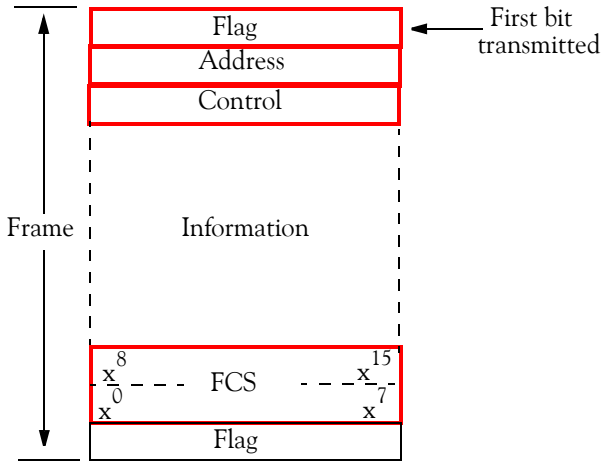


Figure 3.3. Frame Structure in X.25

* *We recall that in synchronous communications, a package of information transmitted as a single unit known as frame. Every frame follows the same basic organization and contains control information, such as synchronizing characters, station address, and an error–checking value, as well as a variable amount of data. For example, a frame used in the widely accepted HDLC and related SDLC protocols begins and ends with a unique flag (01111110).*

Once the receiving end recognizes the first flag, it knows that it is in step with the transmitter and ready to accept the content of the frame. Likewise, when the receiver recognizes the second flag, it knows that all information has been received. The flag bit pattern is 01111110 and in order to insure that a flag sequence is not misinterpreted, the transmitting station examines the frame content between the two flags which includes the address, control, information, and *Frame Control Sequence* (FCS) and inserts a 0 after all sequences of five consecutive 1 bits to insure that a flag sequence is not repeated. The receiving station then removes any 0 bit which directly follows five consecutive 1s.

3.2.2 Sequence of Operation

Figure 3.4 is a simple flowchart that shows a simple binary communications protocol.

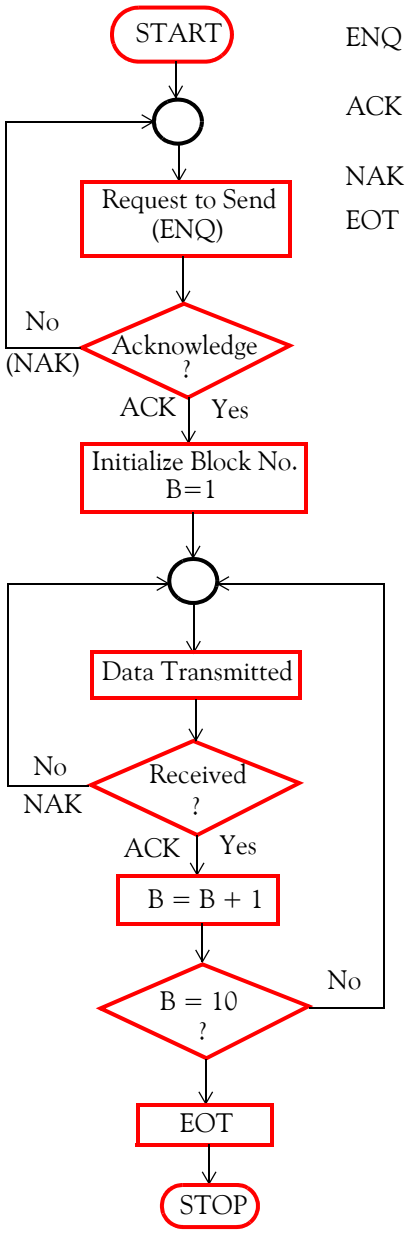
3.2.3 Commands and Responses

The frame structure of the X.25 data link control protocol has three variations and these are shown in Table 3.1.

1. *Information Frames* are used to perform an information transfer and also to respond to a correctly transmitted information frame.
2. *Supervisory Frames* are used to perform link control functions responding to received information frames.
3. *Unnumbered Frames* are used to provide additional link control functions such as those shown in Table 3.1.

TABLE 3.1 Commands and Responses Used in the Frame Control Field, Listed by Frame Type

Information Frames Commands Information Transfer			
Supervisory Frames			
		Responses	
		RR RNR REJ	Receive Ready Receive Not Ready Reject
Unnumbered Frames			
SARM DISC	Set Asynchronous Response Mode Disconnect	UA CMDR	Unnumbered Acknowledge Command Reject



ENQ = Enquiry Signal – It is initiated whenever the transmitter wishes to make contact with the receiver

ACK = Acknowledgement Signal – The receiver responds with this signal informing the transmitter that data may be sent.

NAK = Negative Acknowledgement, Control Code ASCII Character 21

EOT = End Of Transmission

The data to be sent are divided in blocks (frames) and the transmitter keeps track of these by a numbering system. Thus, the transmitter initializes Block Number 1 (B=1) and transmits that block. If the receiver acknowledges reception of the first block and if everything goes well, the transmitter will send the remaining blocks (total of ten for this example) and will check to see if all blocks have been sent. Subsequently, the transmitter will terminate the communication by sending an End of Transmission signal (EOT).

Note: This flow chart is an oversimplification of the actual operation since it suffers from one serious flow, i.e., if the receiver sends a NAK, the flow chart enters an endless loop. This problem is solved by employing a Retry (Time Out) counter that would limit the number of times a transmitter would request to send data to a particular receiver.

Figure 3.4. An oversimplified flow chart to show the initiation of binary transmission

3.2.4 Link Control

The link is controlled by means of the two bytes that follow the opening flag. These bytes are:

1. *The Address Byte* used to distinguish between command and responses made by the DCE or DTE terminals at either end of the link A typical four–wire, full–duplex link is shown in Figure 3.5.

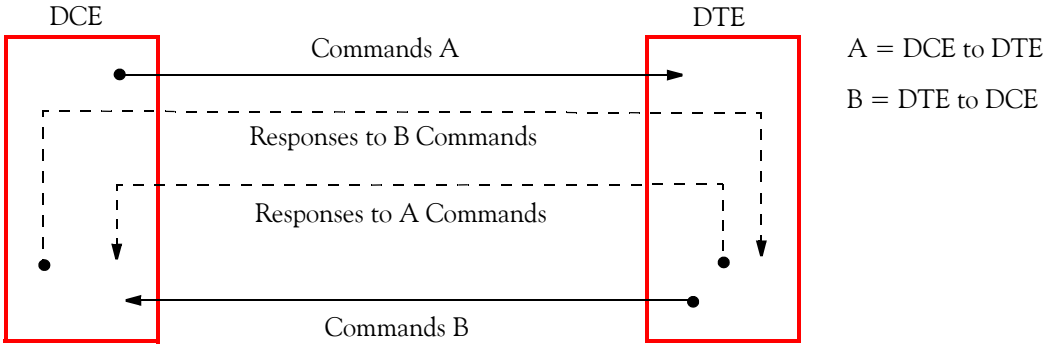
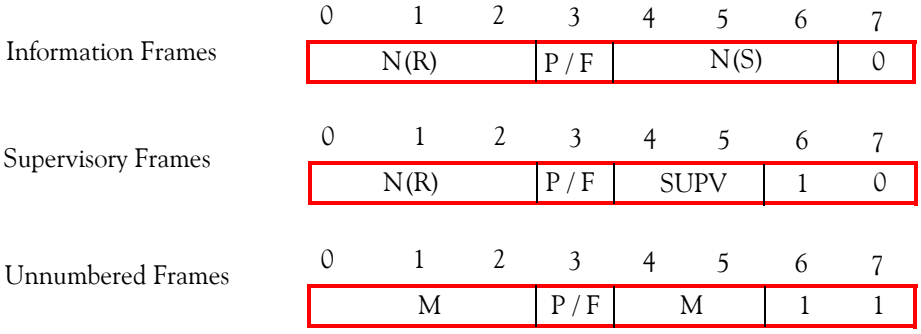


Figure 3.5. Four–wire, full–duplex link

In Figure 3.5, frames containing *commands* transferred from DCE to DTE will contain address A, and frames containing *responses* transferred from DTE to DCE will contain address A also. Likewise, frames containing *commands* transferred from DTE to DCE will contain address B, and frames containing *responses* transferred from DCE to DTE will contain address B also.

2. *The Control Byte* contains specific command and response identification as well as sequence numbers, if applicable. The contents of the control field depend on the frame type, i.e., information, supervisor, or unnumbered as shown in Table 3.1. Figure 3.6 shows the Frame control field listed by frame type.



N(S) = Sequence number of the frame containing this control field

N(R) = Sequence number of the next frame the transmitter expects to receive

P / F = Poll / Final bit – Command sets Poll; Response sets Final

SUPV = Up to four supervisory functions are available

M = Some additional control functions

Figure 3.6. Frame Control Field listed by Frame Type

Next, we discuss the methods of initiating the link, transferring information, and terminating the link.

3.2.5 Initiation of the Link

Each station (DTE or DCE) initiates its own command and response. Initiation is carried out by the *Set Asynchronous Response Mode* (SARM) command whose function is to place the addressed station in the asynchronous mode, thus enabling the two–way simultaneous asynchronous exchange of information. Figure 3.7 shows how the DTE–DCE link is set up.

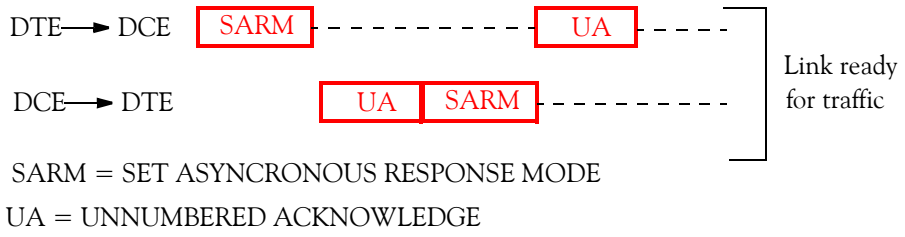


Figure 3.7. Setting up the link (no errors)

When SARM is sent out from DTE to DCE, a timer (not shown) is set–up and when SARM is received, DCE replies with *Unnumbered Acknowledge* (UA), and thus initiation in one direction is established and the timer is reset. Then DCE sends out a SARM and when it receives UA, initiation in both directions is confirmed.

If the timer expires before UA is received, the transmitting station will retransmit SARM and restart the timer as shown in Figure 3.8. The number of tries is specified when the link is implemented.

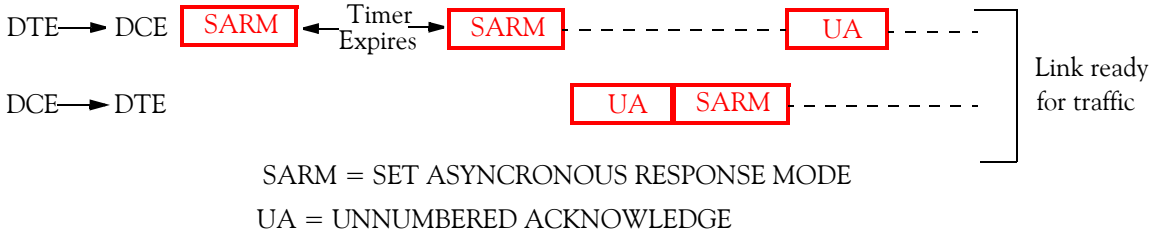


Figure 3.8. Time expiration in setting up the link

The system recovers from transmission errors using cyclic redundancy checking and from procedural errors, such as the receiving station receiving an illegal command, by referring it to the next highest protocol level.

3.2.6 Information Transfer

Information transfer is carried out via the information frame control field format shown in Figure 3.6. Both the transmitting and receiving stations maintain send and receive counters which cycle from 0 to 7 to keep track of the number of outstanding frames awaiting acknowledgement up to a maximum of seven. Figure 3.9 shows a two–way information transfer.

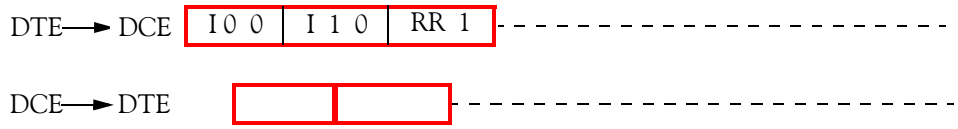


Figure 3.9. Information exchange between transmitter and receiver

In Figure 3.9, the first (left) information frame in the DTE – DCE direction contains *I 0 0* in the control field where *I* is the information frame, the first *0* is the sequence number, and the second *0* is the sequence number of the next frame the transmitter expects to receive. *Receive Ready* (RR) is a supervisory frame. Other supervisory frames are *Receive Not Ready* (RNR), and *Reject* (REJ).

3.2.7 Termination

When the transmission link is no longer required for information transfer, a disconnect command is issued to terminate the link.

3.2.8 Error Detection

The error detection method recommended by the X.25 protocol is the CRC and uses the generator polynomial

$$x^{16} + x^{12} + x^5 + 1$$

3.2.9 Protocol Implementation

Protocol for the data link of X.25 can be implemented using either software or hardware. Years ago, the Motorola MC6854 and Intel 8273 were hardware data link controllers and contained several features such as *Frame Control Sequence* (FCS) generation and checking, flag detection and synchronization, and full–duplex operation.

3.3 Protocols Currently in Use

In this section we will discuss modern day protocol suites in this chapter, we will see how they relate to the OSI model. Before discussing the first suite of protocols, we must define routable and non–routable protocols, and review the definitions of connectionless, and connection–oriented protocols.

3.3.1 Routable Protocols

A *routable* (or routing) protocol is one that is used to route data from one network to another by means of a network address and a device address. TCP/IP is an example of a routable protocol. In other words, a routable protocol coordinates the exchange of routing updates to notify other routers of routing changes and applies an algorithm to recalculate optimal routes through the internetwork.

Routable protocols are more complex than nonroutable protocols since they require more layers to implement the routing changes. In our discussion of protocols in this chapter, we will find out which protocols can be routed and which cannot. In the case of protocol suites, we'll learn which protocol in the suite handles the routing.

We recall from the previous chapter that there are three types of routing protocol architectures, distance–vector routing, link–state routing, and hybrid routing.

3.3.2 Nonroutable Protocols

Nonroutable protocols do not use routers and thus computers that are not located on the same network segment or subnet cannot communicate. They are limited to smaller LANs and thus their use is very limited. *NetBEUI* (NetBIOS Extended User Interface) is an example of an nonroutable protocol. It is an enhanced version of the NetBIOS protocol and allows computers which are within the same local area network to communicate with each another. NetBEUI (pronounced net–BOO–ee) formalizes the frame format (or arrangement of information in a data transmission) that was not specified as part of NetBIOS. NetBEUI was developed by IBM for its LAN Manager product and has been adopted by Microsoft for its Windows NT, LAN Manager, and Windows for Workgroups products. Hewlett–Packard uses it in comparable products.

NetBEUI is the best performance choice for communication within a single LAN. Because, like NetBIOS, it does not support the routing of messages to other networks, its interface must be adapted to other protocols such as Internetwork Packet Exchange or TCP/IP. A recommended method is to install both NetBEUI and TCP/IP in each computer and set the server up to use NetBEUI for communication within the LAN and TCP/IP for communication beyond the LAN.

Another nonroutable protocol is *Data Link Control* (DLC) which is discussed on Page 3–24. This is an error–correction protocol in the *Systems Network Architecture* (SNA), also discussed on Page 3–24, used for transmission of data between two nodes over a physical link. Printers on a network use the DLC protocol.

3.3.3 Connectionless Protocols

Connectionless communication is achieved by passing, or routing, data packets, each of which contains a source and destination address, through the nodes until the destination is reached. No verification that the data reached its destination is required. It is analogous to mailing a letter or package to someone and no delivery receipt was requested. Likewise, connectionless protocols are those that specify how data is being send out across the network with no knowledge as to whether it arrived at the destination device.

A well known connectionless protocol is the *User Datagram Protocol* (UDP) which is a protocol within TCP/IP and operates at the Transport layer in the ISO/OSI model. UDP converts data messages generated by an application into packets to be sent via IP but does not verify that messages have been delivered correctly.

UPD is more efficient than TCP which is connection–oriented, so it is used for various purposes, including SNMP.* Some applications use connectionless protocols to send out e–mail, audio, or video messages.

3.3.4 Connection–Oriented Protocols

In connection–oriented transmission mode, the chain of links between the source and destination nodes forms a logical pathway connection. However, an acknowledgement is required from the destination that the completion of each step of the transmission was successful. This is analogous to certified mail.

3.4 Most Commonly Used Protocol Suites

A *protocol suite* or *protocol stack* is a set of protocols that work together on different levels to enable communication on a network. For example, TCP/IP, the protocol stack on the Internet, incorporates more than 100 standards including *File Transfer Protocol* (FTP), *Internet Protocol* (IP), *Simple Mail Transfer Protocol* (SMTP), *Transmission Control Protocol* (TCP), and Telnet.† TCP/IP is the main protocol used on the Internet.

The protocol suites discussed in this chapter are the most commonly used in networking today, and they provide all the services that most network applications require. Moreover, these protocol suites normally have many protocols with different capabilities, so the needs of the user's applications are met in most cases. Also, a suite may have more than one protocol for the handling of files.

In the past, protocol suites were dependent on the network equipment used. For example, the Digital Network Architecture (DNA) was developed in the 70s by Digital Equipment Corporation's (later Compaq and now Hewllett–Packard) and was used to connect mainframe computers. However, other present–day protocol suites such as TCP/IP and IPX/SPX can be used with many types of equipment. Some protocols and protocol suites can be mapped to the OSI model very nicely, whereas others that were developed before the OSI model development, may be mapped very loosely. The TCP/IP protocol is introduced to Subparagraph 3.4.1, and the IPX/SPX protocol is introduced to Subparagraph 3.4.5.

---

* *SNMP is an acronym for Simple Network Management Protocol. It is the network management protocol of TCP/IP. In SNMP, agents, which can be hardware as well as software, monitor the activity in the various devices on the network and report to the network console workstation. Control information about each device is maintained in a structure known as a Management Information Block (MIB). SNMP is introduced in Chapter 8.*

† *This protocol is mentioned in Chapter 2. Briefly, it described a set of procedures, that enable a user of one computer on the Internet to log on to any other computer on the Internet, provided the user has a password for the distant computer or the distant computer provides publicly available files. Telnet is also the name of a computer program that uses those rules to make connections between computers on the Internet. Many computers that provide large electronic databases, like library catalogs, often allow users to telnet in to search the databases. Many resources that were once available only through telnet have now become available on the easier–to–use World Wide Web. Please refer also to Page 3–19.*

3.4.1 TCP/IP Protocol Suite

The Transmission Control Protocol/Internet Protocol (TCP/IP) was originally developed by the Department of Defense (DoD) for communications between computers. It is built into the UNIX system and has become the de facto standard for data transmission over networks, including the Internet. The TCP/IP protocols were originally designed for a large network that served as a classified DoD project designed to maintain open communications even during war time periods. This classified project was undertaken by a branch of the DoD known as *Advanced Research Projects Agency* (ARPA). This project became known as ARPANet. With the advent of Unix and the advancement of client/server networking architecture, ARPANet was declassified in the 80s and it is now known as the Internet.

As mentioned earlier the TCP/IP protocol suite, also known as the Internet Protocol, is a suite of industry–standard protocols and can handle just about any task for the user. The popularity of TCP/IP emanates from the fact that it is not proprietary to any company, it is suitable with any network software or equipment, and one can connect multiple LANs into a large internetwork. The original designs for TCP/IP were started long before the OSI model was developed; instead of OSI's seven–layer model, TCP/IP was based on a DoD model with four layers it was shown in Figure 2.1 which is repeated here for convenience as Figure 3.10.

The four layers of the TCP/IP can be described in terms of the OSI model as follows:

- **Network Interface:** Also known as Network Access layer, this layer operates at the Physical and Data Link layers of the OSI model. When TCP/IP was developed, it was made to use existing standards for these two layers so it could work with such protocols as Ethernet and Token Ring. We recall from our discussion in Subsection 2.6.2 that transparent bridges can use MAC addresses to filter traffic between segments. Moreover, TCP/IP is suitable for any type of network connection including FDDI* and wireless transmission.
- **Internet layer:** This layer of the TCP/IP defines how IP directs messages through routers over internetworks including the entire Internet. We recall that the Network layer of the OSI model performs a very similar function.

* *FDDI is an acronym for Fiber Distributed Data Interface. It is a standard developed by the American National Standards Institute (ANSI) for high–speed fiber–optic local area networks. FDDI provides specifications for transmission rates of 100 megabits (100 million bits) per second on networks based on the token ring standard. FDDI II, an extension of the FDDI standard, contains additional specifications for the real–time transmission of analog data in digitized form. FDDI is discussed detail in Chapter 4.*

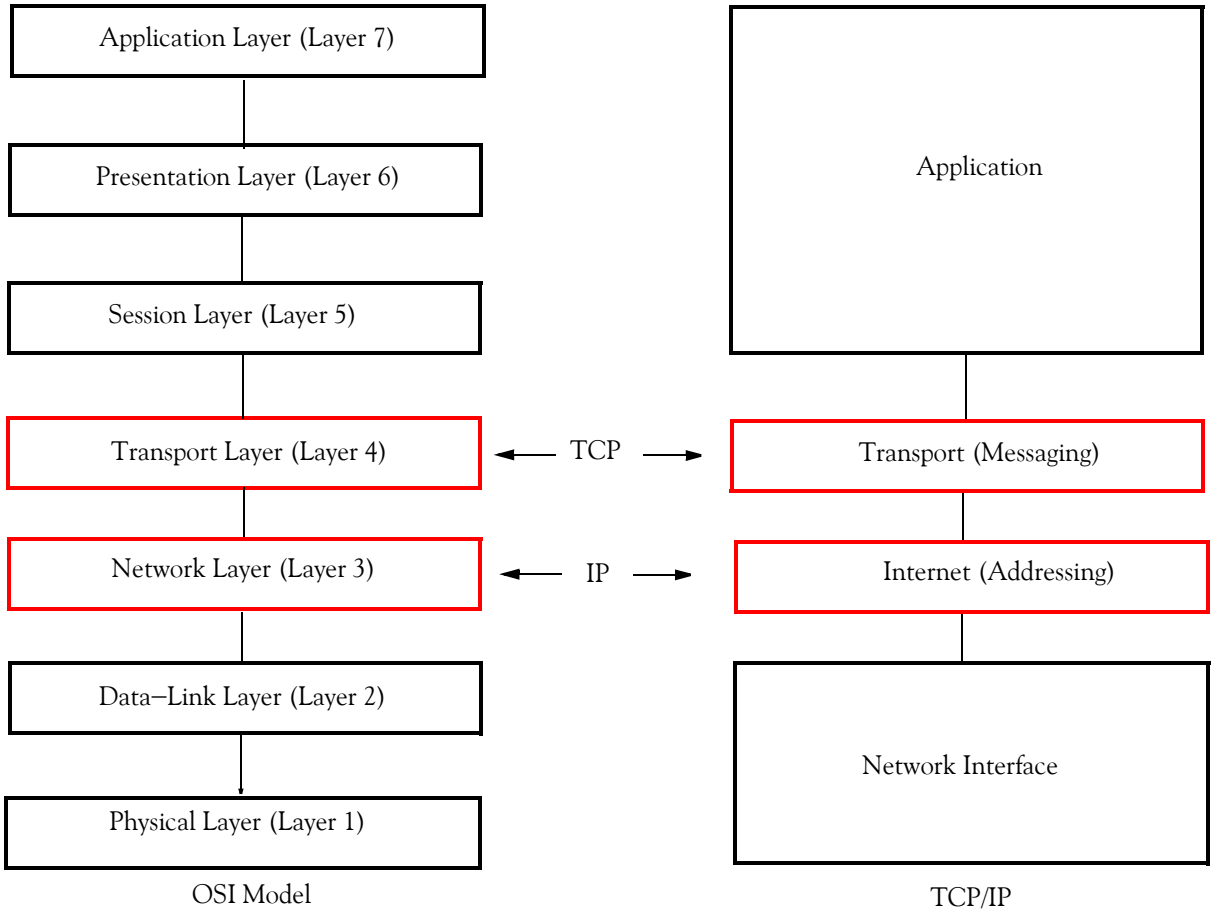


Figure 3.10. The OSI and TCP/IP correspondence (same as Figure 2.1)

- **Transport layer:** This layer is similar to the Transport layer of the OSI model. It controls and guarantees the transmission of the message packets. The User Datagram Protocol (UDP) is a connectionless protocol that is part of the TCP/IP suite. UDP is much faster but does not guarantee that the receiver will receive the data. UDP is used in place of the TCP for less critical messages. Either TCP or UDP protocol provides the transport services that are necessary to escort the messages through the TCP/IP internetworks.
- **Application layer:** This layer defines network applications to perform tasks such as file transfer and e–mail. It performs similar functions as the top three layers of the OSI model.

3.4.2 IP Addressing

All Internet addresses are *IP addresses*. These IP addresses are unique and are assigned by the *Internet Assigned Numbers Authority* (IANA). Every host on a TCP/IP network is given an IP address. This is referred to as *logical address* and it is usually assigned by the network administrator. The logical address should not be confused with the MAC address on a network card which

is a hardware address. *Domain names* such as www.samplename.com uniquely identify a company on the Internet. It is used for Web access through browsers and for e–mail addresses. A domain name is similar to a brand name or trademark. Domain names are not owned; they are leased through the *Internet Corporation for Assigned Names and Numbers* (ICANN). The three–letter extension on a typical domain name identifies the domain category. Table 3.2 lists the most familiar domain categories.

TABLE 3.2 List of common domain categories

Domain Extension	Category
.com	A commercial organization, business, or company
.edu	An educational institution
.int	An international organization
.gov	An nonmilitary government entity
.mil	A military organization
.net	A network administration
.org	Other organizations such as nonprofit, nonacademic or nongovernmental

Presently, IP addresses are 32 bits long and divided into four sections, each 8 bits long, known as *bytes* or *octets*. For convenience, these are represented as dotted–decimal numbers where each byte, separated by periods has been converted to equivalent decimal numbers. Binary–to–decimal and other number conversions are discussed in Appendix C.

In most cases, routers are used with IP addresses to forward message packets through internetworks. With this arrangement, the message packet hops from router to router as shown in Figure 3.11, where we have assumed that the IP address is 204.1.5.153.

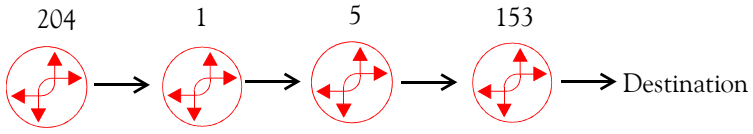


Figure 3.11. Routers used to forward message packets through internetworks.

IP addresses are assigned to both servers and clients. Within the same network, the client IP address is a subset of the server IP address. For example, if a server has the IP address 204.1.1.0, a client within the same network may have the IP address 204.1.53.142.

IP addresses are divided into five general classes. IP address classes are used to segment the pool of addresses into sizes corresponding to various organization sizes. Each class differs in the way the octets are designated for addressing networks, as opposed to hosts. When an organization requests a range of IP addresses, they receive a block from one of these classes:

Class A: Class A addresses contain the range of numbers from 0.0.0.1 to 126.0.0.0 for 126 networks and 16,777,216 hosts. The network numbers 0.0.0.0 and 127.0.0.0 are reserved

for two special classes which are not discuss here. Class A addresses have one byte for the network and three bytes for the host. For example, the address 56.88.1.231 has a network number of 56, and the remaining numbers signify the host.

Class B: Class B addresses contain the range of numbers from 128.0.0.0 to 191.255.0.0 for 16,384 networks and 65,534 hosts.Class B addresses have two bytes for the network address and the remaining two for the host address.

Class C: Class C addresses contain the range of numbers from 192.0.0.0 to 223.255.255.0 for 2,097,152 networks and 254 hosts. Class C addresses have the first 3 bytes for the network address and the fourth byte for the host address. Class C addresses are the most common.

Class D: Class D addresses contain the range of numbers from 224.0.0.0 to 239.255.255. Class D networks support multicasting.

Class E: Class E addresses contain the range of numbers from 240.0.0.0 to 255.255.255. Class E networks are used for experimentation.

The details of splitting TCP/IP addresses into networks and host addresses are discussed in various books devoted to the TCP/IP topic.

3.4.3 Subnetting

As stated above, the five Classes A, B, C, D, and E have different network and host addresses. In a normal configuration where these are used as specified, these addresses are said to be in the default configuration. For instance, in Class C consists of four bytes where the first three represent network addresses and the fourth represents host addresses. Subnetting is a procedure of using more network addresses than specified in the default configuration by infringing on the host addresses. Subnets extend to the right starting from the first byte in the default network address field.

An organization may segment the addresses given to them by using a subnet mask.* All subnet masks are four bytes long. These masks are no longer considered to be addresses; they are now overlays that define how an IP address is to be used. Subnet masks are represented as 255 in dotted–decimal format and they apply to a specific network interface within the configuration file of the router to which the subnetwork is attached. For example, an attached LAN segment may be subnetted by Cisco's software with a statement such as

```
FloorARouter (config-if) #ip address 162.35.2.1 255.255.255.0
```

* *A subnet mask, also known as address mask is a number that, when compared by the computer with a network address number, will block out all but the necessary information. For example, in a network that uses XXX.XXX.XXX.YYY and where all computers within the network use the same first address numbers, the mask will block out XXX.XXX.XXX and use only the significant numbers in the address, YYY.*

where `if` stands for interface. This statement is a command to configure this network interface on the router whose name is `FloorARouter`. The `ip address` is a command used to set the IP address for this network interface. For this example, the logical IP address is `162.35.2.1` and `255.255.255.0` tells the router to subnet the entire third byte as `255` shown in Figure 3.12.

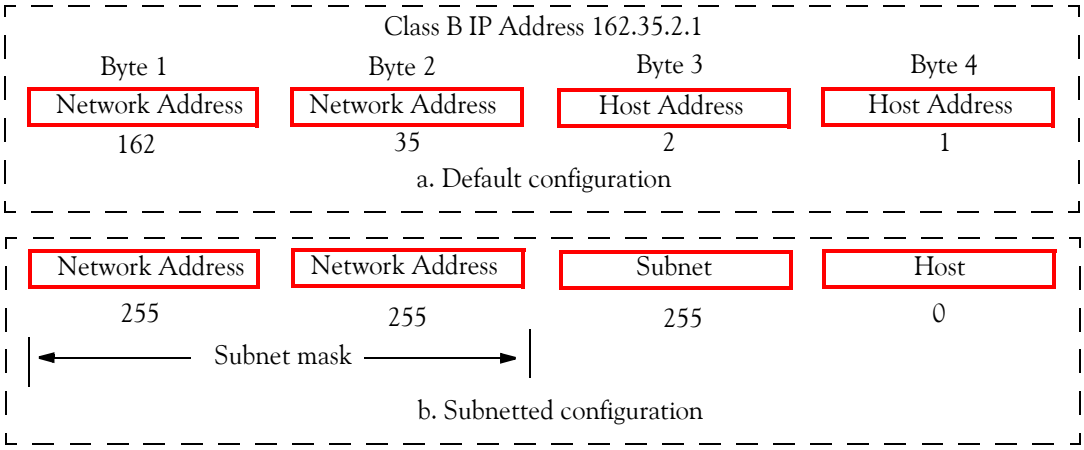


Figure 3.12. An example of subnetting

For convenience, the standard subnet masks Class A, Class B, and Class C are shown in Table 3.3.

TABLE 3.3 Standard Subnet Masks

Subnet Mask	Network Class
255.0.0.0	Class A
255.255.0.0	Class B
255.255.255.0	Class C

3.4.4 Other Protocols within the TCP/IP Suite

The Internet Protocols are made up of a lot more than just TCP and IP, though these are the main two. The following sections cover the main protocols in the TCP/IP suite, but they are by no means the entire suite. It would take many books to cover all the included protocols. Some have been discussed previously but they are repeated here for convenience and continuity.

Internet Protocol (IP): The Internet Protocol (IP) is a connectionless protocol that sits in the Network layer level of the OSI model. The function of the IP is to address and route packets appropriately throughout the network. An IP header referred to as a *datagram*[*] is attached to each

* *Essentially, a datagram is a self–contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.*

packet and includes the source address, destination address, and other information sent to the receiving host. Also, the IP must fragment and reassemble packets that were split up in transit. Some types of networks can support larger packets than other types, and packets may become fragmented when going to a network that cannot support the current packet size. The packet is split up, and then each piece gets a new IP header and is sent to the final destination. When the final host receives the packets, the IP assembles all the pieces together to form the original data.

Internet Control Message Protocol (ICMP): ICMP provides error reporting for IP. Since IP is connectionless, and there is no error checking happening, it cannot detect when an error occurs on the network. It is ICMP's responsibility to report errors back to the host that sent the IP packet. For example, if a device cannot forward an IP packet on to the next network in its journey, it will send back a message to the source of that packet using ICMP to explain the error. Some common types of errors that ICMP can report are Destination Unreachable, Congestion, Echo Request, and Echo Reply (used with the PING* command). The popular Ping utility uses the ICMP Echo and Echo Request messages.

Routing Information Protocols

There are three versions of the Routing Information Protocol: **RIP**, **RIPv2**, and **RIPng**.

- The first version is known as **RIP** (Routing Information Protocol). RIP uses a distance–vector algorithm to determine routes. Before communication between segments can take place, the RIP must calculate which path or route to take. The distance in RIP is the number of routers a packet must cross to reach a destination. Each of these routers is referred to as a hop. The maximum number of hops allowed in RIP is 15. A destination is considered unreachable if the hop count is greater than 15. Routers use the hop count to determine the best route to use for a given packet at a given time. RIP is a UDP–based protocol running on top of the Transport Layer. One RIP deficiency is that there is no router authentication and thus it is vulnerable to unauthorized access. Another is that all subnets in a network class must be of the same size.
- **RIPv2** was developed to provide router authentication and carry variable subnet information. To maintain backwards compatibility with **RIP**, **RIPv2** is also limited to the 15 hop count. Whereas **RIP** uses broadcast routing updates, **RIPv2** uses multicast routing updates.
- **RIPng is an extension RIPv2** to support IPv6.†

* *PING is an acronym for Packet Internet Groper. It is a protocol used for testing whether a particular computer is connected to the Internet by sending a packet to its IP address and waiting for a response. The name actually comes from submarine active sonar, where a sound signal— called a "ping"— is broadcast, and surrounding objects are revealed by their reflections of the sound.*

† *IPv6 (Internet Protocol version 6) is the future Internet Layer protocol for* packet–*switched* internetworks. IPv4 *is* currently *the dominant Internet Protocol version in use. IPv6 supports* 2^{128} *addresses whereas IPv4 supports* 2^{32} *addresses. IPv6 provides flexibility in allocating addresses and routing traffic. The extended address length is intended to eliminate the need for network address translation to avoid address exhaustion, and also simplifies aspects of address assignment and renumbering, when changing Internet connectivity providers.*

- **Interior Gateway Routing Protocol (IGRP)**: This was Cisco's original distance–vector routing protocol, similar to RIP. It has been superseded by a new design known as **Enhanced Interior Gateway Routing Protocol** (EIGRP).
- **Open Shortest Path First (OSPF):** OSPF is a link–state algorithm with more processing power than RIP and allows more control and responds to changes faster than RIP. The OSPF (link–state) protocol creates a graph to define the network's topology. Subsequently, it computes the shortest path according to weights on the arcs of the graph. This graphing and weighting of the paths requires more processor power, but it generally responds to path changes more rapidly than RIP.
- **Intermediate system to intermediate system (IS–IS)**, is a protocol used by network routers to determine the best way to forward datagrams through a packet–switched network.

Transmission Control Protocol (TCP): TCP is a connection–oriented protocol that operates at the Transport layer of the OSI model. TCP opens and maintains a connection between two communicating hosts on a network. When an IP packet is sent between them, a TCP header that contains flow control, sequencing, and error checking is added to the packet. Each virtual connection to a host is assigned a port number (analogous to a mailbox) so datagrams being sent to the host go to the correct destination.

User Datagram Protocol (UDP): UDP is a connectionless transport protocol and is used when the overhead of TCP is not needed. UDP is just responsible for transporting datagrams. UDP also uses port numbers similar to TCP, except that they do not correspond to a virtual connection, but to a process on the other host. For example, a datagram may be sent to a port number of 53 to a remote host. Like TCP, UDP operates at the transport layer of the OSI model. UDP is used instead of the TCP for less critical messages. Both TCP and UDP contain an IP datagram. Which transport protocol is to be used depends on the network application. Network software engineers use the UDP whenever possible because it is simpler. TCP requires more overhead because it must assure delivery and therefore sends many more packets than UDP to manage connections.

Address Resolution Protocol (ARP): ARP is the protocol that resolves the IP logical address to the MAC physical address. After the address has been resolved, it is stored in cache memory until it needs to be retrieved. Thus, if a client computer needs to communicate with another computer and the source computer has the IP address of the destination computer, but not the MAC address that is needed to communicate at the Physical layer of the OSI model, ARP handles the conversion of the address by sending out a discovery packet. The discovery packet is sent out to the broadcast MAC address so every device on the network receives it. In the packet is a request for the owner of the IP address. When the receiving computer with that IP gets the discovery packet, it replies to the originator to let him know that it owns that IP. ARP then constructs and maintains an updated list of IP and MAC addresses so a discovery packet is not needed every time communication takes place.

Domain Name System (DNS): DNS converts user–friendly names such as web sites to the correct IP address. Because domain names are alphabetic, they're easier to remember. As an example,

this publisher's domain name is www.orchardpublications.com whose IP address is 75.0.190.167. This conversion is necessary because the Internet is based on IP addresses.

DNS is a distributed database hierarchy maintained by different organizations. There are a number of main DNS servers that point clients to the more specific servers at each company. To resolve a user–friendly name to the correct IP address, a client computer goes first to one of the main DNS servers, which tells the client which server to contact for the desired domain. The client then goes to that server to resolve the full name to an IP. This way the main servers only need to point a client to a closer server. Administrators can then make changes to their computer names any time they want without having to constantly update a main server. DNS uses port number 53.

File Transfer Protocol (FTP): FTP is a member of the TCP/IP protocol suite that is designed to transfer files between a server and a client computer. This protocol allows bidirectional (download and upload) transfer of binary and ASCII files. The user needs an FTP client to transfer files to and from the remote system, which must have an FTP server. Generally, the user also needs to establish an account on the remote system to FTP files, although many FTP sites permit the use of anonymous FTP that is discussed on the next paragraph. FTP uses the port numbers 20 and 21. One of these port numbers is for the request, and the other for the download.

Anonymous FTP: This is an interactive service provided by many Internet hosts allowing users who not have an account, to transfer documents, files, programs, and other archived data using the Internet's File Transfer Protocol. The user logs in using the special user name "ftp" or "anonymous" and his e–mail address as password. The user then has access to a special directory hierarchy containing the publicly accessible files, typically in a subdirectory called "pub". This is usually a separate area from files used by local users. Sometimes the host name will be followed by an Internet address in parentheses. The directory will usually be given as a path relative to the anonymous FTP login directory. Many FTP sites do not permit anonymous FTP access for security reasons. Those that do permit anonymous FTP normally restrict users to only downloading files also for security reasons.

Trivial File Transfer Protocol (TFTP): TFTP is very similar to FTP. When we use FTP to download a web page, we make use of TCP and thus UDP is not involved. However, when we use TFTP to download, we make use of UDP and TCP is not involved. It can be used to read files from, or write files to, a remote server and has no authentication or encryption capabilities. TFTP uses port number 69.

HyperText Transfer Protocol (HTTP): HTTP is the client–server protocol used on the World–Wide Web for the exchange of HTML documents. By means of URLs, HTTP supports access not only to documents written in HTML, but also to files retrievable through FTP, as well as to information posted in newsgroups. HTTP is not constrained to using TCP/IP and its supporting layers, although this is its most popular application on the Internet. HTTP can be implemented on top of any other protocol on the Internet, or on other networks. HTTP uses TCP and

not UDP because much data must be sent for a web page, and TCP* provides transmission control, presents the data in order, and provides error correction. HTTP uses port number 80.

Simple Mail Transfer Protocol (SMTP): SMTP is also a member of the TCP/IP protocol suite for routing e–mail through internetworks. With the conventional SMTP it is possible for anyone to send an e–mail from any computer, and this allows spammers to send e–mail from forged addresses. Also, it is almost impossible to trace the spammer. However, with the implementation of the **Sender Policy Framework (SPF)** it is possible to trace the spammer. With **SPF** it is also possible to reject unauthorized messages before receiving the content of the message. SMTP uses port number 25.

Dynamic Host Configuration Protocol (DHCP): DHCP is a protocol that provides a means to allocate IP addresses to computers on a local area network using *Dynamic Address Translation*† (DAT). With dynamic addressing, a device can have a different IP address every time it connects to the local area network

Telnet: Telnet is a client program that implements the Telnet protocol. It was developed in the early days of Unix as a means to log into remote computers. Thus, Telnet allows a user to remotely log in to another computer and run applications provided the user has a password for the distant computer or the distant computer provides publicly available files. We can use Telnet to gain access to a router in our network. Telnet can be used to connect with computers of different platforms, i.e., Windows, Linux, Unix. For connections with computers that use Windows, we can use the Windows Remote Desktop feature.‡

Telnet is included in Microsoft's Windows operating system. By default, it is not installed with Windows but it can be installed by performing the following steps using Windows Vista.

1. From the Windows desk top we click `Start>Control Panel>Programs and Features`, and on the left pane we click `Turn Windows features On`. In the Windows Features dialog box, we place a check mark on the `Telnet Client` box and we click OK. The installation may take one to two minutes.
2. We open the Help and Support window and we click the `Telnet: frequently asked questions`. We scroll down the Help and Support window and under `To open Telnet Client` we click • → and the command prompt window appears. At the command prompt we can type `?/h` and options are listed.

* *We recall that TCP is a connection–oriented protocol and as such, it provides transmission control, presents the data in order, and provides error correction. UDP is a connectionless protocol.*

† *Dynamic address translation, or DAT, is the process of translating a virtual address during a storage reference into the corresponding real address.*

‡ *To access the Windows Remote Desktop feature, from the Windows desktop we click the Windows Start icon, we click All Programs, we click Accessories, and we click Windows Remote Desktop. This feature is not available from Windows XP Home and Windows Vista Home editions.*

Network File System (NFS): NFS is a protocol developed by Sun Microsystems. It allows a computer to access files over a network as if they were on its local disks. This protocol has been incorporated in products by more than two hundred companies, and is now a de facto standard. NFS is implemented using a connectionless protocol (UDP) in order to make it stateless.*

3.4.5 IPX/SPX Protocol Suite

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX): IPX/SPX are the network and transport level protocols used by Novell NetWare operating systems, which together correspond to the combination of IP and TCP in the TCP/IP protocol suite. Like TCP/IP, the name comes from the two main protocols in the suite, IPX and SPX. The IPX/SPX suite is relatively new, whereas TCP/IP is older. Because IPX/SPX was created around the time the OSI model was conceived, it can easily be mapped to the OSI model.

The IPX/SPX and is a very efficient protocol and it is claimed that its performance exceeds that of TCP/IP on a LAN. However, the TCP/IP has become the *de facto* standard protocol and it is used in WANs and the Internet.

The IPX/SPX protocol suite can be used, among others, with the IEEE 802.2 and IEEE 802.3 standards. Accordingly, all servers and client computers must use the same standard. Therefore, if the servers are configured with one standard and the client computers with a different standard, communications problems will develop.

The Microsoft version of the IPX/SPX suite is called NetWare Link (NWLink) and includes an implementation of NetBIOS. NWLink packages data so that they will be compatible with client/server services on NetWare Networks. However, NWLink does not provide access to NetWare File and Print Services. To access the File and Print Services the Client Service for NetWare must be installed.

3.4.6 Other Protocols within the IPX/SPX Suite

Internetwork Packet Exchange (IPX): IPX is a Network layer protocol that provides connectionless (datagram) services. It operates at the Network layer of the OSI model. IPX is used for internetwork routing and maintains network logical address. Routing uses the Routing Information Protocol (RIP) to make route selections. IPX provides similar functionality as the User Datagram Protocol (UDP) does in the TCP/IP protocol suite.

---

* *A stateless server is one which treats each request as an independent transaction, unrelated to any previous request. This simplifies the server design because it does not need to allocate storage to deal with conversations in progress or worry about freeing it if a client dies in mid–transaction. A disadvantage is that it may be necessary to include more information in each request and this extra information will need to be interpreted by the server each time. An example of a stateless server is a World–Wide Web server. These take in requests (URLs) which completely specify the required document and do not require any context or memory of previous requests. Contrast this with a traditional FTP server which conducts an interactive session with the user. A request to the server for a file can assume that the user has been authenticated and that the current directory and transfer mode have been set.*

An IPX address is a combination of the physical MAC address on the network card and the logical network address. IPX uses socket* numbers also to successfully deliver data to the correct upper–layer process on the destination device. Socket numbers are the IPX/SPX equivalent of TCP/IP port numbers. IPX decides the best route to a remote device by using one of the built–in routing protocols.

Sequenced Packet Exchange (SPX): SPX is connection oriented, with sequencing and error control. SPX rides on top of IPX in a similar way that TCP sits on top of IP in the TCP/IP suite. SPX is mainly used when a connection is made across an internetwork device such as a router.

Two other protocols within the IPX/SPX suite are the *Multiple Link Interface Driver* (MLID) protocol and the *Link Support Layer* (LSL) protocol. Two better understand these, we will first discuss the *Network Driver Interface Specification* (NDIS) and the *Open Data–Link Interface* (ODI) standards.

Network Driver Interface Specification (NDIS)

NDIS is a Microsoft Windows device driver programming interface allowing multiple protocols such as TCP/IP and IPX/SPX, to share the same *Network Interface Card* (NIC). NDIS was developed by Microsoft and 3COM. The NDIS is a Logical Link Control (LLC) that forms the upper sublayer of the OSI data link layer (layer 2 of 7) and acts as an interface between layer 2 and 3, i.e., the Network Layer. The lower sublayer is the Media Access Control (MAC) device driver.

As we know, whenever we add a piece of hardware to our computer, we must also select and install the appropriate software driver. The hardware is often referred to as Network Interface Card (NIC), and the software driver as network adapter driver. The Network Driver Interface Specification (NDIS) describes the interface between the network transport protocol and the Data Link layer network adapter driver. The following list details the goals of NDIS:

- To provide a vendor–neutral boundary between the transport protocol and the network adapter card driver so that an NDIS compliant protocol stack† can operate with an NDIS–compliant adapter driver.
- To define a method for binding multiple protocols to a single driver so that the adapter can simultaneously support communications under multiple protocols. In addition, the method enables us to bind one protocol to more than one adapter.

The **Open Data–Link Interface (ODI)**, developed by Apple and Novell, serves the same function as NDIS. That is, it allows different Data–Link Layer protocols to share the same driver or adapter in a computer. Originally, ODI was written for NetWare and Macintosh environments. Like NDIS, ODI provides rules that establish a vendor–neutral interface between the protocol

* *Socket is an identifier for a particular service on a particular node on a network. The socket consists of a node address and a port number, which identifies the service. For example, port 80 on an Internet node indicates a Web server.*

† *A protocol stack is another name for a protocol suite. However, some books define a protocol stack as a stack made up of the Transport layer and the Network layer of the OSI model.*

stack and the adapter driver. This interface also enables one or more network drivers to support one or more protocol stacks.

ODI is made up of three components: the Link Support layer, the Transport and Networks layers, and the Multiple Link Interface drivers. Together, these components carry out the same basic function as NDIS, i.e., to enable multiple protocols to bind to a single network card.

- **Link Support Layer (LSL):** LSL is the router that directs the packets to the correct protocol.
- **Transport and Network layers:** These provide the network functionality by routing the packets to the proper destination.
- **Multiple Link Interface Driver (MLID):** MLID has two functions; one is to attach and strip media headers from packets and the other is to send and receive packets at the Physical layer.

Routing Information Protocol (RIP): RIP is discussed in detail on Page 3–16 and it is used in both the TCP/IP and IPX/SPX protocol suites. As stated on Page 3–16, RIP is a simple routing protocol which uses the distance vector method to calculate hop count, that is, it counts the number of times a piece of data crosses a router before reaching its destination, and then chooses the route with the least number of hops.

NetWare Link Services Protocol (NLSP): Like RIP, NLSP is a routing protocol, but unlike RIP which uses the distance vector computation, NLSP uses link state routing.* New routes are entered into a routing table that is updated whenever a routing change occurs. Because routing information is exchanged between routers whenever a change occurs, routing updates travel faster and consume less bandwidth. With the NetWare operating system, the network administrator can choose either NLSP or RIP.

NetWare Core Protocol (NCP): NCP operates at the upper four layers of the OSI model and as such, its function is to offer network services such as error and flow control, interfacing, file, directory, and printing services.

Service Advertising Protocol (SAP): SAP provides device location information and indicates the type of service the device offers. It permits file and print servers to advertise their addresses and services. Also, it notifies other nodes on the network that it is available for access. When a server boots, it uses the protocol to advertise its service; when the same server goes offline, it uses this protocol to announce that it is no longer available.

3.4.7 The Microsoft Protocol Suite

Microsoft Windows can operate on different types of protocol suites. These are described in the following paragraphs.

---

* *Link state routing uses an algorithm to compute the shortest distance to all destinations and updates itself whenever a change occurs. Instead of just hop count, this algorithm takes into consideration latency (the time required for a signal to travel from one point on a network to another) delays, bandwidth, and reliability.*

NetBIOS and **NetBIOS Extended User Interface (NetBEUI)** are discussed in Subsection 3.3.2

Server Message Block (SMB): SMB makes use of both the server and workstation services. These services enable a computer to act either as a server and provide resources to other clients, or act as a client and access other resources on the network. Both functions are accomplished through connection–oriented sessions using other protocols such as TCP/IP and IPX/SPX. SMB operates at the Application layer of the OSI model and file and print services can be shared. SMB is similar in function to Novell's NetWare Core Protocol (NCP), that is, it provides the communication and commands between the client and server to handle resource requests and replies.

SMB operates as an application–level network protocol mainly used to provide shared access to files, printers, serial ports, and communications between the nodes on a network. SMB is used primarily on computers running Microsoft Windows, and for this reason it is often referred to as the "Microsoft Windows Network".

3.5 Cisco Routing Protocols

In the early stages of internetworking the predominant proprietary networks for the implementation of the Ethernet were the IBM SNA and Digital Equipment's (acquired by Compaq and now HP) DECnet. Unix servers were also produced for use with Novell's NetWare IPX LANs. The Routing Information Protocol (RIP) was used in all networks and thus it became a de facto standard. Accordingly, RIP is an open standard, not proprietary to any company.

The RIP's characteristics and limitations, i.e., 15 hop limit, distance vector metrics, network size, and capacity were discussed earlier. To overcome RIP's limitations, Cisco, in the 80s, developed a more efficient protocol named **Interior Gateway Routing Protocol (IGRP)** to replace RIP. However, IGRP is limited to IP–only networks.

RIP and IGRP are both distance–vector routing protocols. However, whereas with RIP there is a 15–hop limit, with IGRP there is no hop limit. Also, while RIP has only one metric (distance by hop count), IGRP has five weighted metrics: hop count, propagation delay, bandwidth, reliability, and load (traffic). Moreover, IGRP allows for multipath routing and *load balancing* – the ability to shift traffic between alternate routes depending on the load of each.

In the 1990s, Cisco improved on IGRP with the **Enhanced Interior Gateway Routing Protocol (EIGRP)**. This protocol is considered to be a hybrid routing protocol, that is, a combination of distance–vector and link–state technology as stated earlier.

3.6 Other Protocols and Services

Ethernet: This is a local area network developed by DEC (later Compaq and now HP), Intel and Xerox as IEEE 802.3. It is now recognized as the industry standard.

Data is broken into packets which are transmitted using the CSMA/CD algorithm until they arrive at the destination without colliding with any other. The first contention slot after a trans-

mission is reserved for an acknowledge packet. A node is either transmitting or receiving at any instant. The bandwidth* varies from 10 Mbps to 10 Gbps depending on the interface devices used. It is reported that the data transfer rate doubles every 15 months.

Ethernet is standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, is the most widespread wired LAN technology. It has been in use from around 1980[1] to the present, largely replacing competing LAN standards such as token ring, FDDI, and ARCNET.

Ethernet cables are classified as "XbaseY", e.g. 10base5, where X is the data rate in Mbps, "base" means "baseband" (as opposed to broadband) and Y is the category of cabling. The original cable was 10base5 ("full spec"), others are 10base2 ("thinnet") and 10baseT ("twisted pair"). The 100baseT ("Fast Ethernet"), and Gigabit (1000 Mbps) Ethernet are now very popular.

High–level Data Link Control (HDLC): HDLC is a protocol for information transfer developed by the ISO. HDLC is a bit–oriented, synchronous protocol that applies to the Data Link (message–packaging) layer of the ISO model. Messages are transmitted in frames, which can contain differing amounts of data but which must be organized in a particular way.

Distributed Database Management System (DBMS): DBMS is a database management system capable of managing a distributed database.

File Transfer Access Method (FTAM): FTAM is a communications standard for transferring files between different makes and models of computers.

X.500: X.500 is an international address–to–name resolution and directory services standard. By supporting a standard directory services protocol, DNA can fit into larger enterprise–wide directory services.

Digital Access Protocol (DAP): DAP is the protocol that governs communications between X.500 clients and servers.

Systems Network Architecture (SNA): SNA is a widely used communications framework developed by IBM to define network functions and establish standards for enabling computers to exchange and process data. Comparable (but not necessarily compatible) layers in the SNA and the IOS model are shown in Figure 3.13.

Data Link Control (DLC): DLC is an error–correction protocol in the Systems Network Architecture (SNA) responsible for transmission of data between two nodes over a physical link. DLC is a nonroutable protocol used for printers connected to the network. It also provides connectivity with IBM mainframes.

* *In computer networks, bandwidth is another name as the transfer rate, that is, the amount of data that can be carried from one point to another in a given time period, usually a second. This bandwidth is expressed in bits per second (bps, Kbps, Mbps, and so on). In signal processing bandwidth is a measure of the width of a range of frequencies measured in hertz (Hz, KHz, MHz, and so on).*

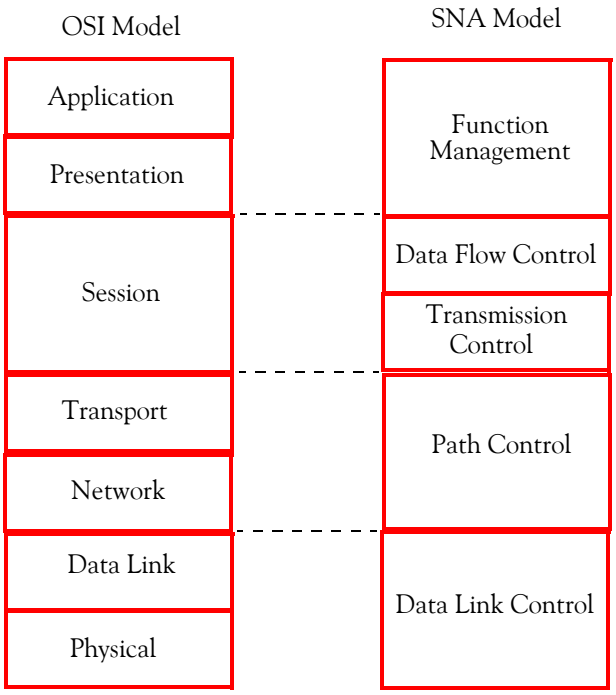


Figure 3.13. Comparable layers in SNA and ISO models

3.7 Wide Area Network Protocols

In this section, we will discuss the popular technologies used by companies to send data across WANs. The protocols we've discussed handle communications between clients and servers, usually over a LAN or a MAN. However, quite often we need to connect our network to another network in a distant location. The desired connection will require additional effort besides the use of telephone lines and the use of a protocol such as TCP/IP or IPX/SPX. For convenience, we will review some of the connection types discussed in Chapter 2.

3.7.1 Connection Types

The best WAN connection would simply be one long wire between sites. This would give usunrestricted, dedicated bandwidth. The main problems with this are, of course, cost and feasibility. Instead of having a dedicated cable, companies buy or lease connections from some sort of service provider. Examples of a service provider are a regional telephone company or a long–distance provider. Leased connections can take two different forms: dedicated or switched.

Dedicated connections

In a dedicated connection, we have full use of the connection as if it were a physical cable. The difference is that the service provider owns and manages the "cable." No one else can use the line

that we have leased. The cost of a dedicated connection usually is high. We pay the same amount whether we use the bandwidth or not.

Switched connections

As we've learned in Chapter 2, switched connections allow several people to use a connection at once. Switched connections take special hardware to manage the connections but give us the benefit of lower cost for the connection. Another advantage of switched connections is that we are normally only charged for the bandwidth used, not the total capable bandwidth. A drawback to this is that bandwidth could be limited due to the possible number of people sharing the connection. Two forms of switching are packet switching and circuit switching.

Packet switching: Packet switching takes the total message and divides it into smaller chunks. These chunks are then routed through the network the best way possible to reach the destination. Packet switching can also use virtual circuits, which are logical circuits set up between devices. There is no real physical connection, just an open channel between the devices.

Circuit switching: We use a circuit switching network all the time, but may not know it. Each time we make a telephone call, a "virtual" circuit between we and the other end is set up automatically for us to use. Only us are using the circuit at that given time. When the call is over, the circuit is torn down and can be used by someone else. The advantage of circuit switching is that we get the features of a dedicated service without the price.

3.7.2 Popular WAN Protocols

WAN protocols allow us to route data over a large internetwork. They do not replace the upper–layer protocol suites such as IPX/SPX or TCP/IP; they carry these protocols through the internetwork so they may deliver the data. Some WAN protocols are discussed below.

Public Switched Telephone Network (PSTN)

The Public Switched Telephone Network (PSTN) is also discussed in Chapter 1. PSTN has been around for a long time and is a very popular way to move data across an internetwork. PSTN is operated by Regional Bell Operating Companies (RBOC) and other long distance providers such as AT&T, MCI, and Sprint. The local telephone company is responsible for all communications between our *demarc point** and their local *Central Office* (CO).

The connection between the CO and our demarc point is known as the local loop. This local loop is usually made up of UTP cable or, if we are lucky, fiber optic. The central offices are then connected to each other through high–capacity trunk lines. Long–distance carriers also tie into this large network of COs to offer long–distance service. Calls made over the PSTN use circuit

* *The demarc point is the point where the phone company connects to our house or building. When the local telephone company installs the telephone lines to our office, they bring the connection to the demarc point.*

switching. Using the PSTN, we can get several different connection types. These are briefly discussed below.

Dial–up connections: The simplest and most common connection over the PSTN is the dial–up connection. We use this connection each time we call up our Internet provider. Using conventional telephone lines and a typical modem, we can attain speeds up to 56 Kbps, but often we are connected at lower speeds.

Dedicated leased lines: Dedicated leased lines are either analog or digital. Presently, most are digital. Because of digital transmission, digital leased lines are faster than analog lines, and they are less susceptible to interference. Digital Data Service **(DDS)** is the class of service offered by telecommunications companies for transmitting digital data as opposed to voice. DDS transmission requires called *Channel Service Unit/Data Service Unit* (CSU/DSU). The Channel Service Unit (CSU) is used to terminate a DS1 or DS0 (56/64 Kbps) digital circuit. It performs line conditioning, protection, loop–back and timing functions. The Data Service Unit (DSU) terminates the data circuit to the Data Terminal Equipment (DTE) and converts the customer's data stream into a bi–polar* format for transmission.

T–carrier system: This system consists of a a series of wideband digital data transmission formats originally developed by the Bell System and used in North America and Japan. The basic unit of the T–carrier system is the DS0, which has a transmission rate of 64 Kbps, and is commonly used for one voice circuit.

A T–carrier is a long–distance, digital communications line provided by a common carrier. Multiplexers at either end merge several voice channels and digital data streams for transmission and separate them when received. T–carrier service, introduced by AT&T in 1993, is defined at several capacity levels: T1, T2, T3, T4. In addition to voice communication, T–carriers are used for Internet connectivity. When we have a need for bandwidth larger than what 56 Kbps connections provide, another option is available. Originally designed in the 1960s to handle multiple voice calls at once, the T–carrier system is now used in data communications. The T–carrier system uses devices called multiplexers, or muxes, to combine multiple communications into one. At the other end, another device called demultiplexer or demux, separates the different communications. T1 is the basic T–carrier system. It consists of twenty–four pulse–code modulated, time–division multiplexed speech signals each encoded in 64 Kbps channels that can be combined for a total bandwidth of 1.544† Mbps. Although originally designed by AT&T to carry voice calls, this high–bandwidth telephone line can also transmit text and images.

T1 lines are commonly used by larger organizations for Internet connectivity. One big feature of this system is that the channels can be split so that some are used for voice traffic and some for

* *In digital transmission, an electrical line signalling method where the mark value alternates between positive and negative polarities.*

† *In reality, 24 signals times 64 Kbps each signal yields 1.536 Mbps. The additional 8 Kbps are used for framing information which facilitates the synchronization and demultiplexing at the receiver.*

data. These 64 Kbps channels are called *Digital Signal Level* 0 (DS–0) signals. A full T1 line is also known as a DS–1, or in European, an E–1. Table 3.4 shows the different T–carrier lines available. T2 and T3 circuits channels carry multiple T1 channels multiplexed, resulting in transmission rates of up to 44.736 Mbps.

TABLE 3.4 T Carrier Systems

Digital Signal	Carrier	Speed (MBps)	# of Channels
DS–0	N/A	0.064	1
DS–1	T1	1.544	24
DS–2	T2	6.312	96
DS–3	T3	44.736	672
DS–4	T4	274.760	4032

By far the most common T–carrier line used is the T1. If we need more speed, we can go to a larger carrier. T2 is used by the Department of Defense (DoD). T3s are becoming more popular, due to the falling cost of bandwidth and the increasing needs of users. T1 and T2 lines use standard copper cable, whereas the T3 and T4 lines use fiber optic.

Serial Line Internet Protocol (SLIP): This is an older protocol used to handle TCP/IP traffic over a dial–up or other serial connection. SLIP is a Physical layer protocol that doesn't provide error checking, relying on the hardware (such as modem error checking) to handle this. It only supports the transmission of one protocol, TCP/IP. A later version of SLIP, called Compressed SLIP (CSLIP), became available. Though the name says compressed, the protocol actually just reduces the amount of information in the headers, and does not compress the transmission.

Point–to–Point Protocol (PPP): PPP provides a Physical and Data Link layer functionality that fixes many problems with SLIP. Basically, our modem is transformed into a network card, as far as upper–level protocols are concerned. At the Data Link layer, PPP provides error checking to ensure the accurate delivery of the frames that it sends and receives. PPP also keeps a Logical Link Control communication between the two connect devices by using the Link Control Protocol (LCP). Besides being less prone to errors, PPP also lets us use almost any protocol we want over the link. TCP/IP, IPX/SPX, and NetBEUI can all be sent over the modem connection. PPP also supports the automatic configuration of the dialed–in computer. Unlike SLIP, where our addresses and other information have to be hard–coded ahead of time, PPP allows the client computer to receive its information from the host it dials into. Most Internet dial–up connections today are made using PPP over modem or ISDN.

Frame relay: Frame Relay is a DTE–DCE interface specification based on LAPD (Q.921), the Integrated Services Digital Network version of LAPB (X.25 data link layer). A common specification was produced by a consortium of StrataCom, Cisco, Digital, and Northern Telecom.

Frame Relay is the result of wide area networking requirements for speed; LAN–WAN and LAN–LAN internetworking, "bursty" data communications, multiplicity of protocols, and proto-

col transparency. These requirements can be met with technology such as optical fibre lines, allowing higher speeds and fewer transmission errors, intelligent network end devices (personal computers, workstations, and servers), standardization, and adoption of ISDN protocols.

Frame Relay uses the same basic data link layer framing and *Frame Check Sequence* (FCS) so current X.25 hardware still works. It adds addressing (a 10–bit Data Link Connection Identifier (DLCI)) and a few control bits but does not include retransmissions, link establishment, windows or error recovery. It has none of X.25's session layer but adds some simple interface management. Any network layer protocol can be used over the data link layer frames.

Integrated Services Digital Network (ISDN): ISDN A set of communications standards allowing a single wire or optical fibre to carry voice, digital network services and video. ISDN was intended to eventually replace the plain old telephone system. As mentioned in Chapter 2, most recently, ISDN service has largely been displaced by broadband internet service, such as xDSL and Cable Modem service.

ISDN was first published as one of the 1984 ITU–T *Red Book recommendations*. The 1988 Blue Book recommendations added many new features. ISDN uses mostly existing Public Switched Telephone Network (PSTN) switches and wiring, upgraded so that the basic "call" is a 64 Kbps, all–digital end–to–end channel. Packet and frame modes are also provided in some places.

Digital Signal or Data Service level (DS): Originally an AT&T classification of transmitting one or more voice conversations in one digital data stream. The best known DS levels are DS0 (a single conversation), DS1 (24 conversations multiplexed), DS1C, DS2, and DS3. These are shown in Table 3. 4 above.

Different services may be requested by specifying different values in the "Bearer Capability" field in the call setup message. One ISDN service is "telephony" (i.e. voice), which can be provided using less than the full 64 kbps bandwidth (64 kbps would provide for 8192 eight–bit samples per second) but will require the same special processing as ordinary PSTN calls.

Asynchronous Transfer Mode (ATM): ATM is a network technology capable of transmitting data, voice, video, and frame relay traffic in real time. Data, including frame relay data, is broken into packets containing 53 bytes each, which are switched between any two nodes in the system at rates ranging from 1.5 Mbps to 622 Mbps. ATM is defined in the broadband ISDN protocol at the levels corresponding to levels 1 and 2 of the ISO/OSI model. It is currently used in local area networks involving workstations and personal computers, but it is expected to be adopted by the telephone companies, who will be able to charge customers for the data they transmit rather than for their connect time.

Switched Multimegabit Data Service (SMDS): SMDS is a very high–speed, switched data transport service that connects LANs and WANs through the public telephone network.

Synchronous Digital Hierarchy (SDH): SDH is an international digital telecommunications network hierarchy which standardizes transmission bit rates at 51.84 Mbps. It is also referred to as STS–1. Higher rates are multiples of this bit rate. Thus STS–3 is 3 times STS–1, STS–12 is 12

times STS–1, and so on. STS–3 is the lowest bit rate expected to carry ATM traffic, and is also referred to as *Synchronous Transport Module–Level 1* (STM–1). SDH specifies how payload data is framed and transported synchronously across optical fibre transmission links without requiring all the links and nodes to have the same synchronized clock for data transmission and recovery (i.e. both the clock frequency and phase are allowed to have variations, or be plesiochronous*).

SDH offers several advantages over the current multiplexing technology, which is known as Plesiochronous Digital Hierarchy. Where PDH lacks built–in facilities for automatic management and routing, and locks users into proprietary methods, SDH can improve network reliability and performance, offers much greater flexibility and lower operating and maintenance costs, and provides for a faster provision of new services.

Under SDH, incoming traffic is synchronized and enhanced with network management bits before being multiplexed into the STM–1 fixed rate frame.

Synchronous Optical Network (SONET): SONET establishes a digital network for a worldwide transport standard. SONET has been designed to take advantage of fiber cable, in contrast to the plain old telephone system which was designed for copper wires. SONET carries circuit–switched data in frames at speeds in multiples of 51.84 Mbps up to 48 * 51.84 Mbps = 2.488 Gbps. For every optical carrier level of 51.84 Mbps, SONET can transmit *n* number of frames at a given time. Groups of frames are called *superframes*. SONET is considered to be the American version of SDH.

Small Computer System Interface (SCSI): SCSI (sometimes pronounced as “skuh'zee” and other times as “sek'si” is one of the most popular processor–independent standard, via a parallel bus, for system–level interfacing between a computer and intelligent devices including hard disks, floppy disks, CD–ROM, printers, scanners, and others.

SCSI can connect multiple devices to a single SCSI adaptor (or "host adaptor") on the computer's bus. SCSI transfers bits in parallel and can operate in either asynchronous or synchronous modes. The synchronous transfer rate is up to 5 Mbps. There must be at least one target and one initiator on the SCSI bus.

Single ended† SCSI can be used with cables up to six meters long. Differential ended SCSI be used with cables up to 25 meters long.

SCSI was developed by Shugart Associates, which later became Seagate. SCSI was originally called SASI for "Shugart Associates System Interface" before it became a standard.

---

* *Plesiochronous means nearly synchronized. It is a term describing a communication system where transmitted signals have the same nominal digital rate but are synchronized on different clocks. According to ITU–T standards, corresponding signals are plesiochronous if their significant instants occur at nominally the same rate, with any variation in rate being constrained within specified limits.*

† *An electrical connection where one wire carries the signal and another wire or shield is connected to electrical ground. This is in contrast to a differential connection where the second wire carries an inverted signal.*

Due to SCSI's inherent protocol flexibility, large support infrastructure, continued speed increases and the acceptance of SCSI Expanders in applications it is expected to hold its market.

The original standard is now called SCSI–1 to distinguish it from SCSI–2 and SCSI–3 which include specifications of Wide SCSI (a 16–bit bus) and Fast SCSI (10 Mbps transfer). SCSI–1 has been standardized as ANSI X3.131–1986 and ISO/IEC 9316.

SCSI allows a large number of different connectors that can be used. The different SCSI types that are currently in use are:

SCSI–1: Uses an 8–bit bus, 25–pin connector, and supports data rates of 4 up to Mbps.

SCSI–2: Same as SCSI–1, uses a 50–pin connector, and can be used with multiple devices.

Wide SCSI: Uses a wider cable to support 16–bit bus.

Fast SCSI: Uses an 8–bit bus, but doubles the clock rate to support data rates up to 10 Mbps.

Fast Wide SCSI: Uses a 16–bit bus and supports data rates up to 20 MBps.

Ultra SCSI: Uses an 8–bit bus, and supports data rates up to 20 Mbps.

SCSI–3: Uses a 16–bit bus and supports data rates up to 40 Mbps.

Ultra2 SCSI: Uses an 8–bit bus and supports data rates up to 40 Mbps.

Wide Ultra2 SCSI: Uses a 16–bit bus and supports data rates up to 80 MBps.

ASPI is a standard Microsoft Windows interface to SCSI devices.

IEEE 1394 (High Performance Serial Bus): IEEE 1394, also known as *FireWire* or *I–Link*, is a 1995 Macintosh/IBM PC serial bus interface standard offering high–speed communications and isochronous* real–time data services. IEEE 1394 can transfer data between a computer and its peripherals at 100, 200, or 400 Mbps, with a planned increase to 2 Gbps. Cable length is limited to 4.5 m but up to 16 cables can be daisy–chained yielding a total length of 72 m.

It can daisy–chain† together up to 63 peripherals in a tree–like structure (as opposed to SCSI's linear structure). It allows peer–to–peer device communication, such as communication between a scanner and a printer, to take place without using system memory or the CPU.

* *A form of data transmission that guarantees to provide a certain minimum data rate, as required for time–dependent data such as video or audio. Isochronous transmission transmits asynchronous data over a synchronous data link so that individual characters are only separated by a whole number of bit–length intervals. This is in contrast to asynchronous transmission, in which the characters may be separated by arbitrary intervals, and with synchronous transmission Asynchronous Transfer Mode and High Performance Serial Bus can provide isochronous service.*

† *A bus wiring scheme in which, for example, device A is wired to device B, device B is wired to device C, etc.*

It is designed to support plug–and–play and hot swapping.* Its six–wire cable is not only more convenient than SCSI cables but can supply up to 60 watts of power, allowing low–consumption devices to operate without a separate power cord.

Universal Serial Bus (USB): We discussed USB in Chapter 2. As a review, USB is an external peripheral interface standard for communication between a computer and external peripherals over an inexpensive cable using serial transmission. USB is standard on current (1999) Macintosh computers and is promoted by Intel as an option for the IBM PC where it is supported by later versions of Windows.

USB works at 12 Mbps with specific consideration for low cost peripherals. It supports up to 127 devices and both isochronous and asynchronous data transfers. Cables can be up to five meters long and it includes built–in power distribution for low power devices. It supports daisy chaining through a tiered star multidrop topology. USB 2 is about 40% faster.

Because of its relatively low speed, USB is intended to replace devices that do not require high speeds. Such devices are serial ports, parallel ports, keyboard, and monitor connectors and be used with keyboards, mice, monitors, printers, and possibly some low–speed scanners and removable hard drives. For faster devices existing IDE, SCSI, or emerging *Fibre Channel–Arbitrated Loop* (FC–AL)† or FireWire interfaces can be used.

3.8 Protocols No Longer in Use

3.8.1 The AppleTalk Protocol Suite

AppleTalk was a proprietary suite of protocols developed by Apple Inc for networking computers. The AppleTalk design was based on the OSI model of protocol layers and was implemented in the Macintosh in the 80s. Apple has now replaced it with the TCP/IP protocol.

AppleTalk contained three protocols to make it self–configuring. The *AppleTalk address resolution protocol* (*AARP*) allowed AppleTalk hosts to automatically generate their own network addresses, and the *Name Binding Protocol* (*NBP*) was a dynamic Domain Name System (DNS) system, mapping network addresses to user–readable names.

---

* *Hot swapping implies the connection and disconnection of peripherals or other components without interrupting system operation, that is, without shutting down the computer system.*

† *FC–AL is a fast serial bus interface standard intended to replace SCSI on high–end servers. FC–AL has a number of advantages over SCSI. It offers higher speed: the base speed is 100 megabytes per second, with 200, 400, and 800 planned. Many devices are dual ported, i.e., can be accessed through two independent ports, which doubles speed and increases fault tolerance. Cables can be as long as 30 m (coaxial) or 10 km (optical). FC–AL enables self–configuring and hot swapping and the maximum number of devices on a single port is 126. Finally, it provides software compatibility with SCSI. Despite all these features FC–AL is unlikely to appear on desktops anytime soon, partly because its price, partly because typical desktop computers would not take advantage of many of the advanced features. On these systems FireWire has more potential.*

Banyan VINES (*Virtual Integrated NETwork Service*) was a computer network operating system. The set of computer network protocols was used to communicate with client machines on the same network. The Banyan company based the VINES operating system on Unix, and the network protocols on the Xerox XNS* stack. VINES formed one of a group of XNS–based systems which also included Novell NetWare and ARCNET. It is no longer in use.

3.8.2 The National Science Foundation Wide Area Network (NSFnet)

NSFnet was a WAN, developed by the National Science Foundation to replace ARPAnet for civilian purposes and served as a major backbone for the Internet until mid–1995. Backbone services in the United States for the Internet are now provided by commercial carriers.

The NSFnet went online in 1986, using a TCP/IP–based protocol that was compatible with ARPAnet, as a backbone to which regional and academic networks would connect. It experienced exponential growth in its network traffic. Essentially, the NSFnet opened up the Internet to the public.

The NSFnet was the principal Internet backbone starting in approximately 1988, bridging between the rather restrictive US DoD creation of the Internet, and its broad commercialization in the mid–1990s. Some Internet technologies, such as the Border Gateway Protocol (BGP) which is discussed below, are a direct result of that period in Internet history. BGP was specifically created to allow the NSFnet backbone to differentiate routes learned via multiple paths from originally the ARPAnet, but also from the regional networks. Subsequently, it turned the Internet into a meshed infrastructure, instead of the single–core architecture which the ARPAnet was using before.

External Gateway Protocol (EGP): EGP was a protocol used for distributing information regarding availability to the routers and gateways that interconnect networks. EGP was also used with MILNET.†

Border Gateway Protocol (BGP): BGP was a protocol used by NSFnet and was based on the External Gateway Protocol (EGP). BGP was a very high level routing protocol that enabled the Internet to function very efficiently.

---

* *XNS (Xerox Network Services) was a protocol suite initiated by Xerox, to provided routing and packet delivery.*

† *MILNET is short for Military Network. It was a WAN for the military side of the original ARPANet. During the 1980s the MILNET expanded to become the Defense Data Network, a worldwide set of military networks running at different security levels. In the 1990s, MILNET became the NIPRNET.*

3.9 Summary

- The X.25 protocol was one of the first protocols developed for packet switching networks.
- The processors within the Public Packet Switching Network (PPSN) are called Data Circuit Equipment (DCE).
- Data Equipment (DTE) can interface with Data Circuit Equipment via the X.25 protocol.
- Data is a term that specifies the procedures of data transfer between the network and the transmitting or receiving terminal.
- Routable protocols can be used across an entire internetwork.
- Nonroutable protocols cannot operate across a router.
- Connectionless protocols do not check if data arrived successfully. They are faster than connection–oriented protocols due to less overhead.
- Connection–oriented protocols are more reliable due to the use of acknowledgments, which ensure that data has arrived successfully.
- The TCP/IP suite of protocols is very popular due to its ability to run on almost any computing platform. TCP/IP is also extremely well suited to large, enterprise–wide internetworks.
- In the TCP/IP protocol suite TCP is a connection oriented protocol whereas IP is a connectionless protocol.
- TCP operates at the Transport layer of the OSI model and IP operates at the Network layer of the OSI model.
- All Internet addresses are IP addresses and every server and client on a TCP/IP network is assigned a unique address by the Internet Assigned Numbers Authority (IANA).
- Datagram is a self–contained, independent entity of data carrying sufficient information to be routed from the source to the destination. An example of datagram is a packet that includes an IP header, source address, destination address, and other information sent to a host.
- The User Datagram Protocol (UDP) is a connectionless protocol within TCP/IP protocol suite and it can be used in place of the TCP for less critical messages.
- IP addresses are divided into three classes: Class A, Class B, Class C, Class D, and Class E.
- Subnetting is a procedure where one can use more network addresses than specified in the default configuration by infringing on the host addresses.
- Subnet masks are represented as 255 in dotted–decimal format.
- The Internet Control Message Protocol (ICMP) provides error reporting for IP.
- There are three versions of the Routing Information Protocol: RIP, RIPv2, and RIPng.

- Open Shortest Path First (OSPF) is a link–state algorithm with more processing power than RIP and allows more control and responds to changes faster than RIP.
- Intermediate system to intermediate system (IS–IS) is a protocol used by network routers to determine the best way to forward datagrams through a packet–switched network.
- The Address Resolution Protocol (ARP) resolves IP logical addresses into MAC physical addresses.
- The Domain Name System (DNS) converts web site names to IP addresses.
- The File Transfer Protocol (FTP) transfers files between a server and a client. Anonymous FTP and Trivial File Transfer Protocol (TFTP) are variants of FTP.
- The HyperText Transfer Protocol (HTTP) is the client–server protocol used on the World–Wide Web for the exchange of HTML documents.
- The Simple Mail Transfer Protocol (SMTP) is used for routing e–mail through internetworks. With the implementation of the Sender Policy Framework (SPF) it is possible to trace a spammer, and it is also possible to reject unauthorized messages before receiving the content of the message.
- The Dynamic Host Configuration Protocol (DHCP) is a TCP/IP protocol that enables a network connected to the Internet to assign a temporary IP address to a host automatically when the host connects to the network.
- Telnet is the Internet standard protocol for remote login. That is, it allows us to login to the network from a remote client terminal
- The Network File System (NFS) was developed by Sun Microsystems. It allows users of Windows and Unix workstations to access remote files and directories on a network as if they were local.
- The IPX/SPX protocol suite is comparable to the TCP/IP protocol suite and was created by Novell, Inc., to be used with their NetWare network operating system.
- The Internetwork Packet Exchange (IPX) in the IPX/SPX protocol suite provides connectionless services. It is comparable to IP in the TCP/IP protocol suite.
- The Sequenced Packet Exchange (SPX) in the IPX/SPX protocol suite is a connection–oriented protocol and it is comparable to TCP in the TCP/IP protocol suite.
- The Routing Information Protocol (RIP) is used in both the TCP/IP and IPX/SPX protocol suites.
- The Network Driver Interface Specification (NDIS) is a Microsoft Windows device driver programming interface allowing multiple protocols to share the same network hardware. NDIS was developed by Microsoft and 3COM. Novell offers a similar device driver for NetWare

called Open Data–Link Interface (ODI) which consists of the Link Support layer, the Transport and Networks layers, and the Multiple Link Interface drivers.

- NetBIOS is an Application Program Interface (API) that can be used by application programs on a local area network consisting of IBM and compatible microcomputers running on the old MS–DOS, OS/2, Windows, and some versions of UNIX.
- NetBEUI is an enhanced NetBIOS protocol for network operating systems, originated by IBM for the LAN manager server and now used with Microsoft networks. It is a small, fast, non-routable protocol used in small Microsoft workgroup networks. NetBIOS is the Applications Programming Interface (API) and NetBEUI is the transport protocol.
- The Interior Gateway Routing Protocol (IGRP) was developed by Cisco to overcome RIP's limitations. The Enhanced Interior Gateway Routing Protocol (EIGRP) is considered to be a hybrid routing protocol, that is, a combination of distance–vector and link–state technology.
- The Ethernet is a local area network recognized as the industry standard.
- The Systems Network Architecture (SNA) is a widely used communications framework developed by IBM to define network functions and establish standards for enabling computers to exchange and process data.
- The Data Link Control (DLC) is an error–correction protocol in the Systems Network Architecture (SNA) responsible for transmission of data between two nodes over a physical link.
- WAN protocols allow us to route data over a large internetwork. They do not replace the upper–layer protocol suites such as IPX/SPX or TCP/IP; they carry these protocols through the internetwork so they may deliver the data.
- The Public Switched Telephone Network (PSTN) offers a practical means of communications in an internetwork.
- Dial–up connections are the simplest and most common connections over the PSTN. Speeds can go up to 56 Kbps but usually don't due to telephone line limitations.
- Digital leased lines are dedicated lines usually called Digital Data Service (DSS) lines. They require special digital equipment to be used, which is called Channel Service Unit/Data Service Unit (CSU/DSU).
- The T–carrier system is a long–distance, digital communications line provided by a common carrier. The most common T–carrier line is the T1.
- The Serial Line Internet Protocol (SLIP) is an older protocol used to handle TCP/IP traffic over a dial–up or other serial connection.
- The Point–to–Point Protocol (PPP) provides a Physical and Data Link layer functionality that overcomes the limitations of SLIP.

- Frame relay is a packet–switching protocol for use on WANs. Frame relay transmits variable–length packets at up to 1.544 Mbps. It is a variant of X.25 but dispenses with some of X.25's error detection for the sake of speed.
- The Integrated Services Digital Network (ISDN) is a set of communications standards allowing a single wire or optical fibre to carry voice, digital network services and video. ISDN is intended to eventually replace the plain old telephone system.
- The Asynchronous Transfer Mode (ATM) is a network technology capable of transmitting data, voice, video, and frame relay traffic in real time. It is currently used in local area networks involving workstations and personal computers.
- The Switched Multimegabit Data Service (SMDS) is a very high–speed, switched data transport service that connects LANs and WANs through the public telephone network.
- The Synchronous Optical Network (SONET) carries circuit–switched data in frames at speeds in multiples of 51.84 Mbps up to 2.488 Gbps. SONET has been designed to take advantage of fibre, in contrast to the plain old telephone system which was designed for copper wires.
- The Synchronous Digital Hierarchy (SDH) is an international digital telecommunications network hierarchy which standardizes transmission around the bit rate of 51.84 Mbps.
- The Small Computer System Interface (SCSI) is one of the most popular processor–independent standard for system–level interfacing between a computer and intelligent devices including hard disks, floppy disks, CD–ROM, printers, and scanners.
- The IEEE 1394 (High Performance Serial Bus) also known as *FireWire* or *I–Link*, is a 1995 Macintosh/IBM PC serial bus interface standard offering high–speed communications.
- The AppleTalk Protocol suite was created by Apple to be used on Macintosh computers. It is no longer in use, it has been superseded by TCP/IP.
- Banyan VINES was a computer network used to communicate with client machines on the same network. The The VINES operating system was based on Unix. It is no longer in use.
- The NSFnet was the principal Internet backbone starting in approximately 1988. It is considered the predecessor of the Internet, and it is no longer in use.
- The External Gateway Protocol (EGP) was a protocol used for distributing information regarding availability to the routers and gateways that interconnect networks. EGP was used with MILNET.
- The Border Gateway Protocol (BGP) was a protocol used by NSFnet and was based on the External Gateway Protocol (EGP).

3.10 Exercises

True/False

1. The X.25 protocol provides communications between a DCE and DTE. _____
2. The Data Link Control (DLC) is an error–correction protocol in the Systems Network Architecture (SNA). _____
3. The User Datagram Protocol (UDP) operates at the Network layer of the OSI model._____
4. Class A IP addresses are the most common. _____
5. Subnet masking can be used in Class A through Class E in IP addressing. _____
6. A Trivial File Transfer Protocol (TFTP) upload or download can be handled by UDP with no TCP involvement. _____
7. Telnet is included in Microsoft's Windows operating system. _____
8. In the IPX/SPX protocol suite, IPX is a connection–oriented protocol. _____
9. RIPng is a routing protocol proprietary to Cisco. _____
10. NSFnet was a WAN developed by the Bureau of Alcohol, Tobacco, and Firearms. _____

Multiple Choice

11. A typical IP address of a client is _____.
    - **A.** http://www.myterminal.com
    - **B.** 64.1.5.156
    - **C.** 00–E0–18–90–1E–CB
    - **D.** 255.255.0.0
12. The _____ protocol resolves IP addresses to MAC addresses
    - **A.** TCP
    - **B.** DNS
    - **C.** UDP
    - **D.** ARP
13. The PING command uses the _____ protocol
    - **A.** TCP
    - **B.** IP

C. ICMP

D. RIP

14. The IPX protocol operates at the _____ layer of the OSI model

A. Session

B. Data Link

C. Network

D. Transport

15. The _____ protocol of the IPX/SPX protocol suite permits file and print servers to advertise their addresses and services.

A. NLSP

B. SAP

C. NCP

D. SPX

16. The _____ protocol can be used for with HP printers connected to the network.

A. DLC

B. EGP

C. SNA

D. PSTN

17. Most Internet dial–up connections are made using _____ over modem or ISDN

A. SLIP

B. PPP

C. ISDN

D. ATM

18. The _____ protocol suite is the primary protocol used on the Internet.

A. TCP/IP

B. IPX/SPX

C. NetBEUI

D. DNA

19. The _____ protocol is the primary protocol used to deliver e–mail to servers on the Internet.

A. SMDS

B. FTP

C. POP

D. SMTP

20. The _____ level having a transmission rate of 64 Kbps, can carry one voice channel (a phone call).

A. T1

B. DS0

C. DS1

D. ATM

Problems

21. You are a network consultant and have been invited by a small company to submit your recommendations for expanding their network. This company is presently occupying a small office in a single floor in a large building and their small network uses the NetBEUI protocol. The company is expanding and will soon be occupying five floors in that building. You have concluded that the expanded network will use internetworking devices to handle the increased network traffic. Would your recommendations include also a change to another protocol? If so, what protocol(s) would you propose?

22. You are the network administrator for your company and you have acquired a new Unix server that uses the entire TCP/IP protocol suite. Your client computers must be able to retrieve the data that is on the server and perform file transfer operations. Will you need additional protocols to satisfy the needs of your client computers? Explain.

23. You are the network administrator for your small network that uses Microsoft Windows–based client computers using NetBEUI. Your company will soon acquire a new NetWare–based server. Your client computers must be able to retrieve the data that is on the server and perform file transfer operations. Will you need additional protocols to satisfy the needs of your client computers? Explain.

3.11 Answers to End–of–Chapter Exercises

True/False

1. T – Review Page 3–2

2. T – Review Page 3–9

3. F – Review Page 3–9

4. F – Review Page 3–14

5. T – Review Page 3–14

6. T – Review Page 3–18

7. T – Review Page 3–19

8. F – Review Page 3–20

9. F – Review Page 3–16

10. F – Review Page 3–33

Multiple Choice

11. B – Review Page 3–13

12. D – Review Page 3–17

13. C – Review Page 3–16

14. C – Review Page 3–20

15. B – Review Page 3–22

16. A – Review Page 3–24

17. B – Review Page 3–28

18. A – Review Page 3–10

19. D – Review Page 3–19

20. B – Review Table 3.4, Page 3–28

Problems

21. NetBEUI is a nonroutable protocol (see Page 3–9) intended for small Microsoft networks, and thus it will not work with the new internetworking devices. Either the TCP/IP suite or the IPX/SPX suite should be proposed since both are appropriate for the new configuration.

22. Since the new Unix server is equipped with the entire TCP/IP protocol suite, it must include the FTP protocol for file transfer. One may also consider adding Sun Microsystems' popular

NFS which, as we recall, allows users of Windows NT and UNIX workstations to access remote files and directories on a network as if they were local.

23. NetBEUI can be replaced with the IPX/SPX protocol suite. Or IPX/SPX suite can be added to NetBEUI so that one would benefit from the speed of NetBEUI, while Microsoft clients communicate with each other and still being able to connect to the NetWare server with IPX/SPX.

Chapter 4

Network Designs and Ethernet Networking

This chapter discusses the various physical network connections. It begins with the different physical topologies, and then the network types including the ARCNet, Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI). A discussion of the wiring types and methods used in each of these network types is also included. Wireless networks are discussed in Chapter 6.

4.1 Physical Topologies

Topology is the configuration formed by the connections between devices on a local area network or between two or more local area networks. Topology can include such aspects as the transmission media, network adapters, and physical design of the network. Topologies specify which of these devices are used to connect systems on the network. The most common topologies are bus, star, ring, and mesh. There are advantages and disadvantages for each type of topology, and careful consideration should be used when choosing which type of network to install. The characteristics of our topology determine how the network functions and affects aspects such as installation and troubleshooting of the network. The layout and components of the four topologies are presented and the network types that implement them are discussed.

4.1.1 Bus Topology

The *bus topology* installation is the simplest. As shown in Figure 4.1, all devices are connect to the trunk cable with terminator caps* and T connectors. Terminator caps and T connectors are described below. Bus topology is not one of the best choices but it can be used with a contention network. Thus, when a device wants to transmit across the bus, it must first determine whether the media is in use. If no other device is transmitting, the signal is sent. Each device receives the signal and then determines whether its address matches that of the recipient. Messages that weren't addressed to the device are ignored.

Bus topologies use coaxial cable. A segment of coaxial cable, or simply coax, is shown in Figure 4.2. The sections are connected with T connectors. These consist of three BNC connectors. A male and female BNC type connector is shown in Figure 4.3. A *T connector* is shown in Figure 4.4. The middle connector is used to connect the devices on the network to the trunk cable, and the end connectors are used to connect to the left and right ends of the trunk cable segments. The extreme left and right connectors on the trunk cable are connected to terminator caps.

* *A terminator cap is a special connector that must be attached to each end of the trunk cable. If one or both terminator caps are missing, the network will not work.*

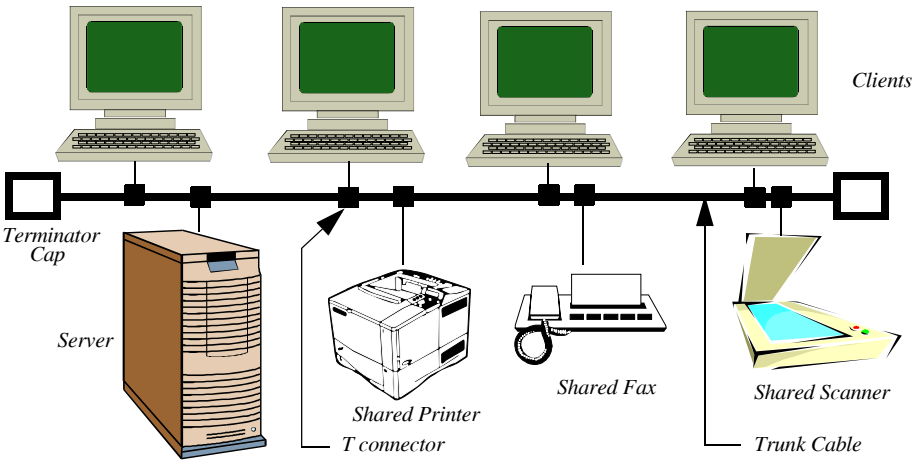


Figure 4.1. Network using Bus Topology

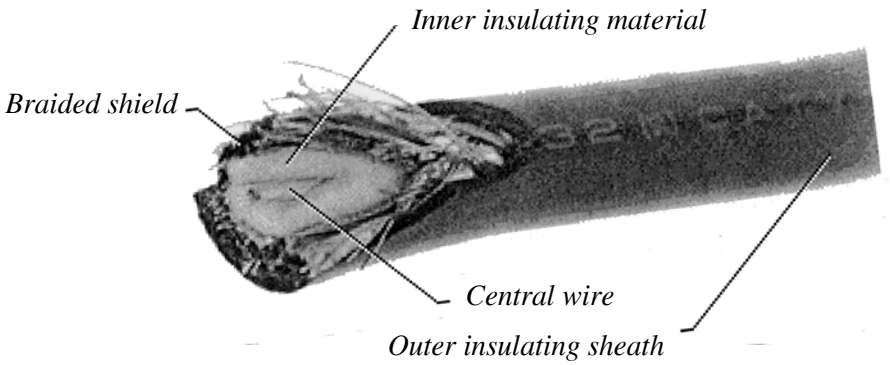


Figure 4.2. The internal construction of a coaxial cable

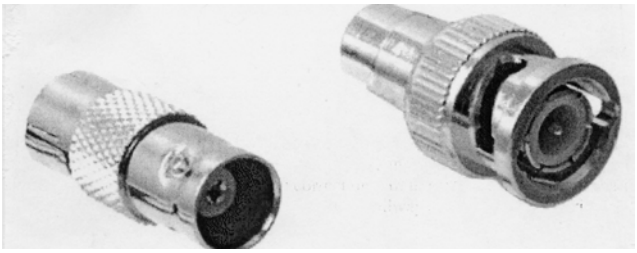


Figure 4.3. Female (left) and male (right) BNC connectors

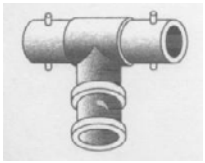


Figure 4.4. T connector

4.1.2 Star Topology

The star topology uses a separate cable for each workstation, as shown in Figure 4.5. The cable connects each workstation to a central device referred to as a hub.*

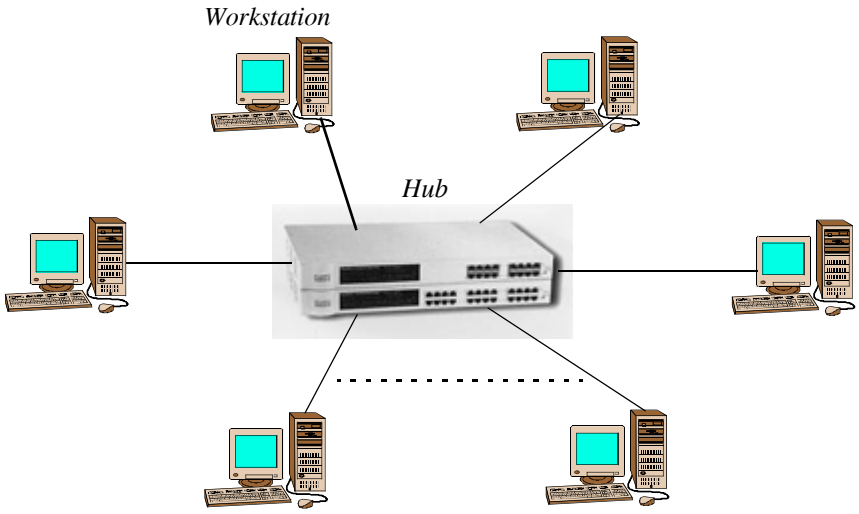


Figure 4.5. Network using Star Topology

The star architecture is more reliable network than the bus and it is easily expanded. With the star, there is no central point of failure within the cable. If there is a problem with one cable that connects a particular workstation to the hub, only that station is affected.

It may appear that a hub may become inoperative causing the entire star network architecture to become inoperative also. This is highly unlikely because the hub is, in general, a passive device. That is, hubs are very similar to patch panels where no power is required. However, some hubs are active, and as such, require external power. Active hubs are employed in cases where it is necessary to regenerate weak signals so that they can be transmitted over greater distances. Hubs are referred to as IEEE Class I and IEEE Class II repeaters. An IEEE Class I repeater is an *active hub* and a Class II repeater is a *passive hub*.

* *A hub is a device joining communication lines at a central location, providing a common connection to all devices on the network.*

Quite often, *a switch* is used to connect hosts to the internetwork. Unlike a hub where the data are routed around the network until they find its intended destination, a switch sends data to a specific location. Both hubs and switches can be used to interconnect several devices in a star network architecture. To add more workstations, one can insert another hub or switch.

A *repeater* is a device that can be added on the network and amplify the data signal that they receive. A repeater is similar to an active hub. Repeaters are rarely used now because they amplify the entire signal that they receive, including any line noise. Repeaters operate at the Physical layer of the OSI.

A *concentrator* is a device that combines signals from multiple sources, such as terminals on a network, into one or more signals before sending them to their destination. With the Fiber Distributed Data Interface (FDDI), hubs are referred to as concentrators.

A Multistation Access Unit (MSAU) is a hub or concentrator that connects a group of computers to a Token Ring local area network (discussed later in this chapter). It is also abbreviated as MAU. * An advantage of an MSAU is that if one computer fails in the ring, the MSAU can bypass it and the ring will remain intact. For instance, four computers might be connected to an MSAU in one office and that MSAU would be connected to a second MSAU in another office that serves also four other computers. The second MSAU could be connected to a third MSAU in another office which would be connected back to the first MSAU, that is, in a star topology. However, in practice, MSAUs are used a ring topology, discussed below, because every message passes through every computer one at a time, each passing it on to the next in a ring.

4.1.3 Ring Topology

The *ring topology* may be thought of as a bus topology with connected ends as shown in Figure 4.6. The ring network functions as a single loop in which the signal passes around the loop in one direction through each workstation. As the signal passes through the workstation, that workstation amplifies that signal before passing it to the next workstation. Obviously, if one of the workstations or any connection fails, the entire network will fail.†

The ring topology may be used in a large geographical area such as a factory or multi–building environment where the signal is regenerated at each workstation before it is sent to its neighbor. The signal is actually retransmitted by each system when passed on to its neighbor. The ring topology uses the so–called token passing method. With this method, a token is passed around the network. The workstation that has the token can transmit data. The data travels around the ring to its destination. The destination device returns an acknowledgment to the sender. The token is then passed on to another workstation, allowing it to transmit.

---

* *MAU is also the abbreviation for the Ethernet Media Attachment Unit.*

† *FDDI networks overcome this vulnerability by sending data on a clockwise and a counterclockwise ring. This topic is discussed later in this chapter.*

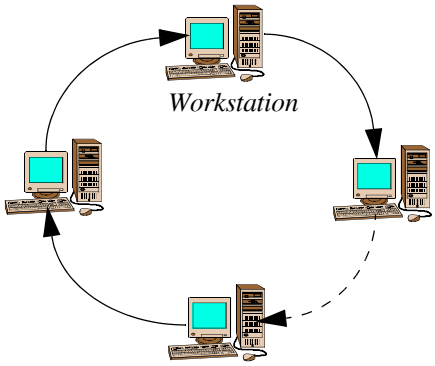


Figure 4.6. Network using Ring Topology

4.1.4 Mesh Topology

A mesh network topology is essentially a hybrid topology which uses separate cables to connect each workstation to every other workstation on the network, providing a direct communications path as shown in Figure 4.7.

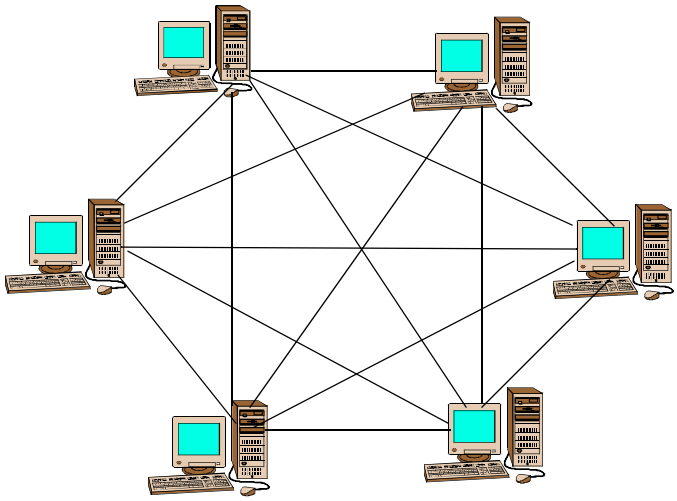


Figure 4.7. Network using Mesh Topology

With a mesh network topology, when a new workstation is added, a direct connection to all existing workstations must be made. Since there is a direct connection among each of the workstations, the mesh network topology has the highest level of reliability. However, this topology requires a large amount of interconnections. And because it is too costly and complex for practical networks, it is only used when there are only a small number of nodes to be interconnected

Table 4.1 lists the advantages and disadvantages of each of the network topologies.

TABLE 4.1 Advantages / Disadvantages among network topologies

Network Topology	Advantages	Disadvantages
Bus	• Requires only one cable • Easy to extend • The nodes are passively interconnected and thus are highly reliable	• Requires proper termination • If many devices are connected to the bus, the signals may have to regenerated
Star	• Requires only a hub as a common node, and thus it is the simplest • Easy to expand • The hub can support different types of cables	• Hub is a single point failure • More cable than the bus topology
Ring	• Can be used in a large geographical area such as a factory or multi–building environment • Can regenerate the signal at each node with the use of active repeaters • Provides an orderly transmission since every device has equal access to the token	• A single malfunction can cause the entire network to become inoperative • Addition or removal of devices may cause changes in entire network
Mesh	• Most reliable since there are dedicated lines between devices • Easy to isolate problems	• Requires dedicated lines and thus limited to small networks • Has the highest cost

4.2 Network Types

Network types are defined by many different characteristics, requirements, and specifications. Thus, maximum number of clients, data rates, distance, and media access type are all defined in the network type specification. Physical topology may also be part of the specification, as some network types can only use certain physical topologies. We should consider the many factors when deciding on the correct network type for our organization such as, cost, data rates, and ease of installation.

The networks discussed in this section are the Attached Resource Computer Network (ARCNet), the Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI).

4.2.1 Attached Resource Computer Network (ARCNet)

ARCNet is one of the oldest, simplest, and least expensive types of LANs. The first commercially LAN was developed by Datapoint Corp. in 1977. ARCNet was proprietary until the late 1980s and had about as large a market share as Ethernet among small businesses. It was almost as fast and was considerably cheaper at that time. Today, the ARCNet remains in an arcane status.

A special advantage of ARCNet is that it permits various types of transmission media – twisted–pair wire, coaxial cable, and fiber optic cable – to be mixed on the same network and can connect up to 255 nodes in a star topology. ARCNet is a data link–based network that uses the token passing access method. ARCNet can transfer data up to 2.5 Mbps and it is used today primarily for small offices with only a few workstations.

The *ARCNet Trade Association* (ATA) is a non–profit organization of ARCNet users and manufacturers formed for the purpose of promoting ARCNet and providing information and standards for users. ATA is accredited by the American National Standards Institute (ANSI) to develop American National Standards.

A new specification, called *ARCNet Plus*, supports data rates of 20 Mbps.

4.2.2 The Ethernet

The Ethernet is by far the most popular network. Industry estimates indicate that as of the turn of the century, over 100 million Ethernets had been installed worldwide. The widespread popularity of Ethernet is mainly due to *scalability*.*

The Ethernet is a LAN and was first described by Metcalfe & Boggs of Xerox PARC in 1976. It was developed DEC (acquired by Compaq and now HP), Intel and XEROX (DIX) as IEEE 802.3 and now recognized as the industry standard. The data rate is about 10 Mbps, and the Disk–Ethernet–Disk transfer rate with TCP/IP is typically 30 Kbps.

Ethernet cables are classified as "XbaseY", e.g., 10baseT, where X is the data rate in Mbps, "base" means "baseband" (as opposed to broadband, e.g., 10BROAD36†) and Y is the category‡ of cabling. The original cable was 10base5** also known as *thicknet*, 10base2†† also known as *thinnet*, and 10baseT where T stands for *Twisted pair*. 100baseTX or 100baseFX (F stands for fiber) also known as *Fast Ethernet*, and 1000baseTX or 1000baseFX also known as *Gigabit Ethernet*, and are also common.

A *Network Interface Card* (NIC) known as *10/100Base–T auto sensing LAN*, allows one to connect 10 Mbps workstations to 100 Mbps workstations. Thus, a NIC using 10/100 Mbps technology will

---

* *Scalability means that newer and faster versions of Ethernet can be integrated into networks with older and slower hardware devices while adding on new segments that run at higher data rates.*

† *This is a 10 Mbps network using broadband coaxial cable with maximum distance of 3.6 Km*

‡ *Category 5, or CAT 5 is the most reliable and widely used type of cabling. We will discuss other categories in Chapter 5.*

** *Here, "5" denotes a signaling rate of 500 meters per cable segment on a bus topology. The cable used is 10 mm "thick" RG–8 or RG–11 coaxial cable with 50 Ohm characteristic impedance. Also known as Thicknet*

†† *This variant is called Thinnet and "2"indicates the approximate cable length, i.e., 200 meters. The actual maximum length is 185 meters on a bus topology. 10Base2 uses the thinner RG–58 coaxial cable with 50 Ohm characteristic impedance that can support cable segments up to 185 meters on a bus topology.*

automatically adjust to the maximum speed of the NIC attached to the workstation to optimize our network's speed.

Each computer that is connected to the Ethernet operates independently of all other stations on the network, that is, there is no central controller. Thus, all stations attached to an Ethernet are connected to a shared signaling system, also called the medium. Ethernet signals are transmitted serially, one bit at a time, over the shared signal channel to every attached station. To send data a station first listens to the medium, and when it is idle the station transmits its data.

Data is broken into packets which are transmitted using the CSMA/CD algorithm until they arrive at the destination without colliding with any other. The first contention slot after a transmission is reserved for an acknowledge packet. A node is either transmitting or receiving at any instant.

After each frame transmission, all stations on the network must contend equally for the next frame transmission opportunity. This ensures that access to the network channel is fair, and that no single station can lock out the other stations. Access to the shared channel is determined by the medium access control (MAC) mechanism embedded in the Ethernet interface located in each station. The medium access control mechanism is based on a system called *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD).

The CSMA/CD protocol can be thought of a group of people around a table where everyone must remain silent. This period is known as *Carrier Sense*. After that short period of time everyone is given an equal opportunity to speak. This period is referred to as *Multiple Access*. If two people start talking at the same instant during the Multiple Access, both must stop talking and this is known as *Collision Detection*.

In Ethernet terminology, each interface must wait until there is no signal on the medium; then, it can begin transmitting. If some other interface is transmitting, a signal on the medium will be generated; this signal is referred to as the *carrier*. All other interfaces must wait until this carrier ceases before attempting to transmit, and this process is called *Carrier Sense*.

None of the Ethernet interfaces gets a higher priority than any other, this is what is implied by Multiple Access. Since signals take a finite time to travel from one end of an Ethernet system to the other, the first bits of a transmitted frame do not reach all parts of the network simultaneously. Therefore, it is possible for two interfaces to sense that the network is idle and to start transmitting their frames simultaneously. If this happens, the Ethernet system has a way to sense the "collision" of signals, stop the transmission, and will re–send the frames. This is called Collision Detection.

If two or more stations happen to transmit on the Ethernet medium at the same moment, then the signals will collide. The stations are notified of this event, and instantly reschedule their transmission using a special procedure. As part of this procedure the stations involved each choose a random time interval to schedule the retransmission of the frame, which keeps the stations from making transmission attempts simultaneously.

Collisions are expected events on an Ethernet. Collision occurrence is not an indication of poor design. As more computers are added to a given Ethernet network, and as the traffic level increases, more collisions will occur as part of the normal operation of the Ethernet.

The design of the system ensures that the majority of collisions on an Ethernet that is not overloaded will be resolved in a few microseconds. A normal collision does not result in lost data. In the event of a collision the Ethernet interface backs off (waits) for some number of microseconds, and then automatically retransmits the data.

On a network with heavy traffic loads it may happen that there are multiple collisions for a given frame transmission attempt. This is also normal behavior. If repeated collisions during transmission occur, then the stations involved will increase the backoff times.

Repeated collisions are an indication of a busy network. The expanding backoff process, formally known as *truncated binary exponential backoff*, is a clever feature of the Ethernet. It provides an automatic method for stations to adjust to traffic conditions on the network. After 15 consecutive collisions for a given transmission attempt the interface will finally discard the Ethernet packet. This can happen only if the Ethernet channel is overloaded for a long period of time.

The Ethernet, as well as other LAN technologies, functions as a “best effort" data delivery system. To keep the complexity and cost of the Ethernet to a reasonable level, no guarantee of reliable data delivery is made. While the bit error rate of a LAN is designed to produce a system that normally delivers accurate data, errors can still occur.

Errors also occur as a result of a burst of electrical noise that may develop somewhere in the cabling system thus causing erroneous data on the Ethernet. Also, in peak periods of data transmission activity, 16 or more collisions may occur rendering packets of information useless. No LAN system will guarantee us 100% error–free transmission.

Network software engineers can make use of higher protocol layers to improve the chances that the data reaches the intended destination correctly. High–level network protocols can do this by establishing a reliable data transport service using sequence numbers and acknowledgment mechanisms in the packets that they send over the Ethernet.

The Ethernet transmits data in frames. A *frame* consists of a set of bits organized into several fields. These fields include address fields, a variable size data field that carries from 46 to 1,500 bytes of data, and an error checking field that checks the integrity of the bits in the frame to make sure that the frame has arrived intact.

The first two fields in the frame carry 48–bit addresses, called the destination and source addresses. The IEEE controls the assignment of these addresses by administering a portion of the address field. The IEEE does this by providing 24–bit identifiers called *Organizationally Unique Identifiers* (OUIs), since a unique 24–bit identifier is assigned to each organization that wishes to build Ethernet interfaces. The organization, in turn, creates 48–bit addresses using the assigned

OUI as the first 24 bits of the address. This 48–bit address is also known as the physical address, hardware address, or MAC address.

A unique 48–bit address is normally assigned to each Ethernet interface when it is manufactured. This simplifies the setup and operation of the network and has two important advantages First, pre–assigned addresses keep us from getting involved in administering the addresses for different groups using the network. Second, it forces different work groups at a large sites to cooperate and obey the same set of rules.

As each Ethernet frame is sent onto the shared signal medium, all Ethernet interfaces examine the first 48–bit field of the frame, which contains the destination address. The interfaces compare the destination address of the frame with their own address. The Ethernet interface with the same address as the destination address in the frame will read in the entire frame and deliver it to the networking software running on that computer. All other network interfaces will disregard the entire frame when they determine that the destination address does not match their own address.

Multicast and Broadcast Addresses

A *multicast address* allows a single Ethernet frame to be received by a group of stations. Network software can set a station's Ethernet interface to listen for specific multicast addresses. This makes it possible for a set of stations to be assigned to a multicast group which has been given a specific multicast address. A single packet sent to the multicast address assigned to that group will then be received by all stations in that group.

There is also the special case of the multicast address known as the *broadcast address*, which is the 48–bit address of all ones. All Ethernet interfaces that see a frame with this destination address will read the frame in and deliver it to the networking software on the computer. An example of the use of the broadcast address will be given shortly when we review the *Address Resolution Protocol* (ARP).

Workstations attached to an Ethernet can send application data to one another using high–level protocol software, such as the TCP/IP protocol suite used on the worldwide Internet. The high–level protocol packets are carried between computers in the data field of Ethernet frames. The system of high–level protocols carrying application data and the Ethernet system are independent entities that cooperate to deliver data between computers.

High–level protocols have their own system of addresses, such as the 32–bit address used in the current version of IP. The high–level IP–based networking software in a given station is aware of its own 32–bit IP address and can read the 48–bit Ethernet address of its network interface, but it does not know what the Ethernet addresses of other stations on the network are.

To establish communications between IP–based stations on the network, we must design the Ethernet in a way to discover the Ethernet addresses of other IP–based stations on the network. For several high–level protocols, including TCP/IP, this is done using yet another high–level pro-

tocol called the *Address Resolution Protocol* (ARP). We discussed the ARP in the previous chapter. We will review it through an example of how Ethernet and one family of high–level protocols interact, so let us take a quick look at how the ARP protocol functions.

The operation of ARP is straightforward. Let us assume that an IP–based station (station "A") with IP address 164.0.5.1 wishes to send data over the Ethernet channel to another IP–based station (station "B") with IP address 164.0.5.2. Station "A" sends a packet to the broadcast address containing an ARP request. The ARP request basically says "Will the station on this Ethernet channel that has the IP address of 164.0.5.2 please tell me what the address of your Ethernet interface is?"

Since the ARP request is sent in a broadcast frame, every Ethernet interface on the network reads it in and hands the ARP request to the networking software running on the station. Only station "B" with IP address 164.0.5.2 will respond, by sending a packet containing the Ethernet address of station "B" back to the requesting station. Now station "A" has an Ethernet address to which it can send data destined for station "B," and the high–level protocol communication can proceed.

A given Ethernet system can carry several different kinds of high–level protocol data. For example, a single Ethernet can carry data between computers in the form of TCP/IP protocols as well as Novell or AppleTalk protocols. The Ethernet is simply a trucking system that carries packages of data between computers; it doesn't care what is inside the packages.

To understand how signals flow over the set of media segments that make up an Ethernet system, one must understand the signal topology of the system. The *signal topology* of the Ethernet is also known as the *logical topology*, to distinguish it from the actual physical layout of the media cables. The logical topology of an Ethernet provides a single channel (or bus) that carries Ethernet signals to all stations as explained below.

Multiple Ethernet segments can be linked together to form a larger Ethernet LAN using a repeater. Through the use of repeaters, as shown in Figure 4.8, a given Ethernet system of multiple segments can grow as a *non–rooted branching tree*. This implies that each media segment is an individual branch of the complete signal system. Even though the media segments may be physically connected in a star pattern, with multiple segments attached to a repeater, the logical topology is still that of a single Ethernet channel that carries signals to all stations.

The name *tree* is just a formal name for systems like this, and a typical network design actually ends up looking more like a complex concatenation of network segments. On media segments that support multiple connections, such as coaxial Ethernet, we may install a repeater and a link to another segment at any point on the segment. Other types of segments known as link segments can only have one connection at each end. This is explained later in this section. *Non–rooted* implies that the resulting system of linked segments may grow in any direction, and does not have a specific root segment. Most importantly, segments must never be connected in a loop. Every segment in the system must have two ends; the Ethernet system will not operate correctly in the presence of loop paths.

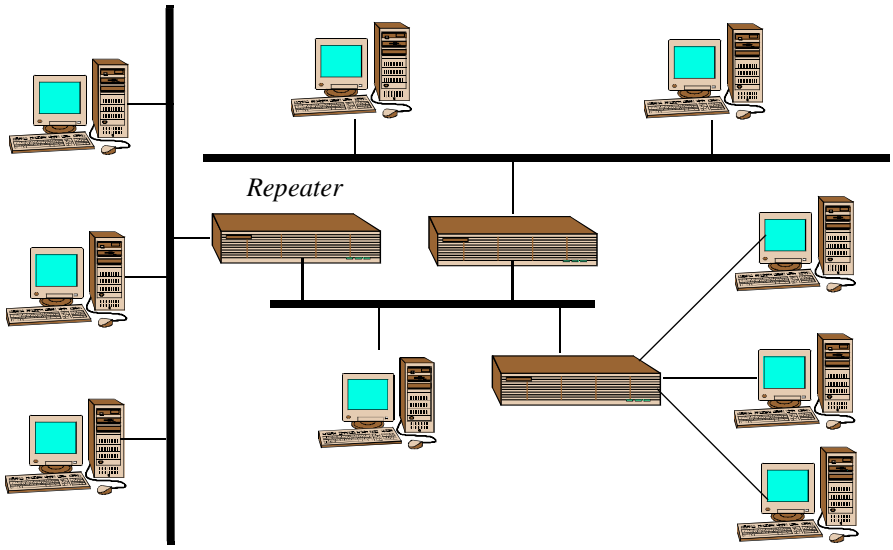


Figure 4.8. Ethernet signal topology

Figure 4.8 shows several media segments linked with repeaters and connecting to stations. A signal sent from any station travels over that station's segment and is repeated onto all other segments. This way it is heard by all other stations over the single Ethernet channel.

As shown in Figure 4.8, the physical topology may include bus cables or a star cable layout. The three workstations connected to a single repeater are laid out in the star physical topology, for example. The fact is that no matter how the media segments are physically connected together, there is one signal channel delivering frames over those segments to all stations on a given Ethernet LAN.

In order for the media access control system to work properly, all Ethernet interfaces must be capable of responding to one another's signals within a specified amount of time. The signal timing is based on the amount of time it takes for a signal to get from one end of the complete media system and back, which is known as the *round trip time*. The maximum round trip time of signals on the shared Ethernet channel is strictly limited to ensure that every interface can hear all network signals within the specified amount of time provided in the Ethernet medium access control system.

The longer a given network segment is, the more time it takes for a signal to travel over it. The intent of the configuration guidelines is to make sure that the round trip timing limits are met, no matter what combination of media segments are used in the system. The configuration guidelines provide rules for combining segments with repeaters so that the correct signal timing is maintained for the entire LAN. If the specifications for individual media segment lengths and the configuration rules for combining segments are not followed, then computers may not hear one another's signals within the required time limit, and could end up interfering with one another.

The correct operation of an Ethernet LAN depends upon media segments that are built according to the rules published for each media type. More complex LANs built with multiple media types must be designed according to the multi–segment configuration guidelines provided in the Ethernet standard. These rules include limits on the total number of segments and repeaters that may be in a given system, to ensure that the correct round trip timing is maintained.

Ethernet was designed to be easily expandable to meet the networking needs of a given site. To help extend Ethernet systems, networking vendors sell devices that provide multiple Ethernet ports. These devices are known as hubs since they provide the central portion, or hub, of a media system.

There are two major kinds of hubs: *repeater hubs* and *switching hubs*. As we've seen, each port of a repeater hub links individual Ethernet media segments together to create a larger network that operates as a single Ethernet LAN. The total set of segments and repeaters in the Ethernet LAN must meet the round trip timing specifications. The second kind of hub provides packet switching, typically based on bridging ports. These are discussed in Chapter 5.

We must remember that each port of a packet switching hub provides a connection to an Ethernet media system that operates as a separate Ethernet LAN. Unlike a repeater hub whose individual ports combine segments together to create a single large LAN, a switching hub enables us to divide a set of Ethernet media systems into multiple LANs that are linked together by way of the packet switching circuits inside the hub. The round trip timing rules for each LAN stop at the switching hub port. This allows us to link a large number of individual Ethernet LANs together.

A given Ethernet LAN can consist of merely a single cable segment linking some number of computers, or it may consist of a repeater hub linking several such media segments together. Whole Ethernet LANs can themselves be linked together to form extended network systems using packet switching hubs. While an individual Ethernet LAN may typically support anywhere from a few up to several dozen computers, the total system of Ethernet LANs linked with packet switches at a given site may support many hundreds or thousands of machines.

From the time of the first Ethernet standard, the specifications and the rights to build Ethernet technology have been made easily available to anyone. This openness, combined with the ease of use and robustness of the Ethernet system, resulted in a large Ethernet market and is another reason Ethernet is so widely implemented in the computer industry.

The vast majority of computer vendors today equip their products with 10–Mbps Ethernet attachments, making it possible to link all manner of computers with an Ethernet LAN. As the 100–Mbps standard becomes more widely adopted, computers are being equipped with an Ethernet interface that operates at both 10–Mbps and 100–Mbps. The ability to link a wide range of computers using a vendor–neutral network technology is an essential feature for today's LAN managers.

Most LANs must support a wide variety of computers purchased from different vendors, which requires a high degree of network interoperability of the sort that Ethernet provides. Ethernet is a

local area network (LAN) technology that transmits information between computers at speeds of 10 and 100 Mbps. Currently the most widely used version of Ethernet technology is the 10/100 Mbps Ethernet.

A given Ethernet system can carry several different kinds of high–level protocol data. For example, a single Ethernet can carry data between computers in the form of TCP/IP protocols as well as Novell or AppleTalk protocols. The Ethernet is simply a trucking system that carries packages of data between computers; it doesn't care what is inside the packages.

10Base5 Ethernet Network

The 10Base5 standard has a transmission speed of 10 Mbps and uses RG–8 or RG–11 coaxial cable to transmit baseband signals in 500 meter segments. This is also known as *Thick Ethernet*. The 10Base5 is the original Ethernet standard and it is also known as *Thick Ethernet* or *Thicknet*. It consists of a stiff, large diameter coaxial cable with characteristic impedance of 50 ohms and with multiple shielding. The outer sheath is usually yellow so it is often just called "yellow cable". The "10" means 10 Mbps, "base" means "baseband", and "5" means a maximum single cable length of 500 meters.

The 10base5 cable is designed to allow *transceivers*[*] to be added while existing connections are live. This is achieved using a *vampire tap*.[†] This is often built into the transceiver and a more flexible multi–wire cable carries the connection between the transceiver and the node. A 10Base–5 network is shown in Figure 4.9.

It became known as Thick Ethernet due to the RG–8 cable used in the standard. The RG–8 cable uses external transceivers and a clamp that fastens directly into the cable that is wired in a linear bus. The transceiver then connects to a transceiver cable that uses an Attachment Unit Interface (AUI). An AUI is a 15–pin connector that is used to connect to the Network Interface Card (NIC) in the workstation. Transceivers must be at least 2.5 meters apart. Each segment cannot be longer than 500 meters, and cannot have more than 100 nodes. That is, we can connect up to 100 devices to a segment.

---

* *A transceiver is a contraction for transmitter–receiver. It is a device that connects a host interface (e.g. an Ethernet controller) to a local area network. Ethernet transceivers contain electronic circuits that apply signals to the cable and sense other host's signals and collisions.*

† *A vampire tap is a connection to a coaxial cable in which a hole is drilled through the outer shield of the cable so that a clamp can be connected to the inner conductor of the cable while other spikes bite into the outer conductor. A vampire tap is used to connect each device to Thicknet coaxial cable in the bus topology of an Ethernet 10BASE–T local area network. A different connection approach, the BNC, is used for the thinner coaxial cable known as Thinnet.*

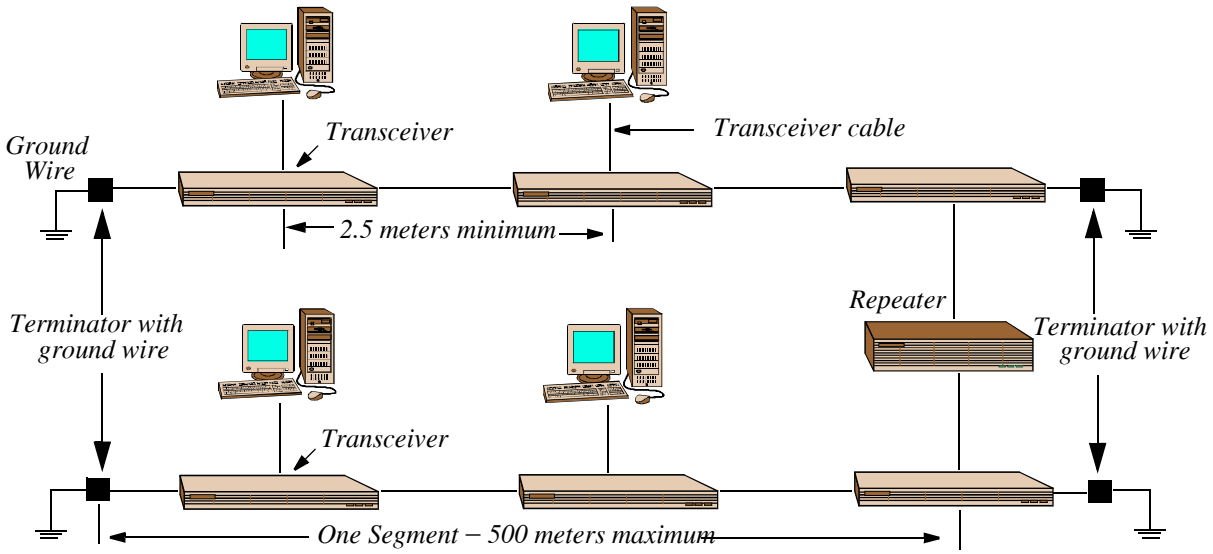


Figure 4.9. 10Base5 Ethernet network (Thick Ethernet)

The 10Base5 network is limited to 2,500 meters in total length; therefore, the entire 10Base5 network cannot have more than five segments. However, no more that three of the segments can be populated with nodes. Moreover, no more than four repeaters are allowed on the network. This is known as the *5–4–3 cabling rule*. This rule is explained below.

The Ethernet and the IEEE 802.3 standard implement a rule, known as the 5–4–3 rule, for the number of repeaters and segments on shared access Ethernet backbones.* The 5–4–3 rule divides the network into two types of physical segments: populated (user) segments, and unpopulated (link) segments. User segments have users' systems connected to them. Link segments are used to connect the network's repeaters together. The rule mandates that between any two nodes on the network, there can only be a maximum of five segments, connected through four repeaters, or concentrators, and only three of the five segments may contain user connections.

The Ethernet protocol requires that a signal sent out over the LAN reach every part of the network within a specified length of time. The 5–4–3 rule ensures this. When a signal goes through a repeater, it adds a small amount of time to the process, so the rule is designed to minimize transmission times of the signals.

The 5–4–3 rule – which was created when Ethernet, 10Base5, and 10Base2 were the only types of Ethernet network available – only applies to shared–access Ethernet backbones. A switched Ethernet network to be discussed shortly, is exempt from the 5–4–3 rule because each switch has a buffer to temporarily store data and all nodes can access a switched Ethernet LAN simultaneously.

* *Backbones are the networks that carry major communications traffic within a large network. In a LAN, a backbone may be a bus.*

The 10base–5 network is limited to 5 segments, 4 repeaters, and only in 3 of the segments can have devices installed on their nodes. The terminators at each end of a segment must include a ground wire that must be connected to the building ground.

10Base2 Ethernet Network

The 10Base2 network has a transmission speed of 10 Mbps and uses RG–58 coaxial cable whose characteristic impedance is 50 Ohms and it is used to transmit baseband signals on 185–meter segments. This is also known as *Thin Ethernet* or *cheapernet*. A 10Base2 network is shown in Figure 4.10.

The 10Base2 network uses T connectors and have a maximum length of 925 meters. The 5–4–3 rule allowing five segments, four repeaters, where only three segments can be populated with nodes, also applies to the 10Base2 networks. The maximum number of nodes on a segment is 30 nodes and thus the maximum number of nodes on the entire networks is 90 nodes. The devices connected on each segment must be at least 0.5 meter apart. The terminators at each end of a segment must include a ground wire that must be connected to the building ground.

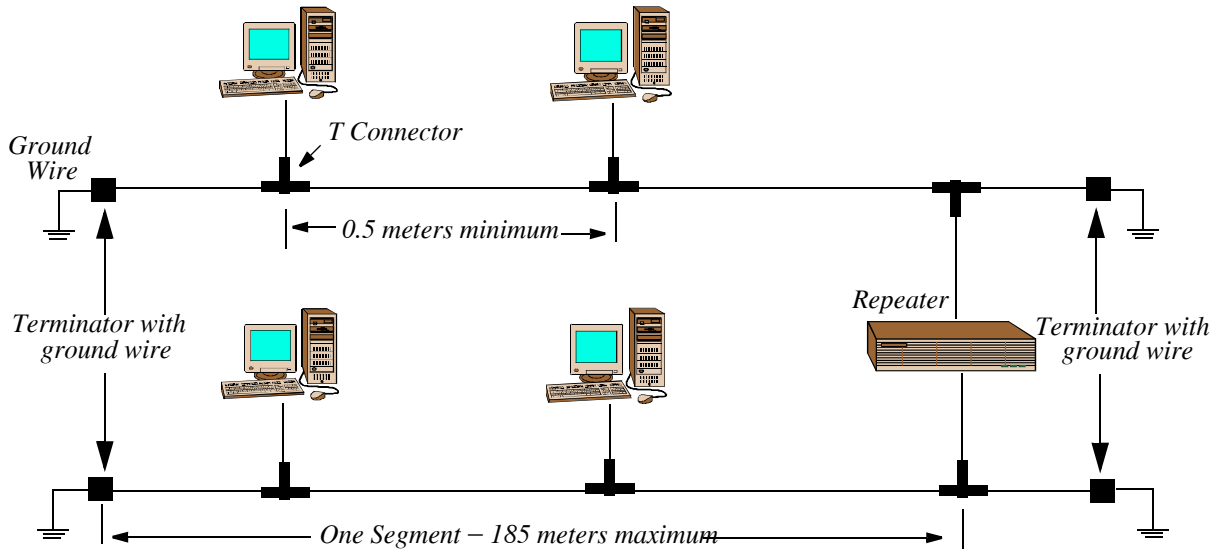


Figure 4.10. 10Base2 Ethernet network (Thin Ethernet)

10BaseT Ethernet Network

The 10BaseT standard (also called Twisted Pair Ethernet) operates at 10 Mbps and uses baseband transmission methods. It uses a twisted–pair cable with maximum lengths of 100 meters. The cable used is 22–AWG Unshielded Twisted 4–Pair (UTP) which is thinner and more flexible than the coaxial cable used for the 10Base2 or 10Base5 standards. Cables in the 10BaseT system connect with RJ–45 connectors. An RJ–45 connector is shown in Figure 4.11.

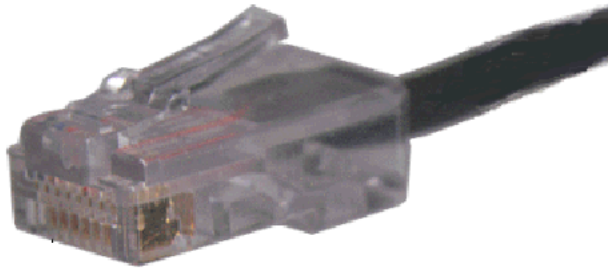


Figure 4.11. RJ–45 Connector

A star topology is common with 12 or more workstations connected directly to a hub or a switch. A 10BaseT network is shown in Figure 4.12.

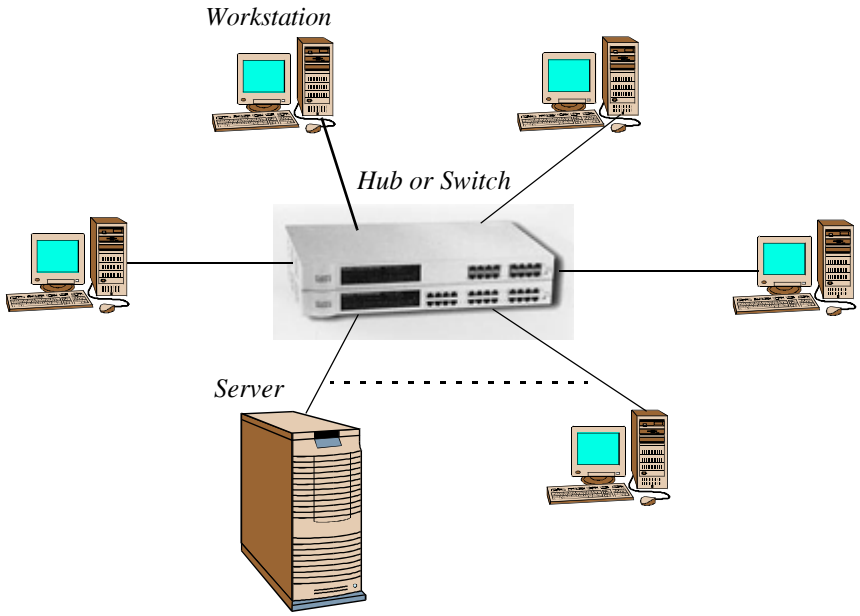


Figure 4.12. 10BaseT Ethernet network (Twisted–pair Ethernet)

As shown in Figure 4.12, each device has a separate UTP cable connecting it to the hub. The workstations and servers must be no more than 100 meters from the hub. Several hubs can be connected for a larger network. This network standard must also follow the 5–4–3 rule, which allows for five segments, four connected hubs or switches, and three populated segments. This network was very popular a few years ago but now is rarely used in new installations.

10BaseFL

The 10BaseFL is a variant of the 10BaseT. It uses fiber–optic cable at 10 Mbps using baseband signaling. Like the 10BaseT network, uses hubs or switches, and it is configured as a star network. Fiber–optic cable allows a network segment of up to 2,000 meters. This network standard is now being replaced by the faster 100BaseFX standard which is discussed on the next subsection.

Twisted Pair Cables and Categories

A twisted pair consists of insulated wires twisted around each other in pairs but electrically not contacting each other. The twisting helps to reduce unwanted signals. Twisted pair is adapted from telephone cable and it is a popular style for network cabling. This wiring may be shielded or unshielded. Cable that is rated Category 1 is shielded and Category 3 is unshielded.

All categories of cable are 4 pairs except Category 1 which is 2 pair. The standard is a category rating of 1, 2, 3, 4, 5 or 6. Category 1 cable includes most telephone cable made before 1983. It is no longer used in new installations.
Category 2 cable also has 4 pairs. It was used primarily between 1983 and 1993 as a phone and network cable standard. It handles data rates of up to 10 Mbps and was used for 4 Mbps transmissions. It has 2 to 3 twists per foot but has poor noise immunity.

Category 3 was the standard cable used for networking until 1993 brought the Category 5 standard It has 4 pairs with 3 twists per foot. Most telephone networks use this cable today.

Category 4 cable is a high grade Category 1, handling up to 20 Mbps data rates. It is constructed with 5 to 6 twists per foot.

Category 5 cable is the current standard for Ethernet and Fast Ethernet networks. It works well for telephone and other low voltage installations that need good noise rejection. It is always found in 4 pair cables although, most installers only use 2 pair per cable to reduce noise. The Category 5 standard states the twisted pairs must have at least 8 twists per foot. The general standard handles data rates of 100 Mbps or better.

Enhanced Category 5 cable has same specifications but handles data rates up to 200 Mbps. Some Enhanced Category 5 cable has 12 twists per foot and costs more.

Category 6 is a new standard. It is made to Category 5 specifications with each pair shielded and all four shielded pairs shielded again. It is designed to handle 400 Mbps data rates.

4.2.3 Fast Ethernet Networks

All of the standards mentioned earlier are only capable of 10 Mbps. New networks operate at 100 Mbps and are known as Fast Ethernets. Recently, there has been increasing interest in Fast Ethernet, which can transmit at either 10 Mbps or 100 Mbps. Fast Ethernets can transmit across UTP or fiber optics. The standards developed are dependent on the type of cable used and are discussed below. Fast Ethernets are known as IEEE 802.3u standards.

100BaseTX

The 100BaseTX network, also known as 100BaseT, is a standard for networking computers at 100 Mbps using Category 5 UTP cable. The workstation–to–hub or switch distance is limited to 100 meters. This standard uses the CSMA/CD method and can co–exist with 10BaseT networks. For 100 Mbps Fast Ethernet, the adapters and hub must be capable of 100 Mbps transfer rates. If

any 10Mbps adapters are detected, the entire network will run at 10 Mbps. Fiber optics provide for greater cable lengths at 100 Mbps than UTP cable. With UTP, we are limited to two hubs between workstations, and the hubs must be connected using a 5–meter cable.

100BaseT4

The 100BaseT4 network uses four–pair Category 3, Category 4, or Category 5 UTP cable. The 100BaseT4 operates at 100 Mbps, and the workstation–to–hub or switch distance is limited to 100 meters. This standard uses the CSMA/CD method and can co–exist with 10BaseT networks.

100BaseFX

The 100BaseFX network is a variant of the 100BaseTX that uses multimode fiber–optic cable. It is normally used as a network backbone. The allowable distance between hubs is 400 meters.

1000BaseFX

The 1000BaseFX fiber optic network, more commonly known as Gigabit Ethernet, can transmit up to 1000 Mbps or 1 Gbps. It has been reported that a new standard known as 1000BaseTX will be capable of transmitting the same rate, i.e., 1 Gbps with Category 5 UTP. Gigabit Ethernets are known as IEEE 802.3z standards.

100VG–AnyLAN

The 100VG–AnyLAN network is also a 100 Mbps Ethernet standard specified to run over four pairs of category 3 UTP wires (known as voice grade, hence the "VG"). It is called 100VG–AnyLAN because it was defined to carry both Ethernet and token ring frame types, hence the name AnyLAN. It was originally proposed by Hewlett–Packard, ratified by the ISO in 1995 but it was not widely accepted and thus now is practically extinct.

Switched Ethernets

Traditional Ethernets, such as those we've discussed thus far, are referred to as *Shared Ethernets*. Shared Ethernets use the same bandwidth. Currently, *Switched Ethernets* are becoming very popular because they are an effective and convenient way to extend the bandwidth of existing Ethernets. A switched Ethernet uses switches to connect individual hosts or segments. In the case of individual hosts, the switch replaces the repeater and effectively gives the device full 10 Mbps bandwidth (or 100 Mbps for Fast Ethernet) to the rest of the network. In a switched Ethernet the hubs are replaced with switches.

With software implementation, switches know the node address of every workstation on its ports. Thus, when a packet is directed at a workstation, the switch receives the packet and sends it directly to the destination port. But when packets are directed to several workstations, or when multiple packets from different workstations are directed to a server, collisions occur. This problem is alleviated by using both pairs of a UTP cable. With this method, one pair sends while the other pair monitors the cable for collisions.

Installing and configuring Ethernet adapters inside the computer case

Many of the current adapters have connections for the Ethernet. They include a 15–pin AUI connector, a coax connector, and an RJ–45 connector for UTP cable. When using coax cable, it is important to connect the trunk using a T connector, which connects to either another cable segment or to a terminator. Figure 4.13 shows a Fast (100BaseTX) Ethernet adapter.

Figure 4.13. Fast Ethernet Adapter (Courtesy 3 Com)

Ethernet USB Adapter

An adapter such as the 10/100 Mbps Ethernet USB adapter shown in Figure 4.14 is the easiest way to get a computer ready to share Internet access is through an available USB port. The Adapter simply plugs in to connect the PC to the cable or DSL modem, and also to share files and peripherals with other computers that are connected to the network. With instant, Plug–and–Play USB and a setup with included software, one can add sharing capability without opening the computer case to install an Ethernet card.

4.2.4 Token Ring

The Token Ring network is a token–passing, ring–shaped local area network that was developed by IBM operating at 4 Mbps. With standard telephone wiring, the Token Ring network can connect up to 72 devices; with shielded twisted–pair wiring, the network supports up to 260 devices. Although it is based on a ring (closed loop) topology, the Token Ring network uses star–shaped clusters of up to eight workstations connected to a wiring concentrator *MultiStation Access Unit* (MSAU), which, in turn, is connected to the main ring.

Figure 4.14. 10/100 Mbps Ethernet USB Adapter (Courtesy Belkin International, Inc.)

The Token Ring network is designed to accommodate microcomputers, minicomputers, and mainframes; it follows the IEEE 802.5 standard. Figure 4.15 shows an IBM token ring configuration with MSAUs.

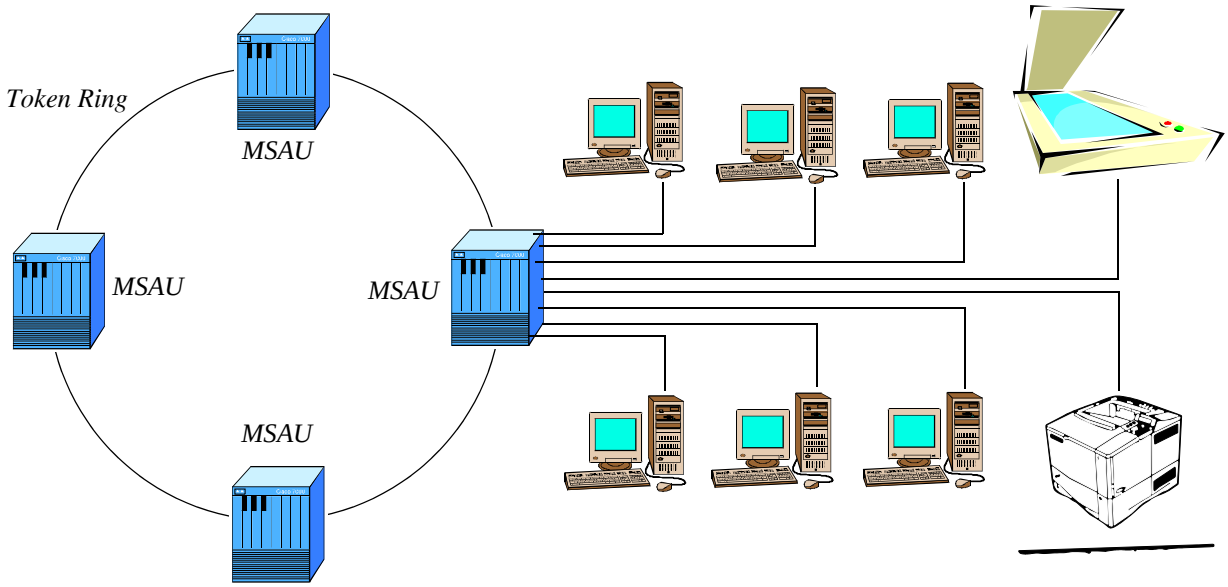


Figure 4.15. IBM Token Ring with MSAUs

While the arrangement of Figure 4.15 seems feasible since it each device is connected to the MAU, inside the central device, the ports are connected in a ring. The ring configuration does have one major weakness: there is a single point of failure. If there is a break in the ring, the entire ring breaks down. To help overcome this deficiency, Token Ring hubs can detect a break in the ring and disconnect that portion of the ring, allowing them to route the ring around the failed area. Figure 4.16 shows a practical ring arrangement on a Token Ring network.

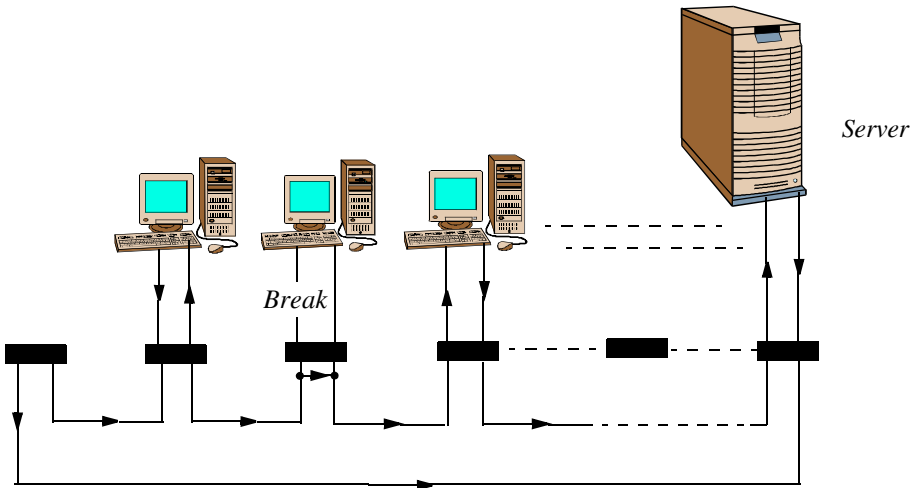


Figure 4.16. Practical ring in a Token Ring network

The major hardware components used in a Token Ring network are:

- **MultiStation Access Unit (MSAU)**: The MSAU, also known as MAU, performs the same function as a hub, but it is used on token–ring networks. To allow for expansion of the ring, each MSAU has ring–in and ring–out ports that can be attached to other MSAUs. The ring out on one MAU is connected to a ring in on the next MSAU. This continues until the ring out on the last MSAU is connected to the ring–in on the fist MSAU, forming a ring.
- **Control Access Unit (CAU):** A CAU is a more intelligent device than a MSAU and it is designed for larger workgroup Token Ring environments. It supports connectivity from 2 to 92 devices. Figure 4.17 shows the IBM 8230 Control Access Unit (CAU).

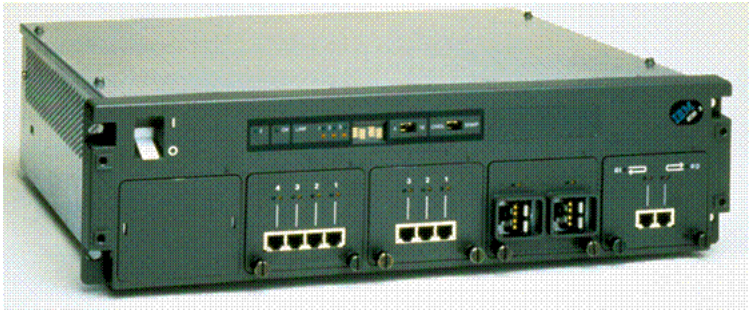


Figure 4.17. The IBM 8230 Control Access Unit (CAU)

- **Lobe Access Module (LAM)**: LAMs are Token Ring lobe extenders that effectively double (or quadruple) the lobe capacity of standard hubs and CAUs. A LAM enables the topology of 4/16 Mbps Token Ring Networks to be expanded or modified, without the need to initiate changes to the existing cabling, or to add ports to the hub or access unit at the wiring center. It is especially useful in eliminating the need for an additional MSAU. By using LAMs to add

workstations to the ring in place of extra lobe cabling, overall installation costs are reduced. The LAM is small, lightweight and easy to install. No external power supply is required.

- **Ring In / Ring Out (RI / RO) Modules**: RI / RO modules operate at 4 Mbps and 16 Mbps data rates. They support Types 1 and 2 cables; these are defined below.

Cables used in Token Ring networks

The following are the seven types of cable that can be used with IBM Token Ring:

- *Type 1:* Shielded Twisted Pair (STP) cable made of two twisted pairs of solid–core, 22–gauge AWG copper wire surrounded by a braided shield. This type of cable is run to wiring closets. It is also used to connect terminals to distribution panels. It is run through conduit and walls.
- *Type 2:* STP cable similar to Type 1 but uses four twisted pairs of telephone wires. This allows hookup of data and telephone equipment with one cable. This cable is used to connect terminals to distribution panels located in the same area.
- *Type 3:* UTP cable made of 22– or 24–gauge wire with four pairs, each twisted two times every 12 feet. This cable is subject to cross talk and is limited to shorter distances than Type 1 and 2.
- *Type 5:* Fiber–optic cable with either a 62.5– or 100–micron diameter. Type 5 cable is used only on the main ring path.
- *Type 6:* STP cable made with two 26–gauge AWG stranded–core copper wires twisted together in a shielded jacket. Type 6 STP is much easier to work with but is limited in distance and is typically only used as a patch cable or as an extension in a wiring closet.
- *Type 8:* STP cable made with two 26–gauge AWG stranded–core wires twisted together. Type 8 cable is designed to run under carpets.
- *Type 9:* STP cable made with two 26–gauge AWG stranded–core copper wires twisted together in a shielded jacket. Type 9 cable is fire retardant and designed for use in ceilings with ventilation systems.

STP is the most common frequently use cable type

Connectors in Token Ring networks

The different cable types require different types of connectors. STP cables are connected to the MSAU using a *hermaphroditic** connector such as that shown in Figure 4.18, and to the NIC using a 9–pin AUI connector. A special patch cable using hermaphroditic connectors on both ends is used to connect the ring–in and ring–out ports on the MSAU. With Token Ring networks, STP is the most frequently used cable type, but Category 5 UTP and fiber–optic cable may also be used.

* *A connector that is the same at both mating surfaces. Hermaphroditic connectors eliminate the need for separate male and female connectors.*

Figure 4.18. hermaphroditic connector (Courtesy Timbercom, Inc.)

Figure 4.19 shows a 50–pin and a 100–pin hermaphroditic connectors made by Meritec of Painesville, Ohio, www.meritec.com.

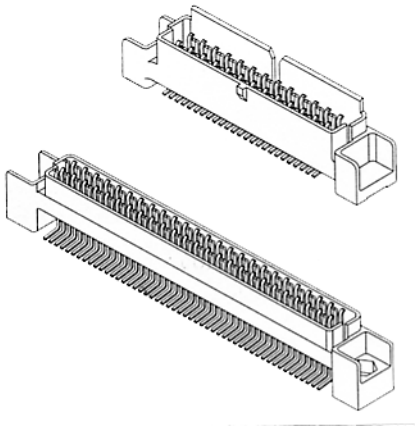


Figure 4.19. 50–pin and 100–pin hermaphroditic connectors (Courtesy Meritec Corp.)

The older Token Ring adapters used switches to configure the settings. Newer adapters have a BIOS* on–board, which stores the configuration parameters. These cards can typically handle either Plug and Play or manual settings. Token Ring adapters can operate at either 4 or 16 Mbps. The first station to be activated in a Token Ring network becomes the active monitor. The other workstations are known as standby monitors and wait for their turn to become active monitors. The active monitor has several responsibilities. It creates the token and initiates the process of identifying devices on the network. Every seven seconds a token is sent from the active monitor to its *Nearest Active Upstream Neighbor* (NAUN). The token is received from the *Nearest Active*

* *Acronym for **B**asic **I**nput/**O**utput **S**ystem. On PC–compatible computers, the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices. The BIOS is stored in read–only memory (ROM) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is invisible to computer users.*

Downstream Neighbor (NADN) and passed on to the nearest active upstream neighbor. This continues until every station has identified itself to the others on the network. During this process, each workstation learns the address of the active monitor and its nearest upstream and downstream neighbors.

Network administrators use software network analyzers to find lost tokens, to check for more than one active monitor, and to correcting problems that occur with a ring that cannot hold the token. When an error occurs, the analyzers may help us locate the device causing the error.

Token Ring networks are preferable for high–utilization networks due to their media access type. Token passing is considered deterministic because a device is guaranteed to have network access. Token passing has more overhead than CSMA and therefore is slower on a network with little congestion. On a congested network it can perform significantly higher than CSMA, though if the network gets too congested, devices will start reporting errors. If the errors increase at an alarming rate, the network administrator must take corrective action immediately; otherwise, the Token Ring network will cease all operations.

A common problem with Token Ring is a card set for 4 Mbps that is put on a 16 Mbps ring. Depending on the type of card installed, it may either remove itself from the network, or begin beaconing* and cause the entire ring to become inoperative. This monitoring process allows workstations in a Token Ring network to participate in a community watch program. Thus, beaconing helps identify fault domains, which are areas on the ring with a problem.

Once a workstation has identified a fault domain, it has the responsibility of removing the packets belonging to the failing workstation from the network. When a computer beacons the network, all systems on the network exit the ring and perform diagnostics to determine if they are responsible for the errors. The failing system tries to repair itself; this is known as *autoreconfiguration*. The failing system will remain disconnected from the ring if it cannot repair itself. Beaconing and autoreconfiguration allow a Token Ring network to attempt to diagnose and repair itself.

4.2.5 Fiber Distributed Data Interface (FDDI)

FDDI is a 100 Mbps ANSI standard local area network architecture, defined in X3T9.5. It is a token–passing ring network similar to Token Ring, but uses a fiber–optic cable†. Unlike Token Ring, FDDI allows several devices to transmit at once. Instead of using hubs, FDDI uses concentrators‡ to connect devices. A concentrator can handle up to 100 dial–up modem calls, support a

* *Beaconing is the process where a workstation sends its address, the address of its nearest active upstream neighbor, and the type of error if that nearest workstation does not receive a message from its neighbor every seven seconds.*

† *Another technology known as Copper Distributed Data Interface (CDDI) was adapted from FDDI to run over UTP cable. Like FDDI, it was intended to be used as a backbone LAN. Neither FDDI or CDDI are presently popular networks.*

‡ *A concentrator is a type of multiplexer that combines multiple channels onto a single transmission medium in such a way that all the individual channels can be simultaneously active. For example, ISPs use concentrators to combine their dial–up modem connections onto faster T1 lines that connect to the Internet.*

certain number of ISDN connections, and support leased line and frame relay traffic while also functioning as a router.

FDDI uses a topology referred to as dual–attached, counter–rotating token ring. The term *dual–attached* refers to the form of FDDI interface where a device is connected to both FDDI token–passing rings, so that uninterrupted operation continues in the event of a failure of either of the rings. All connections to the main FDDI rings are dual–attached. Typically, a small number of critical infrastructure devices such as routers and concentrators are dual–attached.

Host computers are normally single–attached or are dual–homed to a router or concentrator. *Single–attached* means that host computers are connected to only one of the two rings of an FDDI network. This is the kind of connection normally used for a host computer, as opposed to routers and concentrators which are normally dual–attached.

Dual–homed is another term used with FDDI technology. *Dual–homed* is a kind of connection to a FDDI network where a host is simultaneously connected to two separate devices such as two different concentrators in the same FDDI ring. One of the connections becomes active while the other one is automatically blocked. If the first connection fails, the backup link takes over with no perceptible delay. Thus, a dual–homed device can tolerate a fault in one of its "homes" whereas a dual–attached device can tolerate a fault in one of the rings.

Figure 4.20 shows an FDDI ring and Figure 4.21 shows a typical concentrator.

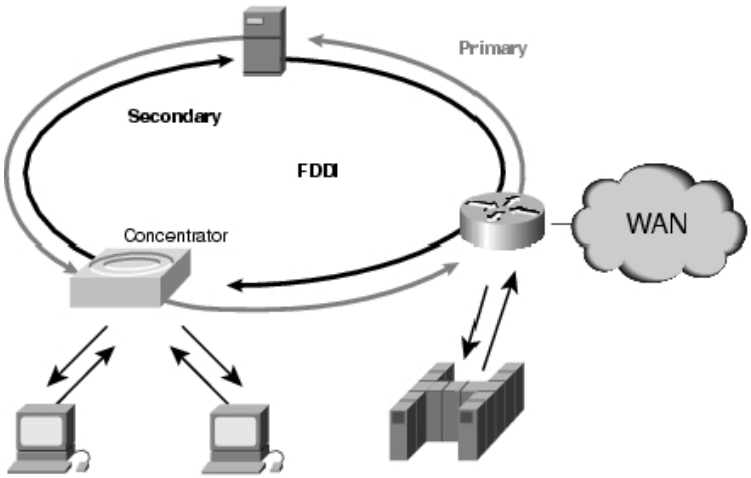


Figure 4.20. FDDI Ring (Courtesy Cisco Systems, Inc.)

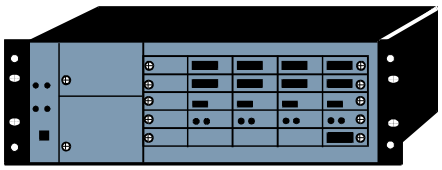


Figure 4.21. FDDI Concentrator (Courtesy 3Com, Inc.)

An FDDI network with single–attached host computers is shown in Figure 4.22. For increased reliability, an FDDI is usually implemented with two rings as shown in Figure 4.23.

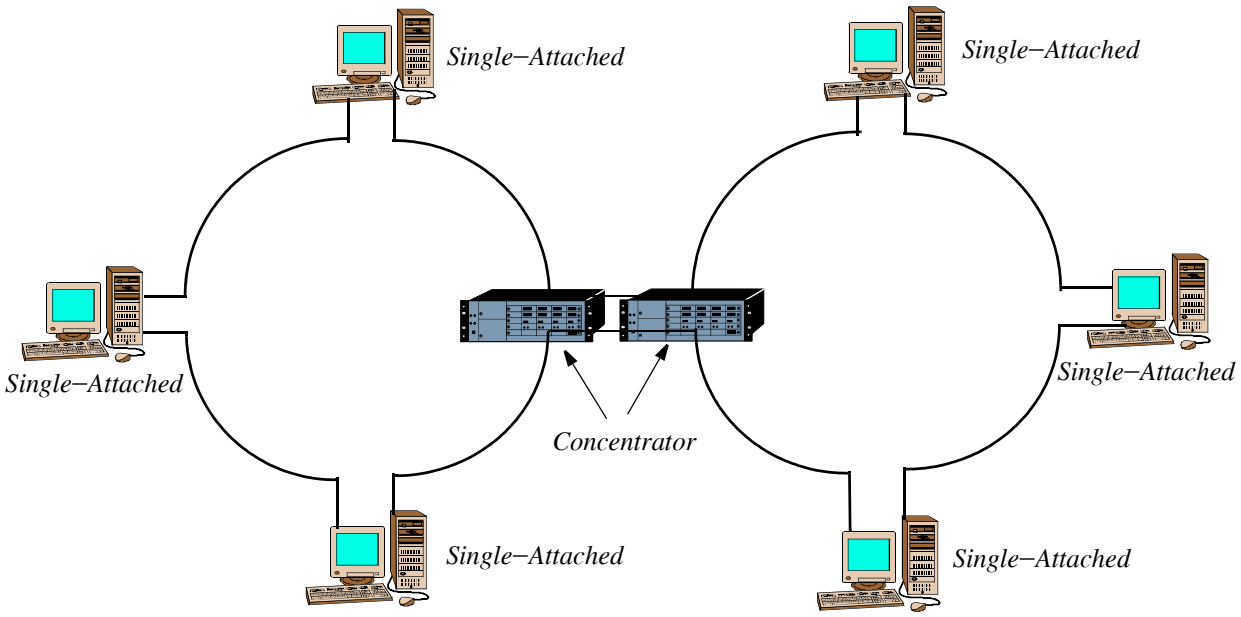


Figure 4.22. Typical connection of a FDDI network with concentrators

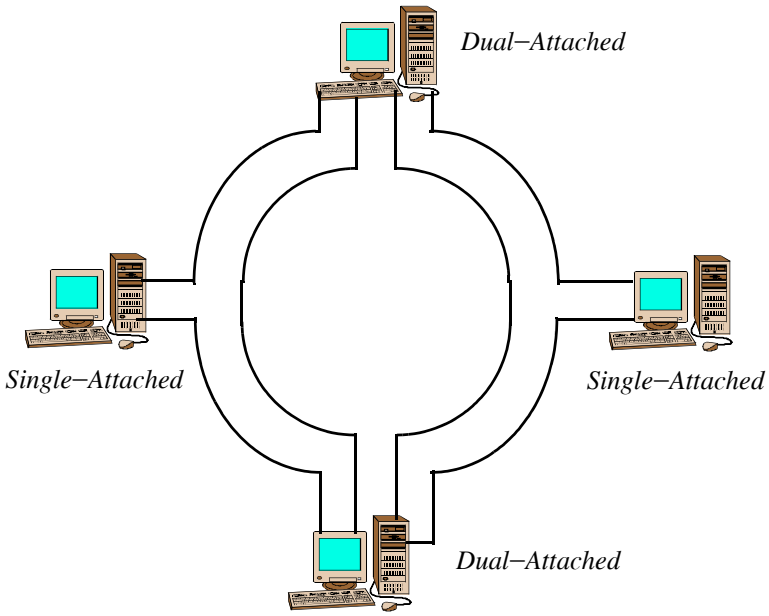


Figure 4.23. Typical connection of a Dual–ring FDDI network

For quick reference, the characteristics of each network type of networks are listed in Table 4.2.

TABLE 4.2 Characteristics of network types

Standard	Topology	Cable Type	Data Rate (Mbps)	Max Number of Nodes per Segment	Min Distance Between Nodes (Meters)	Max Segment Length (Meters)
ARCNet	Bus or Star	RG–62 UTP Fiber Optic	2.5	Variable	Variable	Coax: 600 UTP: 120 Fiber: 3500
Ethernet						
10Base5	Bus	RG–8	10	100	2.5	500
10Base2	Bus	RG–58	10	30	0.5	185
10BaseT	Star	Cat 3–5 UTP	10	1024[a]	2.5[b]	100
10BaseFL	Star	Fiber Optic	10	1024	No minimum	2000
100BaseTX	Star	Cat 5 UTP	100	1024	2.5[c]	No maximum
100BaseT4	Star	Cat 3–5 UTP	100	1024	2.5	No maximum
100BaseFX	Star	Fiber Optic	100	1024	2.5	No maximum
100VG–Any-LAN	Star	Cat 3–5 UTP	100	1024	2.5	No maximum
1000BaseFX	Star	Fiber Optic	1000	1024	2.5	No maximum
Token Ring	Physical Star Logical Ring	UTP STP Fiber Optic	4/16	UTP: 72 STP: 260 33[d]	2.5	UTP: 45 STP:101
FDDI	Ring	Fiber Optic	100	500	No minimum	200,000

a. Maximum number of network nodes and also maximum number of segments
b. Maximum distance from node to hub
c. Minimum distance between nodes
d. Maximum number of segments

Table 4.3 lists the advantages and disadvantages of the four types of networks.

TABLE 4.3 Advantages / Disadvantages of the different types of networks

Network Type	Advantages	Disadvantages
ARCNet	• Simple, reliable, and mature technology • Can operate with different cable types	• Slow speed at 2.5 Mbps • Limited to 255 devices
Ethernet	• Easy expansion • Inexpensive	• Limitation by the 5–4–3 rule
Token Ring	• Can operate at 4 or 16 Mbps	• Expensive installation
FDDI	• Fastest network operating at 100 Mbps • Can operate at distances up to 200 Km	• Expensive installation and maintenance • Expensive cable and equipment

4.3 Wireless Networks

Wireless is rapidly gaining in popularity for both home and business networking. Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a viable alternative to wired networking and continues to improve, while the cost of wireless products continues to decrease.

Most wireless local area networking (WLAN) products conform to the 802.11 "Wi–Fi" standards. A wireless network offers advantages and disadvantages compared to a wired network. Major advantages of wireless include mobility and elimination of cables. Disadvantages include the potential for radio interference due to weather, other wireless devices, or obstructions such as thick walls.

Wireless networks and their components are discussed in detail in Chapter 6.

4.4 Summary

- The four topologies used in networking are bus, star, ring, and mesh.
- In a bus topology all devices are connected to a common cable known as the bus. The bus consists of a set of hardware lines (conductors) used for data transfer among the devices of a computer network system. A bus is essentially a shared highway that connects different parts of the system. Each end of bus requires proper termination.
- In a star topology each device is connected to a central device known as the hub forming a star–shaped configuration.
- A ring topology consists of devices that are connected in a closed loop or ring. It appears like the bus topology with the ends connected.
- A mesh topology consists of devices arranged in a manner where each device is directly connected to every other device.
- The four major network types are ARCNet, Ethernet, Token Ring, and FDDI.
- The ARCNet is one of the oldest, simplest, and least expensive types of local–area network. ARCNet was introduced by Datapoint Corporation in 1977. It uses a token–ring architecture, supports data rates of 2.5 Mbps, and connects up to 255 computers. A special advantage of ARCNet is that it permits various types of transmission media – twisted–pair wire, coaxial cable, and fiber optic cable – to be mixed on the same network.
- The Ethernet is currently the most popular network type. There are several Ethernet standards and all use the CSMA/CD media access method. These standards are listed below.
- 10Base5 is the earliest Ethernet standard also known as thicknet. It is no longer used in new network installations. It was named thicknet because of the thick coax (RG–8 or RG–11) cable used. It was designed to operate at 10 Mbps and was configured in a bus topology.
- 10Base2 was designed to replace 10Base5. Like the 10Base5, 10Base2 is no longer used in new installations. It was known as thinnet because it used thinner coax (RG–58) cable. It was also designed to operate at 10 Mbps and was configured in a bus topology.
- 10BaseT was designed to replace 10Base2. Instead of coax cable, it uses UTP cable. Unlike the 10Base2 that was configured in a bus topology, 10BaseT is connected to hubs to form a star network topology. Like its predecessor, it operates at 10 Mbps but it is considered to be more reliable. Many existing networks have been configured with the 10BaseT standard.
- 10BaseFL is a variant of 10BaseT. It operates at 10 Mbps with fiber optic cable.
- 100BaseTX (or 100BaseT), known as Fast Ethernet, operates at 100 Mbps with Category 5 UTP cable. 100BaseTX networks can co–exist with 10BaseT networks. Fast Ethernets are also known as IEEE 802.3u standards.

- 100BaseT4 is similar to 100BaseTX. It operates at 100 Mbps with Category 3, or Category 4, or Category 5 UTP cable. 100BaseTX networks can co–exist with 10BaseT networks.
- 100BaseFX is a variant of the 100BaseTX network that uses multimode fiber optic cable.
- 1000BaseFX is a fiber optic cable network that can transmit up to 1000 Mbps or 1 Gbps. For this reason, it is known as Gigabit Ethernet. Gigabit Ethernets are also known as IEEE 802.3z.
- 100VG–AnyLAN proposed by Hewlett–Packard, was ratified by ISO in 1995, but it is not widely accepted. It was designed to operate both as an Ethernet and Token Ring networks.
- The IEEE–802.3 that implements the Ethernet has established the so–called 5–4–3 rule. This rule mandates that between any two nodes on the network, there can only be a maximum of five segments, connected through four repeaters, or concentrators, and only three of the five segments may contain user connections.
- MultiStation Access Units (MSAUs) are devices that are used in Token–Ring networks to connect all the computers on the network. Generally, a MSAU has 16 ports to which computers are connected. If the network has more than 16 computers, multiple MSAUs can be connected to act as a single unit
- Token Ring networks provide a viable option for large networks. Token Ring uses the token–passing media access method with the ring topology. MSAUs (Token Ring hubs) are used to form a physical star with a logical ring. Token Ring networks can operate at either 4 or 16 Mbps and operate over UTP, STP, or fiber–optic cable.
- FDDI uses fiber–optic cable in a ring topology with token passing. FDDI operates at 100 Mbps and can support two counter–rotating rings. FDDI provides more fault tolerance than Token Ring. It has the ability to detect a break in the cable and loop the two rings together.
- Although different in design and construction, hubs, MSAUs and concentrators are used interchangeably. In a token ring network configuration, the hub is referred to as a MultiStation Access Unit (MSAU). In the Fiber Distributed Data Interface (FDDI) network, hubs are referred to as concentrators.

4.5 Exercises

True/False

1. In bus topologies, terminator caps are required only at one end of the bus. _____
2. In star topologies, all devices are connected to a central device. _____
3. In ring topologies, signals can flow around the ring in both directions. _____
4. A mesh topology is considered to be the most reliable. _____
5. ARCNet is a data link–based network that uses the token passing access method. _____
6. Some Ethernets use the CSMA/CD protocols and others use the CSMA/CA protocol. _____
7. The Ethernet standards 10Base5 and 10Base2 both use coaxial cable. _____
8. Repeated collisions on a network are probably an indication of a very busy network. _____
9. MultiStation Access Units (MSAUs) are essentially hubs that are used in Token Ring networks. _____
10. A concentrator is a device that combines multiple channels onto a single transmission medium. _____

Multiple Choice

11. The _____ network permits various types of transmission media – twisted–pair wire, coaxial cable, and fiber optic cable – to be mixed on the same network.

    A. ARCNet

    B. Ethernet

    C. Token Ring

    D. FDDI

12. The Enhanced Category 5 cable can handle speeds up to _____ Mbps

    A. 100

    B. 200

    C. 500

    D. 1000

13. The Control Access Unit (CAU) is an intelligent device designed to work with larger _____ environments.

A. ARCNet

B. Ethernet

C. Token Ring

D. FDDI

14. In an IBM Token Ring network, _____ is the most frequently used cable type

A. Coax

B. UTP

C. STP

D. Fiber Optic

15. _____ is the process where a workstation sends its address, the address of its nearest active neighbor, and the type of error to the other devices on the network.

A. Autoconfiguration

B. Single–attached

C. Dual–attached

D. Beaconing

16. _____ refers to a kind of connection where a host is simultaneously connected to two separate devices in the same FDDI ring.

A. Autoconfiguration

B. Single–attached

C. Dual–attached

D. Dual–homed

17. Each Ethernet interface card is assigned a unique _____ bit address.

A. 8

B. 24

C. 48

D. 64

18. When repeated collisions occur on an overloaded Ethernet network, the packet message will be disregarded after _____ consecutive collisions.

A. 7

B. 15

C. 23

D. 31

19. The Ethernet network is defined in the _____ standard.

A. IEEE.802.2

B. IEEE.802.3

C. IEEE.802.5

D. IEEE.802.11

20. The Token Ring network is defined in the _____ standard.

A. IEEE.802.2

B. IEEE.802.3

C. IEEE.802.5

D. IEEE.802.11

Problems

21. As a network administrator, you've been informed by upper management that your company is expanding and is relocating to a new building. You've been informed by the landlord of the new building that all floors were wired with Category 5 UTP cable during the construction of that building. You have been asked to recommend a reliable, inexpensive network that can be easily expanded to accommodate future growth. Very high speed is desirable but cost is the major consideration. What type of network would do you recommend?

22. Your company uses a 16 Mbps Token Ring network. Everything worked fine until some new computers were connected to the network and several users are now complaining that the network speed is now very low. What would be the prime suspect?

23. You were recently hired as a network administrator by a company that uses a Token Ring network. You are told that his network experiences several communications problems. Your initial investigation revealed that the network is wired with STP cable and there are 283 users connected to the network. Based on these findings, can you draw any conclusions about the likely cause of the problem?

4.6 Answers to End–of–Chapter Exercises

True/False

1. F – Refer to Page 4–1
2. T – Refer to Page 4–3
3. F – Refer to Page 4–4
4. T – Refer to Page 4–5
5. T – Refer to Page 4–7
6. F – Refer to Page 4–8
7. T – Refer to Pages 4–14, 4–16
8. T – Refer to Page 4–9
9. T – Refer to Page 4–22
10. T – Refer to Page 4–25 (footnote)

Multiple Choice

11. A – Refer to Page 4–7
12. B – Refer to Page 4–18
13. C – Refer to Page 4–22
14. C – Refer to Page 4–23
15. D – Refer to Page 4–25
16. D – Refer to Page 4–26
17. C – Refer to Page 4–10
18. B – Refer to Page 4–9
19. B – Refer to Page 4–7
20. C – Refer to Page 4–21

Problems

21. 100BaseTX (Fast Ethernet) would be a good choice. The Fast Ethernet uses Category 5 UTP cable and is the most popular standard network today. Since the building is prewired with this type of cable, the only new equipment that may need to be purchased would be adapters and hubs. Moreover, the Fast Ethernet allows for future growth.

22 .Check the network cards installed in the new computers to verify that they are configured to run at 16 Mbps. Quite often, manufacturers use 4 Mbps as the default on their Token Ring network cards.

23. As indicated in Table 4.2, when STP cable is used in a Token Ring network, the number of nodes cannot be more than 260 (72 when UTP cable is used). Since there are 283 users connected to the network, it is logical to conclude that there is a good possibility that the problem with the network is that there are too many users connected to that network.

Chapter 5

Buses, Network Adapters, and LAN Connection Devices

This chapter begins with a discussion of the different buses, past and present. Network adapters are discussed next. The chapter concludes with a discussion of the different components that work together to provide source–to–destination data transmissions between devices on the same network or different networks.

5.1 Bus Architectures

A computer bus or internet *bus* is a set of hardware lines (conductors) used for data transfer among the components of a computer system. A bus is essentially a shared highway that connects different parts of the system— including the microprocessor, disk drive controller, memory, and input/output ports— and enables them to transfer information. The bus consists of specialized groups of lines that carry different types of information. One group of lines carries data; another carries memory addresses (locations) where data items are to be found; yet another carries control signals.

Buses are characterized by the number of bits they can transfer at a single time, equivalent to the number of wires within the bus. A computer with a 64–bit address bus and a 32–bit data bus, for example, can transfer 32 bits of data at a time from any of 2^{32} memory locations. Most computers contain one or more expansion slot into which additional boards can be plugged to connect them to the bus. In this section we will discuss several buses some of which are no longer in use but nevertheless provide some background in bus development by different companies.

5.1.1 Industry Standard Architecture (ISA)

The ISA is an older bus standard that was designed for the IBM PC. It became an open standard so it could be used with IBM compatibles. It is often referred to as "AT bus architecture". ISA is rarely used now, but it can be with devices such as printers, sound cards, and modems that do not require higher than 16–bit transmissions. It allows 16 bits at a time to flow between the motherboard circuitry and an expansion slot card and its associated device(s).

5.1.2 Extended Industry Standard Architecture (EISA)

The EISA (pronounced “eesa”) was designed by several companies as an open standard to be used with IBM compatibles. The EISA extended the ISA bus architecture to 32 bits and allowed more than one CPU to share the bus. Unlike MCA which is discussed in the next subsection, EISA could accept older XT bus architecture and ISA boards. EISA data transfer can reach a peak of 33

megabytes per second. The EISA bus introduced the *Bus Mastering** feature. EISA cards were designed to be configured using software. The manufacturer of the card usually provided a small configuration utility and a disk. All settings could be made using that utility.

5.1.3 Micro Channel Architecture (MCA)

The MCA was designed for multiprocessing and became IBM's proprietary 32–bit bus, used in high–end PS/2 personal computers. MCA eliminated potential conflicts that arose when installing new peripheral devices. MCA was not compatible with either EISA or XT bus architecture so older cards could not be used with it. Consequently, the MCA never became a widely accepted bus as the competing EISA standard.

5.1.4 64–bit Bus

While a 32–bus system can address about 4 gigabytes (2^{32}) of memory, some applications such as graphic games where speed is essential, require more than 4 gigabytes of memory. To this end, Advanced Micro Devices (AMD) introduced the Athlon processor to be used with 64–bus systems which can address about 18 billion gigabytes (2^{64}) of memory. The 64–bit bus is used in Windows Vista, and the Apple Mac Pro and Xserve server. It is reported that in a year or two 64–bit systems could allow computer capabilities to translate international phone calls.

5.1.5 Video Electronics Standard Architecture (VESA)

The VESA became an industry standard in 1989 to be used with IBM compatible personal computers. The first standard it created was the 800 x 600 pixel Super VGA (SVGA) display and its software interface. This standard also defined the VESA Local Bus (VLB). VLB could transfer 32 bits of information at a time, and ran at speeds of up to 40 Mbps, depending on the system's CPU speed. Originally designed for video cards, VESA was later used for hard drive controllers and network cards.

In April, 2007, the Video Electronics Standards Association (VESA) announced the introduction of the DisplayPort™ 1.1 interface standard for use in new designs of flat panel displays, projectors, PCs and peripherals. DisplayPort 1.1 allows manufacturers of LCD panels, monitors, graphics cards, PC chipsets, projectors, peripherals, components, and consumer electronics a next generation digital interface that is designed to replace VGA. It also provides the ability to connect to both internal and external displays with a common digital interface. This common interface capability means that DisplayPort 1.1 can carry pixels directly from any display source to any LCD panel, simplifying the design complexity that is present today.

* *Bus Mastering allows a card in a computer to operate without the main CPU being involved. For example, a disk controller can read and write to a hard disk by itself without involving the CPU. Normally the CPU itself handles the transaction while putting other processes on hold. Bus Mastering greatly helps multitasking operating systems.*

DisplayPort 1.1 adds support for High Bandwidth Digital Content Protection (HDCP)* version 1.3. HDCP support enables viewing of protected content from Blu–ray† and HD–DVD optical media over DisplayPort 1.1 connections.

5.1.6 Peripheral Component Interface (PCI)

Until recently, PCI was the standard for connecting peripherals to a personal computer. It was developed by Intel and released in 1993. PCI was supported by most major manufacturers including Apple Computer. It was superior to VESA's local bus. It ran at 20 to 33 Mbps and carried 32 bits at a time over a 124–pin connector or 64 bits over a 188–pin connector. With PCI, an address was sent in one cycle followed by one word of data.

PCI was used in systems based on Pentium, Pentium Pro, AMD 5x86, AMD K5 and AMD K6 processors, and Cyrix 586 and Cyrix 686 systems. It was designed to be processor independent and so it could work with other processor architectures as well.

Typical PCI cards used in PCs include: network cards, sound cards, modems, extra ports such as USB or serial, TV tuner cards and disk controllers. Historically video cards were typically PCI devices, but growing bandwidth requirements soon outgrew the capabilities of PCI. PCI video cards remain available for supporting extra monitors and upgrading PCs that do not have any AGP or PCI express slots.

Many devices traditionally provided on expansion cards are now commonly integrated onto the motherboard itself, meaning that modern PCs often have no cards fitted. However, PCI is still used for certain specialized cards, although many tasks traditionally performed by expansion cards may now be performed equally well by USB devices.

PCI is also a bridge or *mezzanine*.‡ It includes buffers to decouple the CPU from relatively slow peripherals and allow them to operate asynchronously. A mezzanine card is a smaller form of the more familiar PCI or ISA card. The original and still most popular mezzanine card is the Industry Pack (IP) card. An IP card provides a 16–bit data path. The IP card is 3.9 x 1.8 inches and has two 50–pin connectors that plug into an IP–to–PCI adapter card. The IP–to–PCI adapter card usually holds up to three IP cards.

---

* *HDCP (High–bandwidth Digital Content Protection) is a specified method from Intel for protecting copyrighted digital entertainment content that uses the Digital Video Interface (DVI) by encrypting its transmission between the video source and the digital display (receiver). The video source might be a computer, set–top box, or digital versatile disc (DVD) player, and the digital display might be an liquid crystal display (LCD), television, plasma panel, or projector.*

† *A Blu–ray Disc is an optical disc storage medium. Its main uses are high–definition video and data storage. The disc has the same physical dimensions as standard DVDs and CDs.*

‡ *The term derives from the Italian word, mezzano, which means middle. The more common use of this term is in architecture, where it is a low–ceilinged story between two main stories in a building. In theaters, a mezzanine is a balcony projecting partly over the ground floor below it. In computer language, mezzanine is a term used to describe the stacking of computer component cards into a single card that then plugs into the computer bus or data path. The bus itself is sometimes referred to as a mezzanine bus.*

Another popular mezzanine card is the PCI Mezzanine (PMC) card. This card provides 32 or 64–bit data paths and uses 64–pin connectors. Both types of mezzanine cards are widely used with a *VME bus*[*], which is an expansion bus technology that supports up to 21 cards on a single backplane. [†] The VME bus is widely used in industrial, telecommunication, and military applications.

Interfaces such as PCI–X and PCI Express, are faster but the original PCI is still in use in some systems.

5.1.7 Personal Computer Memory Card International Association (PCMCIA)

PCMCIA is an international trade association that has developed standards for several devices, such as modems, and external hard disk drives. A PCMCIA card can be plugged into notebook computers. PCMCIA cards are about the size of a credit card as shown in Figure 5.1.

Figure 5.1. A typical PCMCIA card

The PCMCIA v1.0 standard defines specifications for memory cards. Later, when other types of devices were needed, v2.0 of the standard was established. This allowed other devices, such as modems, disk drives, and network cards, to be used. PCMCIA cards are available in three different types:

- Type I: 3.3 mm thick. Type I slots on notebooks can only use Type I cards.
- Type II: 5 mm thick. Type II slots can use Type I and Type II cards.
- Type III: 10.5 mm thick. This allows us to use any of the three card types.

The Type III slot is basically two stacked Type II slots. With this arrangement, it is possible to use either two Type II cards or one Type III.

---

* *VME bus is a widely accepted backplane interconnection bus system developed by a consortium of companies led by Motorola, now standardized as IEEE 1014. It has data bus sizes of 16, 32 or 64 bits.VME bus boards can hold CPUs or peripherals.*

† *Backplane refers to a circuit board or framework that supports other circuit boards and devices and the interconnections among devices, and provides power and data signals to supported devices. As opposed to standard cabling schemes where flexible wires are used, a backplane refers to a rigid circuit board that will support higher connection speeds and more logic. For example, many SCSI systems today ship with small SCSI backplanes because the transfer rate of SCSI is getting high enough that standard cables are causing problems connecting devices. Backplanes can offer more features than a standard cable such as the ability to unplug drives without shutting the system down. Another example of a backplane is in network connection devices, such as large enterprise scale switches and routers. Some of them have a high–speed backplane, and we can plug a group of slower network connection devices into the high–speed backplane.*

All three PCMCIA card types use the same 68–pin connector. Also, with the PCMCIA software we can insert and remove cards without first removing power.

5.1.8 FireWire

The *FireWire*, also known as *I–Link* and *IEEE 1394 standard*, is a high performance serial bus interface that can be used with Macintosh and PCs. It offers high–speed communications and *isochronous*[*] real–time data services. The FireWire can transfer data between a computer and its peripherals at 100, 200, or 400 Mbps. Cable length is limited to 4.5 meters but up to 16 cables can be daisy–chained yielding a total length of 72 meters. The IEEE 1394b specification supports data rates up to 3.2 Gbit/s over optical connections up to 100 metres in length.

It can daisy–chain together up to 63 peripherals in a tree–like structure (as opposed to SCSI's linear structure). It allows peer–to–peer device communication, such as communication between a scanner and a printer, to take place without using system memory or the CPU. It is designed to support plug–and–play and hot swapping. Its six–wire cable is not only more convenient than SCSI cables but can supply up to 60 watts of power, allowing low–consumption devices to operate without a separate power cord.

5.2 Network Adapters

A *network adapter*, more commonly known as *Network Interface Card* (NIC), is an expansion board that makes it possible to connect a PC to a network. Network adapters are needed for Ethernet and Token Ring networks, but not for online services which use a modem to make the connection.The adapters in a network are connected to each other by cable.

Network adapters are available in different types such as desktop adapters, mobile adapters, server adapters, and handheld adapters. Figure 5.2 shows the EtherFast® 10/100 LAN Card made by Linksys™ intended for 32–bit PCI local bus computers. It is Windows Plug–and–Play compatible and it is built to run with fastest video, publishing, and database network applications. Besides Windows, it can also be used with NetWare and Linux.

Figure 5.2. The EtherFast® 10/100 LAN Card made by Linksys™

[*] *Isochronous transmission is a form of data transmission that guarantees to provide a certain minimum data rate, as required for time–dependent data such as video or audio. Isochronous transmission transmits asynchronous data over a synchronous data link so that individual characters are only separated by a whole number of bit–length intervals. This is in contrast to asynchronous transmission, in which the characters may be separated by arbitrary intervals, and with synchronous transmission.*

Network adapters operate at the Data Link layer of the OSI model. When a network adapter receives data, it attaches its own header containing a checksum and the network card's address before transmitting the data to its destination. The X Modem protocol, for example, transfers data in 132 byte packets. The first 131 bytes of the packet are the data being transferred, the last byte is the CRC checksum byte.

As discussed in Chapter 2, CRC (Cyclical Redundancy Check) is an algorithm that appends a byte (or bytes) to the end of a packet of bytes that acts as a checksum byte. That is, the CRC is generated by an algorithm at the transmitter and then looked at the receiver end to determine if any of the data bytes in the packet have been corrupted in the transfer. This is a protocol that is implemented with software.

Network adapters include a *transceiver* which is the physical device that connects a host interface (e.g. an Ethernet controller) to a local area network. Ethernet transceivers contain electronic circuits that apply signals to the cable and sense other host's signals and collisions. This term is used in reference to transmitter/receiver devices in cable or fiber optic systems.

A *transceiver cable* is another name for *Attachment Unit Interface* (AUI). This is also known as IEEE 802.3 cable that connects a Media Access Unit (MAU) to the networked device. The term AUI also can be used to refer to the host back–panel connector to which an AUI cable might attach.

5.2.1 Settings in Network Adapters

Presently, most network adapters are configured automatically with *Plug–and–Play* (PnP). This means that a computer can automatically detect and configure new hardware components when they are first installed ("plugged in"), and can they can be used immediately ("played with") without requiring the user to go through tedious installation procedures.Thus, with PnP, we can use a new peripheral as soon as it is plugged in.

Macintosh computers have always been designed with the plug and play capability; for PC users it became available with the introduction of Windows 95. The Plug and Play system was designed to simplify everything through resource arbitration: the operating system keeps track of which resources are allocated to which device.

If some network adapters do not have the PnP capability, we must make sure that they are configured correctly. If we add a device that does not support Plug–and–Play, the manufacturer will hopefully provide explicit directions on how to assign *Interrupt Request* (IRQ) settings for it. If we don't know what IRQ value to specify, we should call the technical support division of the device manufacturer and ask for instructions.

The most important settings are the Interrupt Request (IRQ), Input/Output (I/O), Shared Memory Address, and Direct Memory Access (DMA). Also, other adapters, such as sound and video cards, unless they have the PnP capability, they must be set properly, so their addresses will not

cause a conflict with any other adapters in our workstation. The next paragraphs of this sub–section explain the function these settings perform.

Interrupt Request (IRQ)

An IRQ causes the processor to suspend normal instruction execution temporarily and to start executing an interrupt routine. For instance, every time we press a key on our keyboard, an interrupt is generated on the keyboard IRQ. Some processors have several interrupt request inputs allowing different priority interrupts.

A PC has either 8 or 16 lines which accept interrupts from attached devices (such as a keyboard, SCSI card, scanner, sound card, mouse, etc.). Different devices competing for the same IRQ will cause conflicts. Therefore, an IRQ value must be an assigned location where the computer can expect a particular device to interrupt it when the device sends the computer signals about its operation. For example, when a printer has finished printing, it sends an interrupt signal to the computer.

The signal momentarily interrupts the computer so that it can decide what processing to do next. Since multiple signals to the computer on the same interrupt line might not be understood by the computer, a unique value must be specified for each device and its path to the computer. If we have more than one device sending IRQ signals along the same line, we will get an IRQ conflict that can freeze our computer.

Table 5.1 shows the standard, or common, IRQ usage in computers. However, IRQs can be changed, therefore this table may not always be accurate. This is why it is important to consult the manufacturer. The Cascade IRQ 2 was added to allow for IRQs higher than 8. On the original ISA bus design, only 8 IRQs were allowed, but this number proved to be inadequate. Thus, with the addition of IRQ 2, computers to have interrupt requests up to IRQ 15. However, we must remember that while some computers allow us to use IRQ 2 or 9, some will not, and some only enable us to use one of the two. Usually the only way to find out if they are available is to try them and see if our new device functions properly. We should also consult with the manufacturer.

Input/Output (I/O) Address

An I/O address is a unique address given to a peripheral device for input and output. An I/O address is used to direct traffic to and from devices attached to a computer's serial (COM) and parallel (LPT) ports or expansion cards in internal expansion slots. Each port and slot has a corresponding I/O address. COM1, for example, generally uses I/O address 3F8, although users can change its address. Some expansion cards come with an I/O address preset on the card. If the card is not set up to take advantage of those preset resources, conflicts will occur. COM port settings are not as absolute as I/O addresses, so users can change COM ports to match any I/O address. Typically, the I/O address is in the form of a three–digit hexademical number.*

* *Hexadecimal numbers are introduced in Appendix C.*

TABLE 5.1 IRQ Settings

IRQ Number	Used with
0	Timer
1	Keyboard
2	Cascade IRQ controller or video adapter
3	COM2 and COM4
4	COM1 and COM3
5	LPT2 (second printer port) or Sound Card
6	Floppy Disk Controller
7	LPT1 (first printer port)
8	Real time clock
9	Cascade from IRQ2
10	Generally unassigned. Sometimes is used with SCSI[a] controllers
11	Unassigned
12	PS/2[b] Mouse
13	Math coprocessor
14	Primary Hard Disk Controller, usually IDE[c]
15	Secondary Hard Drive Controller, if installed

a. *SCSI is an acronym for small computer system interface, a standard high–speed parallel interface defined by the X3T9.2 committee of the American National Standards Institute (ANSI). A SCSI interface is used to connect microcomputers to SCSI peripheral devices, such as many hard disks and printers, and to other computers and local area networks.*

b. *The design of the bus in IBM PS/2 computers (except Models 25 and 30). The Micro Channel is electrically and physically incompatible with the IBM PC/AT bus. Unlike the PC/AT bus, the Micro Channel functions as either a 16–bit or a 32–bit bus. The Micro Channel also can be driven independently by multiple bus master processors.*

c. *Acronym for Integrated Device Electronics. A type of disk–drive interface in which the controller electronics reside on the drive itself, eliminating the need for a separate adapter card. The IDE interface is compatible with the controller used by IBM in the PC/AT computer, but offers advantages such as look–ahead caching.*

After a network card has interrupted the CPU with an IRQ, it needs a way to communicate with the main board. Most cards use an input/output, or I/O, address to do this. We give the card a set number that the software driver also knows, and they use this to communicate. We may think of an I/O address like a postal mail address. Any information sent to that address in the computer is picked up by the network card. Table 5.2 shows the common I/O address usage. However, these addresses can change, so they may not be correct on all computers.

TABLE 5.2 Common I/O addresses

Device	Port Number (Hexadecimal)
Game Port	200
Bus Mouse	230
LPT3	270
COM2	2F8
LPT2	370
LPT1	2B0
COM1	3F8

Direct Memory Access (DMA)

Direct memory access, or DMA, enables the network adapter cards to work directly with the computer's memory. Hardware devices, ranging from keyboards to sound cards, attached to PCs can be designed to send their instructions to and from main memory in one of two ways. The default is to ask the CPU to do the work. The more efficient way is to allocate one of the PC's DMA channels to send instructions directly to memory. This leaves the CPU free to do other tasks.

Like IRQs, DMA channels are limited in number, and we cannot allocate one channel to more than one device. Most users come in contact with DMA when they install a sound card that can select the correct channel during setup.

Shared Memory

Shared Memory is memory in a parallel computer, usually RAM, which can be accessed by more than one processor, usually via a shared bus or network. Shared memory can be accessed by more than one process in a multitasking operating system with memory protection. Some Unix variants, e.g., SunOS provide this kind of shared memory.

Cache Memory

Cache is a special memory subsystem in which frequently–used data values are duplicated for quick access. A cache stores the contents of frequently–accessed RAM locations and the addresses where these data items are stored. When the processor references an address in memory, the cache checks to see whether it holds that address. If it does hold the address, the data is returned to the processor; if it does not, a regular memory access occurs. A cache is useful when RAM accesses are slow compared with the microprocessor speed, because cache memory is always faster than main RAM memory.

5.2.2 Adapter Interfaces

After installing and configuring the network adapters, a *network adapter driver* must be installed. These drivers are classified as the *Network Device Interface Specification* (NDIS) and *Open Datalink Interface* (ODI). The main purpose of these driver standards is to allow network card manufacturers to write one driver specification and have it support multiple operating systems. Another important feature of the ODI and NDIS standards is the ability to use more than one protocol on each network card. Before these standards existed, one could only load one driver per protocol, but with these we can load one driver and any number of protocols. They allow third–party vendors to easily write drivers that work with the Microsoft and Novell operating systems.

NDIS

The *Network Device Interface Specification*, or NDIS, was created by Microsoft and 3Com. It is a device driver programming interface allowing multiple protocols to share the same network hardware. For instance, both TCP/IP and IPX/SPX protocols can be used on the same NIC. A protocol manager accepts requests from the transport layer and passes them to the data link layer (routed to the correct network interface if there is more than one).

NDIS can also be used with some ISDN adapters. It is used by most companies in the PC networking community. Novell offers a similar device driver for NetWare called Open Data–Link Interface (ODI).

Besides the Windows operating system, NDIS is used with ArtiSoft's LANtastic*

ODI

The *Open Datalink Interface* (ODI), is used by Novell. It has many of the same features as NDIS and serves much the same purpose.

5.2.3 Network Adapter Connectors

The type of connector that we can use may depend on the type of network adapter we chose or the type of network to which it is to be connected. The most common connectors are listed below.

- **BNC Connector:** This is a connector for coaxial cables that locks when one connector is inserted into another and rotated 90 degrees. BNC connectors are often used with closed–circuit television. BNC connectors are used in Attached Resource Computer Network (ARCNet) and in thin Ethernet (10Base2). Figure 5.3 shows a T connector, which has three BNC con-

* *ArtiSoft is a company, known for the LANtastic range of networking products. Originally providers of proprietary, peer–to–peer network hardware and software for small installations, Artisoft now also sells Ethernet and Novell–compatible hardware and software.*

nectors on it. The T connector is used to connect the network adapter to the two pieces of coaxial cable.

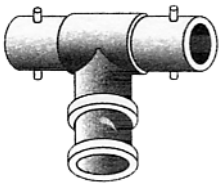


Figure 5.3. T connector with three BNC connections

- **RJ–11:** This is the most common telephone jack. Generally, it consists of six conductors but usually is implemented with four. The RJ–11 jack with four conductors is likely to be the jack that our household or office phones are plugged into from the ordinary "untwisted" wire (sometimes called "gray satin" or "flat wire") people are most familiar with. In turn, the jacks connect to the "outside" longer wires known as twisted pair that connect to the telephone company central office or to a private branch exchange (PBX).

  The four wires are usually characterized as a red and green pair and a black and white pair. The red and green pair typically carry voice or data. On an outside phone company connection, the black and white pair may be used for low–voltage signals such as phone lights. On a PBX system, they may be used for other kinds of signaling. A computer modem is usually connected to an RJ–11 jack. Figure 5.4 shows a phone line cord and a handset line cord with RJ–11 connectors at the ends.

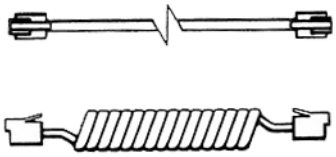


Figure 5.4. RJ–11 phone and handset line cords

- **RJ–14:** The RJ–14 is similar to the RJ–11, but the four wires are used for two phone lines. Typically, one set of wires (for one line) contains a red wire and a green wire. The other set contains a yellow and black wire. Each set carries one analog "conversation" (voice or data).
- **RJ–45:** The RJ–45 is a single–line jack for digital transmission over ordinary phone wire, either untwisted or twisted. The interface has eight pins or positions. For connecting a modem, printer, or a data PBX at a data rate up to 19.2 Kbps, we can use untwisted wire. For faster transmissions in which we are connecting to an Ethernet 10BaseT network, we need to use twisted pair wire. Untwisted is usually a flat wire like common household phone extension wire, whereas twisted is typically round.

There are two varieties of RJ–45: keyed and unkeyed. Keyed has a small bump on its end and the female complements it. Both jack and plug must match. Figure 5.5 shows the RJ–11 and RJ–45 interfaces.

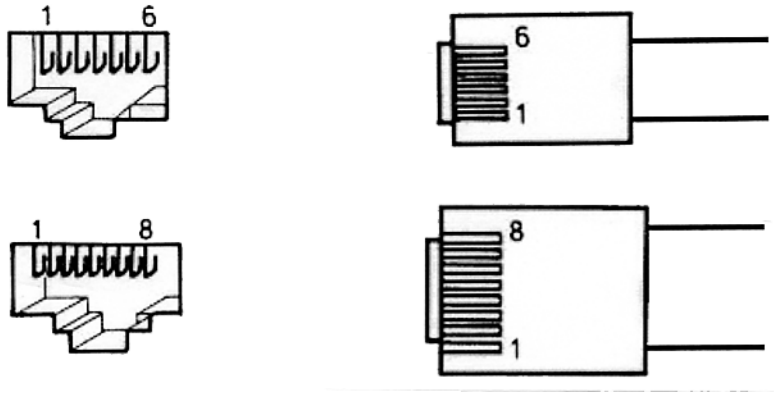


Figure 5.5. The RJ–11 and RJ–45 interfaces

- **AUI Connector:** This is the same as the Attachment Unit Interface (AUI) that we discussed earlier. AUI connectors are used for external transceivers.

5.3 LAN Connection Devices

Eventually our LAN may reach its limit on distance or number of nodes that we can have on a segment. This may happen when our network segment is too long, causing client connection errors or abundant collisions on an Ethernet network. When this happens, we may turn to hardware devices such as repeaters or bridges to extend our network and allow for future expansion.

5.3.1 Repeater

A *repeater* is an active device that receives a signal on an electromagnetic or optical transmission medium, amplifies the signal, and then retransmits it along the next leg of the medium. Repeaters overcome the attenuation caused by free–space electromagnetic–field divergence or cable loss. A series of repeaters make possible the extension of a signal over a distance. Repeaters are used to interconnect segments in a LAN. They're also used to amplify and extend wide area network transmission on wire and wireless media.

A repeater operates at the Physical layer of the OSI model. Repeaters are not concerned with protocols, packet addresses, or anything concerning the data it carries. They only understand the electrical signals shown in Figure 5.6.

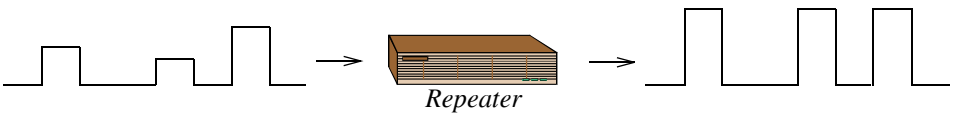


Figure 5.6. Repeater regenerating a digital signal

In addition to strengthening the signal, repeaters also remove the "noise" or unwanted aspects of the signal. Repeaters can do this with digital signals because, unlike analog signals, the original signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are restrengthened with amplifiers which unfortunately also amplify noise as well as information.

Because digital signals depend on the presence or absence of small voltage levels, they tend to attenuate more rapidly than analog signals. Whereas analog signal amplifiers can be spaced at 18,000 meter intervals, digital signal repeaters are typically placed at 2,000 to 6,000 meter intervals. Accordingly, digital signals require more frequent repeating.

In a cable system, a repeater can be simple, consisting of an amplifier circuit and a couple of signal transformers. The impedance of the cable must be matched to the input and output of the amplifier to optimize the efficiency of the amplifier. Impedance matching also minimizes reflection of signals along the cable. Such reflection can produce undesirable echo effects.

In a wireless communications system, a repeater consists of a radio receiver, an amplifier, a transmitter, an isolator, and two antennas. These are discussed in Chapter 6.

In a fiber optic network, a repeater consists of a photocell, an amplifier, and a Light–Emitting Diode (LED) or Infrared–Emitting Diode (IRED) for each light or IR signal that requires amplification. Fiber optic repeaters operate at power levels much lower than wireless repeaters, and are also much simpler and cheaper. However, their installation requires expertise in that field.

A *bus repeater* links one computer bus to a bus in another computer chassis, essentially chaining one computer to another. Repeaters are also used by amateur and commercial radio operators to extend signals in the radio frequency range from one receiver to another. These consist of *drop repeaters*, similar to the cells in cellular radio, and *hub repeaters*, which receive and retransmit signals from and to a number of directions.

Repeaters are not considered to be smart devices. We cannot connect different network types with a repeater. Thus, we cannot interface a CSMA/CD Ethernet to the polling of a Token Ring network. However, same type of networks with different types of cables can be interfaced with a repeater. For example, we can use a repeater to connect an Ethernet segment with UTP cable to another Ethernet network using coax cable.

Most network types have a limit to the number of repeaters that can be used to connect network segments. A *network segment* is a part of an Ethernet or other network, on which all message traffic is common to all nodes, i.e. it is broadcast from one node on the segment and received by all others. This is normally because the segment is a single continuous conductor. In Ethernet, this rule is called the 5–4–3 rule. This rule is discussed in Chapter 4 but it is repeated here for convenience. With this rule, we may have a total of five Ethernet segments, four repeaters, and three populated segments. The extra two segments that cannot be populated are used for distance to reach other locations. The 5–4–3 rule is illustrated in Figure 5.7.

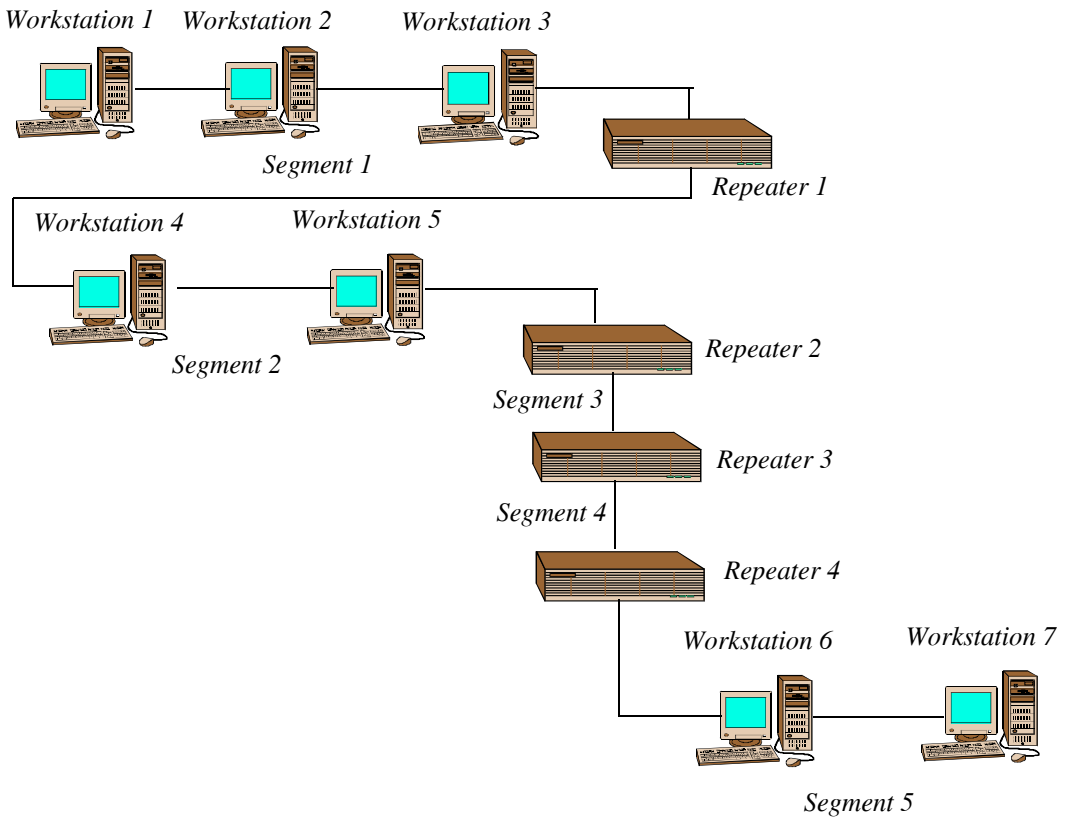


Figure 5.7. The 5–4–3 rule

Repeaters are very inexpensive and provide an easy way to extend a network. However, any more segments or repeaters that would violate the 5–4–3 rule, would cause timing problems and would affect the collision detection used by the Ethernet.

5.3.2 Bridge

A *bridge* is device that connects and controls the flow of traffic between two LANs, or two segments of the same LAN. The two LANs being connected can be alike or dissimilar. For example, a bridge can connect an Ethernet with a Token–Ring network. Bridges are protocol–independent. They simply forward packets without analyzing and re–routing messages.

Bridges operate at the Data Link layer of the OSI model and, like a repeater, attach two different network segments and pass data. The fundamental difference between a repeater and a bridge is that a repeater allows all data to pass through, whereas a bridge checks the data and determines whether they should be allowed to pass or not. For instance, if a network segment has a workstation and a server both on the same side of a bridge and these are exchanging information with each other, the bridge senses this and does not allow passage of the data. Had this been a repeater, the data would have been passed. Figure 5.8 shows two network segments interconnected with a bridge.

5.3.3 Transparent bridge

Transparent bridges are so named because their presence and operation are transparent to network hosts. When transparent bridges are powered on, they learn the workstation locations by analyzing the source address of incoming frames from all attached networks. For example, if a bridge sees a frame arrive on port 1 from Host A, the bridge concludes that Host A can be reached through the segment connected to port 1. Through this process, transparent bridges build a table.

A transparent bridge uses its table as the basis for traffic forwarding. When a frame is received on one of the bridge's interfaces, the bridge looks up the frame's destination address in its internal table. If the table contains an association between the destination address and any of the bridge's ports aside from the one on which the frame was received, the frame is forwarded out the indicated port. If no association is found, the frame is flooded to all ports except the inbound port. Broadcasts and multicasts also are flooded in this way.

Transparent bridges successfully isolate intrasegment traffic, thereby reducing the traffic seen on each individual segment. This is called *filtering* and occurs when the source and destination MAC addresses reside on the same bridge interface. Filtering usually improves network response times, as seen by the user. The extent to which traffic is reduced and response times are improved depends on the volume of intersegment traffic relative to the total traffic, as well as the volume of broadcast and multicast traffic.

We recall from our earlier discussion that each network card has a unique address assigned to it by the manufacturer. Bridges use this information to decide which frames are passed and which are not. Computer addresses are stored in a table, one for each port. When data is received, the destination address is checked, and it is compared against this table. An example follows to illustrate the procedure. Table 5.3 is filled–in as proceeding from one step to the next.

Referring back at Figure 5.8, let us assume power is turned on for the entire network, and the bridge has been initialized. Initially, the MAC address table is empty and will remain empty until a device transmits. Next, let us assume that Work Station 4 transmits data to Server 2. The bridge intercepts this message on Port 2, which is connected to Segment 2. Since the data came from Port 2 and was transmitted by Work Station 4, the bridge concludes that Work Station 4 is on the segment with Port 2, that is, Segment 2. Table 5.4 shows the current MAC address table of the bridge.

At this time, the bridge does not know which segment Server 2 is on, so the bridge allows the data to pass to the other segment, that is, Segment 1. By now, Server 2 has received the message sent by Work Station 4 and replies. The bridge senses that the message that came from Server 2 is on Segment 2. Accordingly, the MAC address of Server 2 is added to the list under Segment 2. The bridge does not allow the data to be passed on to Segment 1 because it now knows that both Work Station 4 and Server 2 are on the same segment, that is, Segment 2. Table 5.5 shows the updated MAC address table.

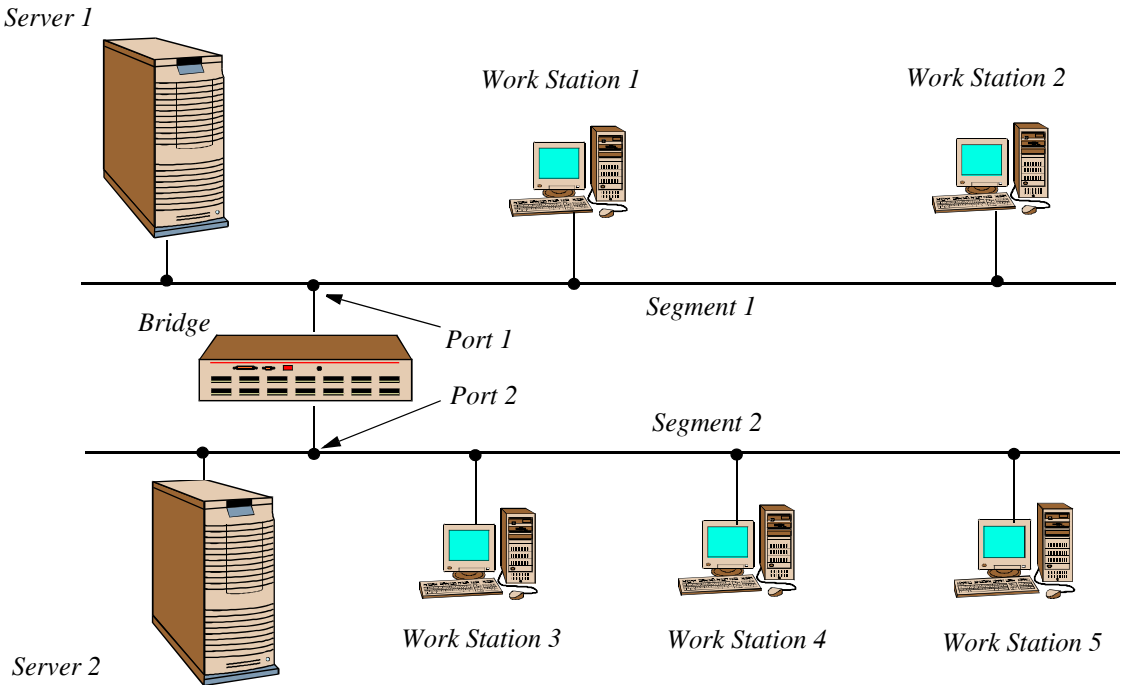


Figure 5.8. Bridged Network

TABLE 5.3 Table to illustrate the example

Segment 1	Segment 2

TABLE 5.4 Table showing that Work Station 4 is on Segment 2

Segment 1	Segment 2
	MAC address for Work Station 4

TABLE 5.5 Table showing that Server 2 is on Segment 2

Segment 1	Segment 2
	MAC address for Work Station 4
	MAC address for Server 2

Next, let us assume that Work Station 2 which is connected on Port 1 in Segment 1, sends data to Server 2. The bridge now will allow the data to pass through and reach Segment 2. Table 5.6 shows the updated MAC address table.

TABLE 5.6 Updated MAC address table with Work Station 1 on Segment 1

Segment 1	Segment 2
MAC address for Work Station 2	MAC address for Work Station 4
	MAC address for Server 2

When all transmissions from all possible sources to all possible destinations have occurred, the MAC address table will be filled with the information provided by the bridge. Table 5.7 shows the completed MAC address table. Once the table is fully filled out, the bridge knows exactly when to pass data and when to filter it.

TABLE 5.7 Completed MAC address table

Segment 1	Segment 2
MAC address for Work Station 2	MAC address for Work Station 4
MAC address for Server 1	MAC address for Server 2
MAC address for Work Station 1	MAC address for Work Station 3
	MAC address for Work Station 5

Broadcast Storming

The term **broadcast** refers to the sending a network message to all receptive parties, normally all users, that an action or activity pertaining to that group is going to, or has happened. In networking, a distinction is made between broadcasting and multicasting. *Broadcasting* sends a message to everyone on the network whereas *multicasting* sends a message to a select list of recipients. Broadcasting is a useful feature in e–mail systems. It is also supported by some fax systems.

A *broadcast storm*, also referred to as *network meltdown*, is a chain reaction that can be caused when an incorrect packet broadcast on a network forces many hosts to respond all at once, and

this may cause the entire network to malfunction. This can happen for various reasons such as hardware failure, configuration errors, and overloading the network. A broadcast storm may also occur when old TCP/IP routers are mixed with devices that support another protocol.

Bridges cannot discriminate between valid broadcast messages and broadcast storms. Broadcast storms can be minimized or eliminated by proper network design to block illegal broadcast messages. To this end, a standard known as *Spanning Tree Algorithm* or *Spanning–Tree Protocol* defined as IEEE 802.1 standard was developed to eliminate broadcast storms by providing distributed routing over multiple LANs connected by transparent bridges.

Multiple active paths between segments cause loops in the network. If a loop exists in the network, messages are often duplicated. The spanning–tree protocol provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two segments.

To provide path redundancy, the spanning–tree protocol defines a tree that spans all bridges in an extended network. It forces certain redundant data paths into a standby (blocked) state. If one network segment in the spanning–tree protocol becomes unreachable, or if paths change, the spanning–tree algorithm reconfigures the spanning–tree topology and re–establishes the link by activating the standby path.

The spanning–tree protocol operation is transparent to end stations, which are unaware whether they are connected to a single LAN segment or a switched LAN of multiple segments.

5.3.4 Source–Route Bridging (SRB)

In transparent bridging, the bridging occurs on a hop–to–hop basis whereas in source–route bridging the entire route to a destination is predetermined, in real time, prior to the sending of data to the destination. Source–route bridging is intended for Token Ring networks. The SRB algorithm was developed by IBM and was proposed to the IEEE 802.5 committee as the means to provide a bridge between all LANs using a translational bridge which is discussed on the next subsection.

In a source–routed network, the source computer sends out an explorer frame. An *explorer frame* is a frame sent out by a networked device in a source route bridging environment to determine the optimal route to another networked device. The explorer frame goes through the network remembering each bridge it passed through getting to the destination device.

Each bridge is identified by a unique number, and parallel bridges must have a different bridge number. When a bridge on a Token Ring network receives an explorer frame, it adds its bridge number to the list of the other numbers, and forwards it to other bridges until it reaches the destination device. Then, the destination device reverses the order of the bridge numbers and sends it back to the source device.

The source device may receive explorer frames with alternate paths. When all explored frames have been received, the source device selects the explorer frame with the shortest list of bridge

numbers. This list is known as *Routing Information Field* (RIF). Subsequently, the source device attaches the message packets to the RIF and sends it to the destination device.

On a very large network, the number of explorer frames that can be created from the initial frame can become very large. Therefore, on a large network, we must use some sort of filtering for these explorer frames so that their length is controllable.

5.3.5 Translational Bridge

A *translational bridge* allows us to interconnect different networks. That is, we can connect a Token Ring network to an Ethernet network with a translational bridge as shown in Figure 5.9.

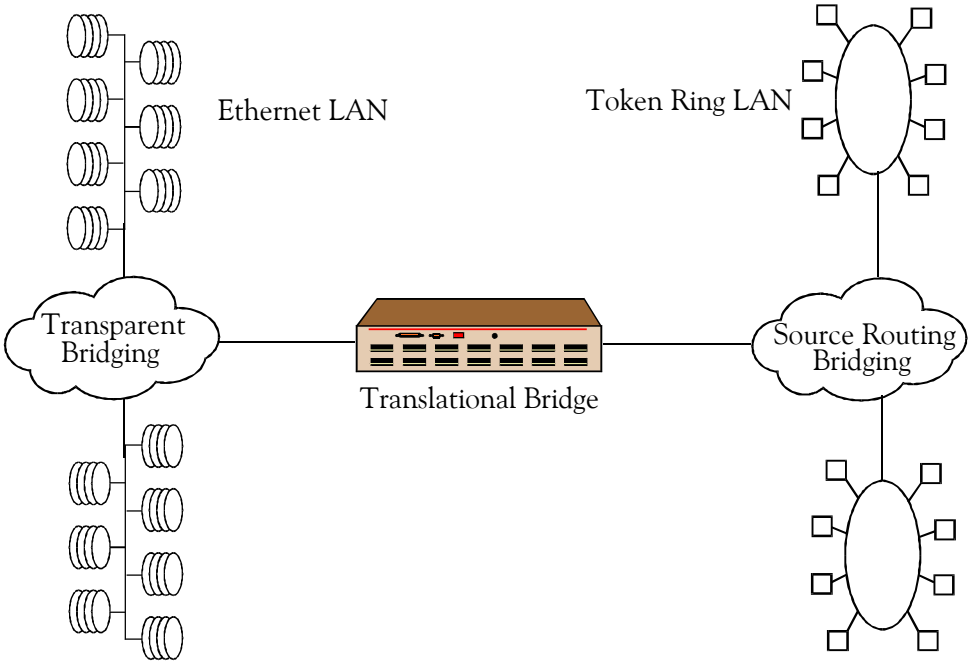


Figure 5.9. Using a translational bridge to interconnect Ethernet LANs to Token Ring LANs

Translational bridges have ports for different network types. They perform the conversion of the frames from one type to another and use the appropriate media access method. There are many translational bridges for connecting Ethernet, Token Ring, and FDDI to each other, and they can be purchased to suit the types of networks that are being connected.

Wireless translational bridges are also available. Cisco's Aironet 340 Bridge is discussed in Chapter 6.

5.3.6 Hub

Hubs range in size from four ports up to several hundred and are specific to the network type. Some hubs are just repeaters; they work the same way and follow the same rules. Hubs just repeat the signal given to them; they are not considered to be smart devices. To achieve greater connec-

tivity, a hub must be connected either to a switch or to a router. Switches and routers are discussed in Section 5.4.

There must be no more than four hubs between any two points on a network to follow the 5–4–3 rule. As discussed in Chapter 4, with UTP, we are limited to two hubs between workstations, and the hubs must be connected using a 5–meter cable.

There are two types of hubs: passive and active. *Passive hubs* provide no signal regeneration. *Active hubs* act as multiport repeaters and regenerate the data signal to all ports. Cisco's product line includes the MicroHub and the FastHub. Both are *stackable** up to 4 individual hubs per stack. The MicroHub has 32 ports per stack, and the FastHub has 96 ports per stack.

5.3.7 Switch

A *switch* is a network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router (to be discussed on the next section), a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a switch is a simpler and faster device than a router, which requires knowledge about the network and how to determine the route. A switch operates at the Data–Link layer.

On larger networks, the trip from one switch point to another in the network is called a hop. The time a switch takes to figure out where to forward a data unit is called its *latency*. The price paid for having the flexibility that switches provide in a network is this latency. Switches are found at the backbone and gateway levels of a network where one network connects with another and at the subnetwork level where data is being forwarded close to its destination or origin. The former are often known as *core switches* and the latter as *desktop switches*.

In the simplest networks, a switch is not required for messages that are sent and received within the network. For example, a local area network may be organized in a Token–Ring or bus arrangement in which each possible destination inspects each message and reads any message with its address.

A large LAN can be broken into smaller LANs and allow for network changes and future growth. Essentially, a switch provides a dedicated connection between the two network devices. Thus, a switched 10BaseT can move data faster in some cases than a 100BaseT hub, because the 100BaseT hub takes up the hub's entire bandwidth with each packet sent. A switched network is shown in Figure 5.10.

Figure 5.11 shows the 10/100 Managed 24–Port GigaSwitch® made by Linksys™ provided with 24 ports that can used with a combination of a 10BaseT, 100BaseTX, and 1000BaseFX networks.

* *Stockable means that individual devices such as hubs, can be connected together to function as a single unit.*

The Cisco Catalyst Series consists of a very large family of LAN switches. They range from the Catalyst 2900 Series that includes four models with 12 to 48 ports for Ethernet/Fast Ethernet 10/100 autosensing. These are not stackable. The Catalyst 6000 and Catalyst 8500 are Cisco's high–end switches and they are suitable for Gigabit and ATM backbones.

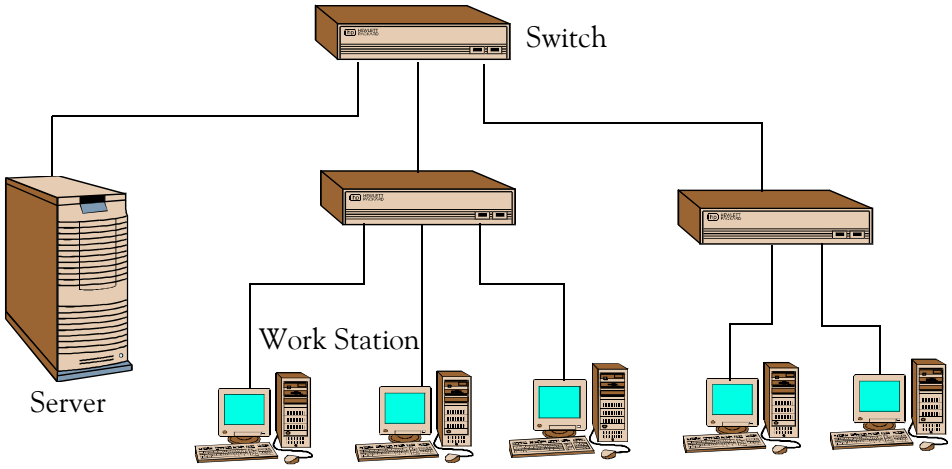


Figure 5.10. Switched network

Figure 5.11. The Managed 24–Port GigaSwitch® made by Linksys™

5.4 Internetwork Devices

This section describes other devices that can be used to interconnect one network with other networks. We will discuss routers, bridging routers (brouters), firewalls, gateways, Channel Service Units (CSUs) / Data Service Units (DSUs), modems, and multiplexers.

5.4.1 Router

A *router* is a device that finds the best path for a data packet to be sent from one network to another. A router stores and forwards messages between networks, first determining all possible paths to the destination address and then picking the most expedient route, based on the traffic load and the number of hops. Routers operate at the Network layer of the OSI model.

Routers use headers and a forwarding table to determine where packets go, and they use the *Internet Control Message Protocol* (ICMP)* to communicate with each other and configure the best route between any two hosts. Routers also act as traffic cops, allowing only authorized users to transmit data into the local network so that private information can remain secure. In addition to supporting these dial–in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.

A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Typically, a packet may travel through a number of network points with routers before arriving at its destination. Routers are more sophisticated than bridges, connecting networks of different types as shown in Figure 5.12.

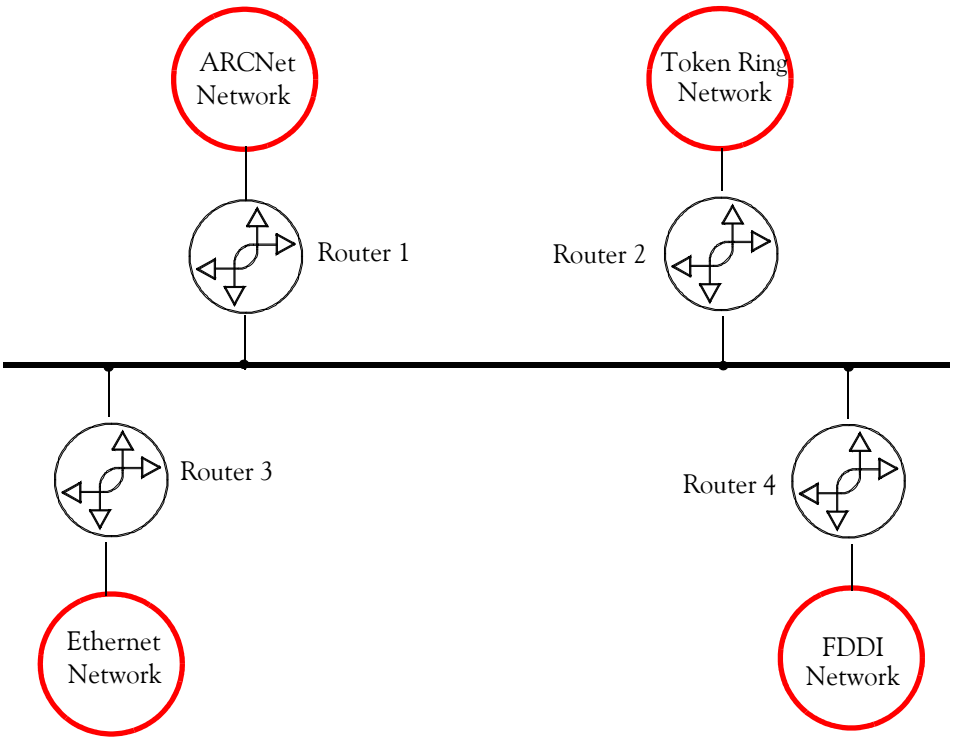


Figure 5.12. Using routers to interconnect different types of networks

Routers, such as Cisco's 4000 Series, can support Ethernet, Fast Ethernet, Token Ring, FDDI, High Speed Serial Interface (HSSI), ISDN, T1, ATM, and DSL. Also, with over 20,000 systems deployed globally, the huge Cisco 12000 Series router is industry's premier Internet routing plat-

* *ICMP is an extension to the Internet Protocol (IP) that allows for the generation of error messages, test packets, and informational messages related to IP. ICMP is a message control and error—reporting protocol between a host server and a gateway (where one network meets another) on the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.*

form based on a unique, modular distributed system architecture that offers configuration versatility, and the highest backbone performance and reliability.

An *edge router* is a device that routes data between one or more local area networks (LANs) and an ATM backbone network, whether a campus network or a wide area network (WAN). In other words, an edge router communicates with the outside world. As an example, an Internet Service Provider (ISP) uses edge routers to connect to the Internet.

The CRS–1 router introduced by Cisco in 2004 is capable of transmitting 92 trillion bits per second, and in 2008, Cisco introduced the ASR 9000* edge router that is designed to work with the core router CRS–1. The ASR 9000 router cam transmit 6.4 terabits per second, and this data is equivalent to 500,000 books, or 250,000 MP3s, or 200 movies.

A *brouter* is a network bridge combined with a router as a single device. A brouter will "bridge" some packets (i.e. forward data based on Data link layer information) and will "route" other packets (i.e. forward data based on Network layer information). The bridge/route decision is based on configuration information.

5.4.2 Firewall

A *firewall* is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users, such as hackers, from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Demilitarized Zone (DMZ), a term used to define the geographic buffer zone that was set up between North Korea and South Korea following the war in the early 1950s, is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company proprietary data.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

* *ASR is an acronym for Aggregation Services Router*

A DMZ is an optional and more secure approach to a firewall and effectively acts as a *proxy server*[*] as well.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ host's security, the Web pages might be corrupted but no other company information would be exposed. Cisco, the leading maker of router, is one company that sells products designed for setting up a DMZ.

DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers to internal networks. Internal DMZ Ethernets link local nodes with routers to the regional networks.

There are four types of firewall techniques:

Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user–defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit–level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. Figure 5.13 shows how a firewall can be used as a path through which all data must pass to access the FTP server.

5.4.3 Gateway

A *gateway* is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end–point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within a company's network or at it's local Internet service provider (ISP) are gateway nodes.

---

* *A proxy server in this case is a firewall component that manages Internet traffic to and from a local area network and can provide other features, such as document caching and access control. It improves performance by supplying frequently requested data, such as a popular Web page, and can filter and discard requests for unauthorized access to proprietary files.*

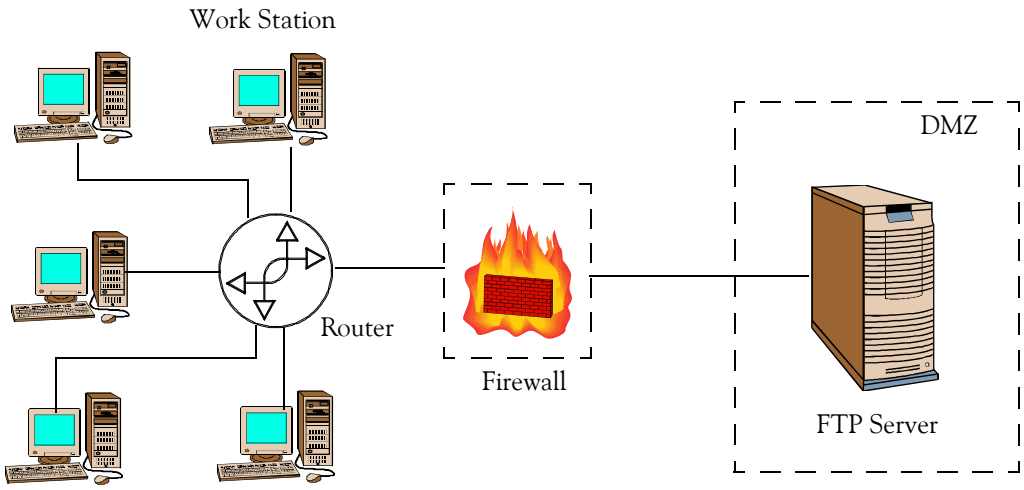


Figure 5.13. The firewall controls access to users

In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet. For this reason, some books use the terms brouter and gateway interchangeably.

However, a gateway can be used to connect networks that use different communications protocols so that information can be passed from one to the other. Thus, a gateway can transfer information and convert it to a form compatible with the protocols used by the receiving network.

Gateways are customized and designed to perform a specific function and are used on a case–by–case basis. Gateways may do anything, from protocol conversion application data conversion. Also, a gateway can be used for e–mail conversions. Gateways can operate at all seven layers of the OSI model.

Gateways can be very useful when a company makes changes from one configuration to another. During the transition, the old and new systems can perform simultaneously.

Gateways also serve as interfaces between the Public Switched Telephone Network (PSTN) telephone calls and *IP telephony* also known as *Voice over IP* (VoIP). This is a new technology that provides voice telephony services over IP connections. We will discuss VoIP on the next subsection. The *International Multimedia Teleconferencing Consortium* (IMTC) is trying to standardize this around the H.323 standard. This standard establishes multimedia standards for IP–based networks. Figure 5.14 shows a gateway that is used to connect to equipment outside the IP network.

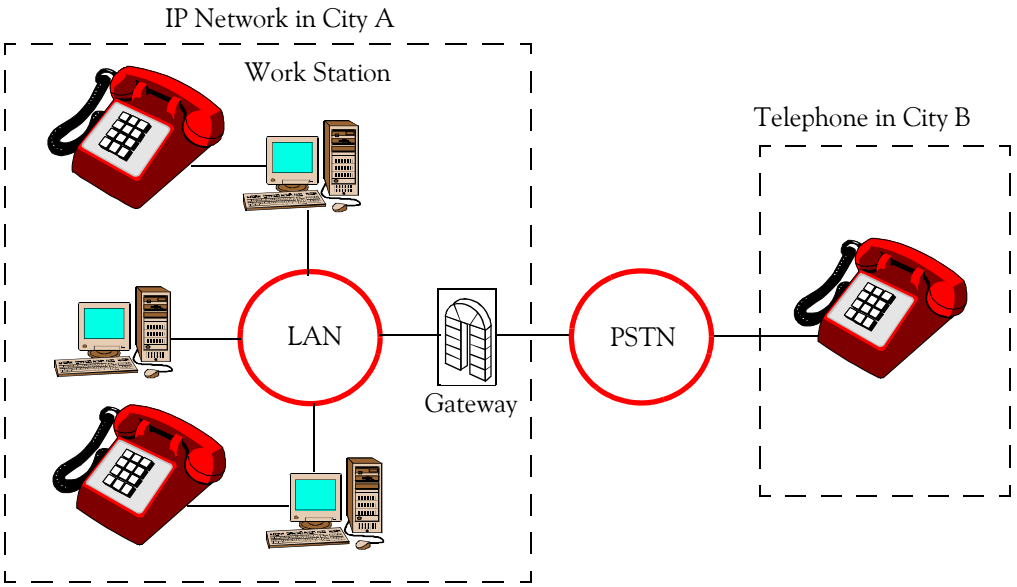


Figure 5.14. Using VoIP to establish communications from the LAN in City A to a telephone in City B

5.4.4 Voice over Internet Protocol (VoIP)

With the conventional phone system, shown in Figure 5.15, the signal travels over a dedicated connection in a continuous stream.

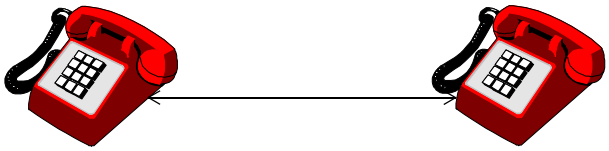


Figure 5.15. Conventional phone system

The difference between conventional phone systems and VoIP is in the transmission. When a call is placed on a traditional system, the connection between the phones stays open for the duration of the call. VoIP systems, as shown in Figure 5.16, break conversations into data packets that flow over the Internet, mixing them over the same lines without dedicated connections, and then sorting out the packets at the end so that the right conversations end up at the right phones in the right order.

To use VoIP and make Internet phone calls, one must have a DSL or cable modem which are discussed in Subsection 5.4.6, a router, and an Ethernet converter as shown in Figure 5.17.

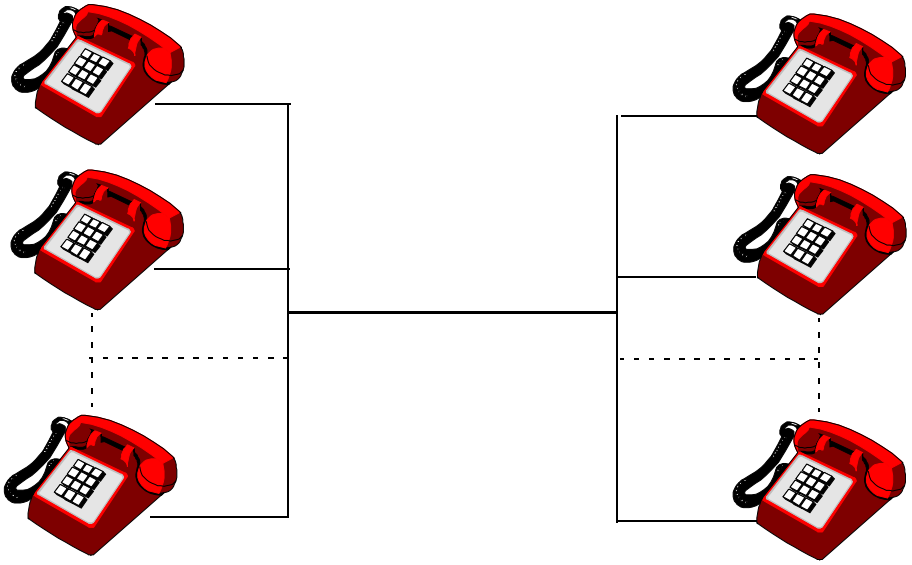


Figure 5.16. VoIP phone system

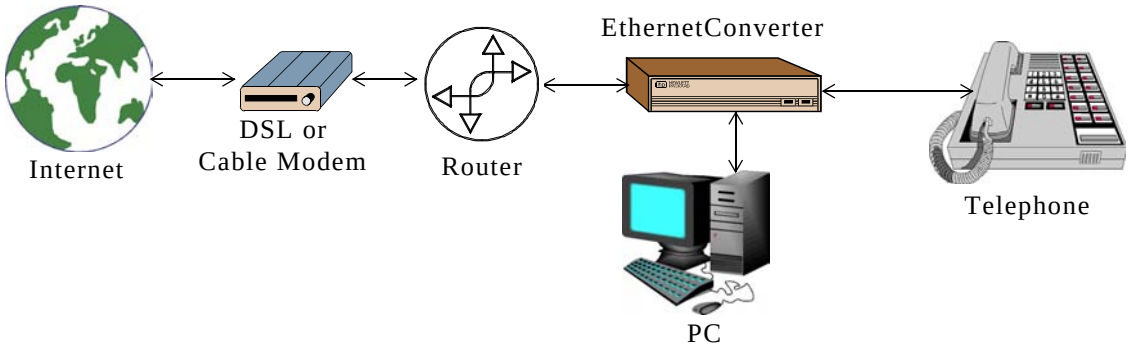


Figure 5.17. Devices used to make VoIP calls with a standard telephone

In Figure 5.17 the DSL or cable modem connects the router to the Internet. The router allows multiple computers and phones to share the internet connection. The *Ethernet converter* can be wired or wireless. Some wired Ethernet converters change signals from 10BaseT UTP to a fiber optic signal utilizing multi–mode fiber optic cable extending distances up to 2 Km, while some wireless Ethernet converters deliver wireless connectivity to any Ethernet based device. The PC can manage phone settings and keep a log of calls.

Table 5.8 lists the advantages and disadvantages of the conventional and VoIP phone systems.

TABLE 5.8 Advantages / Disadvantages of conventional and VoIP phone systems

Phone System	Advantages	Disadvantages
Conventional	• Presently more reliable	• More expensive • May require phone company service
VoIP	• Less expensive to maintain • Works with features like instant messaging • Changes on a central computer can be performed by a networks administrator	• Presently less reliable • May not accommodate large number of users

5.4.5 Channel Service Unit (CSU) / Data Service Unit (DSU)

Digital lines require both a *Channel Service Unit* (CSU) and a *Data Service Unit* (DSU). The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the data encoded in the digital circuit into synchronous serial data for connection to a DTE device. For example, if someone has a Web business operating from his own home and has leased a digital line such as T1 from his phone company or a gateway from an Internet Service Provider, he must have a CSU/DSU between his home and the phone company. A CSU/DSU operates at the physical layer of the OSI model.

The Channel Service Unit (CSU) receives and transmits signals from and to the WAN line and provides a barrier for electrical interference from either side of the unit. The CSU can also echo loopback signals from the phone company for testing purposes. The Data Service Unit (DSU) manages line control, and converts input and output between RS–232C, RS–449, or V.xx frames from the LAN and the time–division multiplexed (TDM) DSX frames on the T1 line. The DSU manages timing errors and signal regeneration. The DSU provides a modem–like interface between the computer as Data Terminal Equipment (DTE) and the CSU. CSU/DSUs are leased from the telephone company that we are getting service from.

5.4.6 MOdulator–DEModulator (Modem)

A *modem* is a device that takes digital computer signal, converts it to analog, and sends it across the phone line. Another modem on the other side does the exact opposite action. Most members connect to ISP services, and ultimately to the Internet, with a modem, though that is quickly changing to high speed cable and DSL. There are both internal and external (to the computer) modems. Modems transfer data at different speeds or rates, called baud. The original modem transfer speed was 50 bps; a few years back 300 bps was the standard. Now, the standard is 56 Kbps. This standard is known as V.90.

Various data compression and error correction algorithms are required to support the highest speeds. Other optional features are auto–dial (auto–call) and auto–answer which allow the computer to initiate and accept calls without human intervention. Most modems support a number of different protocols, and two modems, when first connected, will automatically negotiate to find a common protocol (this process may be audible through the modem or computer's loudspeakers). Some modem protocols allow the two modems to renegotiate ("retrain") if the initial choice of data rate is too high and gives too many transmission errors.

A modem may either be internal (connected to the computer's bus) or external ("stand–alone", connected to one of the computer's serial ports). The actual speed of transmission in characters per second depends not just the modem–to–modem data rate, but also on the speed with which the processor can transfer data to and from the modem, the kind of compression used and whether the data is compressed by the processor or the modem, the amount of noise on the telephone line (which causes retransmissions), and the serial character format which typically consists of one start bit, eight data bits, no parity, and one stop bit.

When two conventional modems are connected through the telephone system (PSTN), the communication is treated the same as voice conversations. This has the advantage that there is no investment required from the telephone company (telco) but the disadvantage is that the bandwidth available for the communication is the same as that available for voice conversations, usually 64 Kbps (DS0) at most. The twisted–pair copper cables into individual homes or offices can usually carry significantly more than 64 Kbps but the telco needs to handle the signal as digital rather than analog.

A *cable modem* is a type of modem that allows us to access the Internet via their cable television service. A cable modem can transfer data at 500 Kbps or higher, compared with 56 Kbps for common telephone line modems, but the actual transfer rates may be lower depending on the number of other simultaneous users on the same cable.

A *DSL modem* uses Digital Subscriber Line (DSL) technology. Digital Subscriber Line is a technology that assumes digital data does not require change into analog form and back. Digital data is transmitted to our computer directly as digital data and this allows the phone company to use a much wider bandwidth for transmitting it to us. Meanwhile, if we choose, the signal can be separated so that some of the bandwidth is used to transmit an analog signal so that we can use our telephone and computer on the same line and at the same time.

DSL technology brings high–bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL. The first technology based on DSL was ISDN, although ISDN is not often recognized as such nowadays. Since then a large number of other protocols have been developed, collectively referred to as xDSL, including High–data–rate Digital Subscriber Line (HDSL), Symmetric Digital subscriber Line (SDSL), Asymmetric Digital Subscriber Line (ADSL), and VDSL.

HDSL is a form of Digital Subscriber Line, providing T1 or E1 connections over two or three twisted–pair copper lines, respectively. Unlike most other forms of DSL, HDSL is not a typical consumer service; it is used mostly to replace traditional T1/E1 connections, such as connecting a PBX to a telephone company. The advantage of HDSL over the Alternate Mark Inversion* (AMI) line coding scheme traditionally used on T1/E1 lines is that it requires about an order of magnitude lower bandwidth to carry the same traffic.

SDSL is digital telecommunications technology that allows data transmission at speeds up to 384 Kbps in both directions through copper wire.

ADSL Technology and equipment allowing high–speed digital communication, including video signals, across an ordinary twisted–pair copper phone line, with speeds up to 9 Mbps downstream (to the customer) and up to 800 kbps upstream.

VDSL A form of Digital Subscriber Line similar to ADSL but providing higher speeds at reduced lengths.

Assuming that someone's home or small business is close enough to a telephone company central office that offers DSL service, he may be able to receive data at rates up to 6.1 Mbps (of a theoretical 8.448 Mbps), enabling continuous transmission of motion video, audio, and even 3–D effects. More typically, individual connections will provide from 1.544 Mbps to 512 Kbps downstream and about 128 Kbps upstream.

A DSL line can carry both data and voice signals and the data part of the line is continuously connected. DSL installations began in 1998 and will continue at a greatly increased pace through the next decade in a number of communities in the U.S. and elsewhere.

Compaq (now HP), Intel, and Microsoft working with telephone companies have developed a standard and easier–to–install form of ADSL called G.*lite* that is, accelerating deployment. DSL is rapidly replacing ISDN in many areas and to compete with the cable modem in bringing multimedia and 3–D to homes and small businesses.

5.4.7 How DSL Works

Traditional phone service (sometimes called POTS for "plain old telephone service") connects our home or small business to a telephone company office over copper wires that are wound around each other and called twisted pair. Traditional phone service was created to let us exchange voice information with other phone users and the type of signal used for this kind of transmission is called an analog signal. An input device such as a phone set takes an acoustic signal (which is a natural analog signal) and converts it into an electrical equivalent in terms of vol-

* *Alternate Mark Inversion (AMI) is a signal–encoding scheme in which a "1" is represented alternately as positive and negative voltage. It does not use translation coding but can detect noise–induced errors at the hardware level. The AMI code is a three–level code (+, –, 0). The 0 level represents a binary zero and the alternate + and – represents the binary 1. An example is presented given in Chapter 6.*

ume (signal amplitude) and pitch (frequency of wave change). Since the telephone company's signalling is already set up for this analog wave transmission, it's easier for it to use that as the way to get information back and forth between our telephone and the telephone company. That's why our computer has to have a modem – so that it can demodulate the analog signal and turn its values into the string of 0 and 1 values that is called digital information.

Because analog transmission only uses a small portion of the available amount of information that could be transmitted over copper wires, the maximum amount of data that we can receive using ordinary modems is about 56 Kbps (with ISDN, which one might think of as a limited precursor to DSL, we can receive up to 128 Kbps). The ability of our computer to receive information is constrained by the fact that the telephone company filters information that arrives as digital data, puts it into analog form for our telephone line, and requires our modem to change it back into digital. Figure 5.17 shows how LANs can be connected via modems.

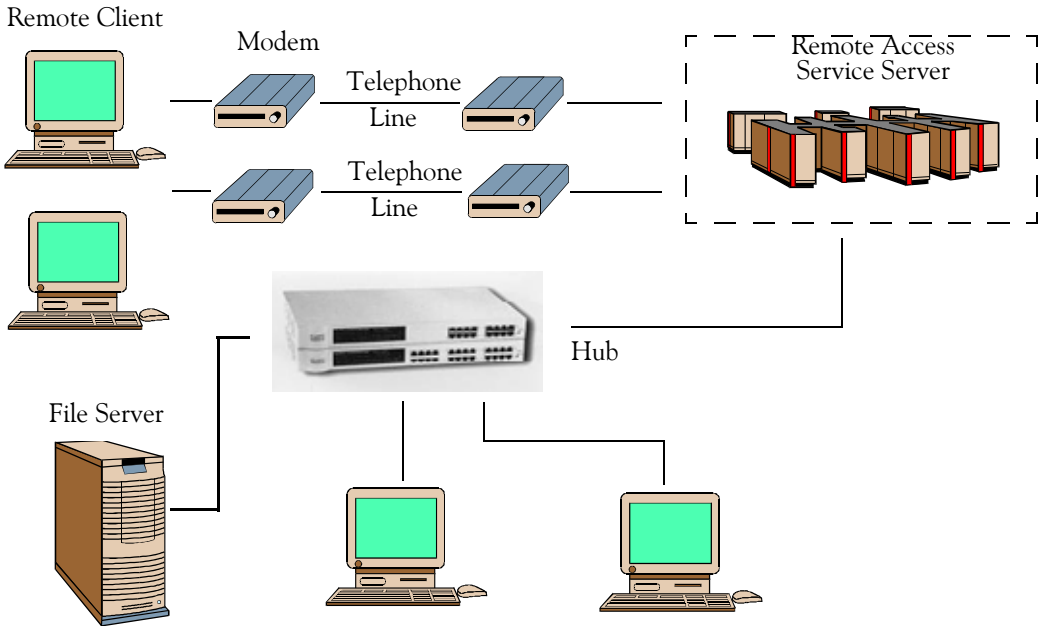


Figure 5.18. LANs connected via modems

5.4.8 Multiplexer / Demultiplexer

Multiplexing is a method of sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end. Analog signals are commonly multiplexed using *Frequency Division Multiplexing* (FDM), in which the carrier bandwidth is divided into subchannels of different frequency widths, each carrying a signal at the same time in parallel. Cable television is an example of FDM.

Digital signals are commonly multiplexed using *Time Division Multiplexing* (TDM), in which the multiple signals are carried over the same channel in alternating time slots. If the inputs take

turns to use the output channel (time division multiplexing) then the output bandwidth need be no greater than the maximum bandwidth of any input. If many inputs may be active simultaneously then the output bandwidth must be at least as great as the total bandwidth of all simultaneously active inputs. In this case the multiplexer is also known as a *concentrator*.

A demultiplexer performs the reverse operation of a multiplexer. Figure 5.19 shows a functional block diagram of a typical 4–line time–division multiplexer / demultiplexer.

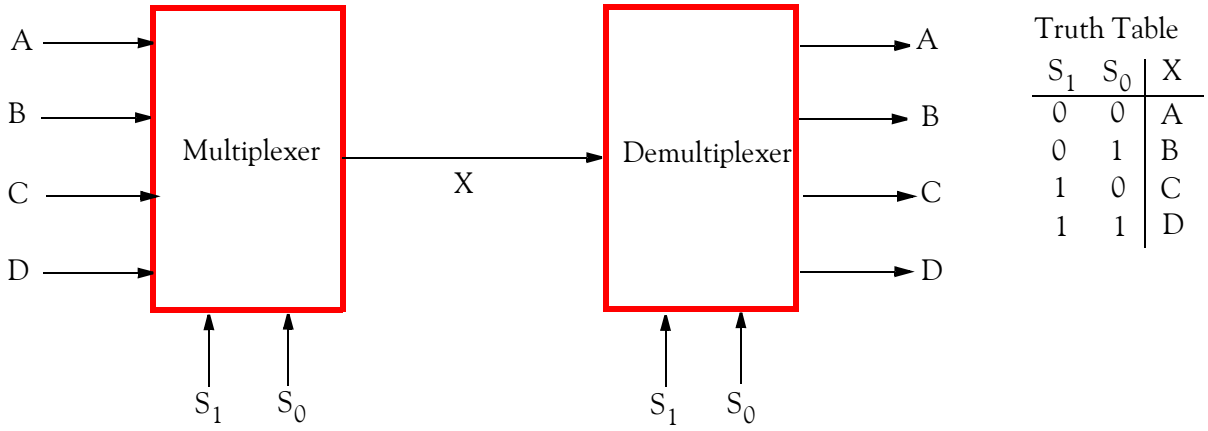


Figure 5.19. Functional Block Diagram for 4–line time–division multiplexer/demultiplexer

In Figure 5.19, *A, B, C*, and *D* represent input data to be multiplexed and appear on a single transmission path denoted as *X*. This path will carry the data of input *A* or *B* or C or *D* depending on the settings of the selection switches S_0 and S_1. These setting must be the same on both the multiplexer and demultiplexer. For instance, if the setting are $S_0 = 0$ and $S_1 = 1$, the output line *X* of the multiplexer will carry the data of signal C and it will appear at the output line C on the demultiplexer. The other combinations are shown in the truth table of Figure 5.16.

Some time–division multiplexers allocate time slots on demand. Thus, transmissions that are time critical, such as voice and video, can be given priority over other transmissions that are less critical.

Another multiplexing method is known as *Code–Division Multiplexing* (CDM). We will discuss it on Chapter 6. Also, in some optical fiber networks, multiple signals are carried together as separate wavelengths of light in a multiplexed signal using *Dense Wavelength Division Multiplexing* (DWDM).

Time–Division Multiplexers are used with Asynchronous* Transfer Mode (ATM) and T1 systems. ATM systems can operate at rates up to 622 Mbps, although a typical speed is 155 Mbps.

* *Asynchronous refers to the fact that transmission times occur at irregular intervals.*

The unit of transmission for ATM is called a *cell*. All ATM cells are 53 bytes long consisting of 5–byte headers and 48 bytes of data. Time–division multiplexers operate at the Physical layer of the OSI model.

A T1 line can operate at approximately 1.544 Mbps, which is a very common line speed for WAN connectivity. The T1 line can be split (fractional T1) into a number of channels, 24 total. This works out to be 24 channels at approximately 64 Kbps. It does not matter what speed the LAN is operating at; each channel can have a throughput of approximately 64 Kbps. In most cases, communication between sites does not need to be more than 64 Kbps. By using a fractional T1, the company will be able to add channels as it grows.

Table 5.9 shows how some of these devices that we've discussed relate to the OSI model.

TABLE 5.9 Internetworking devices related to the OSI model

Device	OSI Layer
Repeater, Modem, Multiplexer, CSU/DSU	Physical
Bridge	Data Link
Router, Brouter	Network
Gateway	All Seven Layers

5.5 Summary

- The Industry Standard Architecture (ISA) bus is an older standard that was designed by IBM to be used with IBM PCs and compatibles. It is no longer used in new systems.
- The Micro Channel Architecture (MCA) bus is also an older standard that was designed by IBM to replace the ISA. The MCA became IBM's proprietary 32–bit bus.
- The Extended Industry Standard Architecture (EISA) bus was similar to MCA but was designed by several companies to be used with IBM compatibles. It is no longer used.
- The Video Electronics Standard Architecture (VESA) standard was the 800 x 600 pixel Super VGA (SVGA) display and its software interface. Originally designed for video cards, VESA was later used for hard drive controllers and network cards.
- The Peripheral Component Interface (PCI), until recently, was the most popular standard for connecting peripherals to a personal computer. PCI was used in systems based on Pentium, Pentium Pro, AMD 5x86, AMD K5 and AMD K6 processors, Cyrix 586 and Cyrix 686 systems, and Apple computers.
- The Personal Computer Memory Card International Association (PCMCIA) has developed standards for several devices, such as modems, and external hard disk drives. A PCMCIA card can be plugged into notebook computers.
- The IEEE 1394 standard, also known as FireWire or I–Link is a new high performance serial bus interface that can be used with Macintosh and PCs. It offers high–speed communications and isochronous real–time data services. The FireWire can transfer data between a computer and its peripherals at 100, 200, or 400 Mbps, with a planed increase to 2 Gbps. Cable length is limited to 4.5 meters but up to 16 cables can be daisy–chained to yield a total length of 72 meters.
- A Network Interface Card (NIC), or Network Adapter, is an board that enable us to connect a computer to a network. Presently, most NICs can be configured automatically with Plug–and–Play.
- The Network Device Interface Specification (NDIS), created by Microsoft and 3Com, is a device driver programming interface allowing multiple protocols to share the same network hardware. For instance, both TCP/IP and IPX/SPX protocols can be used on the same NIC.
- The Open Datalink Interface (ODI), used by Novell, has many of the same features as NDIS and it is used for the same purpose.
- The most common connectors used with NICs are BNC, RJ–45, and AUI.
- Table 5.10 below lists several LAN connection and internetworking devices, their function, and advantages, and disadvantages for each.

TABLE 5.10 Advantages / Disadvantages of networking devices

Device / Function	Advantages	Disadvantages
Repeater Connects segments of similar or different cables but of the same type of networks	• Provides an inexpensive method of extending the length of a LAN • No processing is required • Same type of networks with different types of cables can be interfaced	• Cannot be used to connect segments of different network types • Have limits on the number of repeaters that can be used
Bridge Controls the flow of traffic between two LANs or two segments of the same LAN	• Checks the data and decides whether they should passed on to another device or not • Can interface alike or different networks • Works with all protocols	• Slower than repeaters • Pass all broadcasts; therefore, susceptible to broadcast storms • Higher cost in relation to repeaters
Transparent Bridge Uses a table to facilitate message transmission to proper destination. Use MAC addresses to determine whether to pass data or not.	• Eliminates broadcast storms with the use of the spanning–tree protocol	• Slower performance in relation to conventional bridges • Higher cost in relation to conventional bridges
Source–Route Bridge Used with Token Ring networks. An explorer frame is sent to find and store bridge numbers to establish the shortest path from source to destination.	• Provides an efficient method to determine whether to pass data or not in a Token Ring LAN	• Slower performance in relation to conventional bridges • Higher cost in relation to conventional bridges
Translational Bridge Allows the interconnection of different types of networks	• Allows Ethernet LANs to co–exist with Token Ring LANs	• Slower performance in relation to conventional bridges • Higher cost in relation to conventional bridges
Hub Essentially a multiport repeater. Hubs can be passive or active	• No configuration required after connection to the LAN • Higher data transfer speeds since no processing is required • Can use active hubs to extend maximum allowable distance	• Passive hubs can greatly limit maximum media distance • All data is sent out all ports whether it is needed or not since hubs cannot filter traffic

TABLE 5.10 Advantages / Disadvantages of networking devices

Device / Function	Advantages	Disadvantages
Switch A multi–port bridge or switching hub. Essential for large networks.	• Uses MAC addresses to control and filter traffic • Serves as a dedicated connection between source and destination	• Slower performance in relation to conventional bridges and hubs • Higher cost in relation to conventional bridges and hubs
Router Determines the best path for a data packet to be sent from one network to another Edge Router Routes data between one or more LAN and an ATM backbone network Brouter (Bridge/Router) A bridge and a router combined into a single device	• The smartest device for routing data from one network to another • Allows only authorized users to transmit data • Handles errors, security, and keeps network usage statistics • Supports Ethernet, Fast Ethernet, Token Ring, FDDI, T1, ATM, and DSL • An Edge router can be used to connect an ISP to the Internet • A brouter can be used as a bridge to interconnect routable with nonroutable protocols	• Require more data processing time • More complicated among other devices • Much more expensive than other networking devices
Firewall Prevents unauthorized access to or from a private network.	• Can be configured to allow access to certain information such as company's web site and prevent access to other company proprietary information.	• A DMZ is required as a neutral zone • Very expensive
Gateway Connects networks that use different protocols. Can operate at all seven layers of the OSI model	• Can perform different types of conversion such as protocols, application data, and e–mail • Can support a network in its existing configuration while part or all of the network is upgraded	• Can be very expensive
CSU/DSU Allows connection between an analog and digital telephone line company	• Can be used to connect an analog line to T1 or ATM	• Must be leased from telephone company
Modem Converts analog to digital data and vice–versa	• Relatively inexpensive hardware • Easy to set up and maintain • Mature standards and multiple vendors	• Slow performance
Multiplexer	• High speeds attainable with ATM	• Must be used with ATM or T1

5.6 Exercises

True/False

1. PCMCIA cards are available in four different types. _____

2. The IEEE 1394 Standard is designed to transfer data between a CPU and its peripherals at speeds up to 16 Gbps. _____

3. NICs operate at the Network layer of the OSI model. _____

4. Shared memory is a technique that allows a NIC to bypass the CPU and work directly with the computer memory. _____

5. NDIS allows different protocols to share the same network hardware. _____

6. RJ–45 connectors are used with external transceivers. _____

7. Repeaters can be passive or active _____

8. Bridges are devices that connect and control the traffic between two LANs or between two segments of the same LAN. _____

9. The spanning–tree protocol was designed to eliminate broadcast storms. _____

10. Hubs are not considered to be smart devices. _____

Multiple Choice

11. Digital signal repeaters are typically placed at _____ meter intervals.

A. 500 to 1000

B. 50 to 200

C. 2000 to 6000

D. 8000 to 12000

12. Source–Route Bridging was designed to be used with _____ LANs

A. Ethernet

B. Token Ring

C. FDDI

D. ARCNet

13. A _____ can interconnect Ethernet, Token Ring, FDDI, T1, ATM, and DSL.

A. Cisco's 4000 Series router

B. translational bridge

C. multiplexer

D. modem

14. Repeaters operate at the _____ layer of the OSI model.

A. Physical

B. Data Link

C. Network

D. Transport

15. An active _____ is essentially a multiport repeater.

A. modem

B. multiplexer

C. switch

D. hub

16. A DMZ is used with a _____.

A. translational bridge

B. firewall

C. edge router

D. brouter

17. Routers operate at the _____ layer of the OSI model.

A. Physical

B. Data Link

C. Network

D. Transport

18. A _____ can be used to connect an analog line to T1.

A. modem

B. CSU/DSU

C. gateway

D. router

19. A _____ can perform protocol and e–mail conversions.

A. modem

B. multiplexer

C. brouter

D. gateway

20. Time–division multiplexers operate at the _____ layer of the OSI model.

A. Physical

B. Data Link

C. Network

D. Presentation

Problems

21. You are in charge of an Ethernet network that uses the bus topology. You are currently close to the maximum number of client workstations allowed on a single segment. Which network device would be the best choice to extend your network if your network uses TCP/IP?

22. After installing a new router on your network, you have been hit with a number of broadcast storms. The protocol configuration in the router seems to be correct, but isolating that segment causes the storms to stop. What could be the problem?

23. You have decided to connect the network used by the Engineering department in your company to the network used by Procurement. The network in Engineering is a 10BaseT using UTP cable while the network in the Procurement uses coax cable. After the connection was made, personnel from both Engineering and Procurement are complaining that many errors were occurring. What corrective action would you take?

5.7 Answers to End–of–Chapter Exercises

True/False

1. F – Refer to Page 5–4
2. F – Refer to Page 5–5
3. F – Refer to Page 5–6
4. F – Refer to Page 5–9
5. T – Refer to Page 5–10
6. F – Refer to Page 5–11
7. F – Refer to Page 5–12
8. T – Refer to Page 5–14
9. T – Refer to Page 5–18
10. T – Refer to Page 5–19

Multiple Choice

11. C – Refer to Page 5–13
12. B – Refer to Page 5–18
13. A – Refer to Page 5–22
14. A – Refer to Page 5–12
15. D – Refer to Page 5–20
16. B – Refer to Page 5–23
17. C – Refer to Page 5–21
18. B – Refer to Page 5–28
19. D – Refer to Page 5–25
20. A – Refer to Page 5–33

Problems

21. Either a bridge or a router can be used. A bridge would be preferable since it is inexpensive and easy to install. Your choice of protocol would not affect the use of a bridge. Even though TCP/IP is a routable protocol it can still be bridged since bridging uses MAC addresses. A router would cost more.

22. The new router may be a bridging router (brouter). If it is, disable the bridging capability, or replace it with another router.

23. Installation of a repeater would amplify the signal and eliminate the problem. The repeater can be used to connect segments running the same network type with different cable types,

Chapter 6

Wired and Wireless Media

This chapter focuses on wired and wireless transmissions. The various types of cables used with LANs are discussed in previous chapters. However, for continuity, the cable types and their characteristics are reviewed in this chapter. This chapter concludes with a discussion of various methods of transmitting data via wireless networks.

6.1 Network Cables

Once the network adapters have been installed and interfaced in a computer, one needs a way to connect them to each other. The network media used to do this can be a wire, or it can be wireless. Wired or cable media are discussed first.

6.2 Wired Media

Wired (cable) media are made up of a central conductor (usually copper) surrounded by a jacket material. They are suitable for LANs because they offer high speed, good security, and low cost. Before the cable types are discussed, a review some basics electricity concepts and properties is presented.

6.2.1 Electrical Properties

It is imperative that the proper network cable must be used because the different types of cables have different electrical properties. These properties also determine the maximum allowable distance and the transmission rate in Mbps. One be familiar with the following electrical properties:

- **Resistance:** When electrons moves through a cable they must overcome *resistance*. Pure resistance affects the transmission of Direct Current (DC), and it is measured in ohms. When more resistance is met, more electric power is lost during transmission. The resistance causes the electric energy to be converted to heat. Cables with small diameters have more resistance than cables with large diameters.
- **Impedance:** The loss of energy from an Alternating Current (AC) is *impedance*. Like resistance, it is measured in ohms.
- **Noise:** Noise is a serious problem in cables and in most cases is hard to isolate. Noise can be caused by *Radio Frequency Interference* (RFI) or *Electro–Magnetic Interference* (EMI). Many things can cause noise in a cable. Common causes are problems experienced by adverse weather conditions, fluorescent lights, transformers, and anything else that creates an electric

field. Noise can be minimized if we plan our cable installation properly. We should route new cable away from lights and other EMI sources, use shielded cable when necessary, and ground all equipment.

- **Attenuation:** *Attenuation* is the fading of the electrical signal over a distance. The above properties all affect the rate of attenuation in a cable. After a certain distance, devices at the other end of a cable are unable to distinguish between the real signal and induced noise.
- **Cross Talk:** *Cross talk* occurs when a signal from one cable is leaked to another by an electrical field. An electrical field is created whenever an electrical signal is sent through a wire. If two wires are close enough and do not have enough EMI protection, the signal may leak from one wire and cause noise on the other.

The three common types of wired media are twisted pair, coaxial cable, and fiber optic. These are discussed below.

6.2.2 Twisted–Pair Cable

Twisted–pair cable is lightweight, easy to install, inexpensive, and supports many different types of networks. Transmission rates up to 100 Mbps are achievable with this type of cable. Twisted–pair cables are made up of pairs of solid or stranded copper twisted around each other. The twists reduce the vulnerability to EMI and cross talk. The number of pairs in the cable depends on the type. The copper core of the cable is usually 22–AWG or 24–AWG, as measured on the *American Wire Gauge* (AWG) standard. There are two types of twisted–pair cabling, unshielded twisted pair and shielded twisted pair.

Unshielded Twisted Pair (UTP) is the most common of the two types of twisted pairs. It can be either voice grade or data grade, depending on the application. It has a characteristic impedance of approximately 100 ohms. UTP costs less than shielded twisted pair and is readily available due to its many uses. It is used with most Ethernet LANs. There are five categories of data grade UTP cables. These are:

- **Category 1:** This category is intended for use in telephone lines and low–speed data cable.
- **Category 2:** Category 2 includes cabling for lower–speed networks. These can support transmission rates up to 4 Mbps.
- **Category 3:** This is a popular category for standard Ethernet networks. These cables support up to 16 Mbps but are most often used in 10 Mbps Ethernet LANs.
- **Category 4:** Category 4 cable is used for longer distance and higher speeds than Category 3 cable. It can support up to 20 Mbps.
- **Category 5:** This cable is intended for high–performance data communications. This has the highest rating for UTP cable and can support up to 100 Mbps. Any new installation of UTP should be using this cable rating for later upgrades.

UTP data cable is constructed with either two or four pairs of twisted cables. Cable with two pairs use RJ–11 connectors, and four–pair cables use RJ–45 connectors. They are shown in Figures 5.4 and 5.5, Pages 5–11 and 5–12, Chapter 5.

UTP cable for networks is installed in patch panels* in a similar manner as telephone cables are installed. Devices such as a hubs or routers can be connected to the network through a patch panel.

UTP's main disadvantage is its distance limitation due to attenuation. It is also subject EMI. Accordingly, UTP is the most common type of network cable used in areas where attenuation and EMI are not critical.

Shielded twisted pair (STP) is primarily used in Token Ring LANs. It is similar to UTP but has a mesh shielding that protects it from EMI, which allows for higher transmission rates and longer distances without a large amount of errors. It is defined by different types similar to the categories of UTP cable as listed below.

- **Type 1:** Type I STP has two pairs of 22–AWG, with each pair foil wrapped inside another foil sheath that has a wire braid ground.
- **Type 2:** This type is similar to Type 1 but has four pairs sheathed to the outside to allow one cable to an office for both voice and data.
- **Type 6:** This type has two pairs of stranded, shielded 26–AWG to be used for patch cords.
- **Type 7:** This type of consists of one pair of stranded, 26–AWG wire.
- **Type 9:** This type has two pairs of shielded 26–AWG and it is used for data.

STP cable is more expensive than UTP and coaxial cable which is described below. Also, STP installation is not as easy as with UTP since there is a bending limitation. However, due to the shielding, we can achieve higher transmission rates than UTP. Transmission rates with STP are 16 Mbps, whereas for Category 3 UTP is 10 Mbps.

6.2.3 Coaxial Cable

Coaxial cable is so named because it contains two conductors that are parallel to each other, or on the same axis. The center conductor in the cable is copper. The copper can be either a solid wire or a stranded material. Outside this central conductor is a nonconductive material. It is usually a white, plastic–like material, used to separate the inner conductor from the outer conductor. The outer conductor is a fine mesh made from copper also. It is used to help shield the cable from EMI. Outside the copper mesh is the final protective cover. The TV cable system uses coaxial cable.

* *A patch panel is a mounted hardware unit containing an assembly of port locations in a communications or other electronic or electrical system. In a network, a patch panel serves as a sort of static switchboard, using cables to interconnect computers within the area of a local area network (LAN) and to the outside for connection to the Internet or other wide area network (WAN). A patch panel uses a sort of jumper cable called a patch cord to create each interconnection*

The different layers in a coaxial cable are shown in Figure 6.1.

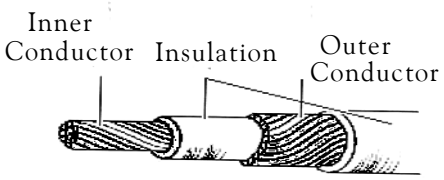


Figure 6.1. Layers of a coaxial cable

In a coax cable network data travel through the center conductor in the cable. and the outer conductor is used for grounding. For proper grounding it should be connected to a wall outlet ground. Thus, EMI is minimized with the use of the outer conductor.

Different types of coax cable are available. The best coax cable is made with a stranded central conductor with a tight mesh outer conductor. Stranded wire is used because it allows us bend the cable easily does not kink as badly as a solid cable. The use of stranded or solid cable does not alter the data transmission rates.

As with other types of wiring, coax cable is rated by gauge and impedance. Gauge is the measure of the cable's thickness. It is measured by the Radio–Grade measurement, or RG number. The higher the RG number, the thinner the central conductor core. Thin cables are identified with higher gauge numbers, whereas thick cables are identified with lower gauge numbers. For instance 16–gauge wire is thicker than a 24–gauge wire.

Coaxial cable is a good choice for a Small Office / Home Office (SOHO)* network. A SOHO network offers an efficient means for expansion in small LANs.

The most common coaxial types are listed below.

- **93–ohm RG–62:** Used with ARCNet as discussed in Chapter 4.
- **50–ohm RG–7 or RG–11:** Used with the thick Ethernet which is one of the three options for cabling an Ethernet network. Discussed also in Chapter 4.
- **50–ohm RG–58:** Used with the thin Ethernet which is one of the three options for cabling an Ethernet network. This was also discussed in Chapter 4.
- **75–ohm RG–59:** Used with cable television

As stated above, the advantage of using coaxial cable is the minimization of EMI interference. In some areas, such as in a factory where heavy machinery is used, most other types of cables will experience excessive interference and thus will not to operate properly. In such cases, coax cable may be the only viable option.

---

* SOHO *is the category of business typically with 10 persons in a home or small office network. Other categories are listed in Table 7.1, Page 7–3, Chapter 7*

6.2.4 Fiber–Optic Cable

Fiber–optic cable transmits light pulses. A laser at one device sends pulses of light through this cable to the other device. The presence of a light pulse is translated into a logical 1 and its absence into a logical 0 at the receiver end. The basic fiber optic cable composition is shown in Figure 6.2.

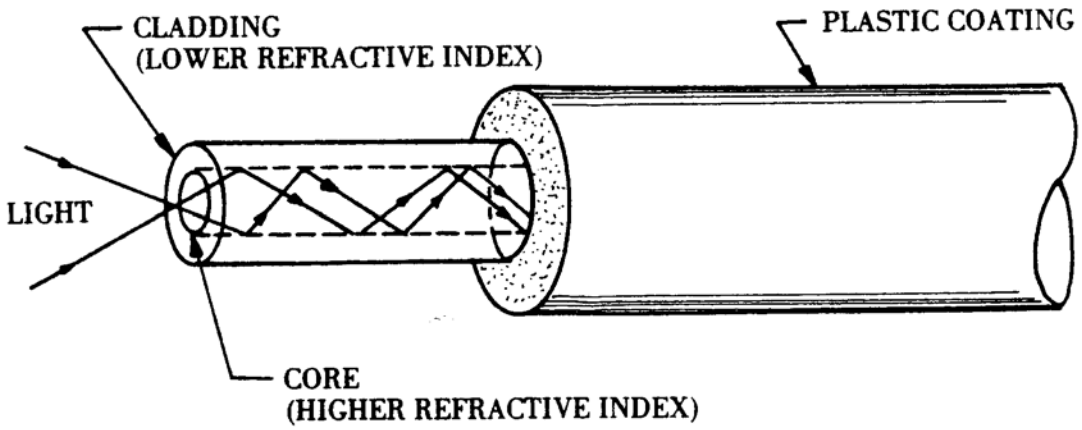


Figure 6.2. Basic fiber optic cable composition

For a two–way communications the fiber optic cable must have two strands, one for each direction.

In the center of the fiber cable is a glass strand, or core. The light from the laser travels through this glass to the other device. Around the internal core is a reflective material known as *cladding*. This reflective cladding prevents light from escaping through the glass core.

Fiber–optic cable was very expensive a few years ago. Fortunately, its price has dropped substantially in recent years, and it is becoming much more common in networks today. Fiber optic installation must be performed by electricians who specialize in this type of cables and thus the installation is more expensive. Accordingly, there is a trade–off between cost and high transmission speeds and distance.

Fiber–optic cable currently has a bandwidth of more than 2 Gbps. With fiber optic cables attenuation is not a problem. Also there is no susceptibility to EMI since the transmission occurs over light.

Fiber–optic cable is available in two types: single mode and multi–mode. Single–mode cable only allows for one light path through the cable, whereas with multi–mode we can have two or more paths. With single–mode fiber optic cable we can achieve faster transmission rates time and longer distances.

Single–mode fiber optic cable costs more than multi–mode. Accordingly, we should use single mode for long distance transmissions. To interconnect nearby buildings we can use multi–mode

fiber which is less expensive.

Fiber cable is listed by core and cladding size. An example of this is 62.5 micron core/140 micron cladding multi–mode. The networks administrator should consult the manufacturer of our network devices to see which size he needs. For connections over 300 meters especially outside or in networks without repeaters, fiber optic cabling is highly recommended.

Fiber optic cables are available in different lengths and are provided with two types of connectors. The square SC connectors are the most common in the United States while the round ST connectors are commonly used in Europe. A fiber optic cable with both types of connectors is shown in Figure 6.3.

Figure 6.3. Fiber optic cable with SC and ST connectors

6.2.5 Hybrid Fiber Coax (HFC) Cable

HFC offers a means of delivering video, voice telephony, data, and other interactive services over coaxial and fiber optic cables. HFC cables are used with networks that consist of a main office, distribution center, fiber nodes, and network interface units. The main office receives information such as television signals, Internet packets, and other data, then delivers them through a SONET* ring to distribution centers. The distribution centers then send the signals to neighborhood fiber nodes, which convert the optical signals to electrical signals and redistributes them on coaxial cables to residents' homes where network interface units send the appropriate signals to the appropriate devices (i.e. television, computer, telephone).

An HFC network provides the necessary bandwidth for home broadband applications, using the spectrum from 5 MHz to 450 MHz for conventional downstream analog information, and the spectrum from 450 MHz to 750 MHz for digital broadcast services such as voice and video telephony, video–on–demand, and interactive television.

---

* *We recall from Chapter 3 that the Synchronous Optical Network (SONET) standard was designed to establish a digital hierarchical network with a consistent worldwide transport scheme. SONET has been designed to take advantage of fibre, in contrast to the plain old telephone system which was designed for copper wires.*

Table 6.1 lists the advantages and disadvantages of each type of cables that is discussed in this chapter.

TABLE 6.1 Cable types and their advantages / disadvantages

Cable Type	Advantages	Disadvantages
UTP	• Low cost • Easy installation • Capable of high speeds	• High attenuation • Susceptible to EMI • Short distances (100 meter limit) due to attenuation
STP	• Medium cost • Easy installation • Faster than UTP and coaxial • Less susceptible to EMI than UTP	• More expensive than UTP and coax • More difficult installation • High attenuation (same as UTP)
Coaxial	• Less attenuation than UTP and STP • Less susceptible to EMI than UTP and STP • Low cost • Easy to install and expand	• Accidental cable break will cause the entire network to become inoperative
Fiber Optic	• Extremely fast • Very low or no attenuation • No EMI interference	• Expensive installation • Highest cost

6.2.6 Multiplexing

Multiplexers are discussed in Chapter 5. Let us review the concept of multiplexing and also discuss frequency division multiplexing. We recall that multiplexing offers an efficient method of using a single high–bandwidth channel to transmit many lower–bandwidth channels. That is, we can combine several low–bandwidth channels form a single high–bandwidth channel for transmitting signals.

A Multiplexer/Demultiplexer (MUX/DEMUX) is the hardware device that allows the channels to be joined for transmission over a single cable and to be separated at the receiving station. Both broadband and baseband transmissions can benefit from this technique. A commonly known use of this technique is cable TV. Many channels are sent across one cable. The channel changer on the cable box is a demultiplexer that separates the signal. The multiplexing method used depends on whether the transmission is broadband or baseband. These two types of multiplexing are *Time Division Multiplexing (TDM)* and *Frequency Division Multiplexing (FDM)*. In TDM all signals use the *same frequency* but operate at *different times*, while in FDM, all signals operate at the *same time* with *different frequencies*.

The concepts of TDM and FDM are illustrated in Figures 6.4 and 6.5 respectively.

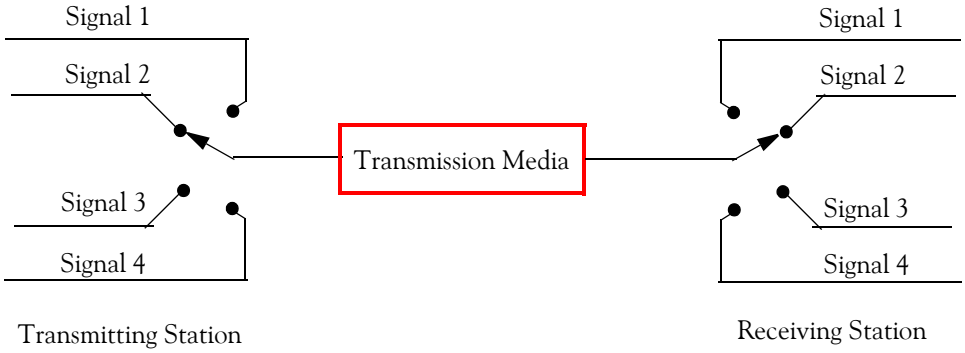


Figure 6.4. Time Division Multiplexing (TDM)

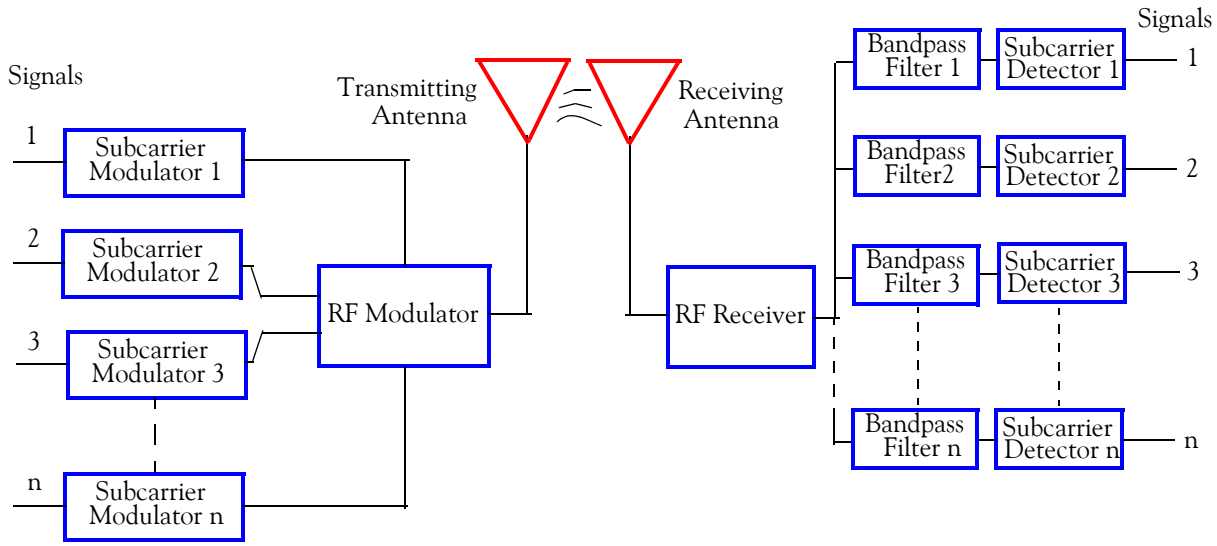


Figure 6.5. Frequency Division Multiplexing (FDM)

Time–Division Multiplexing (TDM) uses time slots to separate channels. Each device is given a time slot to transmit using the entire available bandwidth. This method provides multiple channels on a baseband line. There are two types of TDM. These are:

- ***Synchronous Time–Division Multiplexing*:** All the time slots are the same length, and if there is no traffic in a time slot, the bandwidth goes unused.
- ***Statistical Time–Division Multiplexing*:** This method utilizes time slots more efficiently by allotting time based on how busy a channel is. As a channel gets busy, more bandwidth is allotted. This method requires expensive equipment known as Stat MUXes.

Frequency–Division Multiplexing (FDM) is used in broadband transmissions to transmit analog signals. The channels are on different frequencies with an area of unused frequency ranges separating them. These unused ranges are known as guard bands, and they prevent interference from

other channels. FDM is the form of multiplexing used in cable TV systems and Digital Subscriber Line (DSL) services.

6.3 Wireless Transmission

With wireless transmission the signals propagate through open space. The distance can be very short or very long. The three types of wireless media are *radio wave*, *microwave*, and *infrared*.

6.3.1 Radio Waves

Radio waves are electromagnetic waves propagated through space. Because of their varying characteristics, radio waves of different wavelengths* are employed for different purposes and are usually identified by their frequency. The shortest waves have the highest frequency while the longest waves have the lowest frequency. In honor of German radio pioneer Heinrich Hertz, his name has been given to the cycle per second (hertz, Hz); 1 Kilohertz (KHz) is 1000 Hz, 1 Megahertz (MHz) is 1 million Hz, and 1 Gigahertz (GHz) is 1 billion Hz. Radio waves range between frequencies of 10 KHz to 1 GHz. Radio waves include the following ranges:

- ***Short–wave*:** An electromagnetic wave with a wavelength of approximately 200 meters or less, especially a radio wave in the 20 to 200 meter range.
- ***Very–high frequency* (VHF):** This is the band of radio signal frequencies, ranging from about 30 megahertz (MHz) to 300 MHz, with corresponding wavelengths ranging from about 10 to 1 meters. This frequency is used for FM and amateur radio broadcasting and for television transmission.
- ***Ultra–high frequency* (UHF):** This is a short–wave radio frequency ranging from about 300 MHz to 3000 MHz, with corresponding wavelengths ranging from about 100 to 10 cm. This frequency is used mainly for communication with guided missiles, in airplane navigation, radar, and in the transmission of television signals.

6.3.2 Antennas

In electronics, an *antenna* is device used to propagate radio or electromagnetic waves or to capture radio waves. Antennas are necessary to transmit and receive radio, television, microwave telephone, and radar signals. Most antennas for radio and television consist of metal wires or rods connected to the transmitter or receiver.

When an antenna is used for transmission of radio waves, a transmitter creates oscillating electric currents along the wires or rods. Energy from this oscillating charge is emitted into space as elec-

---

* *The wavelength λ is inversely proportional to frequency f. If the frequency is given in kHZ, the wavelength in meters is found from the relation* $\lambda_m = \frac{300000}{f\ (kHz)}$.

tromagnetic (radio) waves. When an antenna is used for reception, these waves induce a weak electric current in the antenna wire or rod. This current is amplified by the radio receiver.

Depending on the antenna type, radio waves can also be broadcast omnidirectional (in all directions) or in one certain direction. The dimensions of an antenna usually depend on the wavelength, or frequency, of the radio wave for which the antenna is designed.

If one conductor is connected to a grounding cable and the other to the end of a horizontal wire antenna, the antenna is said to be an *end–fed long wire*. If the antenna is split in the middle, with each side connected to one conductor of the transmission line, the antenna is called a *dipole*, the simplest and most fundamental antenna. A dipole transmits or receives most of its energy at right angles to the wire. This allows transmission or reception to be beamed in a particular direction, to the exclusion of signals in other directions.

A *dipole* is a simple antenna, usually fed from the center, consisting of two equal rods extending outward in a straight line. Other simple antennas are the circular (or square) loop antennas and helix antennas. These are known as wire antennas and are shown in Figure 6.6.

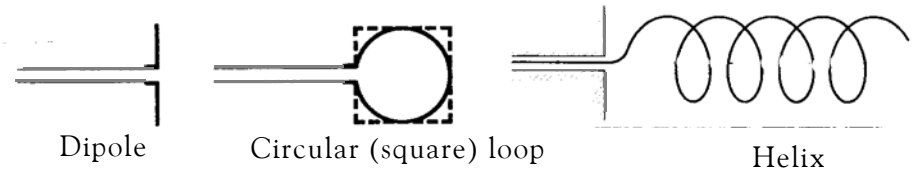


Figure 6.6. Wire Antennas

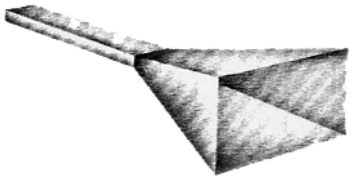
Helix antennas are usually positioned on the ground for space telemetry applications of satellites, space probes, and ballistic missiles to transmit or receive signals that have undergone Faraday rotation* by traveling through the ionosphere.

Another class are the *aperture antennas* shown in Figure 6.7.

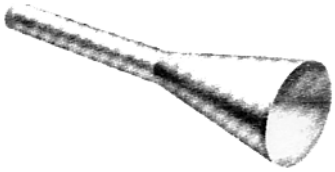
Many communications systems require radiation characteristics that are not achievable by a single antenna element. It is possible however, to combine several elements in such a geometrical arrangement (an array) that will result in the desired radiation characteristic. Figure 6.8 shows two *array antennas*.

Reflector antennas are mostly used for ground–to–satellite and satellite–to–ground communications. Figure 6.9 shows three types of reflector antennas.

* *Faraday rotation is the rotation of the plane of polarization of either a plane–polarized light beam passed through a transparent isotropic medium or a plane–polarized microwave passing through a magnetic field along the lines of that field. Also called Faraday effect.*



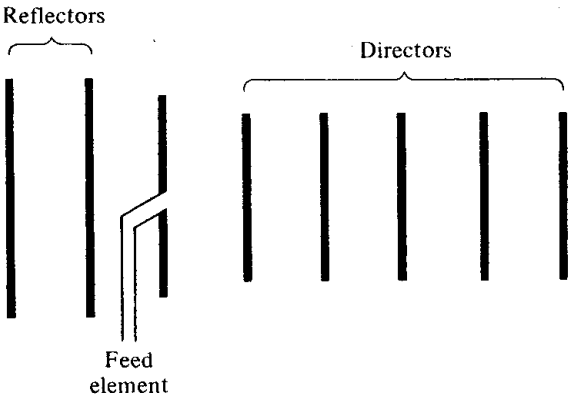
Pyramidal Horn



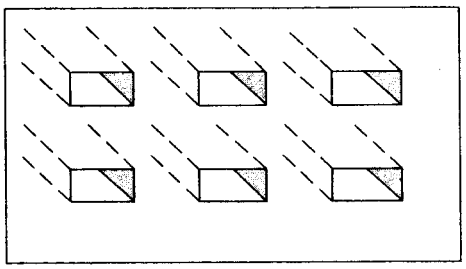
Conical Horn

Rectangular Waveguide

Figure 6.7. Aperture Antennas



Yagi – Uda array



Aperture array

Figure 6.8. Array Antennas

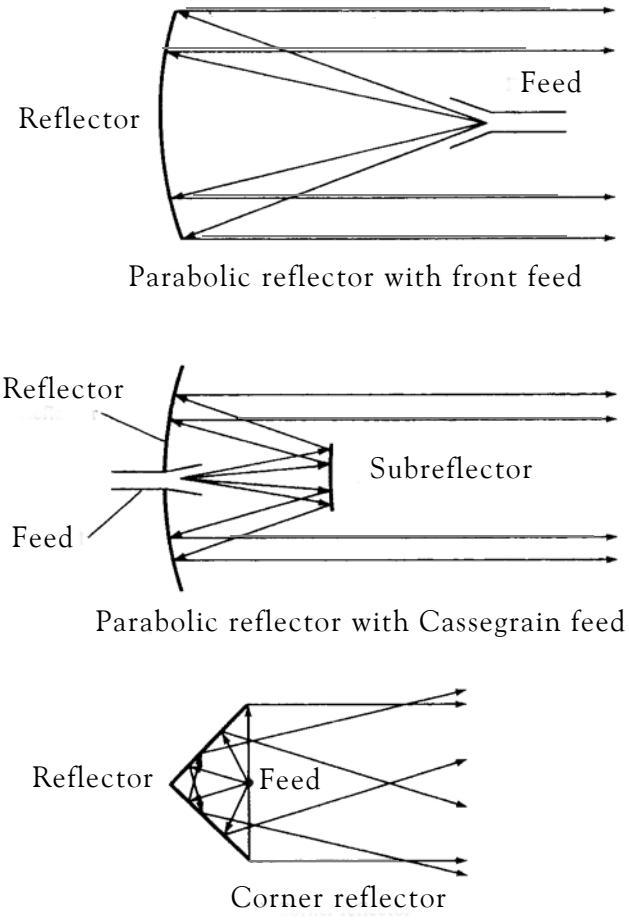


Figure 6.9. Reflector Antennas

Lens antennas are directional microwave antennas that use a dielectric lens in front of a dipole or horn radiator to focus the radiated energy into a concentrated beam. Lens antennas can be used in lieu of reflector antennas when there is a need to transform divergent waves into plane waves to prevent them from spreading into undesired directions. Figure 6.10 shows different types of lens antennas.

Most radio waves transmit on one single frequency. Some operate as low–power transmitters while others operate as high–power transmitters. Another type is the spread spectrum which can spread the frequency over a range of frequencies.

Low power transmissions are restricted to short ranges, typically 20 to 50 meters. Systems that are designed for low power can achieve transmission rates from 1 Mbps to 10 Mbps, and thus can be used for small wireless LANs. For instance, they can be used in an office where everyone has a notebook or portable computer where there would be no need for cables or other networking devices. However, they must be used in areas away from large equipment such as large motors

and generators that can induce considerable EMI.

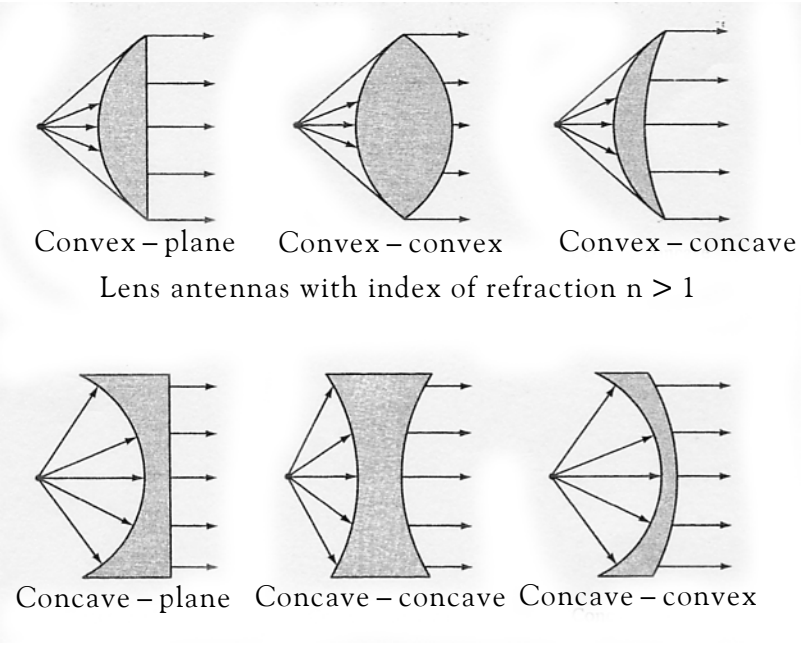


Figure 6.10. Lens Antennas

To establish wireless communications over longer distances, we need to revert to a high power system such as those used by large radio stations. These have the same characteristics as the low power systems except that enable us to communicate over longer distances. Also, with high power systems, transmissions can be either within line–of–sight or out–of–sight since they can be pointed towards the sky, bounce off the atmosphere, and return to earth for reception.

High power systems can be used with networks where users are far away from the main office of a company such as those who travel frequently.

6.3.3 Spread Spectrum

Spread spectrum development began during World War II, with the earliest studies dating from the 1920s. Most papers remained classified until the 1980s. Spread spectrum was originally used by the military to provide reliable data transmissions that are resistant to jamming.* It is still used today in military communications systems.

Commercial applications include cellular telephony and mobile networking. Spread spectrum is also implemented in wireless network communications for security and privacy.

* *Jamming refers to deliberate radiation or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices or systems.*

Spread spectrum coding methods are the Direct Sequence (DS) and Frequency Hopping (FH). Direct Sequence spread spectrum was invented by Paul Kotowski and Kurt Dannehl at Telefunken. Frequency Hopping spread spectrum was first thought of by actress Hedy Lamarr and composer George Antheil. They held a patent filed in 1942.

In *Direct Sequence* frequency hopping, the message is divided into small pieces (chips) and these chips are transmitted across several frequencies as shown in Figure 6.11.

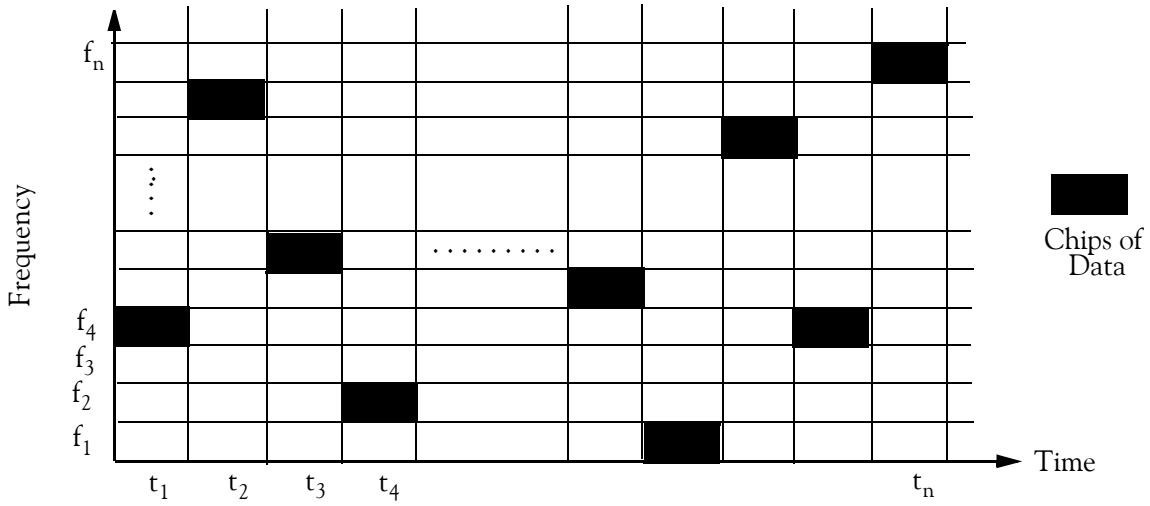


Figure 6.11. Direct Sequence spread spectrum

Of course, the receiving station must know the correct frequencies at the appropriate time intervals in order to reconstruct the entire message. to monitor and which data was false. Direct–Sequence spread spectrum can operate at 2 to 6 Mbps transmission rates in unregulated frequencies.

As shown in Figure 6.11, the entire message transmits in one of the *n* possible frequency slots. The receiver hops in synchronism with the transmitter. Typical Frequency Hopping spread spectrum systems have a maximum transmission rate of 2.4 Mbps.

In *Frequency Hopping* spread spectrum, a frequency synthesizer is driven by a pseudo random sequence of numbers to generate output frequencies that "hop around" in the desired frequency range as shown in Figure 6.12.

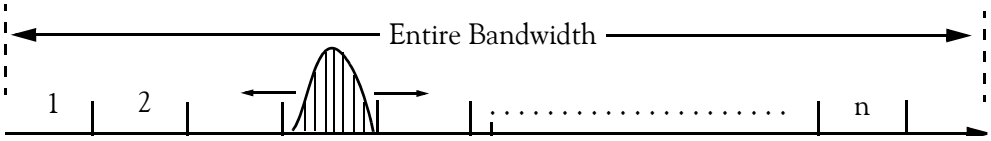


Figure 6.12. Frequency Hopping spread spectrum

Table 6.2 lists the advantages and disadvantages of the three categories of radio wave transmission.

TABLE 6.2 Categories of radio wave transmission – advantages / disadvantages

Category	Advantages	Disadvantages
Low Power, Single Frequency 1 Mbps to 10 Mbps	• Low cost • Easy installation	• High attenuation • Susceptible to EMI • Short distances (20 to 25 meters)
High Power, Single Frequency 1 Mbps to 10 Mbps	• Moderate cost • Low attenuation for long distances	• More difficult installation • Susceptible to EMI
Spread Spectrum 2 Mbps to 6 Mbps	• Moderate cost • Simple Installation • Less susceptible to EMI	• High attenuation

6.3.4 Wireless Networking Standards

The *IEEE 802.11b standard* is the family of specifications created by the Institute of Electrical and Electronics Engineers Inc. for wireless, Ethernet local area networks in 2.4 GHz bandwidth range. It was intended as a way to connect our computers and other devices to each other and to the Internet at very high speed without any complicated wiring, or a high price. It provides much wireless speed at a modest price for a world–wide, anytime, anywhere communication.

Recently, a next–generation wireless networking standard has been approved that will work with older wireless networking technology, allowing companies and consumers to keep existing equipment and possibly boosting the number of wireless connections in homes and businesses. The new standard, called 802.11g, has been tentatively approved by IEEE. It promises data transfer rates of up to 54 Mbps, compared with 11 Mbps on the current 802.11b standard.

The 802.11g standard is compatible with 802.11b, also known as *Wi–Fi* (Wireless Fidelity), or Wireless Ethernet, because the two standards, b and g, both run in the frequency spectrum of 2.4 Gbps. Another standard, the 802.11a, is used in accessing hubs and computer cards, but it operates at a higher frequency, in the 5 Gbps range and isn't compatible with the 802.11b standard. It also gives transfer rates of 54 Mbps.

Wireless local area network chip maker Intersil and chip maker Texas Instruments had been pushing competing technologies to become the 802.11g standards, It it being rumored that IEEE nearly scrapped the entire 802.11g standard because Texas Instruments and Intersil couldn't reach agreement. Both the transmitting and receiving hubs, known as access points, and computer receiver cards that are inserted into desktop PCs or laptops – based on the 802.11g standard are available now.

Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, and Personal Digital Assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short–range wireless connec-

tion. Bluetooth replaces the cables that link cell phones, notebooks and hand–held computers. Using the 2.4 GHz band of the unlicensed spectrum, Bluetooth can send information at up to 1 Mbps, considerably faster than a dial–up modem connection can. It is designed to work reliably at 30 feet, and sometimes reaches farther. The chips consume lithe power and could one day be produced cheaply enough to be built into every device.

Using this technology, users of cellular phones, pagers, and personal digital assistants such as the PalmPilot are able to buy a three–in–one phone that can double as a portable phone at home or in the office, get quickly synchronized with information in a desktop or notebook computer, initiate the sending or receiving of a fax, initiate a print–out, and, in general, have all mobile and fixed computer devices be totally coordinated.

The technology requires that a low–cost transceiver chip be included in each device. Several products with Bluetooth technology, such as HP printers, are now available and more are expected to appear in large numbers in the near future.

With Bluetooth, each device is equipped with a microchip transceiver that transmits and receives in a previously unused frequency band of 2.4 GHz that is available globally (with some variation of bandwidth in different countries). In addition to data, up to three voice channels are available. Each device has a unique 48–bit address from the IEEE 802 standard. Connections can be point–to–point or multipoint.

The maximum range is 100 meters. Data can be exchanged at a rate of 1 Mbps (up to 2 Mbps in the second generation of the technology). A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. Built–in encryption and verification is provided.

Figure 6.13 shows a typical Bluetooth cordless headset.

Figure 6.13. Bluetooth Headset

Wi–Fi, short for wireless fidelity, enables high–speed, low–cost access to the Internet. It has sparked a flurry of innovation and investment and has become one of the few bright spots in the

Wi–Fi makes connections across longer distances, up to about 100 meters. One can see business travelers at airports hogging pay phones, laptops propped on a knee, frantically trying to download or send a few e–mails before boarding. It's a sight that could soon become a thing of the past. A technology being deployed at a growing number of airports allows scores of PC users to download their e–mails at far faster speeds, while lounging comfortably in their seats.

Wi–Fi is not just about airports and business travelers. It could unleash a new spurt of Internet growth, vastly expanding the availability of cheap, high–speed connections, while drastically reducing the need to dig up trenches and wire buildings. But Wi–Fi also faces threats that could significantly undermine its potential. Wi–Fi works a bit like a cordless phone. First we hook up a Wi–Fi broadcast station, whose prices are well below $200, to an existing high–speed Internet connection. Anyone within about 300 feet of the station with a PC or handheld device equipped with an inexpensive Wi–Fi antenna can use that Internet connection.

Wi–Fi access points are being deployed in hotels and college campuses, coffee houses, and urban downtowns. They are being used to connect poor rural areas and Indian reservations. Several companies have built nationwide networks of access points, and business models are proliferating.

6.3.5 Standards on Wireless Communications

802.11b: Also known as Wi–Fi, 802.llb wirelessly connects devices as far as 100 meters apart at up to 11 Mbps, close to the speed of a digital subscriber line or cable modem. Wi–Fi can create ad hoc connections (discussed on Chapter 7) between devices but is most commonly used to tap into existing networks in offices, schools, airport lounges and coffee shops. It also uses the 2.4 GHz band of the unlicensed spectrum, which sometimes creates interference with Bluetooth.

***802.11a*:** Known as Wi–Fi 5, 802.lla is much faster than its market predecessor, running at up to 54 Mbps. Wi–Fi 5, which is just beginning to appear in PC cards and wireless base stations, eliminates some interference problems by operating on 5 GHz, a less crowded band of the spectrum.

802.11G: Still in development, this standard is intended as a higher–speed successor to 802.llb, providing data speeds comparable to those of 802.11a on devices created for the 2.4 GHz band.

Home RF: Originally intended for home networking, it can operate up to a distance of 50 meters in the 2.4 GHz band. Recent improvements have increased its data speeds to a potential 10 Mbps, but Home RF lost ground when Intel decided to pursue other standards.

6.3.6 Multiple Access Systems

Multiple access is defined as the technique wherein more than one pair of earth stations can simultaneously use a satellite *transponder**. Multiple access is used extensively in satellite networking.

* *A transponder is a transmitter and receiver housed together in a single unit and having some circuits in common. In satellite communications a transponder receives a signal from an earth station and retransmits it on a different frequency to one or more other earth stations.*

Most satellite communications applications involve a number of earth stations, communicating with each other through a satellite channel. The word *channel* as used in satellite communications, includes voice, data, and video. The concept of multiple access involves systems that make it possible for multiple earth stations to interconnect their communication links through a single transponder. A transponder may be accessed by single or multiple carriers. These carriers may be modulated by single– or multiple–channel baseband which include voice, data, or video communication signals.

Burst mode is a method of data transfer in which information is collected and sent as a unit in one high–speed transmission. In a burst mode, an input/output device takes control of a multiplexer channel for the time required to send its data. In effect, the multiplexer, which normally merges input from several sources into a single high–speed data stream, becomes a channel dedicated to the needs of one device until the entire transmission has been sent. Burst mode is used both in communications and between devices in a computer system.

Time Division Multiple Access (TDMA) is characterized by the use of a single carrier frequency per transponder, where the bandwidth associated with the carrier is typically the full transponder bandwidth. This bandwidth is time shared among all users on a time–slot–by–time–slot basis. Although the primary advantage of TDMA is realized in the single–carrier–per–transponder arrangement, there are cases where the TDMA bandwidth may be a fraction of the transponder bandwidth. TDMA is suited only for digital transmission and operates in burst mode. A basic TDMA system concept is shown in Figure 6.14.

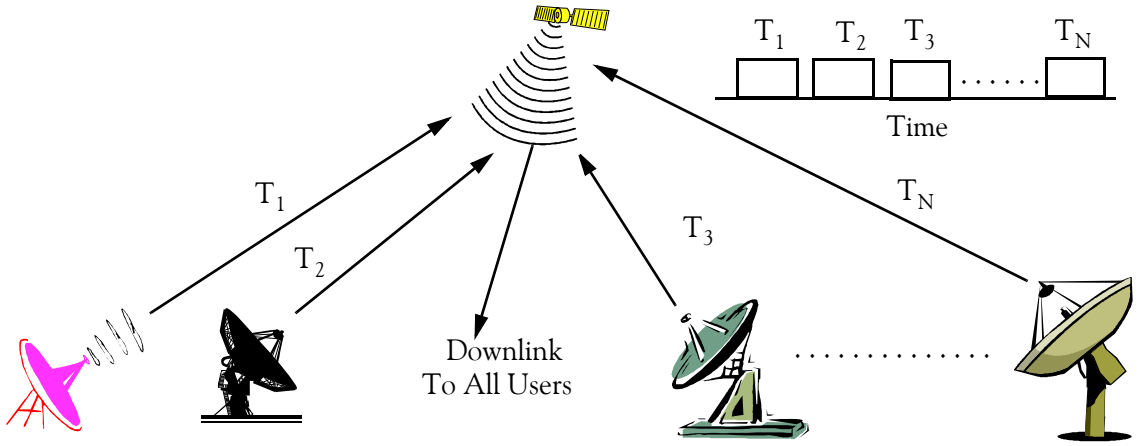


Figure 6.14. TDMA System

Frequency Division Multiple Access (FDMA) systems channelize a transponder using, multiple carriers. The bandwidth associated with each carrier can be as small as that required for a single voice channel. FDMA can use either analog or digital transmission in either continuous or burst mode. An FDMA system is shown in Figure 6.15.

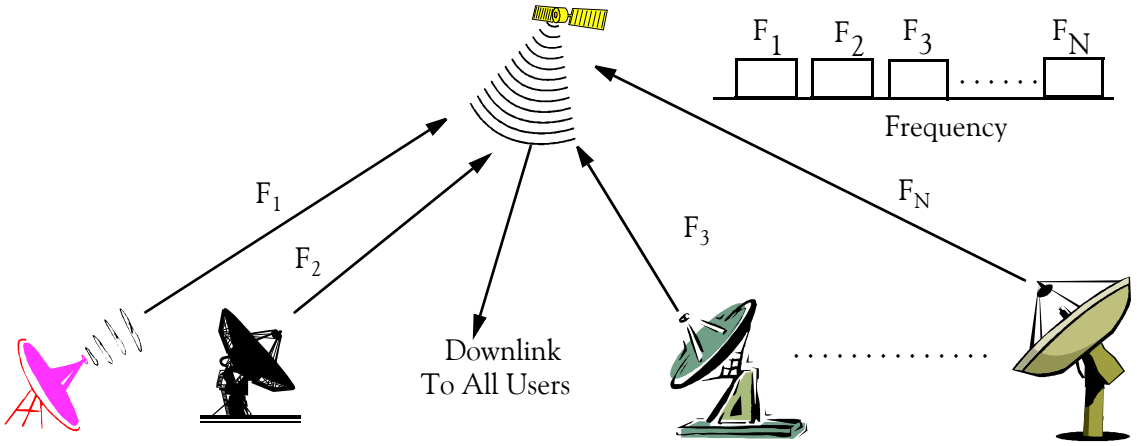


Figure 6.15. FDMA System

***Code Division Multiple Access* (CDMA)** is a form of multiplexing where the transmitter encodes the signal using a pseudo–random* sequence which the receiver also knows and can use to decode the received signal. Each different random sequence corresponds to a different communications channel. The introduction of CDMA into wireless telephone services was pioneered by Qualcomm. Motorola uses CDMA for digital cellular phones. CDMA is suited only for digital transmission. A CDMA system is shown in Figure 6.16.

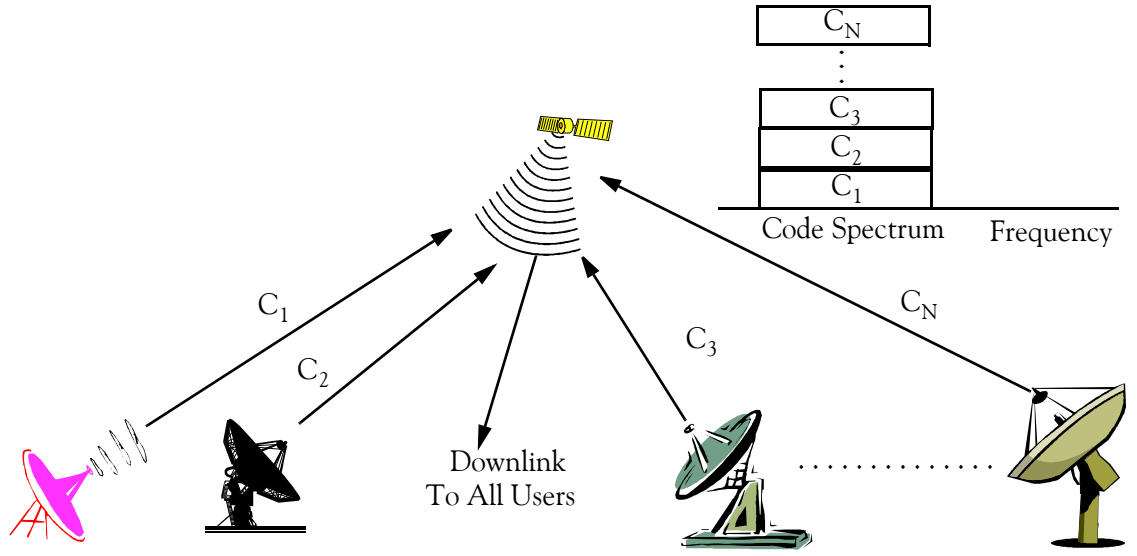


Figure 6.16. CDMA System

* *This term denotes the generation of an unpredictable sequence of numbers in which no number is any more likely to occur at a given time or place in the sequence than any other. Truly random number generation is generally viewed as impossible. The process used in computers would be more properly called "pseudo–random number generation." For a discussion on random number generation, please refer to Introduction to Simulink, Appendix C, ISBN 978–1–934404–09–6.*

Synchronous Code Division Multiple Access (S–CDMA) is a proprietary version of Code Division Multiple Access (CDMA). It was developed by Terayon Corporation for data transmission across coaxial cable networks. This method of data transmission was designed to be secure and extremely resistant to noise. S–CDMA scatters digital data up and down a wide frequency band and allows multiple subscribers connected to the network to transmit and receive concurrently.

6.4 Forms of Data Transmission

Data transmissions across the network can occur in two forms, either *analog* or *digital*. Analog signals exist in an infinite number of values. Just like an analog watch, in which the hands glide across the seconds and minutes, there are many time values displayed. Digital signals exist in a finite number of values. Digital watches display the time down to the second or fraction of a second, but these values are always displayed as definite amounts. Analog transmissions are displayed using a continuous curve in which the signal changes from one value to another; as a value increases from 0 to 1, it becomes every value along the way. Digital transmissions are displayed using pulses to indicate that the change from one value to another is instant; the value changes instantly from 1 to 0. Figure 6.16 shows examples of a digital and analog signal.

6.4.1 Transmission of Analog Signals Using Encoding

A typical analog signal is said to be periodic if it starts at zero, increases to its high peak, recedes past zero to its low peak, and then rises back to zero. This cycle is referred to as the period of the signal. A sine wave is a periodic signal. Most analog signals such as voltage, temperature, pressure, and others are considered periodic although some may have a very long period.

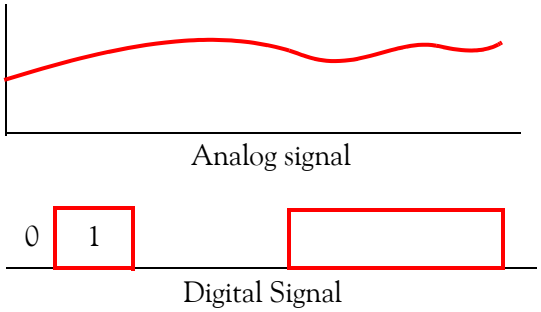


Figure 6.17. Examples of analog and digital signals

An analog signal is generally described as $s(t) = A\cos(2\pi ft + \theta)$ * where A is the amplitude, f is the frequency in cycles per second or Hertz, and θ is the phase of the signal measured either in radi-

* *Although not many analog signals are sine waves, the French mathematician Fourier has shown that any periodic wave of any form can be represented as the sum of sine waves that are harmonically related. Harmonically here means that this sum of sinewaves consists of a fundamental frequency and all others, referred to as harmonics, are exact multiples of this fundamental frequency. For a discussion on Fourier analysis, please refer to Signals and Systems, Fourth Edition, ISBN 978–1–934404–11–9.*

ans or degrees. Phase is determined by comparing the cycles of two signals of the same frequency. Thus, when two signals differ by π radians or $180°$, they are said to be $180°$ out–of–phase. Each of these characteristics can be used to encode data in an analog signal into a code.

The three modulation methods used with analog signals are *amplitude modulation*, *frequency modulation,* and *phase modulation*. With the present technology these are encoded into zeros and ones and are known as *amplitude shift keying*, *frequency shift keying*, and *phase shift keying*. Reference can be made to Figure 6.17 for the discussion of these three methods.

- ***Amplitude Shift Keying*** **(**ASK**):** With this method, also referred to as ***On–Off Keying*** **(OOK)**, a 1 is represented by turning the Radio Frequency (RF) carrier on for the bit duration, and a 0 is represented by turning the carrier off for the same interval. Thus, a fixed–frequency RF carrier is turned on and off in accordance with the bit value. The resulting ASK signal is shown in Figure 6.18 (a).

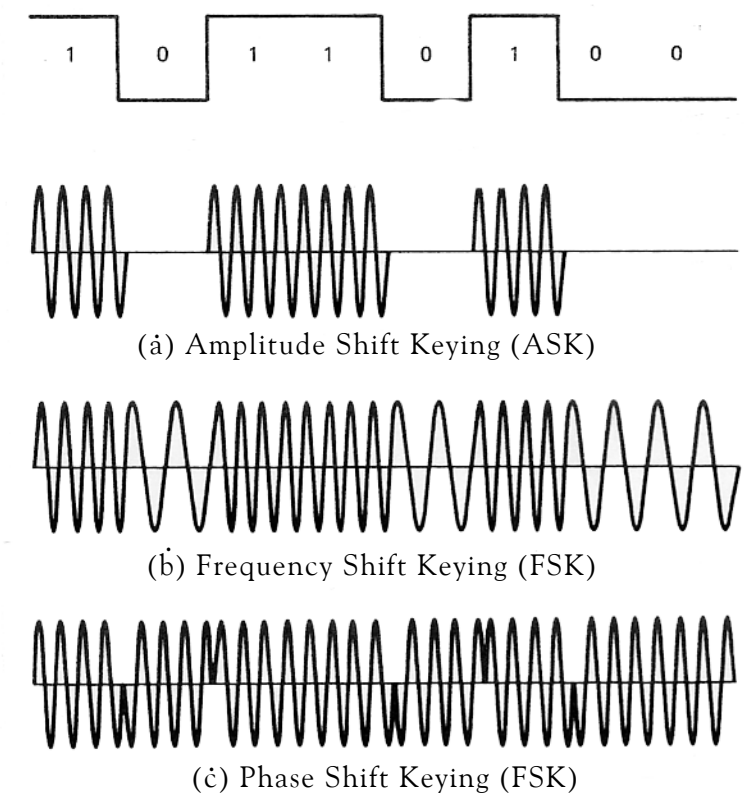


Figure 6.18. Waveforms for ASK, FSK, and PSK modulated signals

- ***Frequency Shift Keying*** **(**FSK**):** With FSK, the carrier transmits two distinct frequencies. A 1 is represented by one frequency, and a 0 by the other frequency. Figure 6.18(b) shows an example of FSK.

- **Phase Shift Keying (PSK):** PSK uses a fixed–frequency sinusoid whose relative phase shift can be changed in abrupt steps. These relative shifts are 0° and 180°. The 180° phase shift occurs whenever there is a change from 1 to 0 or 0 to 1. Figure 6.18 (c) shows an example of PSK.
- **Binary Phase Shift Keying (BPSK):** With BPSK, the phase of the RF carrier is shifted 180 degrees in accordance with a digital bit stream. The digital coding scheme used is called NRZ–M. This and other coding schemes will be discussed on the next subsection. A "one" causes a phase transition, and a "zero" does not produce a transition. Generally, BPSK is preferable to PSK because the latter requires that an absolute phase reference exists at the transmitter and receiver ends, and no phase variations occurrence in the propagation path. Moreover, BPSK offers a 6–dB advantage in signal–to–noise ratio over PSK.
- **Differential Phase Shift Keying (DPSK)** is another special form of PSK. DPSK is easy to implement and it can detect errors easier than BPSK.

6.4.2 Baseband Encoding Formats

The encoding schemes discussed in this are widely used in communications systems. A “mark” denotes 1 and a “space” denotes 0. The most common encoding formats shown in Figure 6.19.

- **NRZ–L:** This is an acronym for *Non–Return–to–Zero Level*. A 1 is always represented by one fixed level of width τ and a 0 is always is always represented by the other level, also of width τ. Thus for the data shown in Figure 6.19, the upper level is 1 and the lower level is zero.
- **NRZ–M:** This is an acronym for *Non–Return–to–Zero Mark*. If a 1 is to be transmitted, there is always a change at the beginning of the bit interval. However, if a 0 is to be transmitted, there is no change. The initial level is arbitrary.
- **NRZ–S:** This is an acronym for *Non–Return–to–Zero Space*. If a 0 is to be transmitted, there is always a change at the beginning of the bit interval. However, if a 1 is to be transmitted, there is no change. The initial level is arbitrary.
- **RZ:** This is an acronym for *Return–to–Zero*. If a 0 is to be transmitted, the signal remains at the 0 (lower) level for the entire bit interval. However, if a 1 is to be transmitted, a pulse of width $\tau/2$ is inserted in a designated part of the bit interval.
- **Biphase–L or Manchester:** This is an acronym for *Biphase–Level*. Within each data bit interval, there are always two states, each of width $\tau/2$. If the data bit is 0, the sequence 01 is inserted. Conversely, if the data bit is 1, the sequence 10 is inserted. This encoding format is also known as *Split–Phase*. Ethernet LANs use Manchester encoding.
- **Differential Manchester (not shown):** This encoding format also uses mid–bit transitions; however, here they are used for clocking. Data is represented by the presence of a transition at the beginning of the bit. Token Ring LANs use Differential Manchester.

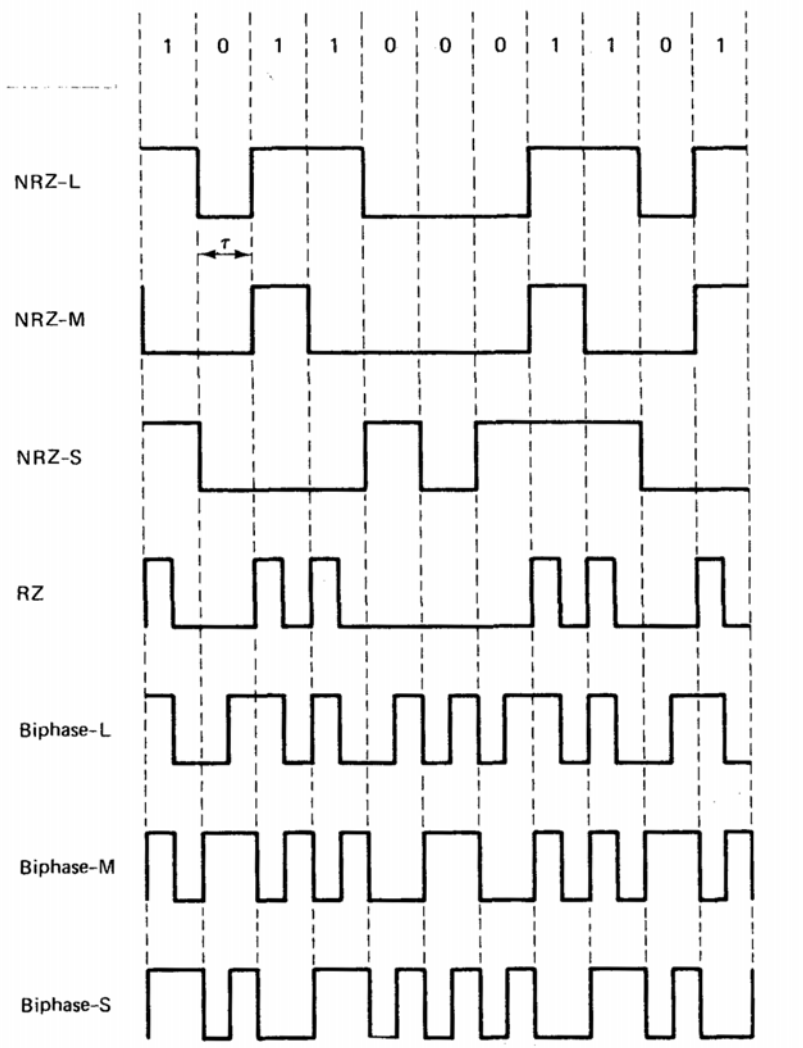


Figure 6.19. Baseband encoding formats

- **Biphase–M:** This is an acronym for *Biphase–Mark*. A transition always occurs at the beginning of a bit interval. If the data bit is 1, a second transition occurs at a time $\tau/2$ later. If the data bit is 0, no further transition occurs until the beginning of the next bit interval. In Figure 6.18, the level just prior to the beginning of the data stream was arbitrarily selected.
- **Biphase–L:** This is an acronym for *Biphase–Level*. A transition always occurs at the beginning of a bit interval. If the data bit is 0, a second transition occurs at a time $\tau/2$ later. If the data bit is 1, no further transition occurs until the beginning of the next bit interval. In Figure 6.18, the level just prior to the beginning of the data stream was arbitrarily selected.
- **Alternate Mark Inversion (AMI):** AMI is used in T1 lines. A signal–encoding scheme in which a "1" is represented alternately as positive and negative voltage. It does not use transla-

tion coding but can detect noise–induced errors at the hardware level. The AMI code is a three–level code (+, –, 0). The 0 level represents a binary zero and the alternate + and – represents the binary 1. An example is shown in Figure 6.20.

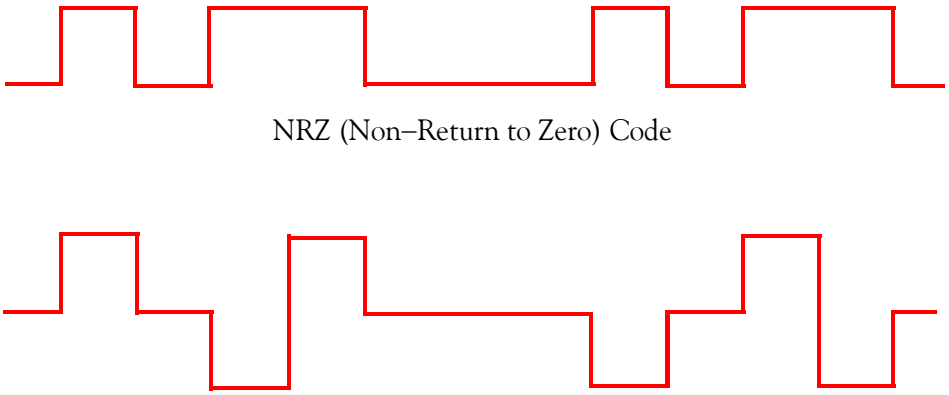


Figure 6.20. AMI encoding format

6.4.3 M–ary Signals

All the encoding formats we have discussed up to this point use only two levels, that is 0 and 1. However, it is possible to use more levels and a number of systems are being used with "m–ary" encoding, a term used to refer to the general class of these systems.

M–ary systems use a number of levels that can be expressed as an integer power of 2 (i.e., 4 levels, 8 levels, and so on. The system that uses 4 levels is referred to as *quartenary* encoding and this encoding is converted to RF for transmission through PSK and thus it is called *QuadriPhase Shift Keying* (QPSK). This and a few others are discussed in the following paragraphs.

Quadrature Phase Shift Keying (QPSK) is a digital frequency modulation action used primarily for sending data over coaxial cable networks, such as cable subscriber networks that connect directly or indirectly to the Internet. Since it's both easy to implement and fairly resistant to noise, QPSK is used primarily for sending data (usually in large quantities of packets) from the cable subscriber upstream to the Internet.

A QPSK signal has four distinct states and these are shown in Figure 6.21. The four phase shifts occur at 90° intervals. Each of the four possible states is referred to as a *dibit*.

QPSK is a 4–ary system, that is, it has 4 different states each represented by a set of 2 binary digits, i.e., 00, 01, 10, 11. Likewise, an 8–ary system has 8 different states each represented by a set of 3 binary digits, i.e., 000, 001, ..., 111, a 16–ary systems has 16 different states represented by a set of 4 binary digits, i.e., 0000, 0001, ..., 1111, and so on.

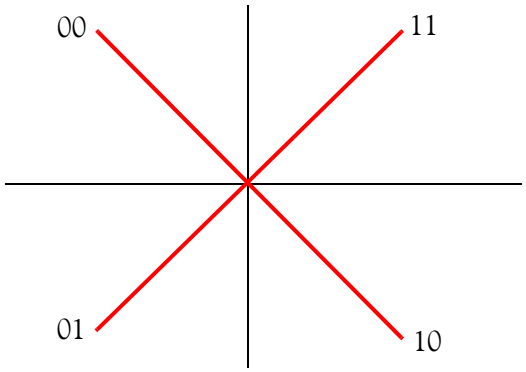


Figure 6.21. Phase sequence of the 4 states in QPSK

Differential Quadrature Phase Shift Keying (DQPSK) is a digital modulation technique commonly used with cellular systems. Motorola's CyberSurf cable modem uses DQPSK to carry data upstream from the subscriber's computer to the Internet on a narrower frequency band than standard QPSK. Narrower bands allow more upstream channels.

64–State Quadrature Amplitude Modulation (64QAM). This digital frequency modulation technique is primarily used for sending data downstream over a coaxial cable network. 64QAM is very efficient, supporting up to 28 Mbps peak transfer rates over a single 6 MHz channel. However, 64QAM is susceptible to interference and thus it is unsuitable for use with noisy upstream transmissions (from the cable subscriber to the Internet).

Vestigial Side Band (VSB) is a digital frequency modulation technique used to send data over a coaxial cable network. It is used with Hybrid Networks for upstream digital transmissions. VSB is faster than the more commonly used QPSK, but it's also more susceptible to noise.

6.5 Microwaves

Microwave radiation is the portion of the *electromagnetic spectrum*[*] just above radio waves. Thus, microwaves travel at higher frequencies than radio waves and provide better throughput as a wireless network media. Microwave transmissions require the transmitter to be within sight of the receiver. These systems use licensed frequencies. Microwaves use terrestrial or satellite communications systems. These are discussed below.

6.5.1 Terrestrial microwave

Terrestrial microwave transmissions are used to transmit wireless signals across a few miles. These systems are often used to cross roads or other barriers that make cable connections difficult. Ter-

---

* *Electromagnetic spectrum is the entire range of radiation extending in frequency from approximately* 10^{23} *hertz to 0 hertz or, in corresponding wavelengths, from* 10^{-13} *centimeter to infinity and including, in order of decreasing frequency, cosmic–ray photons, gamma rays, x–rays, ultraviolet radiation, visible light, infrared radiation, microwaves, and radio waves.*

restrial systems require that direct parabolic antennas be pointed at each other. Relay towers can be used as repeaters to extend the distance of the transmission. These systems operate in the low GHz range and require licensed frequencies. Installation can be difficult because terrestrial microwave transmissions require that the antennas have a clear line of sight.

6.5.2 Satellite microwave

Satellite microwave transmissions are used to transmit signals throughout the world. Satellites in *geosynchronous*[*] orbit remain in a fixed position over a point on the equator, thereby providing uninterrupted contact between ground stations in their line of sight. Satellite dishes are used to send the signal to the satellite where it is then sent back down to the receiver's satellite. These transmissions also use directional parabolic antennas within line–of–site. The large distances the signals travel cause propagation delays.

There are many advantages and certain disadvantages using satellite communications. Some are listed in Table 6.3.

6.6 Infrared

In the electromagnetic spectrum, infrared is between microwaves and visible light. That is, the wavelengths of infrared radiation are shorter than radio wavelengths and longer than light wavelengths. By detecting infrared radiation, astronomers can observe stars and nebulas that are invisible in ordinary light but it emits infrared radiation.

Infrared has many practical applications. Infrared techniques reveal conditions in the body that are not visible to the eye or recorded by X rays. These techniques are used as a diagnostic tool in medicine, monitor crop conditions and quality of products in large agricultural areas, and locate mineral deposits.Infrared is also used in remote sensing such a remote control for a television set. Infrared transmissions can be affected by objects obstructing the space between a transmitter and receiver These transmissions can be point–to–point or broadcast.

6.6.1 Point–to–Point Infrared

Point–to–point infrared transmissions use highly focused beams to transfer signals directly between two systems. Many laptop systems, such as Personal Data Assistants (PDAs), use point–to–point transmissions. Point–to–point systems require direct alignment between devices.

---

* *Geosynchronous is an abbreviation for geographical synchronization. This type of orbit synchronizes its position with that of a point on the Earth. In order to do that, the orbit must be 35,859 Km (22,282 miles) above the equator. For all practical purposes, it appears to be stationary since the satellite's orbit and Earth's rotation are in the same direction and at the same speed. Logically, one would assume such a satellite would be an ideal platform in space for cellular telephone relays and similar digital interactive transmissions. However, due to the great distance involved, the amount of time for sound to travel is not good for cellular calls. Much lower satellites must be used for such calls. They are ideal for streaming media such as TV signals, streaming data and other burst oriented transmissions.*

TABLE 6.3 Satellite communications – Advantages / Disadvantages

Advantages	Disadvantages

• Only one satellite can provide coverage over a large geographical area
• Three satellites in geosynchronous orbit 120 degrees apart can provide almost world–wide coverage with the polar regions excluded
• Inherent flexibility to interconnect large number of users distributed over a wide geographical area
• Rapid expansion of communications into new or isolated areas
• Line–of–sight communications with aircraft, ships, and submarines
• Broadcast capability (from one transmitter to many receivers) and report back capability (from many transmitters to one receiver)
• Conferencing among geographically separated users
• Support for high data rates
• Reliable unattended service over a long time period
• Satellite physically remote from direct attack by enemies
	• Vulnerability to electromagnetic and physical threats such as
	  • Jamming (substantially cheaper than physical attack being a less overt act)
	  • Interception
	  • Disturbance of propagation medium
	  • Nuclear attack
	• Very expensive initial investment

Point–to–point can also provide an alternative to terrestrial microwaves. For instance, if two buildings have direct line–of–site availability, point–to–point can utilize high–power infrared beams. This does not require an FCC license and is immune to EMI. However, these systems are susceptible to interference from anything that can block the path of the beam.

Point–to–point infrared transmission provide a high level of security, as any attempt to interfere with the beam would be detectable. One must be careful when working with infrared devices since they can cause damage to eye and skin tissue.

6.6.2 Broadcast Infrared

Broadcast infrared transmissions use a spread signal to broadcast in all directions instead of a direct beam to allow reception by several receivers. This alleviate the problem of proper alignment and obstructions. Some systems utilize a single broadcast transceiver to communicate with many devices. This type of system is easy to install.

Broadcast infrared transmissions operate in the same frequencies as point–to–point infrared and

are susceptible to interference from light sources. The drawback of this system is that the diffused signal reduces transmission rates to 1 Mbps. This system overcomes some of the problems of point–to–point transmissions, but the trade–off is a decrease in speed.

6.7 Synchronization

Timing is essential if the encoding schemes are going to work. The signal must be examined at the appropriate time to determine what changes have occurred and to interpret the signal correctly. Coordinating timing between the sending device and the receiving device is known as *synchronization*. Synchronization can be either asynchronous or synchronous.

***Asynchronous transmission clock synchronization*:** This requires a start signal at the beginning of the message and a stop bit at the end of the message. When the transmission is ready to begin, the start bit is sent to synchronize clocking on the sender and receiver. The stop bit informs the receiver that the transmission has ended. When no message is being sent, there is no synchronization between devices.

Asynchronous systems also use parity for error checking. The parity options available for asynchronous communications are even, odd, and none. Even parity specifies that the sum of the bits be an even number. Odd parity specifies that the sum be an odd number. None specifies that no parity error checking be used. Parity only detects if there is a problem with one bit. If two bits are incorrect, parity will not report an error. The overhead required in asynchronous communications makes it inefficient for sending data at high speeds.

7

***Synchronous transmission with clock synchronization*:** This relies on other methods to coordinate clocks on the sending and receiving devices. Synchronous communications require the sending and receiving clocks are synchronized at all times. The receiver is constantly awaiting data. No start bit is used to prepare the receiver.

6.8 Baseband and Broadband Transmissions

Some situations require multiple signals to travel across the cable at once, while others may only need one signal at a time. The two different methods of utilizing the cable are baseband and broadband.

6.8.1 Baseband transmissions

Baseband transmissions are those that transmit one signal at a time. The signals can be bidirectional. This method is frequently used in LANs, which use digital signaling to transmit data, but it can also be used with analog signals. Baseband has a cable length limit of 2 Km. As discussed in Chapter 5, one can use repeaters to extend the allowable distance.

6.8.2 Broadband transmissions

Broadband transmissions divide the bandwidth into channels. This allows for multiple transmissions at once. Broadband is less susceptible to attenuation and can transmit further than baseband transmissions. Broadband transmissions can now be used with both analog and digital signals such as in cable TV. Internet access comes in many forms, from standard dial–up to faster broadband. Here are some of the options:

***Dial–up*:** Service comes via a standard telephone line with an average connection speed of less than 56 Kbps. Dial–up service requires a standard modem. With the advent of cable and DSL services described below, this service will soon be extinct.

***Cable*:** Service comes via cable TV wires with download speeds up to 6 Mbps and upload speeds up to 1 Mbps.* This service requires a special modem which is provided by the cable company.

***DSL*†:** Digital Subscriber Line service comes via phone lines, without disturbing the dial tone for phone service, with download speeds up to 6 Mbps and upload speeds up to 1 Mbps. DSL requires special equipment, and it is provided by the telephone company.

***Satellite*:** Service comes via the satellite dish with speeds comparable to DSL It requires special equipment which is provided by the satellite company.

6.9 Portable Videophones

Television reporters use portable videophones to transmit live reports from remote locations to their networks. These videophones are lightweight and thus are easy to carry and set up in remote locations. They can be operated by a single cameraman. Figure 6.22 shows a videophone and the interfacing equipment.

Audio and video signals from the camera are fed into the videophone unit enclosed in a waterproof case. The unit takes video and audio data and converts it to a digital signal. The signal is then is transmitted by satellite phone to a relay satellite. The satellite then relays the signal to a ground station where it is picked up by the news services.

Due to the low transmission rate of satellite phones which have a maximum data rate of 128 Kbps, the received images are low in quality. The quality can be improved by splitting the signal between two satellite phones. Also, there is a half–second delay in a live broadcast because of the distance the signal has to travel to the relay satellite and back to earth.

* *The reason that the upload and download speeds are different is because the upload speed is downgraded, causing it to take considerably longer to upload data to the Internet.*

† *Also referred to ADSL where A denotes "asymmetric" due to the fact that the rated download and upload speeds are not equal.*

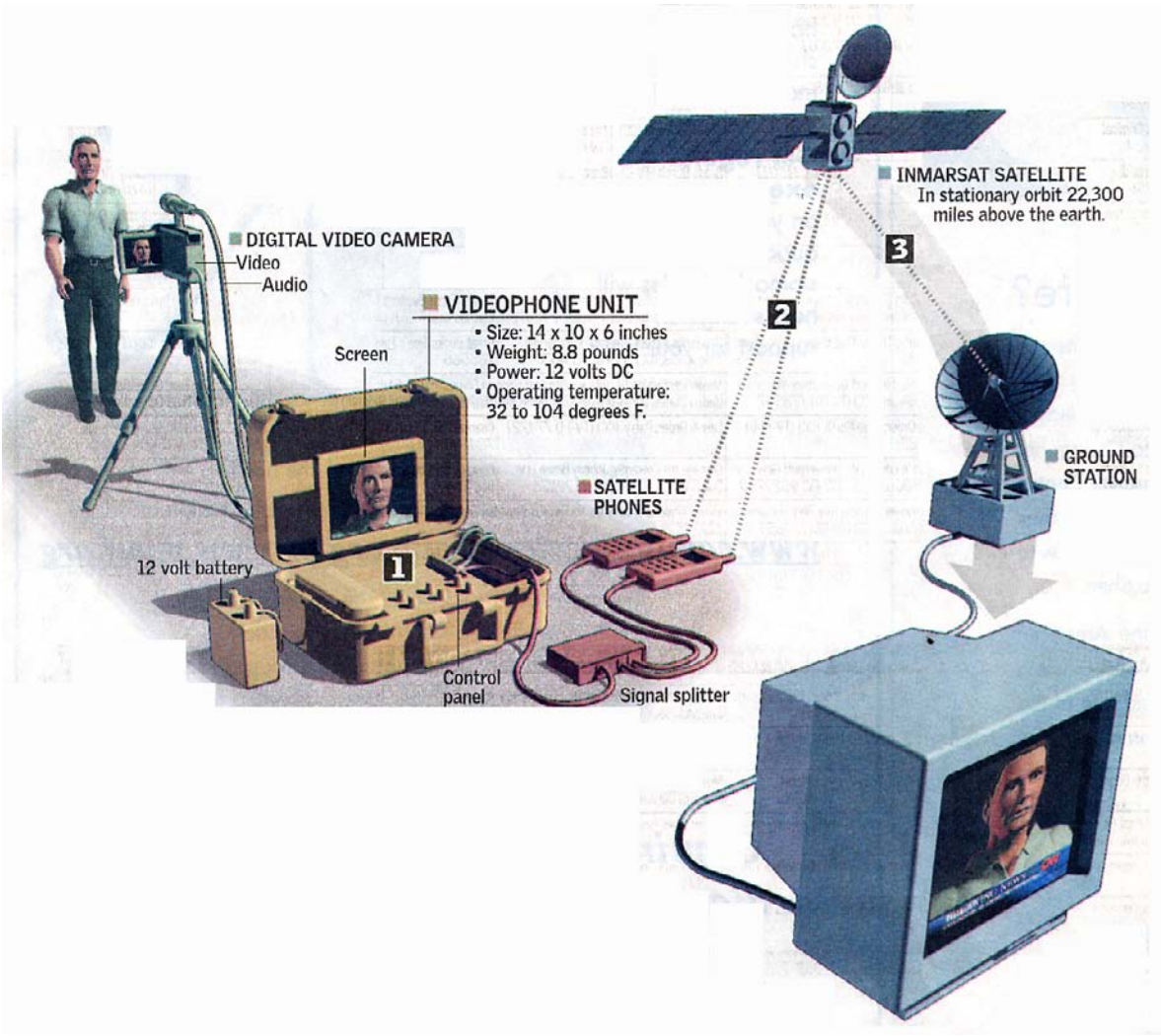


Figure 6.22. Portable videophone to transmit live reports. Courtesy 7E Communications

6.10 Summary

- Resistance, impedance, noise, attenuation, and cross talk are all undesirable effects and must be considered when selecting a cable type.
- UTP data cable is constructed with either two or four pairs of twisted cables. Cable with two pairs use RJ–11 connectors, and four–pair cables use RJ–45 connectors. Networks use four–pair UTP cables.
- STP cable is similar to UTP but has a mesh shielding to protect it from EMI.
- RG–7 or RG–11 is coax cable used with the thick Ethernet.
- RG–58 is used with the thin Ethernet.
- Fiber–optic cable transmits light pulses. The presence of a light pulse is translated into a logical 1 and its absence into a logical 0 at the receiver end.
- Fiber–optic cable is available in two types: single mode and multi–mode. Single–mode cable only allows for one light path through the cable, whereas with multi–mode we can have two or more paths.
- The principle types of multiplexing are Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM). In TDM all signals use the same frequency but operate at different times, while in FDM, all signals operate at the same time with different frequencies.
- The three types of wireless media are radio wave, microwave, and infrared.
- Antennas vary in types and geometrical figures depending on the application.
- Spread spectrum coding methods are the Direct Sequence (DS) and Frequency Hopping (FH).
- Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, printers, and Personal Digital Assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short–range wireless connection.
- Wi–Fi, short for wireless fidelity, enables high–speed, low–cost access to the Internet.
- TDMA, FDMA, CDMA, and S–CDMA are multiple access systems used extensively in satellite communications.
- ASK, FSK, and PSK are three methods of transmitting analog signals using encoding.
- Manchester and Differential Manchester are among several baseband encoding formats used in the transmission of binary signals.
- Microwaves are used in both terrestrial and satellite communications systems.
- Synchronization is essential in data transmissions.

- Baseband transmissions use the entire bandwidth to transmit one signal at a time whereas broadband transmissions divide the bandwidth into channels.
- Portable videophones are used by television reporters to transmit live reports from remote locations to their networks.

6.11 Exercises

True/False

1. The twists in a twisted–pair cables reduce the vulnerability to EMI and cross talk. _____

2. Category 2 UTP cables can support transmission rates up to 20 Mbps. _____

3. STP cable is less expensive than UTP and coax. _____

4. Coax cable is a good choice for a SOHO network. _____

5. For a two–way communications, the fiber optic cable must have four strands, two for each direction. _____

6. Cable TV systems use Time Division Multiplexing (TDM). _____

7. Radio waves operate at frequencies higher than microwaves. _____

8. A dipole transmits or receives most of its energy at right angles to the wire. _____

9. TDMA and CDMA are suited only for digital transmissions. _____

10. Infrared operates at the visible light portion of the electromagnetic spectrum. _____

Multiple Choice

11. EMI is no problem when _____ cable is used.

A. UTP

B. STP

C. coax

D. fiber optic

12. Type _____ STP cable is used for patch cords.

A. 2

B. 6

C. 7

D. 9

13. The _____ is the simplest type of antenna.

A. circular loop

B. square loop

C. dipole

D. helix

14. Direct Sequence spread spectrum communications systems transmit data at _____ Mbps.

A. 1 to 10

B. 2 to 6

C. 12 to 16

D. 20 to 50

15. With Bluetooth, the maximum transmission distance is _____ meters.

A. 10

B. 50

C. 100

D. 1000

16. The _____ method of data transmission was designed to provide secure and noise immune communications across coaxial cable networks.

A. QPSK

B. DQPSK

C. 64QAM

D. S–CDMA

17. _____ communications systems have the flexibility to interconnect a very large number of users over a very wide geographical area.

A. Ground radio

B. Satellite

C. Infrared

D. Spread Spectrum

18. PDAs use _____ transmissions

A. low power radio

B. high power radio

C. point–to–point infrared

D. broadcast infrared

19. _____ systems use parity for error checking.

A. Asynchronous

B. Synchronous

C. Baseband

D. Broadband

20. Broadband transmissions can be used with _____ signals

A. only digital

B. only analog

C. both analog and digital

D. multiplexed

Problems

21. Your company is expanding and needs to install a new network cable system into the same building. However, immediately below the area where the new networks will be located is a manufacturing company that uses many machinery equipment. It is estimated that about 500 meters of new wiring will be required to interconnect the existing network with the new network. What type of cable would you recommend?

22. Your company is expanding with the addition of a new building that is located across a busy highway from the existing building. The management is not interested in obtaining licensing for radio communications. However, security and high transmission rates are highly desirable. Which transmission method would you recommend?

6.12 Answers to End–of–Chapter Exercises

True/False

1. T – Refer to Page 6–2
2. F – Refer to Page 6–2
3. F – Refer to Page 6–3
4. T – Refer to Page 6–4
5. F – Refer to Page 6–5
6. F – Refer to Page 6–9
7. F – Refer to Page 6–25
8. T – Refer to Page 6–10
9. T – Refer to Page 6–17, 6–18
10. F – Refer to Page 6–26

Multiple Choice

11. D – Refer to Page 6–5
12. B – Refer to Page 6–3
13. C – Refer to Page 6–10
14. B – Refer to Page 6–14
15. C – Refer to Page 6–16
16. D – Refer to Page 6–20
17. B – Refer to Table 6.3, Page 6–27
18. C – Refer to Page 6–26
19. A – Refer to Page 6–30
20. C – Refer to Page 6–29

Problems

21. The best choice would be fiber optic. It is immune to EMI interference and can easily transmit over 500 meters. UTP would not be a viable choice because of EMI problems. Also, coaxial cable is not an option because of its distance limitation. The cost of a new repeater to be used with coax would probably be more than the cost of fiber optic cable.

22. Point–to–point infrared would be a good choice. It combines a high level of security and high transmission speeds. Moreover, it does not require FCC licensing.

Chapter 7

Network Design and Administration

This chapter discusses the various types of networks that the networks administrator can use to build for his/her needs, the hardware and software required, and tasks that a network administrator must perform to maintain the network(s) he/she is responsible for. These tasks include security and safeguarding data from internal and external disasters.

7.1 Network Design Considerations

There are many factors that networks administrator must consider before designing the network. The most important consideration is the assessment of the networking needs. The networks administrator must consider which features and benefits are most vital to his network. The word "design," as used here, means the collection and installation of the essential hardware and software that he must possess to assemble and place in operation his network.

The following items are of utmost importance:

- **Versatility:** Networking needs vary from one network to another. In networking there is no such thing as "one size fits all."
- **Expandability:** The original network design must allow for a wide variety in expansion capabilities including scalability.*
- **Affordability:** It is true that advanced technology is no good unless one can afford it. But he can start with an affordable and versatile network and expand in the next level of affordability.

Next, the administrator must provide answers to the following questions:

- Where the computers, printers, and other peripherals will be located?
- Which computers will be networked and how far apart are they? Will all be located in a large open space or in rooms separated by walls?
- What networks speeds are required?
- What applications and operating systems will be used?
- What type of Internet connections will be used?

* *Scalability means that newer and faster versions of LANs can be integrated into networks with older and slower hardware devices while adding on new segments that run at higher data rates.*

- Is the facility prewired for networking or will it be required to install the network cables? If so, what type(s) will be used?
- How many printers, scanners, and other peripheral equipment are to be networked.
- What budget is allocated for buying additional hardware and software?

7.2 Wired Networks

This section presents the main networking technologies that use cable and their features to help the networks administrator decide on the network type that is suitable to his needs.

7.2.1 10/100 and Gigabit Ethernet Networking

The key features of Ethernet Networking are:

- It is the most widely used networking standard
- It can operate from 10 Mbps to 100 Mbps transmission speeds
- It can use either Category 5 UTP (or higher) or fiber optic cabling
- It is adaptable with 10/100 Mbps Network Interface Cards (NICs)
- Provides seamless integration* with different Ethernet speed standards

Table 7.1 provides a list of users that are suited for the 10/100 Ethernet network.

10/100 Networking Hardware

To build the network, the administrator will need most or all of the devices listed below.

- 10/100 Network Adapters or NICs
- 10/100 Hubs and/or Switches
- 10/100 Print Servers
- Routers
- Network Attached Storage (NAS) or Storage Attached Network (SAN)
- Keyboard, Video, and Mouse (KVM) Switches
- Cables

* *Seamless integration implies the favorable result that occurs when a new hardware component or program blends smoothly into the overall operation of the system. It is usually the result of thoughtful design and programming.*

TABLE 7.1 Users suited for the 10/100 Ethernet network

User	Recommendation	Advantages	Disadvantages
Home	• High	• Reliable • High Speed	• High cost relative to small number of users • Exposed cabling can create an unpleasing view especially in expensive homes
SOHO (Small Office/Home Office)	• High	• Reliable • High Speed • Moderate cost for Small Office	• Exposed cabling in home use
SMB (Small to Medium Business)	• High	• Reliable • High Speed • Low cost in relation to number of users	• Wiring installation costs in new buildings
Enterprises (Large Corporations)	• High	• Reliable • High Speed • Very low cost in relation to large number of users	• High cost relative to small number of users

10/100 Network Adapters or NICs

Every desktop PC or notebook must have either a *network adapter* or *a network card*. A network adapter usually refers to a device that is connected externally while a network card is connected internally. Both perform the same function. Henceforth, both will be referred to as NICs.

Before choosing a NIC the user must determine whether his PC or notebook has a 32 or 64–bit bus architecture. Bus architectures are discussed in Chapter 5. It is recalled that the PCMCIA bus is used in notebooks.

NICs operate at various speeds. The 10/100 devices automatically detect connection speeds of either 10 Mbps or 100 Mbps, and adjust their speed to match the highest speed.

Desktop PCs are provided with internal expansion slots on the motherboard. Pentium–based PCs use the 32–bit PCI bus. Newer PCs use the IEEE 1394 bus.

A very useful feature especially for network administrators is the *Wake–on–LAN* (WoL). This refers to a technology developed by the IBM and Intel Advanced Manageability Alliance where a computer motherboard can turn itself on (and off) based on signals arriving at the computers network card. Thus, if all of client PCs are equipped with WoL, the administrator can remotely turn

all PCs on during a Saturday afternoon and perform a network based upgrade without actually going to each PC and powering it on.

As discussed in Chapter 5, unless a PC has the Plug–and–Play (PnP) capability, when a NIC is inserted to the motherboard, it must be configured with and IRQ and I/O address. PnP is available with the latest Windows versions.

When a PCMCIA card is inserted to a PCMCIA slot, the notebook PC automatically senses that a new card has been added and assigns an IRQ and I/O address. Like desktop PCs, notebook PCs use Category 5 UTP cable.

Most notebook PCs today are equipped with a 32–bit CardBus slot where a 32–bit CardBus NIC can be inserted. These are now replacing the older 16–bit PCMCIA cards.

The Universal Serial Bus (USB) is presently one of the most useful devices. USB Version 2 can achieve speeds up to 480 Mbps and can be used with applications such as digital imaging, IP telephony (Voice over IP), and multimedia games.

USB ports can accommodate many devices such as joysticks, mice, scanners, digital cameras, and speakers. Devices connected to USB ports are said to be "hot–swappable" meaning that they can be added or removed without removing power from the PC.

Most that present–day Ethernets are configured in a star topology where the central point is a hub or a switch. Thus, once the administrator has decided on the devices he will use, he can connect them to a hub or switch using Category 5 UTP cables. However, he must be aware that Ethernet and Fast Ethernet cabling rules require that the cable span does not exceed 100 meters from any node to a hub or a switch. Also, if two hubs are used, the distance from each other should not exceed 10 meters. If the distance from a node to a hub or switch exceeds 100 meters, he can use a repeater to extend the distance.

A hub shares its total bandwidth, or speed, among all active users on the network and transfers data in half–duplex mode, like a cell phone. Thus, if a network with 5 users runs at 100 Mbps, each user gets a maximum of 20 Mbps of the hub's bandwidth. A switch, on the other hand, has a dedicated bandwidth of 100 Mbps and this means that no matter how many users are connected to the network, each user can send and at the same time receive data at speeds of 100 Mbps.

Table 7.2 lists the features of hubs and switches and shows the available bandwidth for each user when 10 active users are connected to an Ethernet.

Printers Connected to the Network

If a printer is attached directly to a PC on the network, the user still can share it with PCs but print jobs will slow the performance of the PC which supports the printer. Accordingly, a *print server* should be considered. A print server is provided with multiple ports to accommodate several printers. The user can attach the printer to the parallel port on the print server using a stan-

dard RS–232C cable or an RS–449 cable. The RS 232C cable is limited to 19.2 Kbps and maximum distance of 15 meters. The RS–449 cable can achieve rates up to 2 Mbps and can be used for distances over 15 meters.

TABLE 7.2 Hub / Switch comparison

Device	Mode of Operation	Bandwidth	Data Packet *Handling*	With 10 Active Users
Hub	Half Duplex (Sends or receives data to one node at a time only)	Shared (All users share the hub's bandwidth)	Broadcasting (Broadcasts data packets to all nodes until the right address is found)	10/100 Hub Shared Bandwidth (Shared among 10 users; therefore, speed is 10 Mbps)
Switch	Full Duplex	Dedicated	Direct forwarding to intended destination (Determines the intended destination and sends it there directly)	10/100 Switch Dedicated Bandwidth (200 Mbps total – 100 Mbps each way)

Use of a Router for Network Security

Present–day activities such as online banking, online correspondence, and other issues have changed the public's lifestyles. The consumer is constantly concerned that every time he/she connects to the Internet he subjects himself to possible identity theft and he is vulnerable to hackers. Accordingly, network security should be taken very seriously.

As discussed in Chapter 5, a router is a device that interconnects one network to another directly as if it were a dedicated link between sender and receiver. Therefore, the administrator can use routers to act as firewalls to safeguard against intrusions from outsiders. Firewalls can be established internally to block unauthorized users from accessing other parts of the network. For instance, one can use a router to create a firewall between the maintenance department and the payroll department.

Every node on a network and the Internet has an IP address, just like every house has a street address. *Network Address Translation* (NAT) assigns each node an IP address only known to the router. Thus, the router acts as a mail center to both incoming and outgoing messages to forward data only to the proper address.

Some routers use *Dynamic Host Configuration Protocol* (DHCP) to assign temporary IP addresses for each PC and each address is valid only for a certain time period. These temporary addresses are assigned by a DHCP server when client PCs log on to a network or the Internet. Thus, DHCP serves as a security measure since the temporary addresses expire after a pre–determined amount of time.

Besides the security that a router provides, it computes the most efficient path for a data packet to reach its destination. It does this by constantly updating its routing table and thus it avoids lines that are inoperative or are congested with data traffic.

Once the router has been installed the administrator can use his web browser to connect to a utility that will allow him to manage features such as DHCP, password management, packet filtering, and DMZ hosting.

10BaseT and 100BaseTX Ethernets Networks

The 10BaseT and 100BaseTX (Fast) Ethernets are ideal for new networks or for departmental use within a company. The administrator can choose one or the other depending on the speed requirements. If both are used, they can be interconnected with a 10/100 switch. The ports on these switches automatically sense the speeds of their connections and adjust each port's speed to match.

If a 10 Mbps PC is connected to a 10/100 hub, the hub will adjust its port to run at 10 Mbps. If the 10 Mbps PC is replaced with a 100 Mbps PC, the same hub will adjust its port to run a 100 Mbps. Thus, selected users or departments can be converted to Fast Ethernets first, while other users can remain connected to 10 Mbps PCs until faster hardware can be bought to replace the existing.

Gigabit Ethernet Networks

The Gigabit Ethernets operate at 1 Gbps (1000 Mbps) speeds. That is, a Gigabit Ethernet is 10 times faster than the Fast Ethernet. Seamless integration allows a Gigabit Ethernet to work with a Fast Ethernet. While Gigabit Ethernet Networks are still beyond the budget of most users, prices are falling. A further price decrease is anticipated when the new generation of the Gigabit Ethernet operating at 10 Gbps speeds will be introduced.

Until recently, Gigabit Ehernets were possible with fiber optic cable only. But a new UTP copper cable known as Category 5e can achieve 1 Gbps speeds to and thus it offers a less expensive option. New 1000 Mbps cards, such as the Instant Gigabit™ Network Adapter made by Linksys, are used with servers or the Internet to accelerate network performance.

Adding Ports Using Stackable Hubs

When expansion of an existing Ethernet LAN is anticipated, the administrator should consider using a 10/100 stackable hub. As discussed earlier, these hubs can be connected with a special stacking cable so networks recognize them as a single hub. Stacking cables add more ports to the "same" hub by providing more tightly integrated performance and eliminating data bottlenecks.

Most stacks consist of two, ten or more stackable hubs, all connected with special stacking cables. As discussed in Chapter 4, with UTP, the administrator is limited to two hubs between workstations, and the hubs must be connected using a 5–meter cable. This limitation can be bypassed by placing a switch or repeater between the two hubs, or by using stackable hubs. The

latter option offers the administrator a multitude of expansion possibilities and a flexible number of ports to work with.

Stacking technology is proprietary, so a set of stackable hubs from different manufacturers may not be stacked. The user should make sure that stackable hubs from the same product line in the same company are used. Also, he should not confuse this term with physically stacking hubs on top of each other. Non–stackable hubs placed on top of each other will not act as a single hub.

As stated above, a switch or repeater can be used between the hubs to enhance the signals. Thus, if a 10–port hub is connected to a 16–port switch, all the computers on both segments of the network can communicate with each other. Hubs and switches made by different manufacturers can be used together too, provided they run at compatible speeds.

During the planning phase of the network expansion the networks administrator should make trade–off studies to decide on the best choice of devices. For instance, while a 10/100 hub with high port density or stackability is less expensive than a 10/100 switch, the latter provides full duplex, dedicated connections to each of its ports.

Network–Attached Storage (NAS)

The massive bulk of data exchanged between PCs every day will eventually exhaust the network storage resources. NAS devices provide a quick add–on solution. NAS boxes are basically compact, portable file servers, and some have an IP address of their own. Instead of taking apart file servers to upgrade drive space, NAS units can be installed without down time and moved around the network with ease.

Storage–Attached Network (SAN)

A SAN serves a similar function as a NAS but also offers storage space manageability. While NAS devices are usually much easier to install and more portable than SANs, the latter also provide centralized network manageability. SAN installation can be complex and is usually permanent. NASs and SANs are also discussed in Section 7.14 of this chapter.

Keyboard, Video, and Mouse (KVM) Switches

A KVM switch allows a single keyboard, video display monitor, and mouse to be switched to any of a number of computers when typically a single person interacts with all the computers but only one at a time. The switch provides more table space in addition to saving the cost of multiple keyboards and monitors.

KVM switches are commonly used at Web and other server locations with multiple computers but usually a single administrator or Webmaster. The switches range in price from about $200 U.S. for a system in which up to eight computers can be daisy–chained to about $2,000 for a switch that controls up to 10 Sun workstations. Larger configurations can cost more. KVM switches are not networking products in the traditional sense. Nevertheless, they serve the same networking purpose of pooling resources. These devices are available on a packaged “starter kit” which includes both the KVM switch and the cables.

Cable Options

UTP, STP, or fiber optic cables can be used in Ethernet LANs. The characteristics, advantages, and disadvantages of each are discussed in previous chapters. A brief review is provided for each and when they should be used.

Most Ethernet networks use Unshielded Twisted–Pair (UTP) cabling, which is slightly thicker than a phone cable. Instead of having four internal wires like a phone cable, a twisted–pair cable has eight wires inside and is tipped with RJ–45 connectors. One end of the cable is connected to a PC, and the other end of the cable is plugged into a port on a hub or switch.

UTP cabling comes in different grades called "categories.' Category 5, the highest standard grade, is the most widely used cabling and works extremely well in most Ethernet environments. Also known as "Cat 5," Category 5 cabling is the minimal requirement for 100 Mbps Fast Ethernet networks.

Shielded Twisted–Pair (STP) cabling, is used for Ethernet networks in areas with high EMI, where the foil shield in STP cabling protects data from it. EMI exists around airports, radio towers, and industrial sites with heavy electrical equipment.

The Cat 5 UTP cabling that connects PCs is called *straight–through cabling*[*], meaning pin 8 in the cable's tip is still pin 8 at the other end. If the user holds the tips of the cable side by side, parallel to each other with the wires facing up, the colors of the wires inside will be in the same order from left to right.

Ethernet and Fast Ethernet cabling rules require that a single twisted–pair cable spans no more than 100 meters from any node to a hub or a switch. Two hubs running at 100 Mbps can only be 10 meters from each other. If the distance between two nodes exceeds 100 meters, a repeater or a switch, which acts as a repeater, must be used to amplify incoming data signals before passing it on to the next node.

The standard Category 5 UTP cabling cannot be used outdoors or with long distances such as networks that span the size of a campus. Therefore, many corporate and university networks rely on fiber optic cabling for a sturdy network backbone and high speed data transfer. Although fiber is physically capable of carrying terabits of data per second, the signaling hardware currently on the market can handle no more than a few gigabits of data per second.

With Gigabit and 10 Gigabit Ethernets becoming more common, undoubtedly fiber optic cables will be used for even more of the network backbones in the future The most commonly used and economical type of fiber cabling is Multi–Mode Fiber (MMF) with a 62.5 micron fiber optic core. Single–mode fiber optic cable is more efficient than its multi–mode counterpart, but also it is

* *Another type are the so–called crossover cable. In a crossover cable, wires change position from one end of the cable to the other: pin 1 at one end becomes pin 3 at the other, and so on.*

more expensive due to its smaller optic core that helps retain the intensity of traveling light signals.

A fiber connection always require two fiber cables: one transmits data, and the other receives it. As discussed in Chapter 6, fiber optics cable comes with 2 types of connectors. The square SC connectors are the most common type of connector used in the U.S. ST connectors are round, and are commonly used in Europe. For connections over 300 meters, especially outdoors, or in networks without repeaters (data signal boosters), fiber optic cabling is recommended.

Fiber optic cabling is used primarily for network backbones and distant connections. Made from flexible, optically efficient strands of glass and coated with a layer of rubber tubing, fiber optics use photons of light instead of electrons to send and receive data. Since light tends to dissipate quickly when moving from one material to another, the user should minimize the number of lengths between nodes, or hops. The more connectors used and the longer the fiber cables are, the higher the optical loss will be.

When using fiber optic cabling for long hauls, the networks administrator should buy a hub, switch, or other device with a fiber port. Hubs and switches with multiple fiber ports are available too. Also, the number of hops, the distance between two nodes should be minimized, and a single length of fiber optic cabling as the network backbone should be used instead of joining multiple cables together. If the distance exceeds 2000 meters, a switch or a repeater should be used as a signal booster. A typical wired LAN is shown in Figure 7.1.

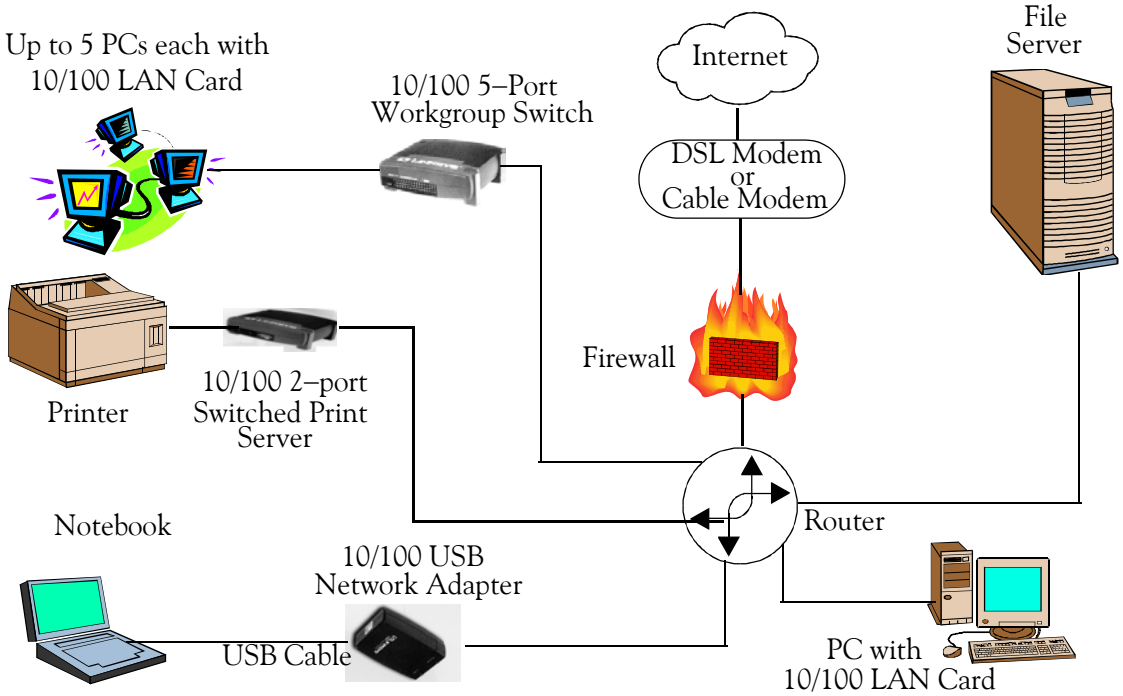


Figure 7.1. A typical wired LAN

7.2.2 Token Ring, CDDI, and FDDI Networks

The Token Ring, CDDI, and FDDI Networks are discussed in Chapter 4. A Token Ring LAN is a group of computers connected in a loop. The group uses a token passing access mechanism. A computer wishing to send data must first receive permission. When it gets control of the network, it may transmit a frame. Each frame transmitted on the ring travels from one computer to the next, until it ultimately returns to the initiator of the transmission.

The Token Passing Ring Network was originally developed by IBM but never attained the popularity of Ethernet LANs. The IEEE 802.5 specification which was modeled after IBM's Token Ring is almost identical and the term Token Ring is used to refer both specifications.

As stated above, in a Token Ring LAN, each station can send a signal along the loop after receiving permission to do so. Only one station may have control on the network at a specified time. The signal will travel from one station to the other until it reaches its destination and returns to the initiator.

Token Ring networks use a priority system that allows stations with high priority to use the network more frequently. The priority is defined by the frame's priority and reservation fields. In order to seize a token a station must have priority which equals or is higher than the priority field of the token. Only then the station can reserve the token for the next pass around the network. This way when the next token is generated, it includes the higher reserving station. Stations must change the priority back to its previous setting after their transmission has completed.

In order to detect and correct network faults, Token Ring networks may dedicate a station for monitoring frames which are circling around without being dealt with. This monitor removes such frames and allow the network to function in a normal manner all over again.

FDDI (Fiber Distributed Data Interconnect) is an improved token ring specification based on fiber as the physical medium. As opposed to Token Ring's single ring, FDDI, uses two to achieve better results. CDDI, yet another standard, resembles FDDI, but uses a copper wire for its ring.

FDDI and CDDI networks implement a recovery mechanism which enable the network to function properly even under a broken ring. FDDI and CDDI use two rings to achieve recovery capabilities. A token is passed simultaneously on the network's inner and outer rings which backup each other. With FDDI and CDDI, in the event of a broken ring connection or station malfunction, the station closest to the break closes the network loop by sending the token it received from the inner (or outer) ring back using the outer (or inner) ring. This process is known as *self–healing*.

Table 7.3 shows the characteristics of these networks.

TABLE 7.3 Comparison of Token Ring Network Types

Network	Data Rates (Mbps)	Max Segment Length (Meters)	Cabling	Rings	Recovery
IBM Token Ring	4/16	72 Unshielded 250 Shielded	Twisted Pair	1	Can handle a computer failure but can't recover from a broken connection
IEEE 802.5	4/16	250	Not specified	1	Can handle a computer failure but can't recover from a broken connection
FDDI	100	Unlimited	Fiber Optic	2	Self–healing
CDDI	4/16	72 Unshielded 250 Shielded	Twisted Pair	2	Self–healing

7.3 Wireless Networking

In an effort to make technology both portable and less cumbersome, many manufacturers have redesigned their products so that they can work without wires. Networking technology has always had more than its fair share of wires—especially for extremely large networks—and this has spurred manufacturers to make wireless products both powerful and effective enough to compete with wired equipment. A whole new breed of wireless networking products is now available to meet practically any networking need. These exciting breakthroughs make wireless the most sought after technology in every segment of the networking market.

Table 7.4 provides a list of users that are suited for wireless networks.

Wireless networks operate in much the same manner that wired networks do, with a few exceptions. Each computer on the network has to be equipped with a network adapter, just as in wired networks, but in a wireless network, a wireless adapter must be used. Each networked computer must be able to connect to the others on the network, the same as in a wired network.

The differences are all about the medium; wired networks use cable to transmit and receive data over the network, while wireless networks transmit that data through the air. This automatically makes some of the demands of wireless networking different than wired networks. These demands can influence the choices about implementing a wireless network.

Wireless networks have more restrictions on distances over which the signal can reach its destination without severe degradation. Generally, a signal sent through open space, unless it is very powerful (as in the case of satellites), deteriorates at a much faster rate than a signal sent over a cable. Therefore, computers on a wireless network must be closer together than computers on a wired network in order to send and receive data clearly, unless equipment is properly set up. Cre-

ating an overlapping array of wireless devices set at effective distances can alleviate this situation. This solution has the added benefit of increasing signal quality as well, which eliminates the frequent occurrence of data errors.

TABLE 7.4 Users suited for wireless networking

User	Recommendation	Advantages	Disadvantages
Home	• High	• No wiring required	• Limited distance • Less secure than wired networks • Slower than wired networks
SOHO (Small Office/Home Office)	• High		
SMB (Small to Medium Business)	• Moderate		
Enterprise (Large Corporations)	• Moderate		

With wireless networks there is also concern about data security. Many networks now handle very security–sensitive data, such as financial records, classified data, and other highly personal information. When this information is transmitted over a wired network, there is already some measure of security in that only the computers on the network have access to that information. But when the data is sent out, there are no restrictions on who can receive it. It is much more likely to be intercepted by someone who is not on the network.

To enhance security, wireless networks use data encryption*. Data encryption is a method of "scrambling" the data before sending it out over the network and "unscrambling" it when it is received. The encryption is based on a key that is shared only between the sender and the receiver, making it a very secure process. The standard for this encryption is even called *Wired Equivalent Privacy* (WEP), meaning that the security of the data is at about the same level as that of data transmitted over wired networks.

Speed is another issue that influences the administrator's decision to use a wireless network. Wired networks can now achieve speeds up to 1000 Mbps, i.e., gigabit speed. Even standard 10/100 Ethernet technology allows for speeds of 100 Mbps. But presently, wireless technology operates at only 11 Mbps which although it may be more than adequate for high speed internet access sharing and almost any standard application, it may not meet the needs of some larger networks or networked applications. There is no way around this particular wireless limitation at present, but the next generation of wireless products is projected to transmit at the substantial higher rate of 54 Mbps.

* *A well–known encryption is the RSA algorithm. It is briefly discussed in Appendix D.*

7.3.1 Wireless Networking Architectures

Wireless networks have two different architectures in which they may be set up: Infrastructure and Ad–Hoc. Choosing between these two architectures depends on whether the wireless network needs to share data or peripherals with a wired network or not.

If the computers on the wireless network need to communicate with a wired network or need to share a peripheral such as a printer that is part of the wired network, the wireless network should be set up in the *Infrastructure mode* as shown in Figure 7.2.

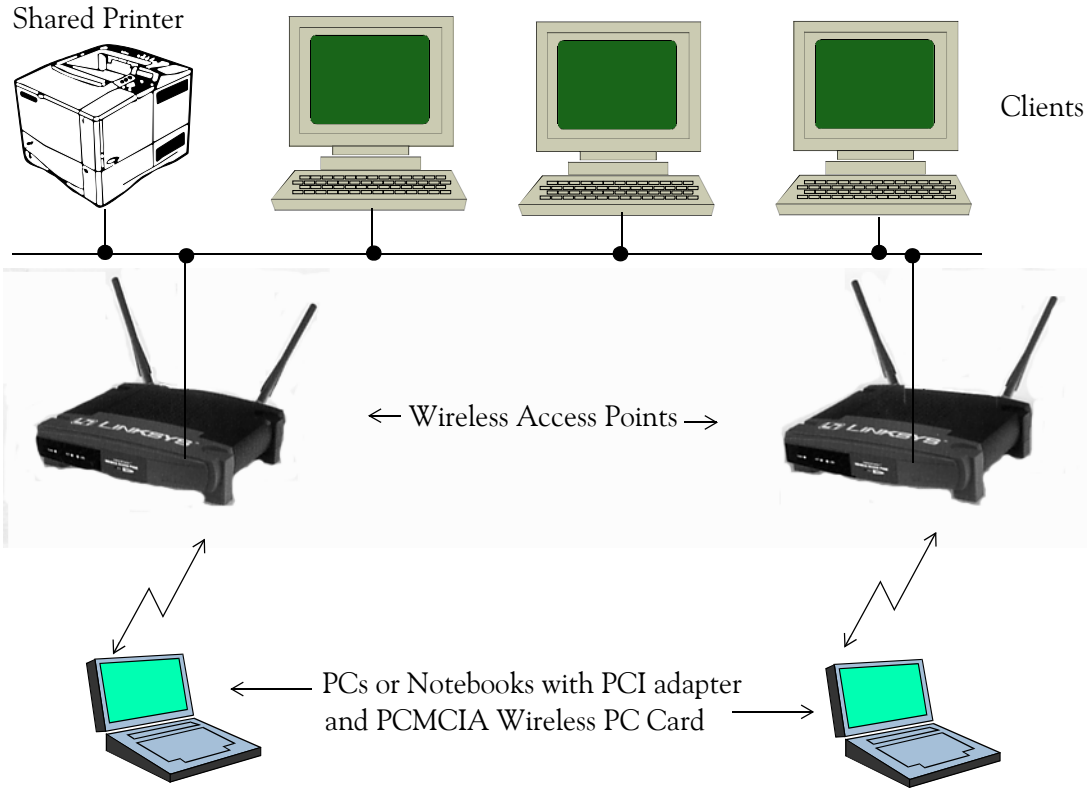


Figure 7.2. Infrastructure architecture of wireless communications

The basis of Infrastructure mode centers around an access point, which serves as the main point of communications in a wireless network. Access points transmit data to PCs equipped with wireless network adapters, which can roam within a certain radial range of the access point. Multiple access points can be arranged to work in succession to extend the roaming range, and can be set up to communicate with the Ethernet hardware as well.

If the wireless network is relatively small and needs to share resources only with the other computers on the wireless network, then the *Ad–Hoc* mode can be used. Ad–Hoc mode allows computers equipped with wireless transmitters and receivers (not shown) to communicate directly with each other, eliminating the need for an access point as shown in Figure 7.3.

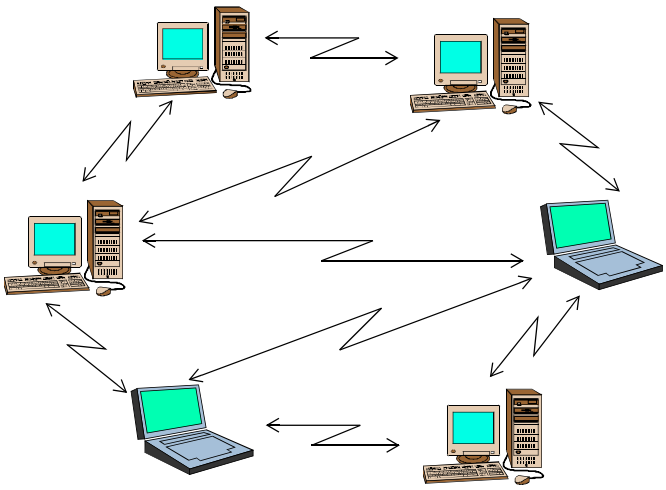


Figure 7.3. Ad Hoc architecture of wireless communications

The Ad–Hoc architecture has the disadvantage that wireless–equipped computers are not able to communicate with computers on a wired network. Also, communication between the wireless–equipped computers is limited by the distance and interference directly between them.

In order to combat this signal loss and overcome distance obstacles, some wireless devices come equipped with automatic "fallback" features—which means that the devices will try to connect at the fastest reliable speed possible under the conditions. For instance, if the device cannot reliably connect at 11 Mbps, it will automatically try the next speed, which is 5.5 Mbps. This feature preserves data integrity and maintains encryption standards for data security. When using access points (Infrastructure mode), proper positioning of the access points on the wireless network can also have a large positive impact on data transmission rates and effective distances as well.

For wireless communications, the desktop and notebook PCs shown in Figures 7.2 and 7.3 require a PCI adapter and a PCMCIA Wireless PC Card which is inserted into the PCI adapter. Together, these two pieces of equipment create the transmitter and receiver that allow the PC to communicate on the wireless network.

This arrangement has two important advantages. First, the PCMCIA Wireless PC Cards can be used in both desktop and laptop computers, and easily switched between each. This can create significant savings for some customers who don't need all their PCs on the wireless network at one time. The other advantage is that once the PCI adapter has been installed, it is no longer necessary to open the computer's case in order to attach it to the wireless network.

7.3.2 Wireless USB Network Adapter

Another viable option to configure a desktop or notebook PC for wireless communications is the the use of a Wireless USB Network Adapter. With this option, the user just plugs this adapter into any available USB port, and his desktop or notebook computer is readily configured for wire-

less networking. It is recalled that USB devices are hot swappable; thus, using this adapter on multiple notebook and desktop PCs is the best alternative for many wireless networking users. Figure 7.4 shows a wireless access point, a PCI adapter, a PCMCIA Wireless PC Card, and a Wireless USB Network Adapter made by Linksys® , now a division of Cisco.

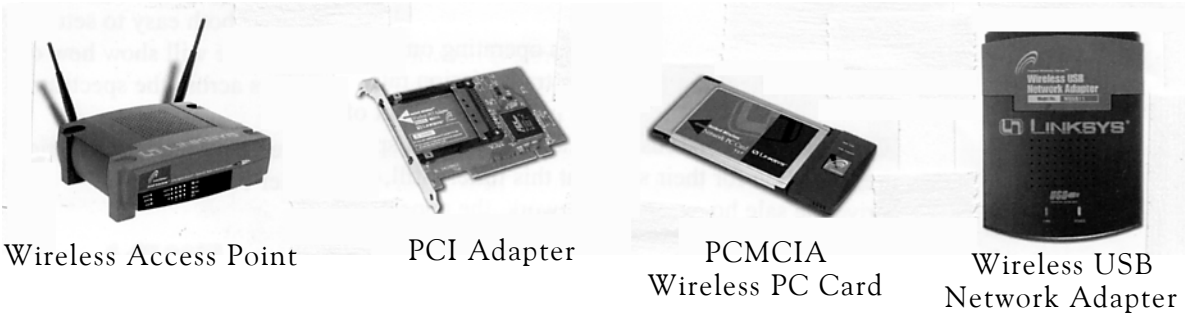


Figure 7.4. Wireless networking products made by Linksys

Access points can be used to extend the effective range of the wireless network. By placing access points in overlapping ranges, the wireless–equipped PCs will be able to reach remotely located users on the network. Some access points also incorporate other features which can enhance network efficiency. An access point can also be a router or a print server. Having all these devices in one compact piece of equipment saves space and usually makes setup and operation easier.

If a wired network is in place and want to add wireless capability to it, a Wireless Access Point is all that the user needs. He can connect this device to an existing hub, switch, or router, and make all the resources of the wired network available to the wireless network.

Cisco's Aironet 340 Access Point has a range of 30 meters indoors and 125 meters outdoors when operating at 11 Mbps, and 100 meters indoors and 500 meters outdoors when operating at 1 Mbps.

A typical wireless network is shown in Figure 7.5.

7.4 Phoneline Networking

A network using standard telephone wires that exist in a home or place of business can be designed. This arrangement is very convenient for many home and small business users, because there is very little required equipment, and it is relatively inexpensive. It does not interfere with normal phone use, because it does not transmit over the portion of the telephone wire that carries a person's voice. Figure 7.6 shows five devices made by Linksys® that can be used with Phoneline networking.

The Phoneline network is designed using these adapters and standard telephone cabling. Computers can be connected directly to each other, commonly known as piggy–backing or daisy–chaining, or the telephone jacks in someone's home or office can be used to create the network.

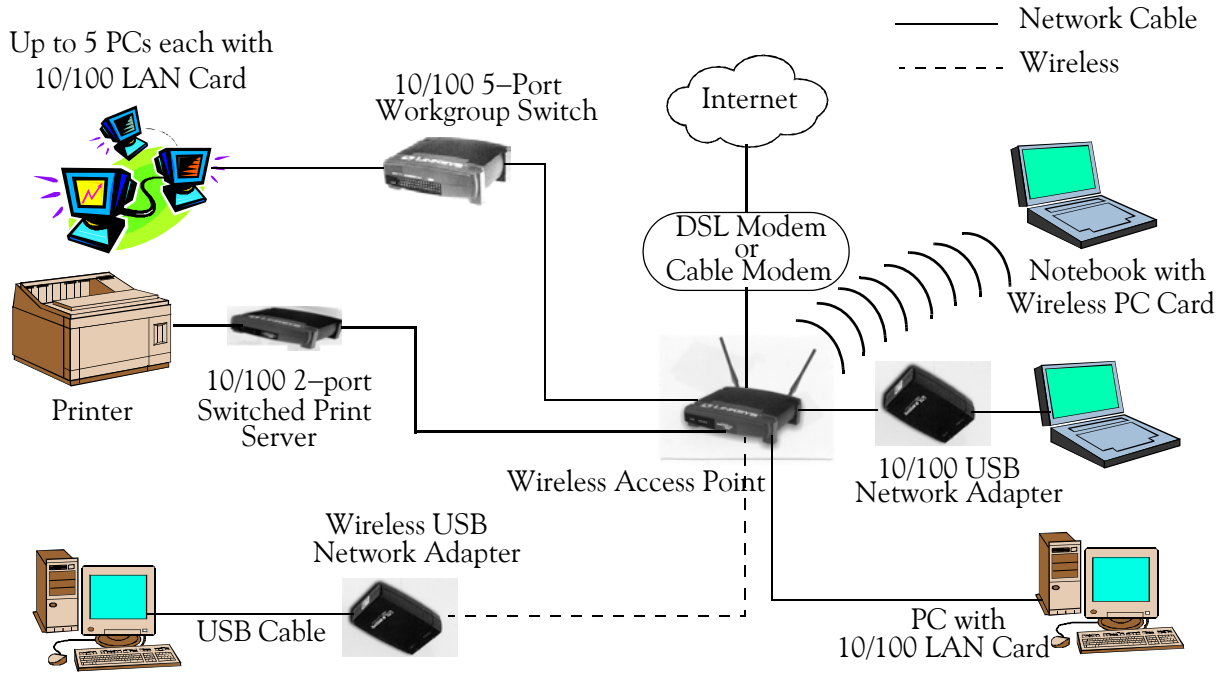


Figure 7.5. A typical infrastructure wireless network

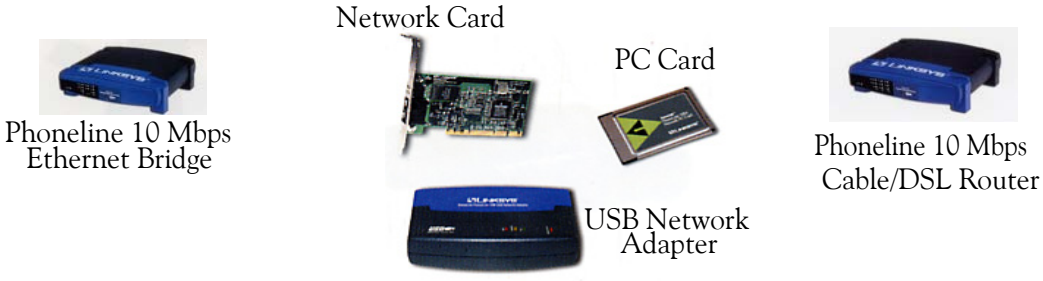


Figure 7.6. Devices made by Linksys® that can used with Phoneline networking

These wall jacks MUST all be on the same phone line (i.e. the same telephone number), and the telephone line MUST be analog (no digital telephone networks, such as PBX, key systems, or ISDN).

Presently, there are two standards for Phoneline network speed, set by the *Home Phoneline Networking Alliance* (HPNA) — HPNA 1.0 or HPNA 2.0). The HPNA 1.0 Phoneline network adapters allow up to 25 computers on a single network loop (same telephone line) spread out over a total distance of 150 meters at a speed of 1 Mbps. The HPNA 2.0 version extended the distance to 300 meters on a single loop, with up to 30 computers supported—all at an increase of speed to 10 Mbps. However, some network applications, especially games, require faster data transfer speeds.

A few manufacturers of phone line network adapters have included Ethernet technology on their adapters as well so that the administrator can use either the phone line or Ethernet connections, but not both at the same time. Even so, if he decides to use phone line technology to create WoL network, products are available that give us a choice.

A typical Phoneline network is shown in Figure 7.7.

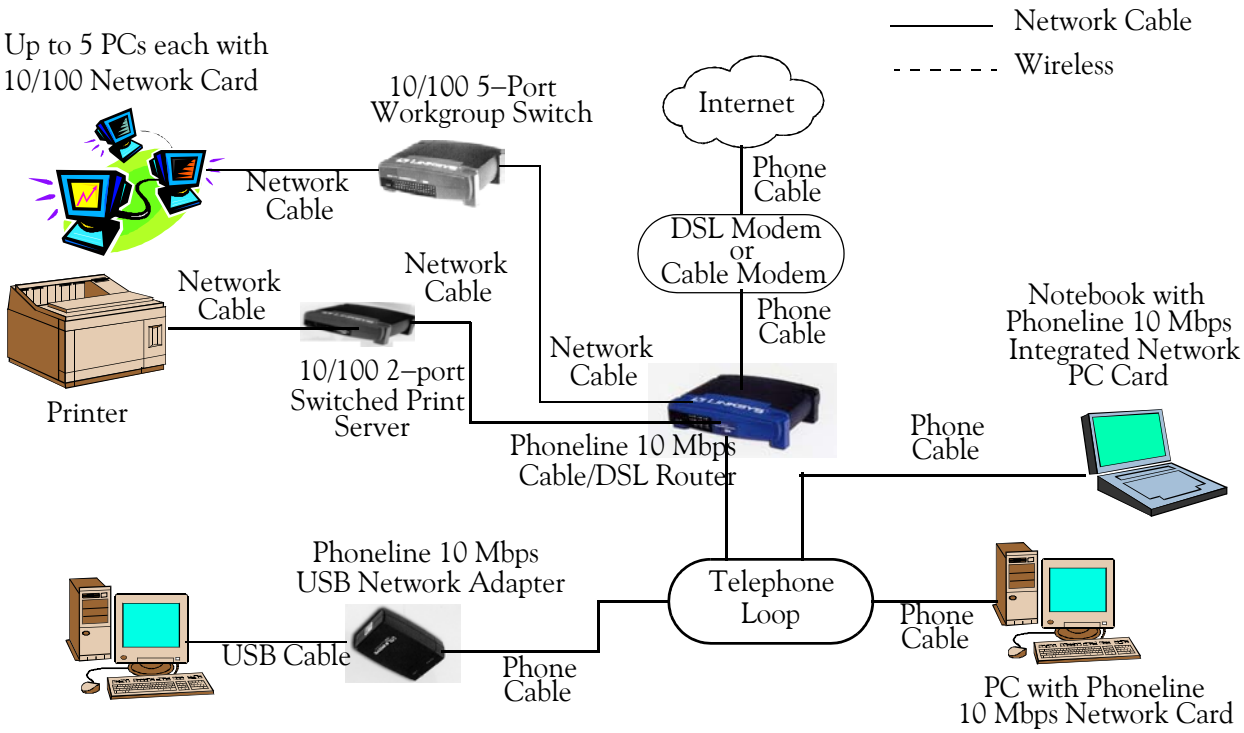


Figure 7.7. A typical Phoneline network

Regardless of the standard, the technology is the same. Network data is transferred over the telephone wires, using Frequency Division Multiplexing (FDM) not used by voice transmissions. In effect, the data is being transmitted on a different "channel" than conversations on the telephone. Thus, telephone calls can be conducted at the same time as data transfer, with one not affecting the other.

Figure 7.8 shows how FDM is used on telephone line cables.

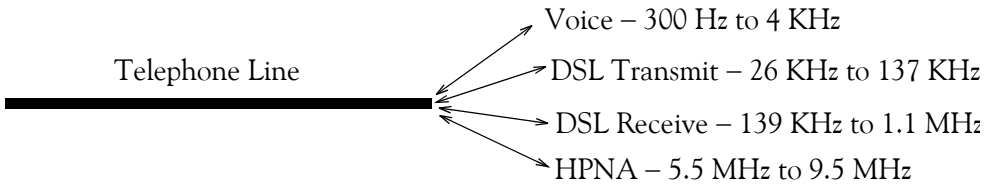


Figure 7.8. FDM used on telephone line cables

Table 7.5 provides a list of users that are suited for Phoneline networks.

TABLE 7.5 Users suited for Phoneline networking

User	Recommendation	Advantages	Disadvantages
Home	• High	• No new wiring is required	• Limited distance • Slow speed
SOHO (Small Office/Home Office)	• Moderate		
SMB (Small to Medium Business)	• Low		
Enterprise (Large Corporations)	• None		

7.5 Network Operating Systems

Every PC must have a Network Operating System, such as Windows, Linux, or Novell, to connect to a network. The Network Operating System controls communication between a PC's applications and the network at large. Network commands are redirected from a user's PC to the network where they are received and acted upon by other PCs. A Network Operating System may handle disk activities, electronic mail, video–conferences, and network printing. Some popular network operating systems include Windows XP, LANtastic, UNIX/Linux, and NetWare. When a Network Operating System sends or receives data, it breaks the data down into packets by a method called a protocol. Windows NT uses the IPX/SPX, NetBEUI, and TCP/IP protocols for network communication. NetWare uses IPXISPX. UNIX, Linux, and the Internet all use TCP/IP. While different protocols usually cannot talk directly with each other, most Network Operating Software can understand more than one protocol. For example, Windows can understand TCP/IP and IPX/SPX, so NT computers can work with NetWare and UNIX/Linux networks.

Novell NetWare

NetWare is a popular client–server network operating system. NetWare runs on server PCs, and can support up to 1,000 users and 32 processors. It features extensive disk compression capabilities for storing extensive amounts of data.

Microsoft Windows

Windows is the most widely used NOS. It is a multitasking, 32– and 64–bit* operating system equipped with advanced security and support capabilities. Also, Windows is used in both peer–to–peer as well as client–server networks.

* *The 64–bit operating system was introduced with the Windows Vista.*

UNIX, Linux, and Solaris

First developed in the 60's, UNIX is a highly popular and widely distributed multitasking NOS. Many administrators favor UNIX for its extensive control capabilities. Based on the UNIX model, the newer Linux is distributed on the Internet as "freeware" without copyright, as an open source code, and users can modify and customize Linux themselves to suit their needs, right down to the code. Solaris, a version of Unix, is Sun Microsystems' operating system.

Internetwork Operating System (IOS)

IOS is Cisco's proprietary operating system for its line of internetworking devices.

Multiple Virtual Storage (MVS)

MVS is a proprietary IBM mainframe operating system. The term MVS is used to describe an entire family of mainframe operating systems. The term *multiple virtual storage* refers to the use of multiple virtual memory areas in the operating system. The MVS/Open Edition (MVS/OE), aimed at the growing open systems market, added TCP/IP and Unix support.

7.6 Network Administration

Installation and configuration of the network is just the beginning of the job for the network administrator. Once the network is in place, there are many maintenance tasks involved in network administration. Users come and go, and new network resources are added, involving network reconfiguration. Other tasks involve providing a fault–tolerant network that can survive the inevitable device failure.

Various responsibilities of managing the network and tools available to make the job easier are discussed below. Before discussing these tools, a quick overview of the basics of networks and their components is presented.

Networks come in two forms: workgroups and domains. When a computer is configured for networking, a computer name must be supplied along with a workgroup or domain name. It is important to maintain a standard naming scheme. Standardizing the naming scheme can make it much easier to locate network resources. Another important reason for a naming scheme is to make sure all of computers have unique names. Workgroups and domains should be given names, which identify either location or function (a combination can also be used). One example of this is to name all workgroups according to department; for example, ACCOUNTING, MARKETING, and HR. Inside the workgroups, The administrator should assign names to specify each machine. Examples RECEIVABLES, PAYABLES, BILLING, and so on. It is important to remember that workgroups, domains, and computers must have names that are unique on the network.

The naming of the servers and workstations should follow some sort of standard defined by the organization. Each computer in a Microsoft network, either a server or a workstation, has a NetBIOS name. This name is how the server is known on the network. It is very common to see servers named after movie characters, pets, or any other convenient name that an administrator may

think of. This may work in a small network with only a few servers. But if this network grows, trying to remember what a server does or where it is located by these types of names can become a serious problem.

The idea behind a naming scheme is to sort out the confusion of many different servers for users. If users cannot locate the resources they need, the network is not helping them. The method used in the naming convention should be based on and decided by the company or organization. Some users may suggest using a name; this may not be a good choice because servers do many functions. A more practical method is to use the server's location name since servers rarely move to a new location and if they do, they are probably serving new users who do not know the original name.

It is important to be consistent and make the names unique. Once the administrator has decided on a scheme, he should stay with it and make sure servers which are not under his control could also use it. This may become a management issue that has to be issued as a policy or procedure. Shared resources should also have a naming scheme. This way it will be easier for users to move from one server to another if they change locations.

7.6.1 Workgroups

A *workgroup* is a group of PCs networked together as in a SOHO network or for departmental use. Workgroups help organize computers in a peer–based network according to department or function. Networks can have a large number of workgroups. Each computer can be a member of one workgroup.

When Microsoft introduced Windows 95, it included a *Network Neighborhood* icon on the desktop. This was a folder that listed computers, printers, and other resources connected to the LAN. With Windows XP, these can be found under My *Network Places*[*] in the Control Panel. Of course, this folder serves no purpose unless the PC is connected to a LAN.

7.6.2 Domains

A *domain* is a group of PCs that are part of a network and share a common directory database in a central file server. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.

An *Active Directory domain* is a collection of PCs defined by the administrator of a network. These PCs share a common directory database, security policies, and security relationships with other domains. An Active Directory domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. An Active Directory is made up of one or more domains, each of which can span more than one physical location.

---

* *With Windows Vista, they can be found under Network and Sharing Center in the Control Panel.*

iA Domain Name System (DNS) domain is any tree or subtree within the DNS namespace. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Active Directory domains.

With Windows XP, TCP/IP can be configured to use DNS with the following procedure provided that the user has logged on as the network administrator. A similar procedure is provided by the Windows Vista documentation.

Click on **Start**, on **Control Panel**, and double–click **Network Connections**.

1. Right–click the network connection we want to configure, and then click **Properties**.
2. On the **General** tab (for a local area connection) or the **Networking** tab (all other connections), we click **Internet Protocol (TCP/IP)**, and then click **Properties**.
3. If it is desired to obtain DNS server addresses from a DHCP server, click **Obtain DNS server address automatically**.
4. If it is desired to configure DNS server addresses manually, click **Use the following** DNS **server addresses**, and in Preferred DNS server and Alternate DNS server, type the preferred DNS server and alternate DNS server IP addresses.
5. To configure advanced DNS properties, click **Advanced**, the DNS tab, and do one or more of the following:

- To configure an additional DNS server IP address:
  1. Under DNS server addresses, in order of use, click **Add**.
  2. In TCP/IP DNS server, type the IP address of the DNS server, and click **Add**.
- To modify the resolution behavior for unqualified DNS names, do the following:
  1. To resolve an unqualified name by appending the primary DNS suffix and the DNS suffix of each connection (if configured), click **Append primary and connection specific DNS suffixes**. If it is also desired to search the parent suffixes of the primary DNS suffix up to the second level domain, select the **Append parent suffixes of the primary DNS suffix** check box.
  2. To resolve an unqualified name by appending the suffixes from a list of configured suffixes, click **Append these DNS suffixes (in order)**, and then click **Add** to add suffixes to the list.
  3. To configure a connection–specific DNS suffix, type the DNS suffix in DNS **suffix for this connection**.
- To modify DNS dynamic update behavior, do the following:
  1. To use a DNS dynamic update to register the IP addresses of this connection and the primary domain name of the computer, select the **Register this connection's addresses** in DNS check box. This option is enabled by default. The primary domain name of the com-

puter is the primary DNS suffix appended to the computer name and can be viewed as the full computer name on the **Computer Name** tab (available in System in Control Panel).

2. To use a DNS dynamic update to register the IP addresses and the connection–specific domain name of this connection, select the **Use this connection's DNS suffix** in DNS **registration** check box. This option is disabled by default. The connection specific domain name of this connection is the DNS suffix for this connection appended to the computer name.

3. To completely disable DNS dynamic update for all names on the computer, clear the **Register this connection's addresses** in DNS and **Use this connection's DNS suffix in DNS registration** check boxes for all connections in Network Connections.

7.6.3 User Accounts

A *user account* is a record that consists of all the information that defines a user to the network. This includes the user name and password* required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the PC and the network, and accessing the network resources. For Windows XP Professional and member servers, user accounts are managed with Local Users and Groups. For Windows Server domain controllers, user accounts are managed with Microsoft Active Directory Users and Computers.

User accounts personalize Windows for each person who is sharing a computer. The user can choose his/her own account name, picture, and password, and choose other settings that will apply only to us. A user account gives provides a personalized view of someone's own files, a list of favorite Web sites, and a list of recently visited Web pages. With a user account, documents created or saved are stored in the user's own **My Documents** folder, separate from the documents of others who also use the computer.

If a person uses a password for his user account, all files are kept secure and private so that other users cannot see them. However, he can still mark certain items as shared if he wants other people to be able to access them. If he does not use a password for his user account, other people will have access to his account and be able to access all of his folders and files.

If the person has a user account and he changes his computer settings, such as the type size or the screen saver, those settings will apply only to his account. As a user with a computer administra-

* *When the user creates or changes his password, he is given an opportunity to type a hint to help us remember it. The password hint should be a word or a phrase that is vague enough so that nobody else can guess his password, but clear enough that it will remind him of his password. For example, if his password is "15JAN32, his hint could be his grandmother's or grandfather's indicated as "grandma" or "grandpa." If the hint still does not help him remember his password, he will need to ask someone with a computer administrator account to create a new password for him. A user with a network administrator account can create and change passwords, and create password hints for all users. Users with limited accounts can only create and change their own passwords, and create their own password hints.*

tor account, one can create, delete, and change all user accounts on the computer. The network administrator can create as many accounts on the computer as he wants, and have full access to all accounts on the computer.

Types of user accounts

There are two types of user accounts available on the computer: computer administrator and limited. Another type, known as guest account is available by default for users with no assigned account on the computer.

Computer administrator account

The computer administrator account is intended for someone who can make systemwide changes to the computer, install software, and access all non–private files on the computer. Only a user with a computer administrator account has full access to other user accounts on the computer. A user with a computer administrator account:

- Can create and delete user accounts on the computer.
- Can change other users account names, pictures, passwords, and account types.
- Cannot change his or her own account type to limited unless there is at least one other user with a computer administrator account. This ensures that there is always at least one user with a computer administrator account on the computer.
- Can manage his or her network passwords, create a reset password disk, and set up his or her account to use a .NET Passport*.

Limited account

The limited account† is intended for someone who should be prohibited from changing most computer settings and deleting important files. A user with a limited account:

- Generally cannot install software or hardware, but can access programs that have already been installed on the computer.
- Can change his or her account picture and can also create, change, or delete his or her password.

---

* *A .NET Passport provides the user with personalized access to Passport–enabled services and Web sites by using his e–mail address. Passport implements a single sign–in service that allows us to create a single user name and password. Once the user has a Passport, he will have only one name and password to remember, and he will be able to use all .NET Passport–enabled services. He can store information about himself in his sign–in profile, so he will not have to retype it when he uses .NET Passport–enabled services. His personal information is protected by powerful encryption technology and strict privacy policies, and he is always in control of the services that have access to his personal information, including his e–mail and mailing addresses. Passport is safe to use on public or shared computers.*

† *Some programs might not work properly for users with limited accounts. If so, the user could change the user's account type to computer administrator account, either temporarily or permanently.*

- Cannot change his or her account name or account type. A user with a computer administrator account must make these kinds of changes.
- Can manage his or her network passwords, create a reset password disk, and set up his or her account to use a .NET Passport.

Guest account

The guest account is intended for use by someone who has no user account on the computer. There is no password for the guest account, so the user can log on quickly to check e–mail or browse the Internet. A user logged on to the guest account:

- Cannot install software or hardware, but can access applications that have already been installed on the computer.
- Cannot change the guest account type.
- Can change the guest account picture.

For convenience, the user account types and authorization to establish or change account information are listed in Table 7.6.

TABLE 7.6 User account types and authorization

Authorization	Administrator Account	Limited Account	Guest Account
Install software and hardware	Yes	No	No
Make network changes			
Access and read all non–private files			
Create and delete user accounts			
Change other users accounts			
Change own account name and type			
Change own picture		Yes	Yes
Create, change or remove own passport		Yes	No

7.7 Security

Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A *password* is a secret word or phrase that gives a user access to a particular program or system.

To enhance security, Windows recommends the *Windows NT File System* (NTFS). This is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk. NTFS is the Windows NT equivalent of the Windows 95 *File Allocation Table* (FAT) and the

OS/2 *High Performance File System* (HPFS). However, NTFS offers a number of improvements over FAT and HPFS in terms of performance, extensibility, and security.

Notable features of NTFS include:

- Support for very large files (up to 2^{64} or approximately 16 billion bytes in size)
- An Access Control List (ACL) that lets a server administrator control who can access specific files
- File compression
- Support for long file names
- Data encryption on both removable and fixed disks

The *Security Administrator's Integrated Network Tool* (SAINT), originally known as Security Administrator Tool for Analyzing Networks (SATAN) is a security tool, written by Dan Farmer and Wietse Venema, which remotely probes systems via the network and stores its findings in a database. The results can be viewed with a web browser. SAINT requires Perl 5.000 or better.

In its simplest mode, SAINT gathers as much information about remote hosts and networks as possible by examining such network services as NFS, NIS, FTP, TFTP, and others. The information gathered includes the presence of various network information services as well as potential security flaws – usually in the form of incorrectly setup or configured network services, well–known bugs in system or network utilities, or poor or ignorant policy decisions.

SAINT can either report on this data or use a simple rule–based system to investigate any potential security problems. Users can then examine, query, and analyze the output with a web browser. While the program is primarily geared towards analyzing the security implications of the results, a great deal of general network information can be gained when using the tool – network topology, network services running, and types of hardware and software being used on the network.

SAINT can also be used in exploratory mode. Based on the initial data collection and a user configurable rule set, it will examine the avenues of trust and dependency and iterate further data collection runs over secondary hosts. This not only allows the user to analyses his own network, but also to examine the real implications inherent in network trust and services and help them make reasonably educated decisions about the security level of the systems involved.

7.8 System Restoration

System Restore is a component of Windows XP and Windows Vista that can used to restore a computer to a previous state, if a problem occurs, without losing personal data files such as word processing documents, spreadsheets, databases, drawings and so on. System Restore monitors changes to the system and some application files, and it automatically creates easily identified restore points. These restore points allow the user to revert the system to a previous time.

The restore points are created daily and at the time of significant system events such as when an application or driver is installed. The user can also create and name his own restore points at any time.

Restoring the computer does not affect or change the personal data files. It is a good idea to back up the data files periodically. For example, the user might copy his data files to removable media, such as a writable compact disc, once a week. It is imperative to verify that the backed–up files are usable.

7.9 Redundant Systems

Another method of safeguarding the user's files with backups is redundancy. With redundancy, data is duplicated or spread across drives. Redundant systems can help quickly restore the system in case of a device failure. *Redundant Arrays of Inexpensive** *Disks* (RAID) provide several levels of redundancy. RAID is available in both hardware and software. The discussion is for hardware only.

The RAID method of redundancy uses of two or more disk drives instead of one disk to provide better disk performance, and error recovery. RAID includes interleaved storage techniques and mirroring of important data. This approach was developed by a research project at the University of California, Berkeley. A new project known as Sequoia 2000 Project, seeks to construct a geographically distributed storage system spanning disk arrays and automated libraries of optical disks and tapes.

The following standard RAID have been developed:

- RAID 0 Non–redundant striped array
- RAID 1 Mirrored arrays
- RAID 2 Parallel array with Error Correction Code
- RAID 3 Parallel array with parity
- RAID 4 Striped array with parity
- RAID 5 Striped array with rotating parity

RAID 0 utilized disk striping which is a procedure that combined a set of same size disk partitions residing on separate disks (from 2 to 32 disks) into a single volume, forming a virtual stripe across the disks that the operating system recognizes as a single drive.

RAID 1 utilized disk mirroring. With disk mirroring, any change made to the original disk is simultaneously made to the other disks, so that if the original disk becomes damaged or corrupted

* *The original (.Inexpensive) term referred to the 3.5 and 5.25 inch disks used for the first RAID system but no longer applies.*

the mirror disks will contain a current, undamaged collection of the data on the original disk. The weakness of disk mirroring is that both drives use the same controller. If the controller fails, then both copies of the data are unusable.

Another version of RAID 1 utilized *disk duplexing*. Disk duplexing is simple disk mirroring with separate controllers. This provided a higher level of fault tolerance.

RAID 2, 3, and 4 were variations of RAID 1 and are rarely used.

RAID 5 utilizes disk striping with rotating (even, odd) parity. Data blocks are striped to several disks with a parity stripe written in varying locations. Striping with parity requires at least three drives. The data are written on the first two of these drives and a parity block is created and written on the third. To illustrate the procedure, let us assume that even parity is being used and the byte 10010011 is written on the first drive and another byte, say 11100100, is written on the second drive. Shown below is the generation of the parity byte.

10010011	First Data Byte
11100100	Second Data Byte
01110111	Parity Byte

Now, if the data of the first data byte is corrupted, it can be reconstructed using the second and parity bytes as shown below.

11100100	Second Data Byte
01110111	Parity Byte
10010011	First Data Byte

RAID 5 provides more efficient storage than RAID 1. However, the write operations for RAID 5 are slower than that of RAID 1 because of the additional time required to write the parity information. Generally, RAID 5 is about 60% slower for writing operations than RAID 1. Read operations are the same for both RAID 1 and RAID 5.

RAID 5 is commonly used in server applications where storage space and fault tolerance are critical. It should not be implemented as software RAID.

7.10 Uninterruptible Power Supply (UPS)

A UPS can be used to safeguard against power outages. A UPS is a battery that operates between the power outlet and the computer. The size of the battery varies, and it is important to purchase a UPS that is powerful enough to support the equipment that is attached to it.

After purchasing a UPS for his network, the administrator can use the Windows UPS service to set options for its operation using Power Options in Control Panel. The UPS tab in Power Options enables us to control how the UPS service works on the network. The UPS settings available depend on the specific UPS hardware installed on the system. The settings can include options such as:

- The serial port where the UPS device is connected.
- The conditions that trigger the UPS device to send a signal, such as a utility power failure, low battery power, and remote shutdown by the UPS device.
- The time intervals for maintaining battery power, recharging the battery, and sending warning messages after power failure.

7.11 Managing and Monitoring Performance

Windows XP and Vista allocate resources according to its settings and manages devices accordingly. The user can, however, change the way Windows uses processor time and computer memory to improve performance. He can also adjust the settings for his computer's visual effects.

7.11.1 Managing Processor Time

System processing is managed by Windows, which can allocate tasks between processors, as well as manage multiple processes on a single processor. However, Windows can be set to allocate more processor time to the program currently running. This can result in faster program response time. Or, if there are background programs, such as printing or disk backup that the user wants to run while working on another task, Windows can share processor resources equally between background and foreground programs.

7.11.2 Managing Memory

When a computer is running low on RAM and more is needed immediately, Windows uses hard drive space to simulate system RAM. This is known as virtual memory, and is often called the paging file. This is similar to the UNIX swapfile. The default size of the virtual memory pagefile (named pagefile.sys) created during installation is 1.5 times the amount of RAM on the computer.

The virtual memory can be optimized by dividing the space between multiple drives and removing it from slower or heavily accessed drives. To best optimize the virtual memory space, it should divided among as many physical hard drives as possible. When selecting drives, one should keep the following guidelines in mind:

- Must not have a pagefile on the same drive as the system files.
- We must avoid putting a pagefile on a fault–tolerant drive, such as a mirrored volume or a RAID 5 volume. Pagefiles don't need fault–tolerance, and some fault–tolerant systems suffer from slow data writes because they write data to multiple locations.
- One must not place multiple pagefiles on different partitions on the same physical disk drive.

A computer's memory usage can be optimized, if the computer is used primarily as a workstation rather than as a server, and in this case more memory can be devoted to the programs. The programs will work faster and the system cache size will be the default size that came with Windows XP or Vista. One can also specify to set aside more computer memory for a larger system cache, if the computer is used primarily as a server, or if he uses programs that require a larger cache.

7.11.3 Changing Visual Effects

Windows provides several options to set the visual effects of a computer. For example, the user can choose to show shadows under menus, giving them a 3–D look. Windows can display the entire contents of a window on the monitor. To make large text more readable, the user can choose to display the smooth edges of screen fonts. He can also enable the Web view in folders which will display a list of hyperlinked tasks and information on the left side of the folder window. Windows provides options for enabling all of the settings (for best appearance), or none of the settings (for best computer performance). The original default settings can also be restored.

7.11.4 Performance

Windows provides a performance tool that consists of two parts, the System Monitor and Performance Logs and Alerts.

The System Monitor part allows the user to collect and view real–time data about memory, disk, processor, network, and other activities in a graph, histogram, or report form.

The Performance Logs and Alerts part enables the user to configure logs to record performance data and system alerts to notify us when a counter's value is above or below a predefined threshold.

Third–party software products are also available to aid the user in performance monitoring. The Simple Network Management Protocol (SNMP) can be a very useful tool for doing performance monitoring on the network. Most network devices now include SNMP as a support protocol. With a good SNMP management software system, the networks administrator can obtain almost any statistical information he desires. SNMP is discussed in Chapter 8.

7.11.5 Event Viewer

Windows XP and Vista include the Event Viewer that maintains logs about program, security, and events on the network. To open the Event Viewer, click on Control Panel, Administrative Tools, and the Event Viewer. The user can get help about using the Event Viewer from the Action drop menu and clicking Help.

The Event Viewer allows the user to view, manage event logs, and gather information about each user's activity, monitor security events, and to view hardware and software problems.

7.11.6 Quality of Service (QoS)

This is feature that provides different prioritization levels for different types of traffic over a network. Various methods are used to achieve quality of service, including the *Resource ReSerVation Protocol* (RSVP).* For example, streaming† video may have a higher priority than *Internet Control Message Protocol* (ICMP)‡ traffic, as the consequences of interrupting streaming video are more obvious than slowing down ICMP traffic.

On the Internet and in other networks, with QoS the transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high–bandwidth video and multimedia information. Transmitting this kind of content dependably is difficult in public networks using ordinary best effort protocols.

7.12 Storage Options

Floppy Disk

Capacity: 1.44 MB, almost extinct.
Price per disc 5 to 10cents Primary usage: Storing small files such as letters and spreadsheets.
Pro: None presently. Not installed on newer PCs, but external drives are still available.
Con: Small capacity.

Recordable Compact Disk (CD)

Capacity: About 700 Mb. Price per disc 5–7 cents
Primary usage: Recording music and photo files easily for personal use or sharing with others
Pro: A CD–ROM or CD–RW drive can be found in most every personal computer.
Con: Physically vulnerable to scratches.

Recordable Digital Video Disk (DVD)

Capacity: 4.7 GB
Price per disc 20 to 25 cents

---

* *RSVP is a set of communication rules that allows channels or paths on the Internet to be reserved for the multicast (one source to many receivers) transmission of video and other high–bandwidth messages. RSVP is part of the Internet Integrated Service (IIS) model, which ensures best–effort service, real–time service, and controlled link–sharing.*

† *Streaming is a term used to describe technology that is capable of playing audio or video while it is still downloading. This saves us some waiting time.*

‡ *This is a TCP/IP messaging protocol that runs specifically over IP (as opposed to UDP). This protocol is used to announce network errors, time–outs and congestion. PING is based over ICMP. The Packet InterNet Gopher (PING) is part of the standard TCP/IP suite of protocols that allows the user to check his connectivity with other devices, or to check whether his own TCP/IP stack is working properly. Normally, the user could type in something like "ping 206.119.148.38," and either a response from that IP address is received or not. PING is extremely useful for debugging network problems.*

Primary usage: Storing video files
Pro: Capacity is large enough to handle video files.
Con: Slightly more expensive than CDs.

ZIP Drives

Capacity: 100MB, 250 MB, or 750 MB
Price per disk $8–$15, depending on capacity
Primary usage: Archiving or transferring large files.
Pro: Disks are durable and easy to use.
Con: Requires zip drive to read the disks.

Flash Memory Sticks

Capacity: 2 Gb to 64 GB
Price per disk $5–$100, depending on capacity.
Primary usage: Floppy replacement products offering larger capacities.
Pro: Small–sized, plugs into a standard USB port.
Con: Easy to lose and misplace.

External Hard Drives

Capacity: 100 GB to 1000 GB
Price per unit $75 to $200, depending on capacity
Primary usage: Backing up hard drives, storing files
Pro: Large capacities, installs into USB or FireWire plugs
Con: Bulky and expensive.

7.13 Network Data Storage

Until recently, network data were stored in the so–called *direct–attached* method where each server processes and stores its own data and cannot use other servers' storage. However, present–day technology makes it possible to store data more efficiently by using a central switch that routes data between banks of processors and separate storage arrays as shown in Figure 7.9.

Usually, the switch in Figure 7.9 is referred to either Network Attached Storage (NAS) if it uses Category 5 UTP cables, or Storage Area Network (SAN) if fiber optic cables are used.

7.14 Future Trends in Networking

Today, the Internet offers the fastest and easiest information access ever, with services such as online banking, shopping, stock trading, news posting, E–mail, and more. Businesses are capitalizing on the Internet with e–commerce opportunities, while the home networking market consumes those services through high–speed cable modem and DSL connections shared over Ethernet networks. With everyone exchanging data almost instantly, it's networking that keeps everyone connected.

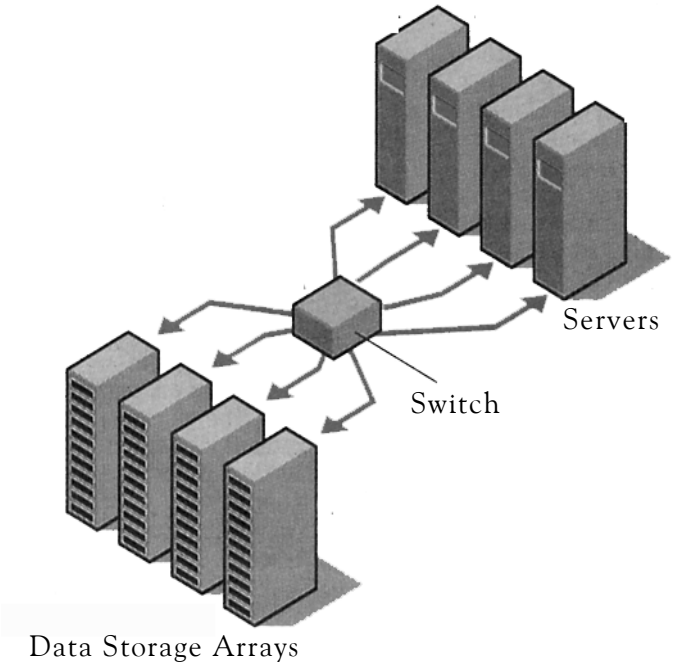


Figure 7.9. Network data storage using a central switch to transfer data between connected units

Networking links us to friends, family, coworkers, and virtually anyone in the world with PC access. It even connects us to the ultimate of all networks, the Internet, where networks of all sizes connect to form a global information system. As more users discover online resources and new applications are developed, networking must become more efficient to support its masses of users. Networking now comprises all forms of communications.

Innovations of all kinds are being proposed to enhance networking applications, and sharing Internet connections through networks is quickly becoming one of the key advantages of networking. On the computing level, Gigabit Ethernet will boost network speeds up to 1000 Mbps, and Network–Attached Storage (NAS) and Storage–Area Network (SAN) media will expand, centralize and manage data storage. Powerline networking transfers data over the electrical wiring, and wireless hardware promises to rid us of cabling altogether.

In a broader outlook, all these factors drive a strong market demand for a universal system of communications connecting more than just PCs. New paths for data transfer are being forged to achieve interoperability among PCs, TVs, cellular phones, PDAs, cameras and other multimedia devices. Bluetooth and Wi–Fi are two of the exciting developments in wireless technology, bridging data lines between PCs, cellular phones and other small electronic devices using short–range radio wave transmission. As data transfer finds new paths and wireless technology frees it from physical lines, a complete package for voice, data, and entertainment convergence is inevitable.

In fact, the market already affirms convergence as the future of networking. Network data can now travel over all types of cabling, including Ethernet cable, fiber optic cable, phone lines, and

power lines. Hybrid devices are combining multiple technologies and hardware functions into a single multi–tasking device, such as set–top boxes for merging TV and PC data and residential gateways for handling a home network's security and high–speed Internet connections. To take it one step further, those gateways are expected to evolve into a single device, controlling home security on top of network security, as well as networking household appliances like refrigerators and central air conditioning.

The next generation of Internet users have much to anticipate. Information will flow more freely as voice, video, and data merge to travel over the same pathways. The Internet itself will be revamped with IPv6, or Internet Protocol Version 6, increasing the number of IP addresses and implementing IPSec (Internet Protocol security) to enhance security on the internet and support the development of VPNs, or Virtual Private Networks. IP telephony, or Voice Over IP (VoIP) will allow two–way audio transmission, meaning free or low–cost long–distance phone conversations via the Internet, as well as faster downloading of music and video files as well.

As the development of gateways suggest, the future will bring us a system of connected devices that all share and process the same digital data. Each day builds new connections, and networking will be the cohesive force that unifies these connections into a completely integrated reality.

7.15 Summary

This chapter is devoted on the design of computer networks and equipment selections. The selection decisions must primarily based on versatility, expandability, and affordability. The networks administrator should make decisions based on the following issues:

- Where the computers, printers, and other peripherals will be located?
- Which computers will be networked and how far apart are they? Will all be located in a large open space or in rooms separated by walls?
- What networks speeds are required?
- What applications and operating systems will be used?
- What type of Internet connections will be used?
- Is a facility prewired for networking or will it be required to install the network cables? If so, what type(s) the networks administrator will be using?
- How many printers, scanners, and other peripheral equipment are to be networked.
- What is the budget allocation for buying additional hardware and software?

The key features of 10/100 Ethernet Networking are:

- It is the most widely used networking standard
- It can operate from 10 Mbps to 100 Mbps transmission speeds
- It can use either Category 5 UTP (or higher) or fiber optic cabling
- It is adaptable with 10/100 Mbps Network Interface Cards (NICs)
- Provides seamless integration with different Ethernet speed standards

To build a 10/100 Ethernet network, the administrator will need the devices listed below.

- 10/100 Network Adapters or NICs
- 10/100 Hubs and/or Switches
- 10/100 Print Servers
- Routers
- Network Attached Storage (NAS) or Storage Attached Network (SAN)
- Keyboard, Video, and Mouse (KVM) Switches
- Cables

- Every desktop PC or notebook must have either a network adapter or a network card. A network adapter usually refers to a device that is connected externally while a network card is connected internally. Both perform the same function.
- Before choosing a NIC the networks administrator must find out whether his PCs or notebooks has a 32 or 64–bit bus architecture. Bus architectures are discussed in Chapter 4. The PCMCIA bus is used in notebooks.
- NICs operate at various speeds and the 10/100 devices automatically detect connection speeds of either 10 Mbps or 100 Mbps and adjust their speed to match the highest speed.
- Desktop PCs are provided with internal expansion slots on the motherboard. Pentium–based PCs use the 32–bit PCI bus. Newer PCs use the IEEE 1394 bus. Windows Vista introduced the 64–bit bus.
- A very useful feature especially for network administrators is the *Wake–on–LAN* (WoL). This refers to a technology developed by the IBM and Intel Advanced Manageability Alliance where a computer motherboard can turn itself on (and off) based on signals arriving at the computers network card.
- Unless PCs have the Plug–and–Play (PnP) capability, when a NIC is inserted to the motherboard, it must be configured with and IRQ and I/O address.
- When a PCMCIA card is inserted to a PCMCIA slot the notebook PC automatically senses that a new card has been added and assigns an IRQ and I/O address. Like desktop PCs, notebook PCs use Category 5 UTP cable.
- Most notebooks today are equipped with a 32–bit CardBus slot where a 32–bit CardBus NIC can be inserted. These have replaced the older 16–bit PCMCIA cards.
- The Universal Serial Bus (USB) is presently one of the most useful devices. USB Version 2 can achieve speeds up to 480 Mbps and can be used with applications such as digital imaging, IP telephony (Voice over IP) and multimedia games.
- USB ports can accommodate many devices such as joysticks, mice, scanners, digital cameras, and speakers. Devices connected to USB ports are said to be "hot–swappable" meaning that they can be added or removed without removing power from the PC.
- The Ethernet and Fast Ethernet cabling rules require that the cable span does not exceed 100 meters from any node to a hub or a switch. Also if two hubs are used, the distance from each other should not exceed 10 meters. If the distance from a node to a hub or switch exceeds 100 meters, a repeater can be used to extend the distance.
- A hub shares its total bandwidth, or speed, among all active users on the network and transfers data in half–duplex mode, like a cell phone. Thus if a network with 5 users runs at 100 Mbps, each user receives a maximum of 20 Mbps of the hub's bandwidth. A switch has a dedicated

bandwidth of 100 Mbps and this means that no matter how many users are connected to the network, each user can send and at the same time receive data at speeds of 100 Mbps.

- Table 7.2 lists the features of hubs and switches and shows the available bandwidth for each user when 10 active users are connected to the Ethernet.
- Routers can be used to act as firewalls to safeguard against intrusions from outsiders. Firewalls can be established internally to block unauthorized users from accessing other parts of the network. For instance, a router can be used to create a firewall between the maintenance department and the payroll department in an organization.
- Network Address Translation (NAT) is a method that firewalls use to assign each node an IP address that the router only knows. Thus, the router acts as a mail center to both incoming and outgoing messages to forward data only to the proper address.
- Some routers use Dynamic Host Configuration Protocol (DHCP) to assign temporary IP addresses for each PC and each address is valid only for a certain time period. These temporary addresses are assigned by a DHCP server when client PCs log on to a network or the Internet. Thus, DHCP serves as a security measure since the temporary addresses expire after a predetermined amount of time.
- The 10BaseT and 100BaseTX (Fast) Ethernets are ideal for new networks or for departmental use within a company. The choice between one or the other depends on the speed requirements. If both are used, they can be interconnected with a 10/100 switch. The ports on these switches automatically sense the speeds of their connections and adjust each port's speed to match.
- The Gigabit Ethernets operate at 1 Gbps (1000 Mbps) speeds. Seamless integration allows a Gigabit Ethernet to work with a Fast Ethernet.
- New UTP copper cable known as Category 5e can achieve 1 Gbps speeds to and thus it offers a less expensive option.
- When expansion of an existing Ethernet LAN is planned, the networks administrator should consider using a 10/100 stackable hub. Stacking cables add more ports to the "same" hub by providing more tightly integrated performance and eliminating data bottlenecks.
- Non–stackable hubs placed on top of each other will not act as a single hub.
- A switch or repeater can be used between the hubs to enhance the signals. Thus, if a 10–port hub is connected to a 16–port switch, all the computers on both segments of the network can communicate with each other.
- Hubs and switches made by different manufacturers can be used together too, provided they run at compatible speeds.

- During the planning phase of the network expansion the networks administrator should make trade–off studies to decide on the best choice of devices. For instance, while a 10/100 hub with high port density or stackability is less expensive than a 10/100 switch, the latter provides full duplex, dedicated connections to each of its ports.
- Network–Attached Storage (NAS) devices provide a quick add–on solution. NAS boxes are basically compact, portable file servers, and some have an IP address of their own.
- A Storage–Attached Network (SAN) serves a similar function as a NAS but also offers storage space manageability.
- Keyboard, Video, and Mouse (KVM) switches allow a single keyboard, video display monitor, and mouse to be switched to any of a number of computers when typically a single person interacts with all the computers but only one at a time.
- UTP, STP, or fiber optic cables can be used in Ethernet LANs. Most Ethernet networks use UTP cables.
- Category 5 cabling is the minimal requirement for 100 Mbps Fast Ethernet networks.
- Shielded Twisted–Pair (STP) cabling, is used for Ethernet networks in areas with high EMI, where the foil shield in STP cabling protects data from it. EMI exists around airports, radio towers, and industrial sites with heavy electrical equipment.
- Ethernet and Fast Ethernet cabling rules require that a single twisted–pair cable spans no more than 100 meters from any node to a hub or a switch. Two hubs running at 100 Mbps can only be 10 meters from each other. If the distance between two nodes exceeds 100 meters, a repeater or a switch, which acts as a repeater, must be used to boost incoming data signals before passing it on to the next node.
- The standard Category 5 UTP cabling cannot be used outdoors or with long distances such as networks that span the size of a campus.
- A fiber connection always requires two fiber cables: one transmits data, and the other receives it. Fiber comes with 2 types of connectors: square SC connectors are the most common type of connector used in the U.S. ST connectors are round, and are commonly used in European networks. For connections over 300 meters, especially outdoors, or in networks without repeaters (data signal boosters), fiber optic cabling is recommended.
- Fiber optic cabling is used primarily for network backbones and distant connections. Made from flexible, optically efficient strands of glass and coated with a layer of rubber tubing, fiber optics use photons of light instead of electrons to send and receive data. The more connectors used and the longer the fiber cables are, the higher the optical loss will be.
- When using fiber optic cabling for long hauls, the administrator should buy a hub, switch, or other device with a fiber port. Hubs and switches with multiple fiber ports are available also.

- In a Token Ring LAN, each station can send a signal along the loop after receiving permission to do so. Only one station may have control on the network at a specified time. The signal will travel from one station to the other until it reaches its destination.
- FDDI (Fiber Distributed Data Interconnect) is an improved token ring specification based on fiber as the physical medium. As opposed to Token Ring's single ring, FDDI, uses two to achieve better results. CDDI, yet another standard, resembles FDDI, but uses a copper wire for its ring.
- FDDI and CDDI networks implement a recovery mechanism which enable the network to function properly even under a broken ring. FDDI and CDDI use two rings to achieve recovery capabilities.
- Wireless networks operate in much the same manner that wired networks do, with a few exceptions. Each computer on the network has to be equipped with a network adapter, just as in wired networks, but in a wireless network, a wireless adapter must be used. Each networked computer must be able to connect to the others on the network, the same as in a wired network.
- Wireless networks have more restrictions on distances over which the signal can reach its destination without severe degradation.
- With wireless networks there is also concern about data security. To enhance security, wireless networks use data encryption.
- Speed is another issue that influences the networks administrator decision to use a wireless network. Presently, wireless technology operates at only 11 Mbps which although more than adequate for high speed internet access sharing and almost any standard application, it may not meet the needs of some larger networks or networked applications.
- Wireless networks have two different architectures in which they may be set up: Infrastructure and Ad–Hoc. Choosing between these two architectures depends on whether the wireless network needs to share data or peripherals with a wired network or not.
- Some wireless devices come equipped with automatic “fallback” features—which means that the devices will try to connect at the fastest reliable speed possible under the conditions. For instance, if the device cannot reliably connect at 11 Mbps, it will automatically try the next speed, which is 5.5 Mbps.
- Wireless PC Cards can be used in both desktop and laptop computers, and easily switched between each. This can create significant savings for some customers who don’t need all their PCs on the wireless network at one time.
- Another viable option to configure a desktop or notebook PC for wireless communications is the use of a Wireless USB Network Adapter. With this option, the user just plugs this adapter

into any available USB port, and his desktop or notebook computer is readily configured for wireless networking.

- Access points can be used to extend the effective range of the wireless network. By placing access points in overlapping ranges, the wireless–equipped PCs will be able to reach remotely located users on the network.
- Phoneline networking uses standard telephone wires that exist in a home or place of business. This arrangement is very convenient for many home and small business users, because there is very little required equipment, and it is relatively inexpensive.
- Windows XP, LANtastic, UNIX/Linux, NetWare, Cisco's IOS, and IBM's MVS/OS are common operating systems used in networks.
- Networks are divided in two forms: workgroups and domains. When a computer is configured for networking, a computer name must be supplied along with a workgroup or domain name. It is important to remember that workgroups, domains, and computers must have names that are unique on the network.
- A workgroup is a group of PCs networked together as in a SOHO network or for departmental use. Workgroups help organize computers in a peer–based network according to department or function. Networks can have a large number of workgroups. Each computer can be a member of one workgroup.
- A domain is a group of PCs that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name.
- An Active Directory domain is a collection of PCs defined by the administrator of a network. These PCs share a common directory database, security policies, and security relationships with other domains.
- A user account is a record that consists of all the information that defines a user to the network. This includes the user name and password.

A user with a computer administrator account:

- Can create and delete user accounts on the computer.
- Can change other users account names, pictures, passwords, and account types.
- Cannot change his or her own account type to limited unless there is at least one other user with a computer administrator account. This ensures that there is always at least one user with a computer administrator account on the computer.
- Can manage his or her network passwords, create a reset password disk, and set up his or her account to use a .NET Passport.

- Limited accounts are intended for those who should be prohibited from changing most computer settings and deleting important files.
- Guest accounts are intended for use by those who have no user account on the computer. There is no password for the guest account, so the user can log on quickly to check e–mail or browse the Internet.
- Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised. Most security measures involve data encryption and passwords.
- To enhance security, Windows recommends the Windows NT File System (NTFS). This is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk.
- The Security Administrator's Integrated Network Tool (SAINT) remotely probes systems via the network and stores its findings in a database. The results can be viewed with a web browser.
- System Restore is a component of Windows XP and Vista that can used to restore a computer to a previous state, if a problem occurs, without losing personal data files.
- Redundant systems can help quickly restore the system in case of a device failure. Redundant Arrays of Inexpensive Disks (RAID) provide several levels of redundancy.
- RAID 5 is the predominant among all RAIDs. It utilizes disk striping with rotating (evened) parity. Data blocks are striped to several disks with a parity stripe written in varying locations. Striping with parity requires at least three drives.
- An uninterruptible power supply (UPS) can be used to safeguard against power outages. A UPS is a battery that operates between the power outlet and the computer.
- Windows can be used to allocate resources such as processor time, computer memory, visual effects to the user's preferences.
- Windows provides a performance tool that consists of two parts, the System Monitor and Performance Logs and Alerts.
- The Event Viewer allows us to view, manage event logs, and gather information about each user's activity, monitor security events, and to view hardware and software problems.
- RSVP is a protocol that reserves bandwidth to assure Quality of Service (QoS).

7.16 Exercises

True/False

1. The 10/100 Ethernet network is the most widely used. ____

2. The RS–232C cable can achieve rates up to 2 Mbps and can be used for distances over 15 meters. ____

3. A Hub operates in the full duplex mode. ____

4. Frequencies on a typical telephone cable can vary from 300 Hz to 9.5 MHz.____

5. The MVS/OE is a proprietary IBM operating system. _____

6. The latest editions of Windows are used in both peer–to–peer as well as client–server networks.____

7. In Windows XP or Vista, restore points are automatically created on a weekly basis. ____

8. NTFS can support files up to 4 billion bytes in size. ____

9. Read operations are the same for both RAID 1 and RAID 5. ____

10. Pagefiles do not need fault–tolerance. ____

Multiple Choice

11. Using a _____ the administrator can remotely turn all PCs on from a main station

    A. PCMCIA

    B. IEEE 1394 Bus

    C. WoL

    D. USB

12. The _____ is a method that firewalls use to assign each node on a network an IP address that the router only knows.

    A. DHCP

    B. NAT

    C. HPNA 1.0

    D. HPNA 2.0

13. Phoneline networking is most inappropriate in _____ installations

    A. Enterprise

    B. SOHO

C. Home

D. SMB

14. The _____ operating system is distributed on the Internet as freeware

A. Unix

B. NetWare

C. Cisco's IOS

D. Linux

15. A(n) _____ is a group of PCs that are part of the network and share a common directory database.

A. workgroup

B. domain

C. account

D. SAINT

16. All account users can change their own _____.

A. picture

B. name and type

C. passport

D. account

17. The main feature(s) of NTFS is (are) _____.

A. File compression

B. Support for long file names

C. Data encryption on both fixed and removable disks

D. All of the above

18. A version of _____ utilizes disk duplexing

A. RAID 0

B. RAID 1

C. RAID 4

D. RAID 5

19. For writing operations, RAID 5 is approximately _____.

A. 25% faster than RAID 1

B. 60% faster than RAID 1

C. as fast as RAID 1

D. 60% slower than RAID 1

20. In a Windows XP or Vista based network, the administrator can make changes in _____.

A. processor time to the program currently running

B. size of the virtual memory

C. in the visual effects

D. All of the above

Problems

21. You are the administrator of a small company network where there is no central file server to serve as a common directory database. You have decided to migrate to Windows XP. Would you choose to implement workgroups or domains?

22. You are informed by a user in your network that another unauthorized user has gained access to the company's management files. Which Windows XP or Vista feature would you use to verify that this is true and provide proof to your management?

23. Your network includes a large server and fault tolerance is very critical. Management has asked you to recommend a reliable hardware or software backup system. What system would you recommend?

7.17 Answers to End–of–Chapter Exercises

True/False

1. T – Refer to Page 7–2

2. F – Refer to Page 7–5

3. F – Refer to Page 7–4

4. T – Refer to Page 7–18

5. F – Refer to Page 7–20

6. T – Refer to Page 7–20

7. F – Refer to Page 7–27

8. F – Refer to Page 7–26

9. T – Refer to Page 7–29

10. T – Refer to Page 7–30

Multiple Choice

11. C – Refer to Page 7–3

12. B – Refer to Page 7–5

13. A – Refer to Table 7–5, Page 7–18

14. D – Refer to Page 7–20

15. B – Refer to Page 7–22

16. A – Refer to Table 7–6, Page 7–26

17. D – Refer to Page 7–26

18. B – Refer to Page 7–28

19. D – Refer to Page 7–29

20. D – Refer to Page 7–30

Problems

21. With no central server, a domain cannot be implemented. Accordingly, workgroups can be formed in a peer–to–peer based network where each department is a separate workgroup.

22. You can access the Event Viewer Security log to use as proof.

23. A RAID 5 hardware system is a viable choice.

Chapter 8

Introduction to Simple Network Management Protocol (SNMP)

This chapter is an introduction to the Simple Network Management Protocol (SNMP). SNMP and Remote Monitoring (RMON), discussed in Chapter 9, are closely related network standards that allow us to capture real time information across the entire network. Both are written in accordance with Management Information Base (MIB) guidelines and thus are platform independent.

8.1 SNMP Defined

The *Simple Network Management Protocol* (SNMP) is a network management standard widely used in networks that support the TCP/IP Protocol. SNMP provides a method of managing network hosts such as workstation or server computers, routers, bridges, and hubs from a centrally–located computer running network management software. SNMP performs management services using management systems and agents.

SNMP can be used to:

- **Configure remote devices**. Configuration information can be sent to each networked host from the management system. For instance, the network administrator can use SNMP to disconnect an interface on our router or check the speed at which a network adapter is operating.
- **Monitor network performance**. The speed of processing and network throughput, and collect information about the success of data transmissions can be tracked. For example, the user could check the temperature of our power supply inside his system and shut it down if the temperature exceeds a predetermined value.
- **Detect network faults or inappropriate access**. Configure trigger alarms on network devices when certain events occur. When an alarm is triggered, the device forwards an event message to the management system. Common types of alarms include a device being shut down and restarted, a link failure being detected on a router, and inappropriate access.
- **Audit network usage**. Both overall network usage to identify user or group access, and types of usage for network devices and services can be monitored.

While SNMP's predecessor, the *Simple Gateway Management Protocol* (SGMP), was developed to manage internet routers only, SNMP was designed to manage almost any type of software and hardware device. For example, SNMP can be used to manage Unix operating systems, Microsoft Windows systems, printers, faxes, modems, and so on. Moreover, SNMP can be used to manage web servers and databases.

SNMP was developed to monitor the network constantly and alert someone when a failure such as an overloaded router seems imminent. Thus, the network administrator can be notified promptly, even at a remote location, that a credit card processor takes too long to process a transaction. It is also possible that the problem can be corrected by the network administrator from a remote location.

One of the most important functions of network management is the monitoring of an entire network rather than individual devices such as routers. *Remote Network Monitoring* (RMON) was developed to help the networks administrator to understand how the entire network is functioning in addition to the individual devices. RMON can be used to monitor not only LANs but also WANs. RMON is discussed in Chapter 9.

8.2 Requests For Comments (RFCs)

The standards for SNMP and other protocols such as TCP/IP, are published in a series of documents called *Requests for Comments* (RFCs). RFCs are an evolving series of reports, proposals for protocols, and protocol standards that describe the internal workings of each standard. RFCs are authored by individuals who voluntarily write and submit a draft proposal for a new protocol or specification to the *Internet Engineering Task Force* (IETF) and other working groups. Submitted drafts are first reviewed by a technical expert, a task force, or an RFC editor, and then assigned a status.

If a draft passes this initial review stage, it is circulated to the larger Internet community for a period of further comment and review, and assigned an RFC number. This RFC number remains unchanged. If changes are made to the proposed specification, drafts that are revised or updated are circulated by using a new RFC (a number higher than the original RFC number) to identify more recent documents.

RFCs are given the following status assignments:

- **Standard Protocols:** Official standard protocols
- **Draft Standard Protocols:** Under consideration and review to become a standard protocols
- **Proposed Standard Protocols:** Protocols that in the future may become a standard protocols
- **Experimental Protocols:** Protocols designed for experimental purposes. An experimental protocol is not intended for operational use.
- **International Protocols:** Protocols developed by another standards organization that are included for the convenience of the Internet community.
- **Historic Protocols:** Protocols that have been superseded or obsoleted by other protocols

There are many RFCs that are supported by TCP/IP. Some are listed in Table 8.1.

TABLE 8.1 Some RFCs supported by TCP/IP

RFC Number	Protocol Title
768	User Datagram Protocol (UDP)
783	Trivial File Transfer Protocol (TFTP)
791	Internet Protocol (IP)
792	Internet Control Message Protocol (ICMP)
793	Transmission Control Protocol (TCP)
826	Address Resolution Protocol (ARP)
854	Telnet Protocol (TELNET)
894	IP over Ethernet
959	File Transfer Protocol (FTP)
1042	IP over Token Ring
1157	Simple Network Management Protocol (SNMP)
1188	IP over FDDI
1201	IP over ARCNet

8.3 SNMP Versions

The following list includes the SNMP versions. The entire list can be obtained from the *Simple Times*, an online publication. Subscription to this publication is free and it is highly recommended to all who work with SNMP. Details and quarterly published issues can be found in URL *http://www.simple–times.org*. RFCs related to SNMP and RAMON are frequently superseded by updated RFCs with different numbers, and can be found in the Simple Times.

- SNMP Version 1 (*SNMPv1*) is the standard version of the SNMP protocol. It is defined in RFC 1157 and it is a full Internet Engineering Task Force (IETF) standard. Security in SNMPv1 is based on the so–called *communities* which are just passwords. There are three communities in SNMPv1, *read–only*, *read–write*, and *trap*[*]. Read–Only allows us to read data values but we cannot modify the data. The Read–Write community allows us to read and also modify the data. Trap allows us to receive traps.
- SNMP Version 2 (*SNMPv2*) was developed to provide the security functions that did not exist in SNMPv1. It is defined in RFCs 1905, 1906, and 1907. It is often referred to as *community*[†] string–based SNMPv2.

* *Trap here means to intercept an action or event before it occurs, usually in order to do something else. Trapping is commonly used by debuggers to allow interruption of program execution at a given spot.*

† *The pairing of two SNMP entities that can communicate with each other is referred to as SNMP community.*

- SNMP Version 3 (*SNMPv3*) was developed to provide the best possible security in SNMP management. It is defined in RFCs 2571, 2572, 2573, 2574, and 2575. It provides a framework for the previous versions and future developments in SNMP management with minimum impact on existing systems.

8.4 Network Management Stations (NMSs) and Agents

SNMP uses two basic components: the *Network Management Station* (NMS), also referred to as *manager*, and *agents*. A manager and an agent communicate via UDP as shown in Figure 8.1.

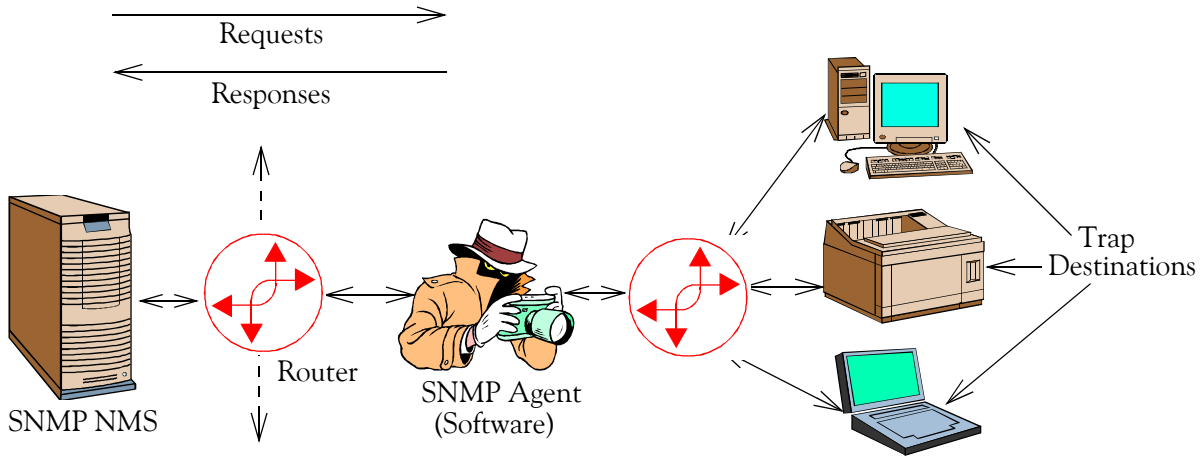


Figure 8.1. Communications between manager and agent in SNMP

An NMS is a server running software that can handle management tasks for a network. An agent is simply software that responds to the manager's request for information. An NMS frequently polls agents in search of status information.

Agents do not write messages. However, an agent can initiate traps, that is, alarm triggering events such as unauthorized system reboot, and illegal access to the network. A trap is a way for the agent to tell the NMS that an unexpected event has occurred. Traps are sent asynchronously, not is response to interrogations from NMSs.

The agent can be a separate program, such as a *daemon*,* or it can be incorporated into the operating system (for example Cisco's IOS on a router, or the low–level operating system that controls a UPS).

When an NMS receives a trap from an agent, it must initiate some corrective action. For instance, if there is a problem in the T1 circuit and this causes the system to become inoperative,

* *A daemon is a program associated with UNIX systems that performs a utility function without being called by the user. It sits in the background and is activated only when needed, for example, to correct an error from which another program cannot recover.*

a router can send a trap to the manager to initiate corrective action.

Presently, most IP devices have some kind of SNMP agent built in to make the networks administrator's job much easier. Thus, the agent provides management information to NMS by keeping track of a device's performance. For example, the agent on a router is able to keep track of the state of each of its interfaces; which are on or off or which are functioning properly and which are not. When the agent observes that something has gone wrong, it sends a trap to the manager.

Some devices on the network will send an "everything is OK now" message when there is a transition from an abnormal to a normal condition. This is very useful when we want to know whether a problem has been corrected.

8.5 SNMP and UDP

As discussed in Chapter 3, UDP is an acronym for User Datagram Protocol. UDP is the connectionless protocol within TCP/IP and corresponds to the transport layer in the OSI model. UDP is defined in RFC 768. SNMP uses the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed devices. Every device that implements SNMP must use these port numbers as the defaults. If these defaults are changed, the NMS must be notified so it can query the device on the correct ports.

UDP converts data messages generated by an application into packets to be sent via IP but does not verify that messages have been delivered correctly since it is a connectionless transport protocol that transports datagrams. However, when used with SNMP, UDP provides a more efficient method of communications between an NMS and an agent. This is possible with the implementation of a time–out feature. That is, in an SNMP application, if the timeout. has expired and the NMS has not received a response, it assumes that the datagrams are lost and re–transmit them. On the other hand, if an agent sends a trap and the traps never arrives, the NMS has no way of knowing that it was ever sent. We must remember that since there are no restrictions on when the NMS can query the agent or when the agent can send a trap, polls and traps can occur simultaneously.

As stated in Chapter 3, TCP/IP is the protocol suite used on the Internet. Thus, any system such as Windows XP or Vista, Unix servers, Cisco routers, etc. that wishes to communicate on the Internet, must use this protocol. The TCP/IP protocol suite is shown in Figure 8.2. This model is referred to as a protocol stack since each layer uses the information from the layer directly below it and provides a service to the layer above it.

When either an NMS or an agent wishes to perform an SNMP function, (e.g., a request or trap), the Application layer, UDP, IP, and Network Access Protocol perform the following functions:

Application Layer

The Application layer provides services to an end user, such as an operator requesting status information for a port on an Ethernet switch. The SNMP application (NMS or agent) decides what to do. For instance, the application can send an SNMP request to an agent through the

NMS, send a response to an SNMP request (this would be sent from the agent to NMS), or send a trap from the agent to NMS.

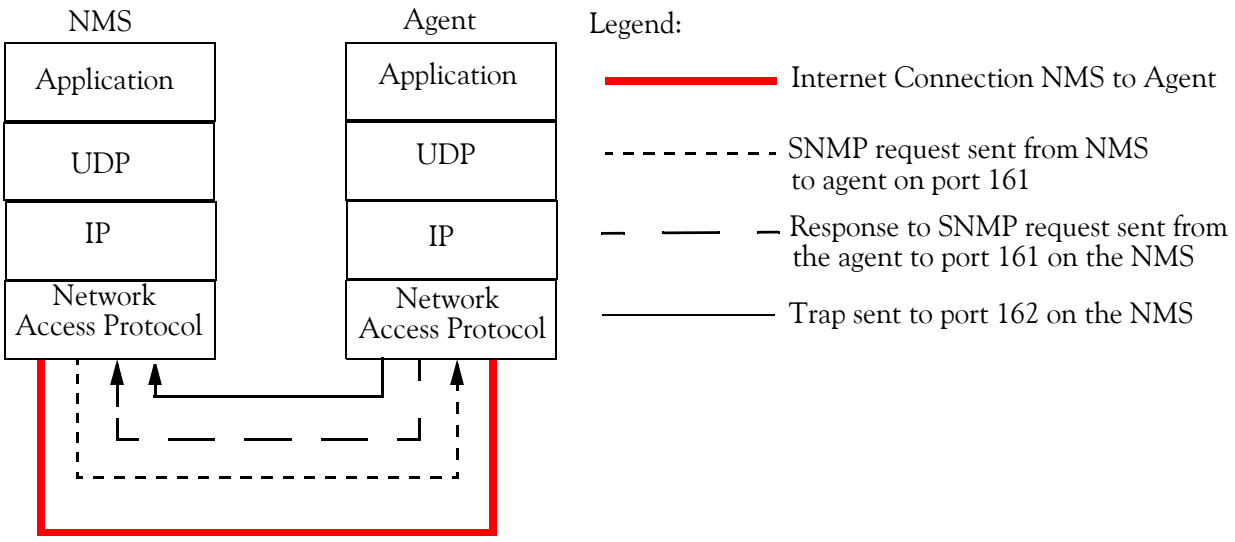


Figure 8.2. TCP/IP communication model and SNMP

UDP

The next layer, UDP, allows two hosts to communicate with each other. The UDP header contains the destination port of the device to which it is sending the request or trap. The destination port will be either 161 (query) or 162 (trap).

IP

The IP layer delivers the SNMP packet to its intended destination as specified by its IP address.

Network Access Protocol

The final event that must occur for an SNMP packet to reach its destination is to be forwarded to the physical network where it can be routed to its final destination. We recall that the MAC layer is comprised of the network adapters and their drivers and these place our data onto a physical device such as an Ethernet card.

8.6 Managed Devices and SNMP Polling

Agents reside on the so–called managed devices. In other words, a *managed device* is a piece of equipment with an SNMP agent (software) built into it. The managed devices can be configured to collect specific pieces of information on device operations. Most of the information consists of totals, such as total bytes, total packets, total errors, and others. Agents can be based on a variety of devices such as those listed below.

- Routers
- Switches
- Access servers
- Hubs
- Servers (Windows XP, UNIX, Linux, MVS, IOS)
- Workstations (PCs, Macs, and UNIX desktops)
- Printers
- UPS power backup systems

NMS is the internetwork's control center. Usually, there's just one NMS for an autonomous system, although many large internetworks use more than one manager and they are typically arranged in a hierarchical order. Most NMSs today operate on UNIX, Microsoft XP, IOS servers, and Solaris.

SNMP is a fairly simple request/response protocol where the manager polls managed devices periodically for updated information. The polling frequency can be set by the network administrator. There are three types of polling:

- **Monitor Polling:** To check that devices are available and to trigger an alarm when one is not
- **Threshold Polling:** To detect when conditions deviate from a baseline number by a percentage greater than allowed (usually plus or minus 10 percent to 20 percent) and to notify the manager for review
- **Performance Polling:** To measure ongoing network performance over longer periods and to analyze the data for long–term trends and patterns

The agent responds to the poll by returning a message to the manager. It does that by capturing and storing information on subjects that it has been configured to monitor. These subjects are usually processes associated with the flow of packets.

8.7 Managed Objects and Object Instances

Managed objects are the operating characteristics of managed devices. The managed devices can be anywhere in the topology–backbone devices, servers, or end systems. Managed objects can be physical devices, such as routers and network interfaces, software, or a group of these.

A managed object could also be the collection of User Datagram Protocols (UDPs), but a single operating characteristic such as a UDP session on a single managed device is referred to as *object instance*. Figure 8.3 shows an example of managed object and object instance.

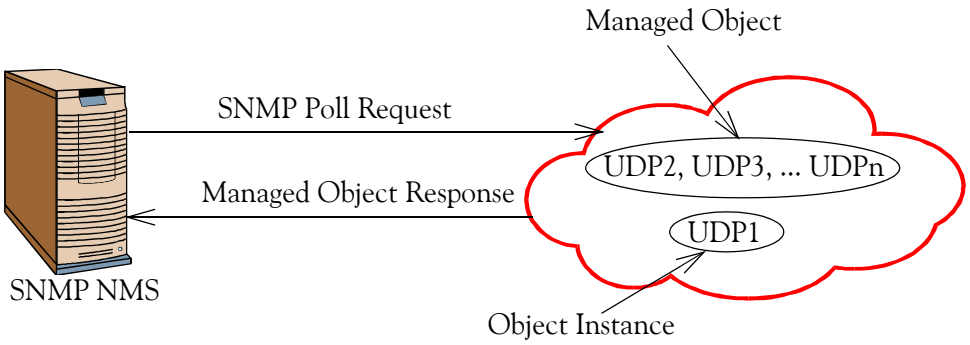


Figure 8.3. SNMP gathering information on managed objects

8.8 Management Information Bases (MIBs)

A *Management Information Base* (MIB) is a database of managed objects accessed by network management protocols. An SNMP MIB is a set of parameters which an SNMP management station can query or set in the SNMP agent of a network device such as a router. Figure 8.4 shows an MIB that counts all data passing through a router.

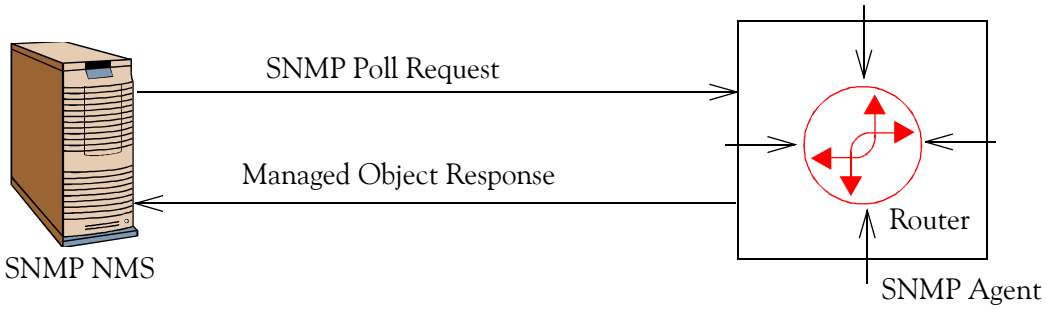


Figure 8.4. An MIB that counts all data passing through an router

In Figure 8.4, the data count obtained from each interface, shown by an arrow, is a managed object instance, but the total count of data from all four interfaces is a managed object.

SNMP contains two standard MIBs. The first, MIB I, established in RFC 1156, was defined to manage the TCP/IP–based internet. MIB II, defined in RFC 1213, is basically an update to MIB I. MIB–II refers to the current definition. SNMPv2 includes MIB–II and adds some new objects.

There are MIB extensions for each set of related network entities that can be managed. For example, there are MIB definitions specified in the form of Requests for Comments (RFCs) for Domain Name System (DNS), Fiber Distributed–Data Interface (FDDI), and RS–232C network objects. Product developers can create and register new MIB extensions. Companies that have created MIB extensions for their sets of products include Cisco, Fore, IBM, Novell, QMS, and Onramp.

8.8.1 Types of MIBs

MIBs are categorized in accordance to the job they perform. They are referred to as *MIB objects*. Basic MIBs usually come packaged inside the network device operating system. For example, Cisco's Internetwork Operating System (IOS) comes packaged with MIB objects for most network management jobs.

MIB objects are organized into a tree–like hierarchy shown in Figure 8.5. This is the basis for SNMP's naming scheme. SNMP follows the form of the *Structure of Management Information* (SMI) standard. SMI is a standard dedicated to specifying a machine–independent syntax for every data type. These data types are independent of the data structures and representation techniques unique to particular computer architectures. SMI specifies the syntax for data types such as object identifiers, counters, rows, tables, octet strings, network addresses, and other SNMP elements.

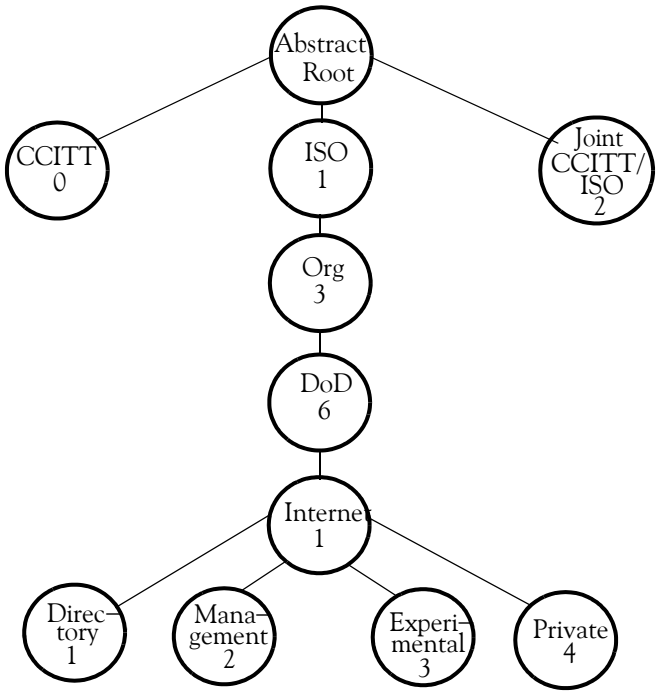


Figure 8.5. SMI Object Tree

The node at the top of the tree is called the *root*, and anything below is called a *subtree* (or *branch*). Thus, in the tree of Figure 8.5, iso(1), org(3), dod(6), internet(1), directory(1), mgmt(2), experimental(3), and private(4) are all subtrees. The subtrees ccitt(0) and joint(2) presently have no relation to SNMP.

Figure 8.5 also shows the development of the Internet. ISO is the International Standards Organization, and DoD is the U.S. Department of Defense which started it all with the ARPANet. CCITT is the Consultative Committee for International Telegraph and Telephone. The CCITT

is concerned with telephony and other communications standards. It is now known as the International Telecommunications Union (ITU), but the CCITT acronym still appears in several standards.

An *object identifier* is a series of integers based on nodes in the tree, and separated by dots (.). Thus, iso(1).org(3).dod(6).internet(1) in object identifier form is represented as 1.3.6.1 or in textual form as *iso.org.dod.internet*. Thus, each MIB object has a numerical object identifier and an associated textual name, much like the association of DNS and IP.

The directory(1) subtree is not currently used. The mgmt(2) subtree defines a standard set of Internet management objects. MIBs are listed below the mgmt(2) subtree. The experimental(3) subtree is reserved for testing and research purposes. Objects under the private(4) subtree are used by individuals and organizations to define other objects under this subtree.

8.8.2 Lexicographic Order

In SNMP, the request operations follow a *lexicographic order*. A lexicographic order is best illustrated with an example. Therefore, let us arrange the numbers on the left column in Table 8.2 in the lexicographical order shown on the right column of the table.

To convert a sequence of numbers from a numerical order, it is convenient to write the numbers in ascending order as shown on the left column of table above. Next, to write these numbers in lexicographic order, we start with the lowest integer in the leftmost character, which in this case is 1. Before increasing the order in the first position, we select the lowest integer in the second position from the left, which is 11. There are two numbers (116 and 1117) that start with 11. We anchor at 11 for the first two positions, and then move on to select the lowest digit in the third position. This yields 111. We then move to the fourth position and obtain 1117 as the second number. Now, we return to the third position and retrieve 116 as the third number. Having exhausted ls (ones) in positions two to four, we select 7 for the second position, and retrieve 173 as the next number. We continue this process until we reach 9.

For simplicity, the sequence of numbers in Table 8.2 were expressed as whole numbers, that is, without dots between. We will now apply the lexicographic sequence to ordering the object identifiers in a MIB with dotted numbers as shown in Table 8.3.

The MIB associated with the example of Table 8.3 is shown in Figure 8.6. Because they're more user–friendly, text strings are usually used to describe MIB objects in directories. Object identifiers are mainly used by software to create compact, encoded representations of the names.

TABLE 8.2 An example of lexicographic order

Numerical Order	Lexicographic Order
1	1

TABLE 8.2 An example of lexicographic order

3	1117
9	116
19	173
25	19
58	25
61	3
116	3465
173	58
743	61
859	743
1117	859
3465	9

TABLE 8.3 The MIB lexicographic order for the example of Table 8.2

1
1.1.1.7
1.1.6
1.7.3
1.9
2.5
3
3.4.6.5
5.8
6.1
7.4.3
8.5.9
9

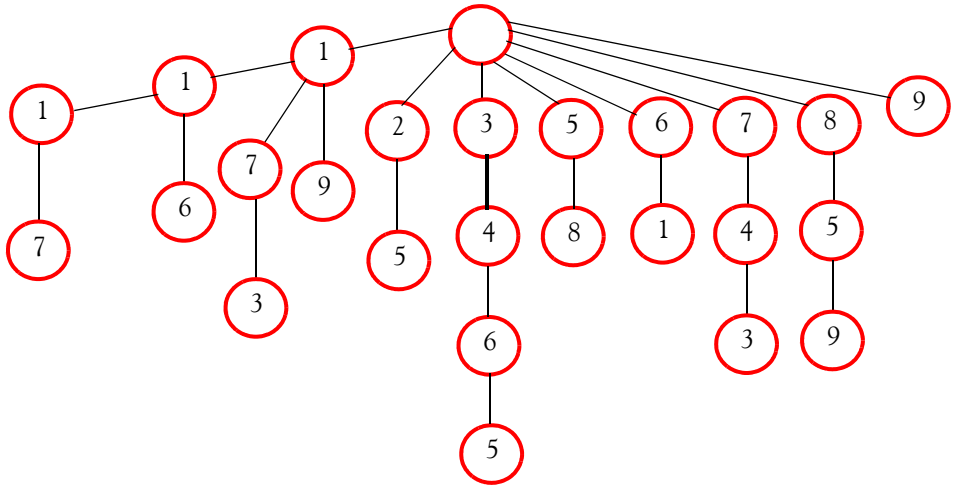


Figure 8.6. MIB tree form for the example in Table 8.3

8.8.3 The Structure of Management Information (SMI) standard

The SNMP is not dependent on specific hardware or software. It supports computers and networks based on TCP/IP and IPX protocols. SNMP provides an optional service that can be installed after the TCP/IP protocol has been successfully configured.

As stated earlier, SNMP follows the form of the *Structure of Management Information* (SMI) standard. SMI is a standard dedicated to specifying a machine–independent syntax for every data type. These data types are independent of the data structures and representation techniques unique to particular computer architectures. SMI specifies the syntax for data types such as object identifiers, counters, rows, tables, octet strings, network addresses, and other SNMP elements.

MIBs are programmed by vendors using a standard referred to as the *Abstract Systems Notation One* (ASN.1). Therefore, any MIB software package that is written in accordance with the SMI specifications, could be used on IBM MIBs, Cisco MIBs, HP MIBs, and others. Thus, using ASN.1 it is possible for a PC running Windows NT to communicate with a Sun SPARC.

A managed object is encoded into a string of octets (bytes) using the *Basic Encoding Rules* (BER). In other words, BER defines how the objects are encoded and decoded so they can be transmitted over a transport medium such as the Ethernet.

As mentioned earlier, an agent is a piece of software used to communicate with the Network Management Station (NMS). Some companies, such as Cisco, have made provisions that the agent software is integrated with the device, say a router, and thus it requires no installation. However, other platforms such as Windows, have no software build into a device and thus it is necessary to install a third party SNMP package such as Castle Rock SNMPc 5.0.

The Structure of Management Information (SMI) defines the syntax of management information stored in the Management Information Base (MIB). As an example, let us consider how a letter is addressed and delivered by the post office to the addressee. As we know, a particular post office is identified by a ZIP code which is a five digit number. Each day thousands pieces of mail arrive at that particular post office, the mail carrier sorts them out by address, then by house number and delivers them. These three pieces of information (ZIP code, address, and house number) define the syntax (format) for mail processing. Similarly, the SMI provides the syntax to identify and process information for managed objects.

The Management Information Base (MIB) can be thought of as a database of managed objects that an agent can track. Any sort of status or statistical information that can be accessed by the NMS is defined in an MIB. A particular MIB referred to as MIB–II (RFC 1213) is a standard that defines variables such as interface statistics (data rates, bytes sent, bytes received, location, etc.). The main goal of MIB–II is to provide general TCP/IP management information. However, it may not cover all options that the network administrator wishes for a particular device. MIB–II is discussed in more detail in Section 8.10.

There are several draft and proposed standards for managing networks. Some of these are:

- ATM MIB (RFC 2515)
- Frame Relay DTE Interface Type MIB (RFC 2115)
- Mail Monitoring MIB (RFC 2249)
- DNS Server MIB (RFC 1611)

Of course, there are many other draft and proposed standards. Moreover, a company that designs and manufactures a router with new features may define its own MIB (referred to as proprietary MIB).

8.8.4 Standard MIBs and Private MIBs

The standard Internet MIB hierarchy is shown in Figure 8.7. We observe that each branch is marked both by a name and a number. We use the numbers to define object identifiers.

As seen in Figure 8.7, the Internet root's object identifier is 1.3.6.1, which can also be written as iso.org.dod.internet. As stated earlier, the Directory(1) subtree is not currently used and the Experimental(3) subtree is reserved for testing and research purposes. Therefore, the two main branches beyond the Internet root are the Management and Private MIBs.

Industry–standard MIBs go through the management branch to become *iso.org.dod.internet.mgmt.mib* with the object identifier 1.3.6.1.2.1. Private MIBs become *iso.org.dod.internet.private* or 1.3.6.1.4. Cisco's private MIB is represented as iso.org.dod.internet.private.enterprise.cisco, or object identifier 1.3.6.1.4.1.9. Likewise, Novell's private MIB is represented as object identifier 1.3.6.1.4.1.23, and HP's private MIB is represented as 1.3.6.1.4.1.11.

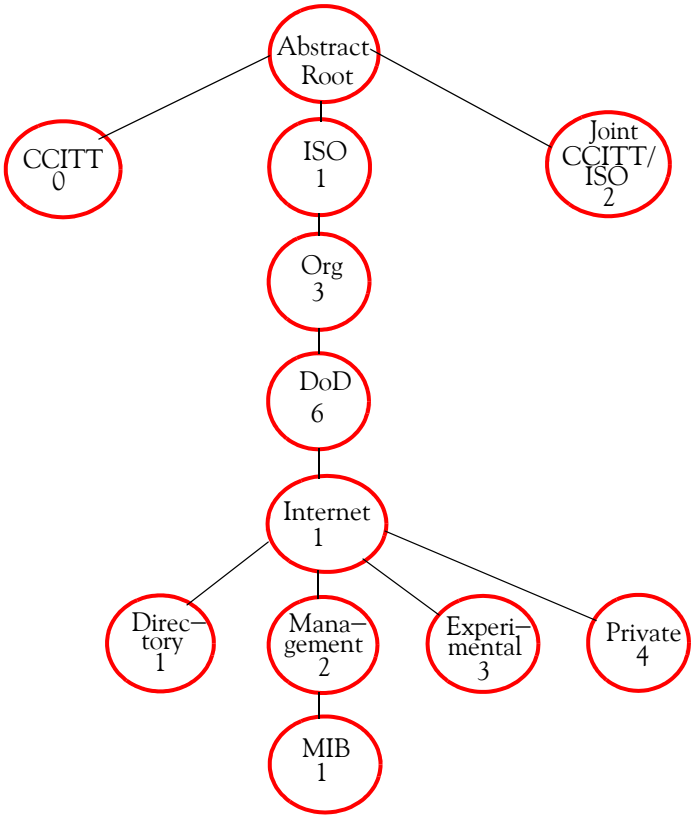


Figure 8.7. The standard Internet MIB hierarchy

Vendors can build private MIBs by extending standard MIB branches. In this way, they can customize MIBs to better fit their particular needs. Figure 8.8 shows Cisco's private MIB hierarchy. We can see how private MIBs extend from the standard Internet MIB.

The Local Variables, Cisco Management Variables, and Temporary Variables which appear in Figure 8.8, are presented in alphabetical order in Appendix D.

As we can see from Figure 8.8, support for other networks such as Novell's NetWare, DECnet, and Xerox XNS can be managed using Cisco's MIBs.

In Figure 8.8, the local subtree contains MIB objects defined prior to Cisco Internetwork Operating System (Cisco IOS) Release 10.2. These MIB objects implemented the SNMPv1 Structure of Management Information (SMI). Beginning with Cisco lOS Release 10.2, however, Cisco MIBs are defined according to the SNMPv2 SMI. MIBs defined with SNMPv2 are placed in the ciscoMgmt subtree also shown in Figure 8.8. MIBs currently defined in the local subtree are being gradually deprecated by Cisco and replaced with new objects defined in the ciscoMgmt subtree. For example, the TCP group that was formerly in the local group has been deprecated and replaced with a new Cisco TCP group in the cisco Mgmt tree.

Referring again to Figure 8.8, we see that the Local Variables group is identified by 2; the system group is identified by 1; and the first variable is *romId* with a value of 1. Therefore, the variable *romId* has a value of 1.3.6.1.4.1.9.2.1.1.0. The appended *instance identifier* 0 (zero) indicates that 1.3.6.1.4.1.9.2.1.1.0 is the one and only instance of *romId*.

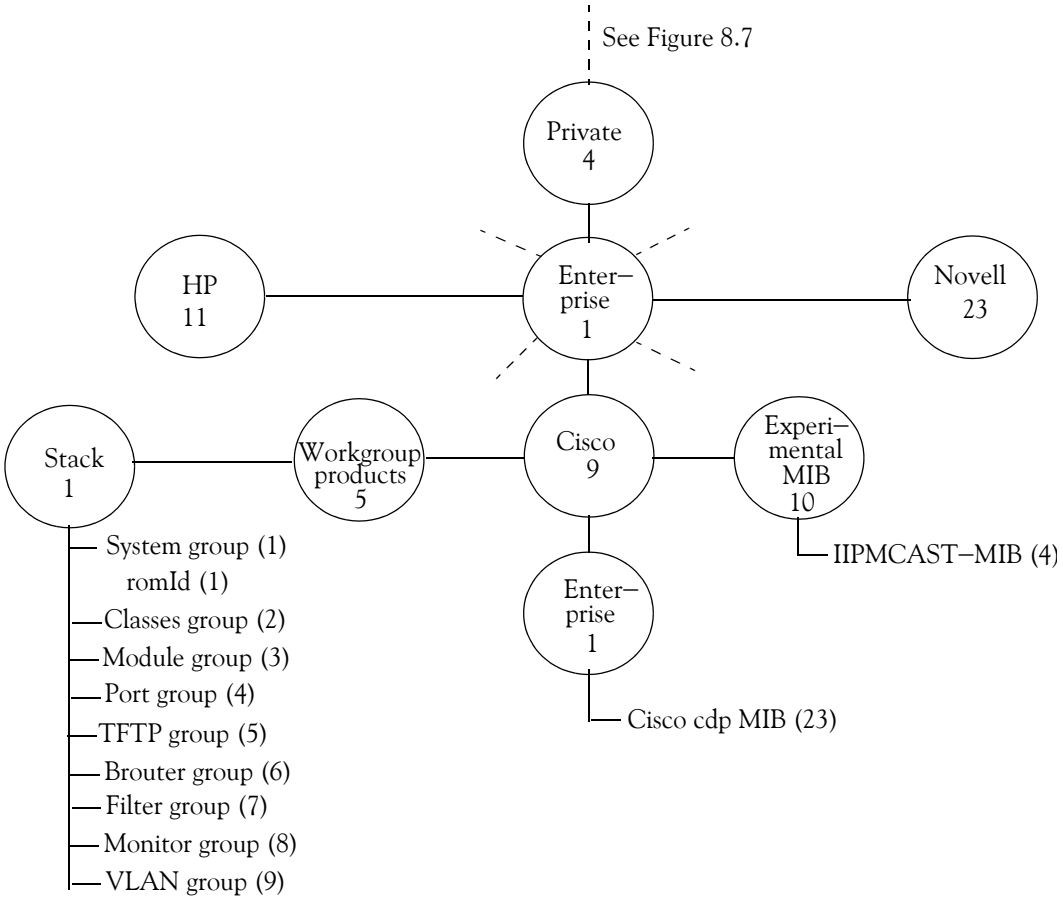


Figure 8.8. Cisco's private MIB hierarchy branches

8.8.5 Interpreting Cisco's Object Identifiers

When network management protocols use names of MIB variables in messages, each name has a suffix appended. This suffix is an instance identifier. For simple variables, the instance identifier 0 refers to the instance of the variable with that name.

An MIB can also contain tables of related variables. In the case of a table, we can select a specific row of the table; for instance, 1 denotes the first row, 2 the second row, and so on.

As described above with the romID example, an *instance identifier* is appended with a zero. Each group of Cisco MIB variables is accompanied by an illustration that indicates the specific *object identifier* for each variable.

Consider the object identifier for the Cisco MIB variable shown in Table 8.4.

TABLE 8.4 Object Identifier Example for a Cisco MIB Variable

Name identifier	Number Identifier
iso.org.dod.internet.private.enterprise.cisco.local variables.system group.	1.3.6.1.4.1.9.2.1
.....	.....
.....	.....
iso.org.dod.internet.private.enterprise.cisco.local variables.system group.hostConfigAddr	1.3.6.1.4.1.9.2.1.51

In Table 8.4, the *object identifier* 1.3.6.1.4.1.9.2.1 at the top row indicates the labeled nodes. The last row indicates the number of the Cisco MIB variable. The MIB variable, in this case, is *hostConflgAddr* is shown by the number *51.* Thus, the object identifier for *hostConflgAddr* is defined as *iso.org.dod.internet.private.enterprise.cisco.local variables.system group.hostConfigAddr* or *1.3.6.1.4.1.9.2.1.51.*

8.8.6 MIB Groups and Data Collection

To facilitate SNMP data collection, it is highly recommended that MIBs are grouped in related managed objects that can be analyzed and reported as an entity. Figure 8.9 shows MIB groups for three different classes of equipment in an internetwork: the backbone switches, routers, and application servers.

In an NMS database, SNMP can collect and store vast amounts of data on every device in a network. However, for historical purposes the data can be stored in a permanent database. Figure 8.10 shows a scheme similar to the stock market records kept by brokerage houses.

8.8.7 Thresholds, Alarms, and Traps

A *threshold* is a point separating conditions that will produce a given effect from conditions of a higher or lower degree that will not produce the effect. In SNMP, a threshold defines an acceptable value or a range of acceptable values for an SNMP variable. A threshold can be established as the values between a maximum and a minimum as shown in Figure 8.11.

The curve in Figure 8.11 could represent the acceptable values of a device's temperature where values above or below the maximum and minimum would create an alarm condition.

At other times we are concerned with values exceeding or falling below a predetermined value but not both. For instance, if we are concerned about the data rates entering or leaving a router, we are only interested in the condition where the data rates fall below an established threshold as shown in Figure 8.12.

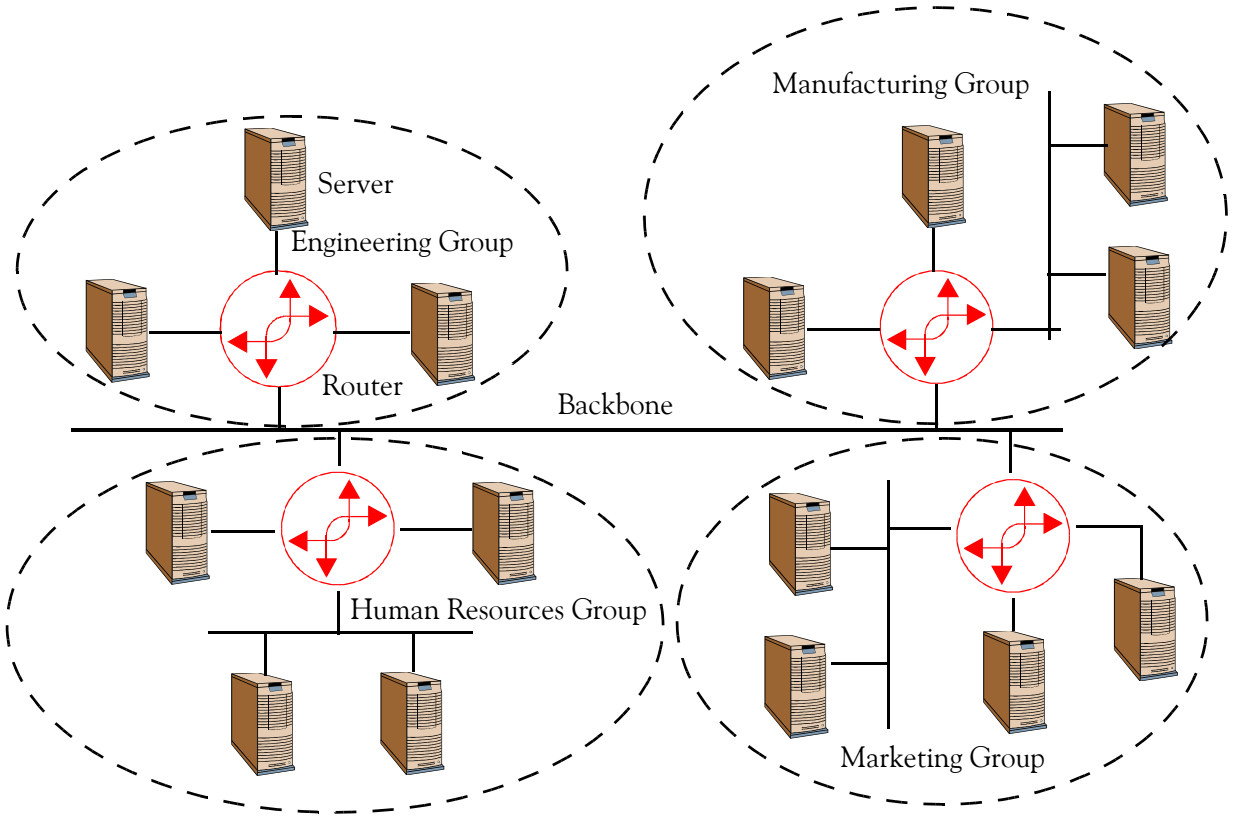


Figure 8.9. Grouping MIBs by related managed objects

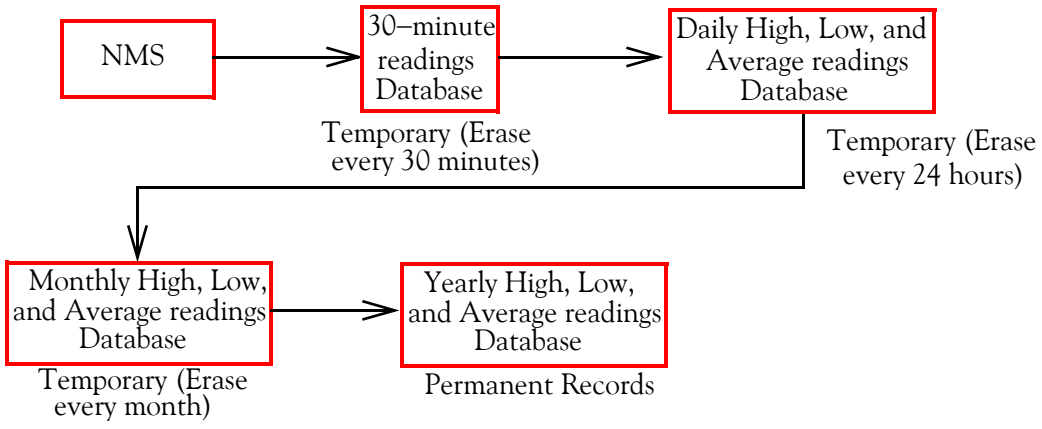


Figure 8.10. Data collection

When a seemingly abnormal condition such as a value below an established threshold occurs, the network administrator can decide how the SNMP agent should respond. The event can either be logged or an alarm to be sent to the NMS can be created. As mentioned earlier, this type of an SNMP alarm message is called a trap, since it catches (or traps) the device's abnormal condition.

As discussed earlier, traps are unsolicited messages sent from an agent to an NMS. Accordingly, the method of using traps offers an effective method of notifying the administrator since network traffic is facilitated with the use of traps.

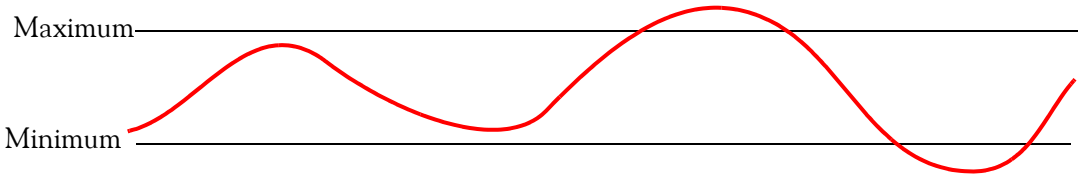


Figure 8.11. Thresholds between maxima and minima

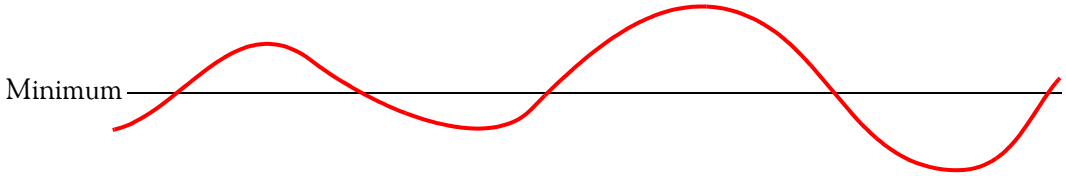


Figure 8.12. Threshold defining acceptable values those above the minimum.

Figure 8.13 shows how an alarm can be detected and how an administrator can be notified when an abnormal condition occurs.

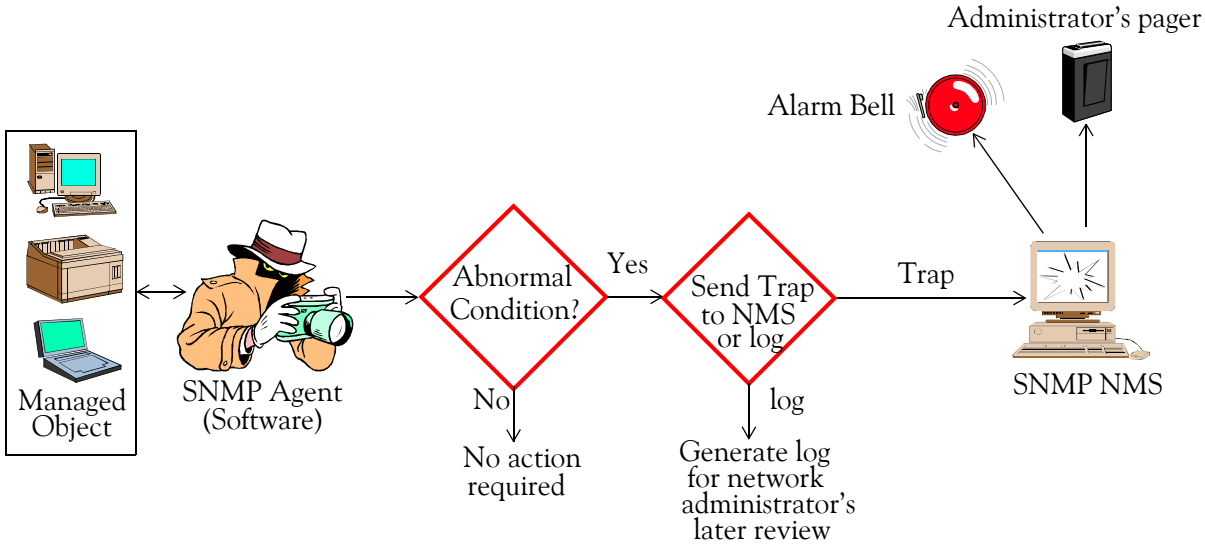


Figure 8.13. An SNMP trap reporting an event to NMS

8.8.8 SNMP Communities

in this subsection, the meaning and functions of the *SNMP communities* are discussed in more detail. Both SNMPv1 and SNMPv2 use communities to establish the exchange of information between NMSs and agents. An agent is configured with three community names: read–only, read–write, and trap. The community names are essentially passwords.

As stated earlier, the read–only community string allows us only to read the data. For example, it will allow the networks administrator to read the number of packets that have been transferred through the ports on his router, but does not allow him to reset the counters. The read–write community allows him to read and modify the data. This community allows him to read the counters, reset them if desired, and also alter the interfaces in our router's configuration. The trap community allows him to receive traps from the agent.

Most manufacturers ship their equipment with default community strings, typically *public* for the read–only community and private for the read–write community. The network administrators should change these defaults before using these new equipment on their networks. Also, it is advisable to avoid using names such as father's, mother's, or spouse's names. Alphanumeric string with mixed upper– and lower–case letters would be the best choice.

The networks administrator can use a *Virtual Private Network* (VPN) to protect his community strings from unauthorized users. A VPN is a set of nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being received and understood by unauthorized users as if the nodes were connected by private lines.

8.8.9 SNMP's Independency on Platforms

The SNMP standard is platform–independent because it requires that every MIB object have an object identifier and a syntax. An object identifier is used to identify the object to the system, indicate what kind of MIB to use, and what kind of data the object collects.

A *field* is a certain part of a file. A *file* represents data in binary (zeros and ones), and a set of binary positions are reserved for each field within the file. To understand the contents of a field, an operating system such as Cisco's IOS must know whether the field contains a number, text, a counter, or other type of data. These are called *data types*. Data types specify the syntax to be used for a data field. A *data field* is a group of data, such as a model number or temperature reading. All fields must be specified as a data type; otherwise, the data will not be processed.

Computer hardware architectures, operating systems, programming languages, and other environments specify the data types that can be recognized and processed. A data type represents the interface where software meets hardware. It tells the machine what syntax to use to interpret a field's contents. Accordingly, a different syntax is used for floating–point numbers, integer numbers, dates, text strings, and other data types. The following code is from a Cisco router's configuration file. It shows the SNMP settings made for the device.

davisrouter(config)**#snmp–server community public RO**

davisrouter(config)**#snmp–server community private RW**

davisrouter(config)**#snmp–server enable traps snmp**

davisrouter(config)**#snmp–server enable traps isdn**

davisrouter(config)**#snmp–server enable traps config**

davisrouter(config)**#snmp–server enable traps bgp**

davisrouter(config)**#snmp–server enable traps frame relay**

davisrouter(config)**#snmp–server enable traps rtr**

davisrouter(config)**#snmp–server host 10.1.1.13 traps public**

The first two lines establish a device as a member of a certain management group by using the Read–Only (RO) and Read–Write (RW) community strings. The third through the eighth lines create SNMP traps for this file. They inform the SNMP agent on the device to send trap messages if any changes occur. The designation bgp on the sixth line denotes the Border Gateway Protocol (BGP) which is a high–level routing protocol that uses metrics (measurements) to maintain routing tables so that it can determine the best path to a particular network. The last line specifies the IP address of the NMS, so the agent knows where to send the trap messages. The community string `public` will be included in the traps.

8.8.10 SNMPv1 Operations

SNMPv1 uses the following four operations:

`Get` Used by the NMS to retrieve object instances from an agent

`GetNext` Used to retrieve subsequent object instances after the first object instance.

`Set` Used to set values for object instances within an agent (such as a threshold)

`Trap` Used to instruct an agent to notify the NMS of an event (without being polled).

8.8.11 SNMPv2 Operations

SNMPv2 uses two additional operations, the `GetBulk` and `Inform`. Thus, SNMPv2 uses the following six operations:

`Get` Used by the NMS to retrieve object instances from an agent

`GetNext` Used to retrieve subsequent object instances after the first object instance.

`GetBulk` Only one GetBulk operation is necessary to retrieve both the first and all subsequent instances in a managed object (replaces the need for iterative GetNext operations in SNMP version 1).

`Set` Used to set values for object instances within an agent (such as a threshold)

`Trap` Used to instruct an agent to notify the NMS of an event (without being polled).

`Inform` New for SNMP version 2, this operation instructs one NMS to forward trap information to one or more other NMSs.

Generally, SNMP operations are embedded into computer programs. For example, in Cisco's IOS if an administrator enters the location of a router in an inventory screen in the Essentials console, a process is initiated from Essentials that invokes the `set` snmp location operation in IOS inside that router.

The `get` and `set` are SNMP's two fundamental operations. The `set` operation is used to set managed parameters in managed objects. The code below shows a `set` operation that configures the managed device to supply its physical location.

phillipsrouter»**set snmp location ""San Francisco""**

The `get` operation is used to fetch stored variables from agents and bring them back to the NMS. The following example requests a specific MIB object be reported by calling out a specific object identifier of a private Cisco MIB:

jonesrouter»**getsnmp 1.3.6.1.4.1.9.9.13**

After the object identifiers are defined, we write the actual object definitions. Every object definition begins with the following format:

`<name> OBJECT–TYPE`

`SYNTAX <data type>` – i.e., number, text, counter, etc.

`ACCESS <either read–only, read–write, write–only, or not–accessible>`
(non–accessible means that the object cannot be accessed by an agent. For example, an agent may have access to some entries on a table, but not the entire table.)

`STATUS <either mandatory, Optional, or obsolete>`
(STATUS means current or obsolete. If current, can be either mandatory or optional. In SNMPv2 is current. Mandatory means that the agent must implement this object to comply with the MIB specification.)

`DESCRIPTION`
(Textual description describing this particular managed object.)
`::= { <unique object identifier that defines this object> }`

The notation `::=` in the last line above is an operator used for an SMI definition.

Shown below is an excerpt of the information on the IP Routing table known as *lipRoutingTable* from the associated Cisco MIB file. `lip` stands for local IP

lipRoutingTable OBJECT–TYPE
SYNTAX SEQUENCE OF lipRouteEntry
ACCESS not–accessible
STATUS mandatory
DESCRIPTION
"A list of IP routing entries."

:: { lip 2

lipRouteEntry OBJECT–TYPE

SYNTAX LlpRouteEntry

ACCESS not–accessible

STATUS mandatory

DESCRIPTION

"A collection of additional objects in the

cisco IP routing implementation."

INDEX { ipRouteDest }

:: { lipRoutingTable 1)

LlpRouteEntry ::

SEQUENCE {

locRtMask

IpAddress,

locRtCount

INTEGER,

}

The local IP Routing table, lipRoutingTable, is described in Table 8.5.

TABLE 8.5 IP Routing for lipRoutingTable

ipRouteDest	locRtMask	locRtCount
131.104.111.1	255.255.255.0	3
133.45.244.245	255.255.255.0	1

The `lipRoutingTable` contains two variables: `locRtMask` and `locRtCount`. The index for this table is the destination address of the IP route, or `ipRouteDest`. If there are *n* number of routes available to a device, there will be *n* rows in the IP Routing table. In Table 8.5 the route with the destination IP address of 131.104.111.1 has an IP Routing table network mask of 255.25 5.255.0. The number of parallel routes within the routing table is 3 shown in the `locRtCount` column.

Typically, an instance identifier might be a unique interface number or a 0, as described earlier with the *romId* example. An instance identifier can also be an IP address. For example, to find

the network mask for the route with a destination address of 131.104.211.243, we use the variable `locRtMask` with an instance identifier of 131.104.211.243. Thus, the format is

`locRtMask`.131. 104.211.243.

When variables belong to a table, they are listed in the section describing the table. The following tag is used to indicate the end of a table:

End of Table

All variables before this tag are part of the table.
The next paragraphs will help us understand how object identifiers are used with the Structure Management Information (SMI) definition.

As stated above, the notation `::=` is an operator used for an SMI definition. Thus, the definition of the internet subtree is

internetOBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) 1 }

This definition declares `internet` as the object identifier 1.3.6.1, which is defined as a subtree of iso.org.dod, or 1.3.6 as shown in Figure 8.5.

Next, the subtrees *directory, mgmt, experimental,* and *private* are defined in terms of the *internet* subtree above as

directoryOBJECT IDENTIFIER ::= { internet 1 }

mgmtOBJECT IDENTIFIER ::= { internet 2 }

experimentalOBJECT IDENTIFIER ::= { internet 3 }

privateOBJECT IDENTIFIER ::= { internet 4 }

These subtrees belong to the `internet`. Thus, for the *directory* subtree, the notation `{ internet 1 }` implies that it is part of the internet subtree and its object identifier is 1.3.6.1.1. Likewise, the object identifier for *mgmt* is 1.3.6.1.2, and so on.

Currently, there is one subtree under the private subtree. It is used to allow networking equipment manufacturers to define their own private objects for any type of hardware or software they want managed by SNMP. For this subtree, the SMI definition is

enterpriseOBJECT IDENTIFIER ::= { private 1 }

All private enterprise number assignments for individuals, institutions, and organizations are managed by the Internet Assigned Numbers Authority (IANA). As we already know, Cisco System's private enterprise number is 9, so the base object identifier is defined as iso.org.dod.internet.private.enterprise.cisco, or 1.3.6.1.4.1.9.

8.8.12 Defined Object Identifiers

To provide a method of defining the kind of information contained in a managed object, SMIv1 supports the following types:

`INTEGER`
This is a 32–bit number that is used to specify enumerated data types of a simple managed object. For instance, the operational status of a router interface can be *active, inactive*, or *disconnected*. With enumerated data types, 1 would represent *active*, 2 *inactive*, and 3 *disconnected*. RFC 1155 does not permit the use of the number zero (0) as an enumerated data type.

`OCTET STRING`
A string of zero or more octets (bytes) used to represent strings or physical addresses.

`COUNTER`

A 32–bit number with minimum value of zero (0) and maximum value $2^{32} - 1$ (4,294,967,295). When the maximum value is reached, it wraps back to zero and starts over. It's primarily used to track information such as the number of octets sent and received on an interface or the number of errors and discards seen on an interface. A Counter is monotonically increasing, in that its values should never decrease during normal operation. When an agent is rebooted, all Counter values are set to zero. Finite increments are used to determine if anything useful can be said for successive queries of Counter values. A finite increment is computed by querying a Counter at least twice in a row, and taking the difference between the query results over some time interval.

`OBJECT IDENTIFIER`
A dotted–decimal string that represents a managed object within the object tree. For example, 1.3.6.1.4.1.9 represents Cisco Systems's private enterprise Object Identifier.

`SEQUENCE`
Defines lists that contain zero or other ASN.l data types.

`SEQUENCE OF`
Defines a managed object that is made up of a sequence of ASN.l types.

`IPAddress`
Represents a 32–bit IPv4 address. Neither SMIvl nor SMIv2 discusses 128–bit IPv6 addresses.

`NetworkAddress`
Same as the `IPAddress` type, but can represent different network address types.

`Gauge`

A 32–bit number with minimum value of zero (0) and maximum value $2^{32} - 1$ (4,294,967,295). Unlike a `Counter`, a `Gauge` can increase and decrease at will, but it can never exceed its maximum value. The interface speed on a router is measured with a `Gauge`.

TimeTicks

A 32–bit number with minimum value of zero (0) and maximum value $2^{32} - 1$ (4,294,967,295). `TimeTicks` measures time in hundredths of a second. Time elapsed on a device is measured using this enumerated data type.

Opaque

Creates data types based on previously defined data types. Its use is limited because its size is undefined and thus it causes implementation problems. These object types define managed objects. Previously, we mentioned that a MIB is a logical grouping of managed objects as they pertain to a specific management task, manufacturer, etc. The MIB can be thought of as a specification that defines the managed objects that a vendor or device can supports.

Cisco has has defined many MIBs for its product line. For example, its Catalyst device has a separate MIB from its 7000 series router. Both devices have different characteristics that require different management capabilities. Vendor–specific MIBs typically are distributed as human–readable text files that can be inspected or modified with a standard text editor.

Most Network Monitoring Station (NMS) products maintain a compact form of all the MIBs that define the set of managed objects for all the different types of devices they're responsible for managing. NMS administrators will typically compile a vendor's Management Information Base (MIB) into a format the NMS can use. Once an MBI has been loaded or compiled, administrators can refer to managed objects using either the numeric or named object identifier.

Generally, MIBs are named using a convention that indicates the MIB category. For example, a Cisco MIB object that deals with a specific network interface will have *if* in its name (from the letters *i* and *f* in *i*nter*f*ace). `In` and `Out` specify whether the MIB object is to measure incoming or outgoing traffic. Thus, the `ifInErrors` MIB object monitors incoming packet errors on an interface and `ifOutErrors` monitors the outgoing errors. Likewise, `sysLocation` reports a the network location of a device on the network. The basic MIB categories used in most SNMP systems are listed below.

Configuration

Configuration MIBs report basic management information such as device name, contact person, device location, and uptime. MIB configuration objects are `sysName`, `sysDescr`, `sysContact`, `sysLocation, sysUpTime, ifNumber, romID`, and others.

Interface error rates

These are MIBs that monitor specific interfaces. Packet errors are a normal condition, but watching their trends indicates device health and helps isolate faults. For Ethernet interfaces, we use `ifInErrors, ifOutErrors, locifCollisions, locIfInRunts, locIflnGiants, locIfCRC`, and others. For serial interfaces, we use `locIflnFrame, locIfInAbort, locIfInIgnored, locIfResets, locIfRestarts`, and others.

Bandwidth

The *Internet Control Message Protocol* (ICMP) is a protocol that reports on IP packet processing. It's best known for its echo command used to verify the presence of other devices by pinging* them. *Timed pings* are used to determine how far away a device is (much like SONAR used in the submarines). SNMP sends ping input and output messages to measure available bandwidth. Cisco's MIB objects for this are `icmpInEchos, icmpInEchoReps`, `icmpOutEchos`, and `icmpOutEchoReps`. These are the only SNMP messages not sent as User Datagram Protocol (UDP) messages.

Traffic flow

This category measures traffic flow. There are Cisco MIBs to measure traffic rates both as bits per second and packets per second. The objects are `loclfInBitsSec, locIfOutBitsSec, locIfInPktsSec,` and `locIfOutPktsSec`.

Unreachable address

The object to measure how often a router is asked to send messages to an unreachable address is `icmpOutDesUnreachs`.

SNMP data

We can also use objects to measure how much time the router spends handling SNMP messages. These objects include `snmpInGetRequests, snmpOutGetRequests, snmpInGet-Responses, snmpOutGetResponses,` and others.

It is possible to set a MIB to gather information on a single object instance only, called a *scalar object.* Most managed objects, however, are composed of several related object instances. This practice, called *tabular objects*, is the rule in most MIBs because it is more efficient to manage as much as possible from a single data collection point. As the name implies, a tabular MIB keeps the information straight by storing it in rows and tables.

8.9 Extensions to the SMI in SNMPv2

SMIv2 extends the SMI object tree by adding the Security and SNMPv2 branches to the internet subtree, adding several new datatypes, and making a number of other changes. Figure 8.14 shows how the SNMPv2 objects fit into SMIv2.

* *Ping, as used in an IOS environment indicates whether "echo" packets are reaching a destination and returning. For example, if we use the command ping10.1.1.1, IOS will return the percentage of packets that echoed back from the 10.1.1.1 interface.*

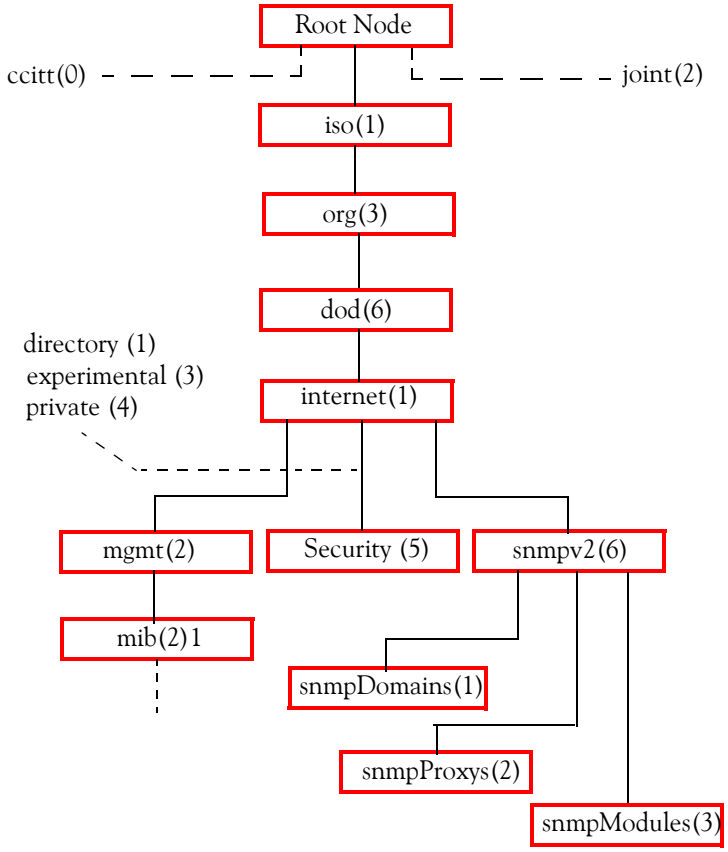


Figure 8.14. SMIv2 object tree for SNMPv2. Compare with Figure 8.5 for SMIv1

Thus, the object identifier (OlD) for `snmpModules(3)` is 1.3.6.1.6.3, or *iso.org.dod.internet.snmpV2.snmpModules*. SMIv2 also defines some new datatypes which are summarized below.

`Integer32`
Same as `INTEGER` in SMIv1.

Counter32
Same as `Counter` in SMIv1.

`Gauge32`
Same as `Gauge` in SMIv1.

`Unsigned32`

Represents decimal values in the range of 0 to $2^{32} - 1$ inclusive.

`Counter64`
Similar to `Counter32`, but its maximum value is 18,446,744,073,709,551,615. `Counter64` is ideal for situations in which a `Counter32` may wrap back to 0 in a short amount of time.

BITS
An enumeration of named bits.

There are differences between object definitions between SMlv1 and SMlv2. Specifically, in SMIv2 we have new optional fields. The syntax of an object definition for SMlv2 is shown below where the changes in SMIv2 from SMIv1 are shown in bold characters.

<name> OBJECT–TYPE
SYNTAX <datatype>
UnitsParts <Optional, see below>
MAX–ACCESS <see below>
STATUS <see below>
DESCRIPTION
"Describes a particular managed object."
AUGMENTS { <name of table> }
::= (<Unique OlD that defines this object> }

UnitsParts
Describes the units (seconds, milliseconds, etc.) used to represent the object.

MAX–ACCESS
An object–type's access can be MAX–ACCESS in SNMPv2. The valid options for MAX–ACCESS are *read–only, read–write, read–create, not–accessible,* and *accessible–for–notify*.

STATUS
This clause has been extended to allow the current, obsolete, and deprecated keywords. Also, *current* in SNMPv2 is the same as *mandatory* in an SNMPvl MIB.

AUGMENTS
In some cases it is useful to add a column to an existing table. AUGMENTS allows us to extend a table by adding one or more columns, represented by some other object. This clause requires the name of the table the object will augment.

SMIv2 defines a new trap type, called NOTIFICATION–TYPE, which it is discussed in Subsection 8.12.2. SMIv2 also introduces new textual conventions and these are defined in RFC 2579. These textual conventions are used in SNMPv2. They are listed below.

DisplayString
This is a string of ASCII characters. Maximum length is 255 characters.

PhysAddress
A media– or physical–level address, represented as an OCTET STRING.

MacAddress
Defines the media–access address for IEEE 802 (the standard for local area networks) in canonical* order. This address is represented as six octets.

TruthValue
Defines both `true` and `false` Boolean values.

TestAndIncr
Prevents two management stations from modifying the same managed object at the same time.

AutonomousType
An object identifier that is used to define a subtree with additional MIB–related definitions.

VariablePointer
A pointer to a particular object instance, such as the `ifDescr` for interface 7. In this case, the `VariablePointer` would be the object identifier `ifDescr.7.`

RowPointer
A pointer to a row in a table. For example, `iflndex.5` points to the fifth row in the `ifTable.`

RowStatus
Used to manage the creation and deletion of rows in a table, since SNMP has no way of doing this via the protocol itself. `RowStatus` can keep track of the state of a row in a table, as well as receive commands for creation and deletion of rows. This textual convention is designed to promote table integrity when more than one manager is updating rows. The following enumerated types define the commands and state variables: `active(1), notInService(2), notReady(3), createAndGo(4), createAndWait(5), and destroy(6).`

TimeStamp
Measures the amount of time elapsed between the device's system uptime and some event or occurrence.

TimeInterval
Measures a period of time in hundredths of a second. `TimeInterval` can take any integer value from 0 to 2147483647.

DateAndTime
An `OCTET STRING` used to represent date and time information.

StorageType
Defines the type of memory an agent uses. The possible values are `other(1), volatile(2), nonVolatile(3), permanent(4),` and `readOnly(5)`.

TDomain
Denotes a transport service.

TAddress
Denotes the transport service address. `TAddress` is from 1 to 255 octets in length.

---

* *Canonical order means that the address is represented with the least–significant bit first.*

8.10 MIB–II

MIB–II is the second version of the original MIB. Section 6 of RFC 1213 defines the object identifiers for the mib–2 subtree as follows:

mib–2 OBJECT IDENTIFIER :: = { mgmt 1 }
system OBJECT IDENTIFIER :: = { mib–2 1 }
interfaces OBJECT IDENTIFIER :: = { mib–2 2 }
at OBJECT IDENTIFIER :: = { mib–2 3 } – (address translation)
ip OBJECT IDENTIFIER :: = { rnib–2 4 }
icmp OBJECT IDENTIFIER :: = { mib–2 5 } – (Internet Control Message Protocol)
tcp OBJECT IDENTIFIER :: = { mib–2 6 }
udp OBJECT IDENTIFIER :: = { mib–2 7 }
egp OBJECT IDENTIFIER :: = { mib–2 8 } – (External Gateway Protocol)
transmission OBJECT IDENTIFIER :: = { mib–2 10 }
snmp OBJECT IDENTIFIER :: = { mib–2 11 }

mib–2 is defined as *iso.org.dod.internet.mgmt.1*, or 1.3.6.1.2.1. From here, we can see that the system group is mib–2 1, or 1.3.6.1.2.1.1, and so on. Figure 8.15 shows the MIB–II subtree of the *mgmt* branch.

A brief description of each of the subtree names under mib2(1) in Figure 8.15 is provided below. A detailed description is given in RFC 1213.

`system 1.3.6.1.2.1.1`
Defines objects that pertain to system operation such as system contact, system name, system location, and service information regarding the managed node.

`interfaces 1.3.6.1.2.1.2`
Monitors the status of each interface on a managed entity.

`at 1.3.6.1.2.1.3`
The address translation (`at`) is declared deprecated in RFC 1213.

`ip 1.3.6.1.2.1.4`
Keeps track of IP datagrams and IP routing.

`icmp 1.3.6.1.2.1.5`
Tracks ICMP* errors. There are no changes to this group.

* *As stated earlier, ICMP is an acronym for Internet Control Message Protocol. It is a network–layer (ISO/OSI level 3) Internet protocol that provides error correction and other information relevant to IP packet processing. For example, it can let the IP software on one machine inform another machine about an unreachable destination.*

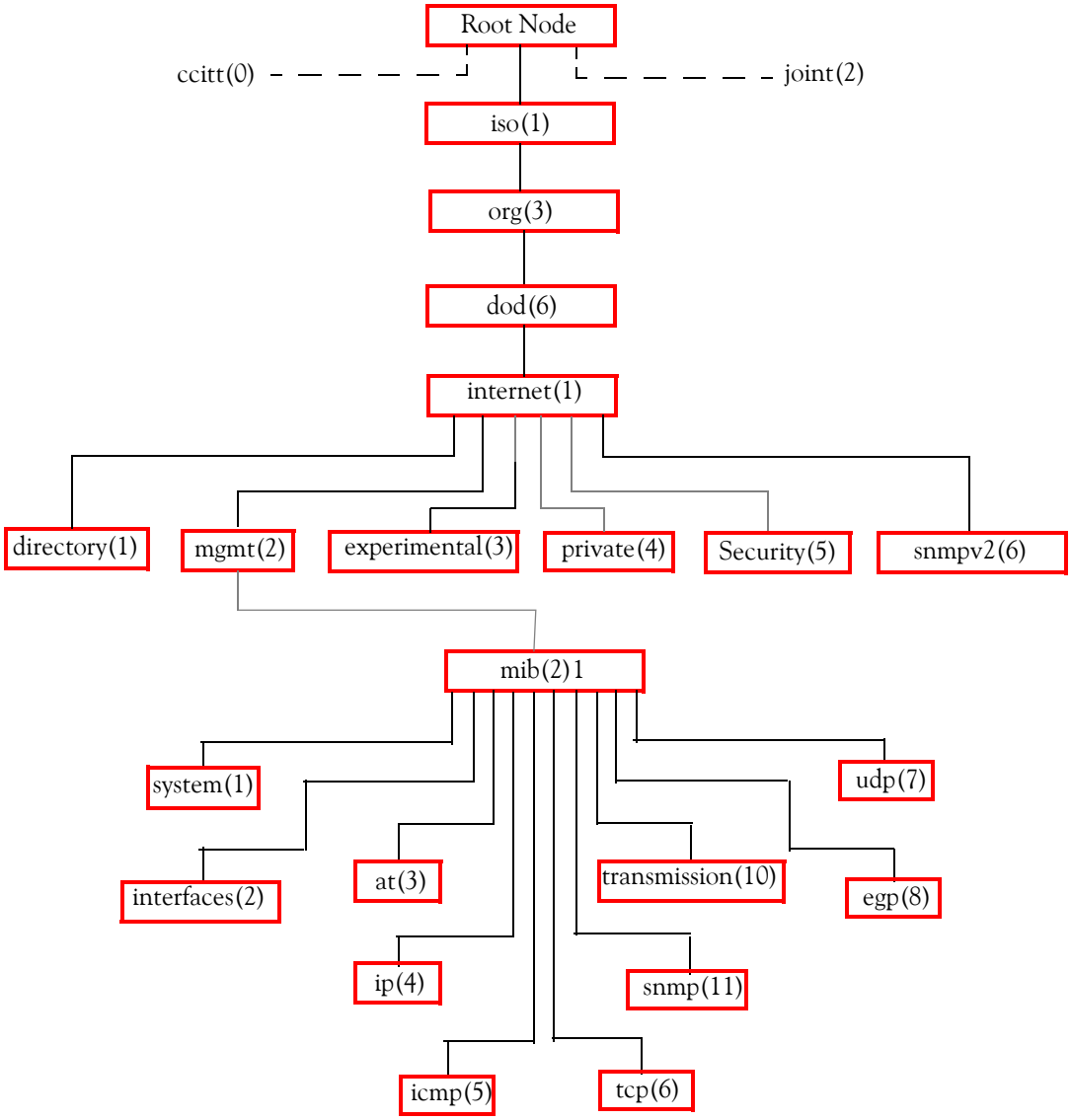


Figure 8.15. MIB–II subtree

`tcp 1.3.6.1.2.1.6`
Keeps track of the number of incoming TCP segments in error and the number of resets generated by a TCP.

`udp 1.3.6.1.2.1.7`
Used for UDP statistics. A new table defined as udpTable is added.

`egp 1.3.6.1.2.1.8`
Defines new objects that are useful in External Gateway Protocol (EGP) monitoring.

transmission 1.3.6.1.2.1.10
It is used to provide a prefix for the name of objects defined for managing transmission media.

snmp 1.3.6.1.2.1.11
Has added a new group that enhances statistical information.

Example 8.1

MIB files follow the format outlined below. This example will help the reader to understand MIB files. Anything preceded by – – is a comment.

The first line of the file defines the name of the Management Information Base (MIB). For this example it is RFC1213 that defines MIB–II. The format of this definition is always the same. As stated earlier, the notation `::=` is an operator used for an SMI definition. Thus, the first line is

RFC1213–MIB DEFINITIONS :: = BEGIN
The file may include an `IMPORTS` section of the Management Information Base (MIB). The user can import data types and object identifiers from other MIB files using `IMPORTS`. This MIB imports the following object identifiers from RFC 1155 which defines SMIv1.

- `mgmt`
- `NetworkAddress`
- `IPAddress`
- `Counter`
- `Gauge`
- `TimeTicks`

Each group of items imported using `IMPORTS` is followed by `FROM` to define the MIB file from which the objects are extracted. Thus, for this example, the `IMPORTS` section is written as

IMPORTS
mgmt, NetworkAddress, IpAddress, Counter, Gauge, TimeTicks
FROM RFC1155–SMI

MIB files are written by using definitions from RFC 1212. `OBJECT–TYPE` is added from this RFC as follows:

OBJECT–TYPE
FROM RFC 1212;

The line below indicates that the MIB–II structure is as shown in Figure 8.15. We observe that `mib(2)` is the only node under `mgmt(2)`. Thus, the objects defined in MIB–II have the `OBJECT IDENTIFIER` prefix:
mib–2 OBJECT IDENTIFIER ::= { mgmt 1 }

Next, the following comment line is inserted:

– – groups in MIB–II
As stated earlier, anything preceded by – – is a comment line

The object identifiers that will be used throughout the remainder of this example will follow the MIB–II structure shown in Figure 8.15. We already know that *mgmt* is equivalent to 1.3.6.1.2. and thus *mib–2* is 1.3.6.1.2.1. The *interfaces* group under *mib–2* is defined as or 1.3.6.1.2.1.2 or as {`mib–2 2`}.

The next step is to write the object definitions. All object definitions have the following format:

```
<name> OBJECT–TYPE
SYNTAX <datatype>
ACCESS <either read–only, read–Write, write–only, or not–accessi-
ble>
STATUS <either mandatory, Optional, or obsolete>
DESCRIPTION
"Textual description describing this particular managed object."
::= { <unique OID that defines this object> }
```

It is assumed that the first managed object in our subset of the MIB–II definition is *ifTable*, which represents a table of network interfaces on a managed device. The object names are defined using mixed case, with the first letter in lowercase. Here is its definition using ASN.l notation where we have used SYNTAX of *ifTable* is `SEQUENCE OF IfEntry`. The name of the sequence `IfEntry` is also a mixed case but the first letter, unlike the object definition *if Table*, is capitalized, and this is how a sequence* is defined. This means that *ifTable* is a table containing the columns defined in `IfEntry`. The object for this example is assumed to be *not–accessible*; this means that we have no access to the entire table but we may have access to some of the table entries. Its status is mandatory (current), which means that an agent must implement this object in order to comply with the MIB–II specification. The DESCRIPTION describes what exactly this object is. The unique object identifier is 1.3.6.1.2.1.2.2, *or iso.org.dod.tnternet.mgmt.interfaces.* Thus, for this example, the next section is written as

```
ifTable OBJECT–TYPE

SYNTAX SEQUENCE OF IfEntry

ACCESS not–accessible

STATUS mandatory

DESCRIPTION
```

* *A sequence is a list of columnar objects and their SMI datatypes which defines a table.*

"A list of interface entries. The number of entries is given by the value of `ifNumber`."

```
::= { interfaces 2 }
```

`IfEntry` is defined as follows:

```
IfEntry ::=
SEQUENCE {
ifIndex
INTEGER,
ifDescr
DisplayString,
ifType
INTEGER,
ifInOctets
INTEGER,
ifSpecific
OBJECT IDENTIFIER
 }
```

As stated above `IfEntry` defines a table and in that table one expects to find variables defined by *ifindex, IfDescr, ifType*, etc. This table can contain any number of rows and the rows contained in a table are managed by the agent. How the `set` operation can be used to add rows to a table will be discussed later.

The `IfEntry` is also used to specify what will be found in any row of the table, so one can look back to the definition of `ifEntry` (the actual rows of the table) itself:

```
ifEntry OBJECT–TYPE
SYNTAX IfEntry
ACCESS not–accessible
STATUS mandatory
DESCRIPTION
```

"An interface entry containing objects at the subnetwork layer and below for a particular interface."

```
INDEX { ifIndex }
::= { ifTable 1 }
```

`ifEntry` defines a particular row in the `ifTable`. Its definition is almost identical to that of `ifTable`, except that a new clause, `INDEX,` has been introduced. The `index` is a unique key used to define a single row in the `ifTable`. It's up to the agent to make sure the index is unique within the context of the table. If a router has seven interfaces, `ifTable` will have seven rows in it. The object identifier for `ifEntry` is 1.3.6.1.2.1.2.2.1, or *iso.org.dod.internet.mgmt.interfaces.lfTable.ifEntry*. The index for `ifEntry` is `ifIndex` which is defined as:

```
ifIndex OBJECT–TYPE

SYNTAX INTEGER

ACCESS read–only

STATUS mandatory

DESCRIPTION

"A unique value for each interface. Its value ranges between 1
and the value of ifNumber. The value for each interface must
remain constant at least from one reinitialization of the
entity's network–management system to the next reinitialization."

::= { if Entry 1 }

END
```

The `ifIndex` object is read–only, which means we can see its value, but we cannot change it. The final object that the MIB defines is `ifDescr` which is a textual description for the interface represented by that particular row in the `ifTable`. The MIB example ends with the `END` clause, which marks the end of the MIB. In the actual MIB–II files, each object listed in the `IfEntry` sequence has its own object definition. In this version of the MIB only two of them are listed.

8.11 SNMP Operations

In this section, we will discuss how SNMP gathers information.
The Protocol Data Unit (PDU) is the message format that managers and agents use to send and receive information. There is a unique PDU format for each of the following SNMP operations:

- **get**
- **get–next**
- **get–bulk** (SNMPv2 and SNMPv3)
- **set**
- **get–response**

- **trap**
- **notification** (SNMPv2 and SNMPv3)
- **inform** (SNMPv2 and SNMPv3)
- **report** (SNMPv2 and SNMPv3)

Each of these operations is defined below.

8.11.1 The `get` Operation

It is recalled from an earlier discussion that managed objects can be physical devices, such as routers and network interfaces, software, or a group of these or the operating characteristics of managed devices. A managed object is also referred to as a *variable*, and a variable has a value associated with it. When we combine a variable with its associated value, we form a pair and this pair is referred to as *variable binding* or *VarBind* for short.

The `get` request operation is initiated by the NMS and sends it to an agent. The agent receives the request which includes a VarBind, gathers the requested information, and sends a `get–response` back to the NMS where it is processed. The procedure is shown in Figure 8.16.

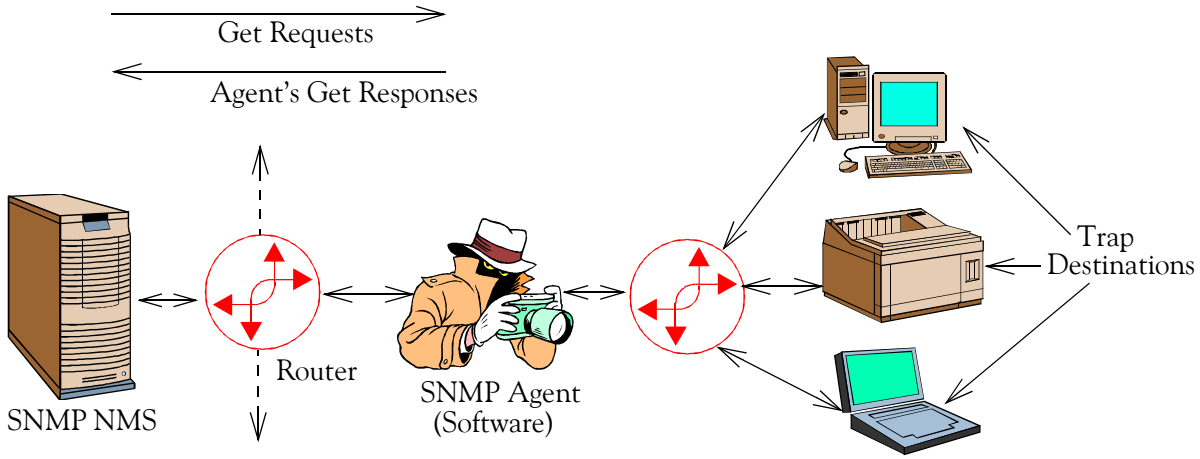


Figure 8.16. The get operation sequence

The statements below provide an example of a command on a Unix host.

```
$ snmpget cisco.name.com public .1.3.6.1.2.1.1.6.0
system.sysLocation.0 = " "
```

The first line above is written in Cisco's IOS and contains the operation `snmpget`. Generally, we use `snmpget` to query a router and, in case of a malfunction, obtain the administrator's name. It contains three arguments on the command line: the name of the device we would like to query (`company.name.com`), the read–only community string (`public`), and the object

identifier (`.1.3.6.1.2.1.1.6.0`) that we are interested at.

Referring back to Figure 8.15, Page 8–31, it is seen that `1.3.6.1.2.1.1` is the `system` group, and at the end of the object identifier are two more numbers, i.e., `.6` and `.0`. The number `.6` represents the MIB variable that the user wants to query; it represents the name `sysLocation`. In this example, he may want to see what the system location is set to on the Cisco router. The response appears on the second line and it appears as `system.sysLocation.0 = " "`. This indicates that the router is not set to anything. Also, it is seen that the response from `snmpget` is in variable binding format, that is, `object identifier = value`.

The last number `.0` following `.6`, is the *instance identifier*. Instance identifiers indicate a specific row in a table. Thus, instance identifier 1 is in the first row of a table, instance identifier 2 in the second row, and so on. An instance identifier with the number 0 is not defined as a row in a table. Therefore, when looking for values in a table of interfaces (`ifTable`), a nonzero instance identifier should be used to select a particular row in the table, i.e., a particular network interface.

Most recent SNMP packages are supplied with graphical NMS applications. With graphical applications it is not necessary to use operations such as the above to retrieve management information. This example was presented to illustrate the `get` operation.

The `get` operation is useful for retrieving a single MIB object at a time. However, when it is desired to retrieve more than one object over a period of time, it is prudent to use the `get–next` operation which is discussed next.

8.11.2 The get–next Operation

The `get–next` operation allows us to use this single operation to retrieve a group of values from an MIB. The `get–next` operation travels through a subtree in lexicographic order. Since an object identifier is a sequence of integers, it makes it easy for an agent to start at the root of its SMI object tree and proceed downwards to find the object identifier that it is looking for. When the NMS receives a response from the agent for the `get–next` operation it just issued, it subsequently issues another `get–next` operation. When there are no more objects to get, the agent returns an error, signifying that the end of the MIB has been reached.

The `get–next` request has two main advantages. One advantage is that the user needs not to know the object identifier of the next entity. This is because if he knows the current object identifier, he can retrieve the next one following the lexicographic order. Also, in the case of an aggregate object, the number of rows may be changing dynamically, that is, it is updated periodically and thus he does not know how many rows a table contains at a particular time. This presents no problem when we use the `get–next` request.

The `get–next` operation is illustrated with another example using the `snmpwalk` operation This operation simply facilitates the `get–next` procedure for us. It is similar to the `snmpget` operation, except that it allows us to specify which branch to start at. This example begins with the systems group below.

```
$ snmpwalk cisco.name.com public system
system.sysDescr.0 = "Cisco Internetwork Operating System Soft-
ware
..IOS (tm) 2500 Software (C2500–I–L). Version 11.2(5), RELEASE
SOFTWARE (fc1) ..Copyright (c) 1986–1997 by Cisco Systems, Inc...
Compiled Mar–01–04 15:49 by chuckjohnson"
system.sysObjectID.0 = OlD: enterprises.9.1.19
system.sysUpTime.0 = Timeticks: (36210723) 4 days, 4:35:07.23
system.sysContact.0 = ""
system.sysName.0 = "cisco.name.com"
system.sysLocation.0 = ""
system.sysServices.0 = 6
```

The first line above is written in Cisco's IOS and contains the `snmpwalk` operation. The remaining lines indicate responses. The last seven lines include the administrator's name who compiled it, the system object identifier (OID), and the time that the system has been on.

8.11.3 The get–bulk Operation

The `get–bulk` operation is defined in SNMPv2. This operation enables an NMS, through an agent, to retrieve a section of a table with a single operation. The user can also use the simple `get–next` operation to retrieve more than one MIB object at once, but the message sizes are limited by the agent's capabilities. With the `get–next` operation, if the agent cannot supply the NMS with responses to all requests, it returns an error message with no data. The `get–bulk` operation, on the other hand, tells the agent to gather send as much information as it possibly can. Thus, incomplete responses are possible with the `get–bulk` operation.

The `get–bulk` operation includes two additional fields referred to as *non–repeaters* and *max–repetitions*. The non–repeaters field indicates the number of non–repetitive objects (scalars) to be retrieved with a simple `get–next` operation. The max–repetitions field tells the `get–bulk` operation to retrieve the remaining objects such as the number of rows in an aggregate object. Figure 8.17 shows the `get–bulk` operation where the requested bindings are: `sysDescr`, `ifInOctets`, and `ifOutOctets`. Of course, there could be many more bindings.

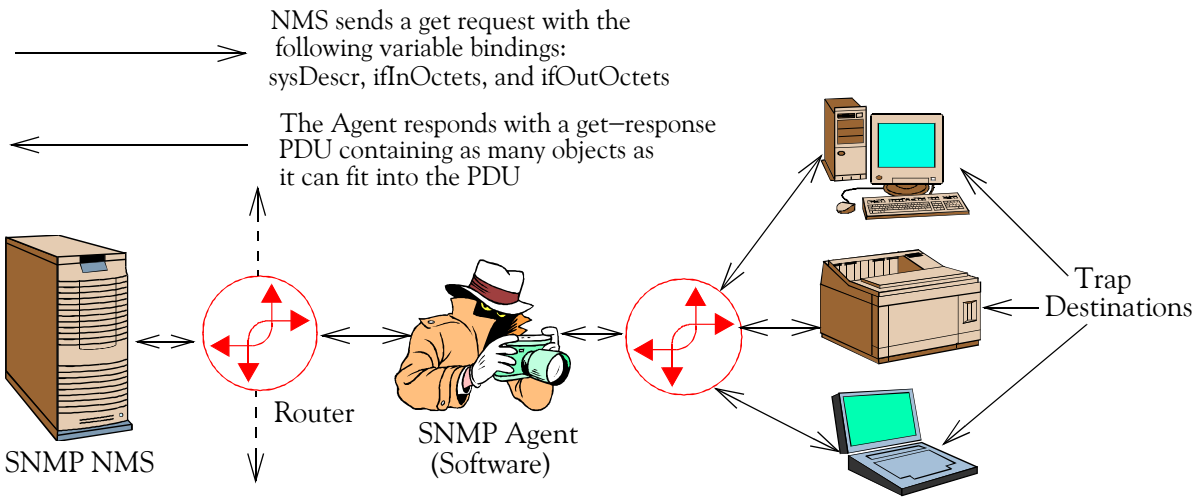


Figure 8.17. The get–bulk operation

8.11.4 The `set` Operation

The `set` request operation is shown in Figure 8.18.

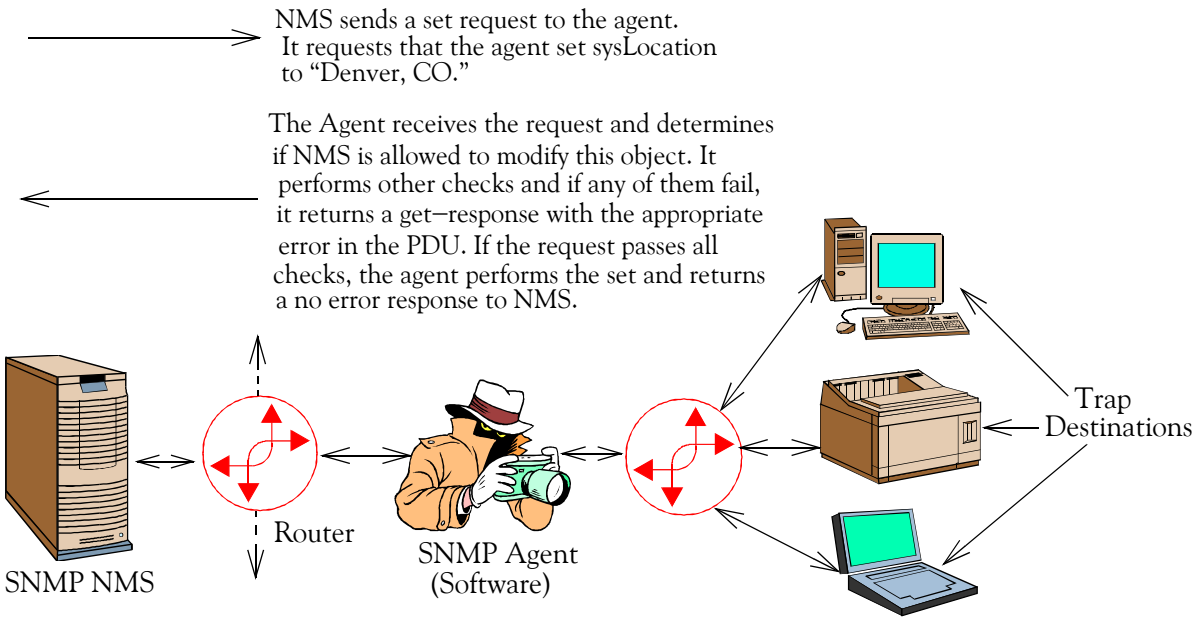


Figure 8.18. The `set` request operation

The `set` operation is used to change the value of a managed object or to create a new row in a table. Objects that are defined in the MIB as read–write or write–only can be altered or created using this operation. It is possible for an NMS to set more than one object at a time. The following example queries the `sysLocation` variable, then sets it to a value.

```
$ snmpget cisco.name.com public system.sysLocation.0
system.sysLocation.0 = " "
```

The operation above is similar to the `get` operation and displays the current value of `sysLocation`. For this example, it is undefined.

For the next example, we will issue an operation using the `snmpset` operation. For this operation, we supply the hostname, the read–write community string (private), and the variable we want to set, in this case, `system.sysLocation.0`) with its new value (`s "Denver, CO"`). The `s` indicates that `snmpset` that we want to set the value of `sysLocation` to a string; and `"Denver, CO"` is the new value. The `SYNTAX` for `sysLocation` is `DisplayString (SIZE (0 ..255))` indicating that that it contains a string with a maximum length of 255 characters.

The definition of `sysLocation` in RFC 1213 is:

```
sysLocation OBJECT–TYPE
SYNTAX DisplayStrinq (SIZE (0 ..255 ))
ACCESS read–write
STATUS mandatory
DESCRIPTION
"The physical location of this node (e.g., 'telephone closet, 3rd
floor')."
::= { system 6 }
$ snmpset cisco.name.com private system.sysLocation.O s "Denver,
CO"
system.sysLocation.O = "Denver, CO"
```

We can verify that the above operation was executed properly by re–issuing the above command without the string, as shown below.

```
$ snmpget cisco.name.com public system.sysLocation.0
system.sysLocation.O = "Denver, CO"
```

It is possible to set more than one object at a time, but if any of the sets fail, they all fail. That is, all values remain unchanged.

8.11.5 Frequently used ASN.1 Constructs

The ASN.1 construct for the `get, get–next, get–bulk,` and `set` PDU type messages for SNMPv1 is shown below.

```
-- request/response information
RequestID ::=
     INTEGER
ErrorStatus ::=
     INTEGER {
noError(0)
tooBig(1)
noSuchName(2)
badValue(3)
readOnly(4)
genErr(5)
     }
ErrorIndex ::=
     INTEGER
-- variable bindings
VarBind ::=
     SEQUENCE {
          name ObjectName,
          value ObjectSyntax
     }
VarBindList ::=
     SEQUENCE OF
         VarBind
```

As stated earlier, the Protocol Data Unit (PDU) is the message format that managers and agents use to send and receive information. There is a unique PDU format for each SNMP operation. For convenience, these PDUs are shown in Figure 8.19.

PDU Type	RequestID	Error Status	Error Index	VarBind1 Name	VarBind1 Value	VarBind2 Name	VarBind2 Value	.....

Figure 8.19. The `get, get–next, get–bulk,` *and* `set` *PDUs*

The `trap` PDU is shown in Figure 8.20.

PDU Type	Enterprise	Agent Address	Generic Trap Type	Specific Trap Type	Timestamp	VarBind1 Name	VarBind1 Value	VarBind2 Name	VarBind2 Value	...

Figure 8.20. The `trap` *PDU*

In SNMPv1 the PDU type for each of these requests/responses are defined in RFC 1157 as shown in Table 8.6.

TABLE 8.6 SNMPv1 PDU types

Request/Response	PDU Type
get request	0
get–next request	1
set request	2
get response	3
trap	4

As stated earlier, an SNMP message consists of a version identifier, an SNMP community name, and a Protocol Data Unit (PDU). The version and community name is added to the data PDU and it is passed on to the transport layer as SNMP PDU. Then, a PDU header is added at the transport layer which forms the transport PDU for the network layer. An IP header is added at the network layer and it is passed on to the Data link layer. Finally, a Data link header is added and it is sent to the Physical layer.

The IP and UDP are connectionless protocols and as such, are not reliable. It is therefore necessary to use a method for detecting lost messages. As indicated above, RFC 1157 makes provision for error status such as `noError(0), ....., genErr(5)`. These are SNMPv1 error messages. The error status for each error is shown in parentheses.

`noError(0)` No problem was encountered in performing the request.
`tooBig(l)` The response to our request is too big to fit into one response.
`noSuchName(2)` An agent was asked to get or set an object identifier that it cannot find.
`badValue(3)` A read–write or write–only object was probably set to an inconsistent value.
`readOnly(4)` Equivalent to `noSuchName`.
`genErr(5)` If an error occurs for which none of the previous messages is appropriate, a `genErr` is issued.

SNMPv2 provides additional error messages which are listed below.

`noAccess(6)` A set to an inaccessible variable was attempted.
`wrongType(7)` An object was set to a type that is different from its definition.
`wrongLength(B)` A string object was set to a value that exceeds its maximum length.
`wrongEncoding(9)` A set operation was attempted using the wrong encoding.
`wrongValue(10)` A variable was set to an invalid value.
`noCreation(11)` An attempt was made to create a variable that does not exist in the MIB.
`inconsistentValue(12)` A MIB variable is in an inconsistent state.
`resourceUnavailable(13)` No system resources are available to perform a `set`.
`commitFailed(14)` An error for `set` failures.

`undoFailed(15)` A `set` failed and the agent was unable to undo previous `sets`.
`authorizationError(16)` An SNMP command could not be authenticated.
`notWritable(17)` A variable did not accept a `set`.
`inconsistentName(18)` It was attempted to `set` a variable, but that attempt failed because the variable was in some kind of inconsistent state.

8.12 Traps

A *trap* is a message that an agent uses to inform the NMS that some abnormal condition or a change has occurred. Figure 8.21 shows the trap–generation sequence.

The trap is generated by the agent and is sent to the trap destination which is the IP address of the NMS. No acknowledgment is sent from the NMS to the agent, so the agent does not know whether the trap is received by the NMS. SNMP uses UDP, and traps are designed to report problems with our network, but traps could be lost. However, in a well–designed network, most traps will reach the NMS.

Listed below are typical messages that a trap might report:

- A network interface on the device has failed.
- A previously failed network interface on the device is now working.
- An incoming call to a modem is unable to establish a connection.
- The fan on a power supply has stopped working.

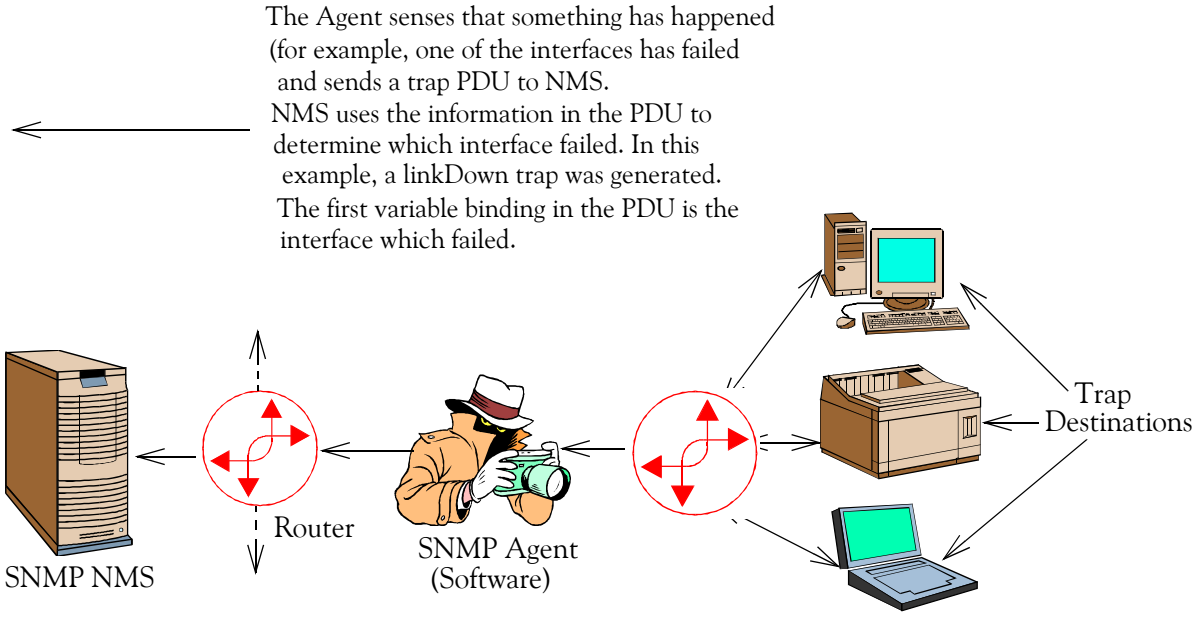


Figure 8.21. Trap generation

8.12.1 Trap Interpretations

When an NMS receives a trap, it must interpret it correctly. This is accomplished by the use of generic trap numbers. The seven generic trap numbers numbered 0 through 6 as shown below.

`coldStart(0)`
This trap indicates that the system is reinitialized and all variables will be reset; that is, `Counters` and `Gauges` will be reset to zero (0). The agent will sense the new hardware that may have been added to the network and will initiate a trap to inform the NMS.

`warmStart(1)`
This trap indicates that the system is reinitialized in such a way that no changes will occur. That is, the agent has reinitialized itself but none of the variables will be reset.

`linkDown(2)`
This trap is sent when an interface on a device goes down. The first variable binding identifies which interface went down.

`linkUp(3)`
This trap is sent when an interface on a device comes back up. The first variable binding identifies which interface came back up.

`authenticationFailure(4)`
This trap indicates that someone has tried to query our agent using an incorrect community string. It is useful in determining if someone is trying to gain unauthorized access to one of our devices.

`egpNeighborLoss(5)`
This trap indicates that an Exterior Gateway Protocol (EGP)* neighbor has gone down. The Trap–PDU of `egpNeighborLoss` contains as the first element of its variable–bindings, the name and value of the `egpNeighAddr` instance for the affected neighbor.

`enterpriseSpecific(6)`
This trap indicates that some enterprise–specific event has occurred. The specific–trap field identifies the particular trap which occurred. SNMP vendors and users define their own traps under the private–enterprise branch of the SMI object tree. For example, when Cisco defines special traps for its private MIBs, it places them all in *(iso.org.dod.internet.private.enterprises.cisco)*, i.e., in its enterprise–specific MIB tree. We are free to define our own enterprise–specific traps; however, we must register our own enterprise number with the Internet Assigned Numbers Authority (IANA).

As we already know, a trap contains information in the form of MIB objects and their values, and these object–value pairs are known as variable bindings. For the generic traps 0 through 5 above,

* *It is recalled from Chapter 3 that EGP is a protocol used for distributing information regarding availability to the routers and gateways that interconnect networks.*

this information is built into the NMS software or trap receiver. However, the variable bindings contained by an enterprise–specific trap (6) are determined by whomever defined the trap. For instance, if a power supply fails, the agent may send a trap to the NMS informing it of the failure. Obviously, this trap will be an enterprise–specific trap defined by the power supply manufacturer.

Traps for the *Relational Database Management System* (RDBMS) do also exist. RFC 1697 is a proposed standard for the RDBMS MIB. One of the traps defined by this MIB is `rdbmsOutOfSpace` as follows:

```
rdbmsOutOfSpace TRAP–TYPE
ENTERPRISE rdbmsTraps
VARIABLFS { rdbmsSrvInfoDiskOutOfSpaces }
DESCRIPTION
"An rdbmsOutOfSpace trap signifies that one of the database servers managed by this agent has been unable to allocate space for one of the databases managed by this agent. Care should be taken to avoid flooding the network with these traps."
::= 2
```

The enterprise is `rdbmsTraps` and the specific trap number is 2. This trap has one variable binding, `rdbmsSrvInfoDiskOutOfSpaces`. This variable is a scalar object and its definition is:

```
rdbmsSrvInfoDiskOutOfSpaces OBJECT–TYPE
SYNTAX Counter
ACCESS read–only
STATUS mandatory
DESCRIPTION
"The total number of times the server has been unable to obtain disk space that it wanted, since server startup. This would be inspected by an agent on receipt of an rdbmsOutOfSpace trap."
:: = { rdbmsSrvInfoEntry 9 }
```

The `DESCRIPTION` text for the `TRAP–TYPE` about "taking care to avoid flooding" provides an important reminder. It indicates that if the `rdbms` is unable to allocate space for the database, the agent will send a trap. If one of the database servers is unable to allocate space, a trap with the same information will be sent to NMS continuously.

Some commercial RDBMS vendors, such as Oracle, provide an SNMP agent with their database engines. Agents such as these typically have functionality above and beyond that found in the RDBMS MIB.

8.12.2 SNMPv2 Notification

Earlier, it was mentioned that SNMP follows the form of the Structure of Management Information (SMI) standard. SMI is a standard dedicated to specifying a machine–independent syntax for

every data type. *Notification* in SMIv2 is equivalent to trap in SMIv1. In SMIv1, the trap is formally specified an ASN.1 macro `TRAP–TYPE`. In SMIv2, notification is specified by an ASN.1 macro `NOTIFICATION–TYPE`.

Referring back to Table 8.6, Page 42, we see that SNMPv1 traps have a different PDU than those of the `get` and `set` PDUs. In SNMPv2, the PDU associated with the trap information is made consistent with the other PDUs. That is, in SNMPv2, the format of the trap PDU shown in Figure 8.20, has been changed to be the same as that of Figure 8.19.

Shown below is an example where a trap is defined using the NOTIFICATION–TYPE macro. The OBJECTS clause is used instead of VARIABLES that defines the variable bindings. In this example we wish to find out what interface is associated with a `linkUp` trap.

```
linkUp NOTIFICATION–TYPE
OBJECTS { ifIndex, ifAdminStatus, ifOperStatus }
STATUS current
DESCRIPTION "A linkUp trap signifies that the SNMP entity, acting
in an agent role, has detected that the ifOperStatus object for
one of its communication links left the down state and transi-
tioned into some other state (but not into the notPresent state).
This other state is indicated by the included value of ifOperSta-
tus."
::= { snmpTraps 4 }
```

The object identifier for this trap is 1.3.6.1.6.3.1.1.5.4, or *iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps .linkUp*.

8.12.3 SNMPv2 inform

SNMPv2 provides an `inform` capability to allow for NMS–to–NMS communication. When an `inform` is sent from one NMS to another, the receiving NMS sends a response to the sending NMS to acknowledge receipt of the message. We can use an SNMP `inform` to send SNMPv2 traps from an agent to an NMS. In this case, the agent will be notified by the NMS that the trap has been received.

8.12.4 SNMPv2 report

The `report` operation was intended for SNMPv2 but it was never implemented. However, it is used in SNMPv3 to enable SNMP engines to communicate with each other and report problems with processing SNMP messages. SNMP engines are discussed in Subsection 8.14.2.

8.13 Using SNMP with Windows

Windows Vista and Windows Server 2008 support SNMPv1 and SNMPv2c. Considerable information about the SNMP service in Windows can be obtained by clicking on Start, Help and Support Center, and typing SNMP. Overviews, articles, and tutorials can be found there.

On computers running Microsoft Windows XP/Windows 2000/Windows NT, the SNMP agent is implemented by the SNMP service (SNMP.EXE). The SNMP manager is typically a third-party SNMP management console application. The management console application does not need to run on the same host as the SNMP agent. To use the information the Microsoft SNMP service provides, the user needs at least one SNMP management console application. The system includes libraries that support SNMP management console applications, but it does not include an SNMP management console application at this time.

SNMP supports the use of IPv6 starting with Windows Vista. However, SNMP supports IPv6 only for networks running Windows Server 2008 and Windows Vista. This is because SNMP requires the updated protocol stack available in these operating systems for its IPv6 support. Unless the network is solely a Windows Server 2008 network, IPv6 communications will fail, even if an IPv6 protocol stack is separately installed on those computers that run earlier versions of Windows. For example, SNMP agents that run on Windows Server 2003, or Windows XP, Windows Vista, or Windows 2000, respond only to queries that are made to their IPv4 addresses.

The Microsoft® Windows® SNMP Application Programming Interface (the WinSNMP API) versions 1.1a and 2.0 allows the user to develop SNMP-based network management applications that execute in the Windows® 2000 operating environment or later. WinSNMP has been jointly developed with the cooperation, input, and support from several companies, associations and individuals.

The first part of this overview provides information about the WinSNMP 2.0 Addendum, SNMP versions, and a list of the relevant Requests for Comments (RFCs). It also describes the WinSNMP model, and the components and features of the Microsoft WinSNMP implementation. It also provides information about data management and communications concepts you need to program in the WinSNMP environment.

Below is a list of the WinSNMP related programming tasks:

Opening and closing a WinSNMP application

The WinSNMP application must call the **SnmpStartup** function successfully before it calls any other WinSNMP function. The **SnmpStartup** function enables the Microsoft WinSNMP implementation to perform initialization procedures. The function also returns to the application the version of the WinSNMP API that the implementation supports, the level of SNMP communications it supports, and the implementation's default translation and retransmission modes.

The WinSNMP application must call the **SnmpCleanup** function when the application no longer requires the implementation's services. Even though **SnmpCleanup** enables the implementation

to deallocate all resources allocated to the application, it is recommended that the application first call the **SnmpClose** function once for each open WinSNMP session, to maximize the implementation's performance. The WinSNMP application must call **SnmpCleanup** as the last WinSNMP function before it terminates.

Opening and closing a WinSNMP session

To open a session, an application calls the **SnmpCreateSession** function. If the function completes successfully, the Microsoft WinSNMP implementation opens a session, and the function returns a session identifier in the form of an **HSNMP_SESSION** handle. All WinSNMP functions that return handle variables include the session identifier as an input parameter. This enables the implementation to use the handle to efficiently manage resources at the session level.

An application can have multiple sessions open at one time. Multiple sessions within an application can share handle variables. If the implementation cannot open a session because of resource limitations, it returns SNMPAPI_FAILURE when the application calls **SnmpCreateSession**. If the application subsequently calls the **SnmpGetLastError** function, it returns SNMPAPI_ALLOC_ERROR. A call to the **SnmpClose** function enables the implementation to free any remaining resources and to close the session.

Managing traps and notifications

The WinSNMP application must register to receive traps and notifications by calling the **SnmpRegister** function with SNMPAPI_ON. The application can unregister and disable traps and notifications by calling the function with SNMPAPI_OFF.

Several options are available when the application calls **SnmpRegister**. The application can register or unregister for the following traps and notifications:

- One type of trap or notification
- All traps and notifications
- All sources of trap and notification requests
- Traps and notifications from all management entities
- Traps and notifications for every context

To register and receive a predefined trap or notification type, the application must define an object identifier (an **smiOID** structure) for each predefined type. The structure must contain a pattern–matching sequence for the type of trap or notification. RFC 1907, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)," defines trap and notification object identifiers.

To retrieve outstanding trap data and notifications for a WinSNMP session, a WinSNMP application must call the **SnmpRecvMsg** function with the session handle returned by the **SnmpCreateSession** function.

Working with variable binding lists

A *variable binding* is the pairing of an SNMP object instance name with an associated value. A *variable binding list* is a series of variable binding entries. In WinSNMP, a protocol data unit (PDU) includes a variable binding list.

The details of the variable binding list structure are restricted to the Microsoft WinSNMP implementation. A WinSNMP application can access a variable binding list with a handle of type **HSNMP_VBL**. More information, is provided in Resource Handle Objects.

The WinSNMP application can construct and manipulate variable binding lists, and include them in PDUs. To perform these operations, the application uses the WinSNMP variable binding functions.

A new variable binding list is created with the **SnmpCreateVbl** function. If the WinSNMP application specifies a variable name and a value, the function creates the list and adds the name and value as the first entry in the list. If the application specifies NULL for the variable name, the function creates an empty list.

The **SnmpDuplicateVbl** function is used copy a variable binding list. The function creates a new variable binding list and initializes the new list with a copy of the data in the source variable binding list.

The **SnmpCreateVbl** function and the **SnmpDuplicateVbl** function allocate any necessary memory for the new variable binding list. The WinSNMP application must release the resources associated with these lists. It is recommended that the application do this by matching each call to **SnmpCreateVbl** and **SnmpDuplicateVbl** with a corresponding call to the **SnmpFreeVbl** function when it is appropriate to free the allocated memory.

The **SnmpGetVb** function retrieves variable binding information from a variable binding list. The function retrieves the variable name and the variable's associated value from the variable binding entry specified by the WinSNMP application.

To update variable binding entries in a variable binding list, the **SnmpSetVb** function can be called. The **SnmpSetVb** function also appends new variable binding entries to an existing variable binding list.

The WinSNMP application must call the **SnmpDeleteVb** function to remove entries from a variable binding list.

To retrieve, modify or delete a variable binding entry, the WinSNMP application must specify the position of the entry in the variable binding list.

A call to the **SnmpSetPduData** function associates a variable binding list with a PDU. A call to the **SnmpGetPduData** function retrieves a variable binding list from a PDU. An individual variable binding is not directly associated with a PDU, but it is indirectly associated through its inclusion in a variable binding list.

Working with protocol data units

The Simple Network Management Protocol (SNMP) sends operation requests and responses as SNMP messages. An SNMP message is an SNMP protocol data unit (PDU) plus additional message header elements defined by the relevant RFC. A PDU includes a variable binding list.

The structure of a PDU is restricted to the Microsoft WinSNMP implementation. A WinSNMP application can access a PDU with a handle of the type **HSNMP_PDU**. The WinSNMP application must create a PDU before it calls the **SnmpSendMsg** function or the **SnmpEncodeMsg** function.

The application can extract and update the data elements of a PDU, and release resources allocated for PDUs. To perform these operations, the application uses the WinSNMP PDU functions. The following table lists topics that discuss working with PDUs in the WinSNMP programming environment.

To create and initialize a PDU a WinSNMP application calls the **SnmpCreatePdu** function. The application must call **SnmpCreatePdu** before it calls the **SnmpSendMsg** function to request that the Microsoft WinSNMP implementation transmit a PDU. The application must also call **SnmpCreatePdu** before it calls the **SnmpEncodeMsg** function to request encoding of an SNMP message. The application must call the **SnmpFreePdu** function to release the resources that the **SnmpCreatePdu** function allocates for new PDUs.

A WinSNMP application can retrieve and update selected PDU fields by using the **SnmpGetPduData** and the **SnmpSetPduData** functions. The application can retrieve the PDU type, request identifier, error status, and error index fields from a specific PDU. It can also retrieve the handle to the variable binding list. The application can update the PDU_type and request_id fields. If the PDU type is equal to SNMP_PDU_GETBULK, the application can also update the non_repeaters and the max_repetitions fields of the PDU.

The **SnmpDuplicatePdu** function duplicates a PDU, allocating any necessary memory. To release resources allocated by **SnmpDuplicatePdu** for a new PDU, a WinSNMP application must call the **SnmpFreePdu** function.

When the WinSNMP application calls the **SnmpSendMsg** function or the **SnmpEncodeMsg** function, the Microsoft WinSNMP implementation verifies the validity of the PDU and the other function parameters. The value of one PDU data component (or field) can be valid individually, but it may be invalid in combination with values for other fields. For example, unless the PDU_type field of the PDU is SNMP_PDU_GETBULK or SNMP_PDU_RESPONSE, both the error_status and error_index fields must be equal to zero. Any other value combination constitutes an invalid PDU.

The implementation rejects invalid PDUs and returns the error status SNMPAPI_FAILURE. It sets an extended error code equal to SNMPAPI_PDU_INVALID.

The order in which the WinSNMP application receives SNMP responses may not match the

order in which the application submits SNMP operation requests. To match the response with the request, the application must use the request identifier field (the **request_id**) of the response. The **request_id** field is a unique numeric value that identifies the PDU. Applications can assign request identifiers by calling the **SnmpCreatePdu** function or the **SnmpSetPduData** function. The **SnmpGetPduData** function can be called to retrieve a PDU's **request_id**.

Sending SNMP messages

A WinSNMP application initiates a transmission request by sending an SNMP message. SNMP messages include an SNMP protocol data unit as discussed above. A WinSNMP application must call the **SnmpSendMsg** function to request that the Microsoft WinSNMP implementation transmit the PDU, with the other required message elements defined by the relevant RFC. In addition to the destination entity, the application must specify the source entity and a context for the request. The **SnmpSendMsg** function executes asynchronously.

The WinSNMP application must call the **SnmpRecvMsg** function to retrieve the response to an **SnmpSendMsg** request. A WinSNMP application initiates a transmission request by sending an SNMP message. SNMP messages include an SNMP protocol data unit. For more information, see Working with Protocol Data Units.

A WinSNMP application must call the **SnmpSendMsg** function to request that the Microsoft WinSNMP implementation transmit the PDU, with the other required message elements defined by the relevant RFC. In addition to the destination entity, the application must specify the source entity and a context for the request. The **SnmpSendMsg** function executes asynchronously.
The WinSNMP application must call the **SnmpRecvMsg** function to retrieve the response to an **SnmpSendMsg** request. The implementation verifies the validity of the PDU and the other message elements when an application calls **SnmpSendMsg**.The implementation verifies the validity of the PDU and the other message elements when an application calls **SnmpSendMsg**.

Receiving SNMP messages

The WinSNMP application must call the **SnmpRecvMsg** function to retrieve the response to an **SnmpSendMsg** request. The **SnmpCreateSession** function passes an application window handle and a notification message identifier to the Microsoft WinSNMP implementation. When the application window receives this message, it signals the application to call the **SnmpRecvMsg** function using the session handle returned by **SnmpCreateSession**.
The **SnmpRecvMsg** function returns two entity handles, a context handle, and the handle to a PDU. It is recommended that the WinSNMP application free these resources using the **SnmpFreeEntity**, **SnmpFreeContext**, and **SnmpFreePdu** functions. For additional information about managing the time between a call to the **SnmpSendMsg** function and the receipt of the corresponding response, see About Retransmission. For additional information about using the **request_id** PDU field to match a response PDU with its request PDU, see Matching Response and Request PDUs.

Managing object identifiers

The WinSNMP API provides several WinSNMP utility functions that simplify the manipulation of object identifiers for WinSNMP applications. The **SnmpOidToStr** function converts the internal binary representation of an object identifier to its dotted numeric string format. When you call **SnmpOidToStr**, specify a string buffer of MAXOBJIDSTRSIZE length (1408 bytes) to ensure that the output buffer is large enough to hold the converted string. To convert an object identifier from the dotted numeric string format to its internal binary representation, call the **SnmpStrToOid** function.

To copy an SNMP object identifier call the **SnmpOidCopy** function. This function allocates any necessary memory for the new object identifier. A WinSNMP application must call the **SnmpFreeDescriptor** function to free resources allocated for the **ptr** member of the **smiOID** structure specified by both the **SnmpStrToOid** and the **SnmpOidCopy** functions.

The **SnmpOidCompare** function compares two SNMP object identifiers. The WinSNMP application can specify the number of subidentifiers to compare. Call **SnmpOidCompare** to determine whether two object identifiers have common prefixes. For additional information about managing the memory allocated for object identifiers, see Allocating WinSNMP Memory Objects.

Freeing WinSNMP Descriptors

The WinSNMP programming environment assigns the deallocation of descriptor resources to the WinSNMP implementation or the WinSNMP application, depending on which component allocates the memory for the descriptor. To free the resources for an **smiOID** or an **smiOCTETS** descriptor, the following rules apply:

- For input parameters

  Because the WinSNMP application allocates the memory for input objects with variable lengths, the application must free that memory using an appropriate function. For example, if the application allocated the resources with a call to the **GlobalAlloc** function, it should use the **GlobalFree** function to deallocate the resources. If the application allocated the resources with a call to the **HeapAlloc** function, it should call the **HeapFree** function.

- For output parameters

  A call to any of the following functions results in the implementation allocating memory for an **smiOID** or an **smiOCTETS** descriptor: **SnmpGetVb**, **SnmpEncodeMsg**, **SnmpOidCopy**, **SnmpContextToStr**, and **SnmpStrToOid**. Because the implementation allocates the memory for these output objects, the application must call the **SnmpFreeDescriptor** function to deallocate the resources. This function enables the implementation to free the memory allocated for the **ptr** member of these structures.

To free the resources for an **smiVALUE** structure, a WinSNMP application must check the **syn-**

tax member of an **smiVALUE** structure to correctly evaluate the **value** member of the structure. If the **syntax** member indicates that the **value** member is an **smiOCTETS** or an **smiOID** descriptor, and the implementation allocated the resources for the descriptor, the application must call **SnmpFreeDescriptor**. This enables the implementation to free the memory. If the application allocated the resources, it must free the memory using an appropriate function, as indicated earlier.

Setting the Entity and Context Translation Mode

The WinSNMP application can specify the interpretation and translation of entity and context parameters by setting the entity and context translation mode. The Microsoft WinSNMP implementation stores the mode in a database. The setting of the entity and context translation mode determines the manner in which the **SnmpStrToEntity** function and the **SnmpStrToContext** function interpret input strings. The setting also determines the type of output string that the **SnmpEntityToStr** and the **SnmpContextToStr** functions return. For more information, see Support for IPX Address Strings in WinSNMP.

The implementation returns the current default entity and context translation mode in the *nTranslateMode* parameter of the **SnmpStartup** function. To retrieve the current entity and context translation mode in effect for the implementation, an application can call the **SnmpGetTranslateMode** function at any time. The valid entity and context translation modes are shown in Table 8.7.

TABLE 8.7 Valid entity and context translation modes for WinSNMP applications

Mode	Function
SNMPAPI_TRANSLATED	The implementation uses its database to translate user–friendly names for SNMP entities and managed objects. The implementation translates them into their SNMPv1 or SNMPv2C components.
SNMPAPI_UNTRANSLATED_V1	The implementation interprets SNMP entity parameters as literal SNMP transport addresses, and context parameters as literal SNMP community strings. For SNMPv2 destination entities, the implementation creates outgoing SNMP messages that contain a value of zero in the version field.
SNMPAPI_UNTRANSLATED_V2	The implementation interprets SNMP entity parameters as SNMP transport addresses, and context parameters as literal SNMP community strings. For SNMPv2 destination entities, the implementation creates outgoing SNMP messages that contain a value of 1 in the version field.

The implementation tries to associate resources in its database with the literal transport address of the management entity. To change the entity and context translation mode setting a WinSNMP application must call the **SnmpSetTranslateMode** function. If the requested translation mode is invalid, the function fails, and **SnmpGetLastError** returns the error code SNMPAPI_MODE_INVALID.

Managing the Retransmission Policy

The WinSNMP application can request that the Microsoft WinSNMP implementation execute the application's retransmission policy. When the implementation manages retransmission, it uses the time–out period and the retry count values in its database. The implementation identifies the default retransmission mode in a return value from the **SnmpStartup** function during initialization. The mode can be one of the following values shown in Table 8.8

TABLE 8.8 Mode for executing the application retransmission policy in WinSNMP

Value	Function
SNMPAPI_ON	The implementation is executing the application's retransmission policy.
SNMPAPI_OFF	The implementation is not executing the application's retransmission policy.

A WinSNMP application can retrieve at any time the current retransmission mode in effect for the implementation by calling the **SnmpGetRetransmitMode** function. The WinSNMP API provides other database functions that simplify management of the retransmission policy. At any time during program execution, the WinSNMP application can adjust execution of the policy by performing one of the following steps:

- Request that the implementation start or stop executing the retransmission policy by calling the **SnmpSetRetransmitMode** function. An application can set the retransmission mode with a call to the **SnmpSetRetransmitMode** function. The new retransmission mode applies to subsequent calls to the **SnmpSendMsg** function.

  When the application calls **SnmpSetRetransmitMode** with the retransmission mode value SNMPAPI_ON, the Microsoft WinSNMP implementation begins execution of the application's retransmission policy. The new retransmission mode does not affect outstanding SNMP messages. An outstanding message is one that has no response at the time the application changes the retransmission mode.

  When the WinSNMP application calls the **SnmpSetRetransmitMode** function with the retransmission mode value SNMPAPI_OFF, the implementation stops executing the retransmission policy. The implementation cancels retransmission attempts for outstanding SNMP messages. This is because it may not be possible for the implementation to handle all outstanding SNMP requests and operations plus new requests, before an application time–out or retry counter signals an event.

- Modify the time–out period and retry count values in the implementation's database. The Microsoft WinSNMP implementation provides retransmission policy support by storing a time–out value and a retry count for the WinSNMP application in a database. The implementation stores values for individual destination entities. The implementation initially supplies default values for these elements, but an application can add or modify values for individual entities.

A call to the **SnmpGetTimeout** and **SnmpGetRetry** functions returns the time–out and retry count values for a specific destination entity. To change the time–out value, a WinSNMP application must call the **SnmpSetTimeout** function. To change the retry count value the application must call the **SnmpSetRetry** function. The updated settings affect new SNMP message requests to the destination entity.

- Call the **SnmpCancelMsg** function to cancel the retransmission cycle and release internal data structures associated with a single SNMP message request. If there is no response to a communication request within the time–out period specified for a destination entity, and if retransmissions are specified for the entity, the Microsoft WinSNMP implementation retransmits the request. A call to the **SnmpCancelMsg** function can cancel this retransmission cycle and release internal data structures associated with the message request.
- It is possible for a destination entity to receive an SNMP message that has been canceled by a call to the **SnmpCancelMsg** function. It is also possible that a destination entity can respond to a canceled SNMP message. This is because transaction queuing occurs at multiple levels. However, once a message has been canceled by a call to **SnmpCancelMsg**, the Microsoft WinSNMP implementation will not retransmit the message, submit a response PDU, or send a time–out notification to the application for that message.

The application can execute its own retransmission policy. In this case, execution may or may not be based on the values in the database.

Writing WinSNMP Applications with Multiple Threads

A *thread* is the entity within a process that can be scheduled for execution. All threads of a process share its virtual address space and system resources. Each process is started with a single thread, but can create additional threads from any of its threads.The Microsoft WinSNMP implementation ensures that the WinSNMP operations of one process do not modify the WinSNMP settings of another process. A WinSNMP application with multiple threads must ensure that WinSNMP operations that set application–level parameters are thread–safe. The functions that set application–level parameters are **SnmpSetTranslateMode** and **SnmpSetRetransmitMode**. These functions modify settings for the entity and context translation mode and the retransmission mode.

The **CreateThread** function creates a new thread for a process. The creating thread must specify the starting address of the code that the new thread is to execute. Typically, the starting address is the name of a function defined in the program code (for more information, see **ThreadProc**). This function takes a single parameter and returns a **DWORD** value. A process can have multiple threads simultaneously executing the same function.

The calling thread uses the **WaitForMultipleObjects** function to persist until all worker threads have terminated. The calling thread blocks while it is waiting; to continue processing, a calling thread would use **WaitForSingleObject** and wait for each worker thread to signal its wait object. If the handle to a worker thread is closed before it terminated, this will not terminate the worker

thread. However, the handle will be unavailable for use in subsequent function calls.

The following is a simple example that demonstrates how to create a new thread that executes the locally defined function, MyThreadFunction.

```
#include <windows.h>
#include <tchar.h>
#include <strsafe.h>

#define MAX_THREADS 3
#define BUF_SIZE 255

DWORD WINAPI MyThreadFunction( LPVOID lpParam );
void ErrorHandler(LPTSTR lpszFunction);

// Sample custom data structure for threads to use.
// This is passed by a void pointer so it can be any data type
// that can be passed using a single void pointer (LPVOID).
typedef struct MyData
{
    int val1;
    int val2;
}
MYDATA, *PMYDATA;

int _tmain()
{
    PMYDATA pDataArray[MAX_THREADS];
    DWORD   dwThreadIdArray[MAX_THREADS];
    HANDLE  hThreadArray[MAX_THREADS];

    // Create MAX_THREADS worker threads.

    for( int i=0; i<MAX_THREADS; i++ )
    {
        // Allocate memory for thread data.

          pDataArray[i] = (PMYDATA) HeapAlloc(GetProcessHeap(),
HEAP_ZERO_MEMORY,
                sizeof(MYDATA));

        if( pDataArray[i] == NULL )
        {
          // If the array allocation fails, the system is out of memory
           // so there is no point in trying to print an error message.
           // Just terminate execution.
            ExitProcess(2);
        }
```

```
        // Generate unique data for each thread to work with.

        pDataArray[i]->val1 = i;
        pDataArray[i]->val2 = i+100;

        // Create the thread to begin execution on its own.

        hThreadArray[i] = CreateThread(
            NULL,                   // default security attributes
            0,                      // use default stack size
            MyThreadFunction,       // thread function name
            pDataArray[i],          // argument to thread function
            0,                      // use default creation flags
            &dwThreadIdArray[i]);   // returns the thread identifier

        // Check the return value for success.
        // If CreateThread fails, terminate execution.
        // This will automatically clean up threads and memory.

        if (hThreadArray[i] == NULL)
        {
           ErrorHandler(TEXT("CreateThread"));
           ExitProcess(3);
        }
    } // End of main thread creation loop.

    // Wait until all threads have terminated.

    WaitForMultipleObjects(MAX_THREADS, hThreadArray, TRUE, INFINITE);

    // Close all thread handles and free memory allocations.

    for(int i=0; i<MAX_THREADS; i++)
    {
        CloseHandle(hThreadArray[i]);
        if(pDataArray[i] != NULL)
        {
            HeapFree(GetProcessHeap(), 0, pDataArray[i]);
            pDataArray[i] = NULL;    // Ensure address is not reused.
        }
    }

    return 0;
}
```

```
DWORD WINAPI MyThreadFunction( LPVOID lpParam )
{
    HANDLE hStdout;
    PMYDATA pDataArray;

    TCHAR msgBuf[BUF_SIZE];
    size_t cchStringSize;
    DWORD dwChars;

    // Make sure there is a console to receive output results.

    hStdout = GetStdHandle(STD_OUTPUT_HANDLE);
    if( hStdout == INVALID_HANDLE_VALUE )
        return 1;

    // Cast the parameter to the correct data type.
    // The pointer is known to be valid because
    // it was checked for NULL before the thread was created.

    pDataArray = (PMYDATA)lpParam;

    // Print the parameter values using thread-safe functions.

    StringCchPrintf(msgBuf, BUF_SIZE, TEXT("Parameters = %d, %d\n"),
        pDataArray->val1, pDataArray->val2);
    StringCchLength(msgBuf, BUF_SIZE, &cchStringSize);
     WriteConsole(hStdout, msgBuf, (DWORD)cchStringSize, &dwChars,
NULL);
    return 0;
}

void ErrorHandler(LPTSTR lpszFunction)
{
    // Retrieve the system error message for the last-error code.

    LPVOID lpMsgBuf;
    LPVOID lpDisplayBuf;
    DWORD dw = GetLastError();

    FormatMessage(
        FORMAT_MESSAGE_ALLOCATE_BUFFER |
        FORMAT_MESSAGE_FROM_SYSTEM |
        FORMAT_MESSAGE_IGNORE_INSERTS,
        NULL,
        dw,
        MAKELANGID(LANG_NEUTRAL, SUBLANG_DEFAULT),
        (LPTSTR) &lpMsgBuf,
        0, NULL );

    // Display the error message.
```

```
    lpDisplayBuf = (LPVOID)LocalAlloc(LMEM_ZEROINIT,
         (lstrlen((LPCTSTR)lpMsgBuf)+lstrlen((LPCTSTR)lpszFunc-
tion)+40)*sizeof(TCHAR));
    StringCchPrintf((LPTSTR)lpDisplayBuf,
        LocalSize(lpDisplayBuf) / sizeof(TCHAR),
        TEXT("%s failed with error %d: %s"),
        lpszFunction, dw, lpMsgBuf);
    MessageBox(NULL, (LPCTSTR)lpDisplayBuf, TEXT("Error"), MB_OK);

    // Free the error-handling buffer allocations.

    LocalFree(lpMsgBuf);
    LocalFree(lpDisplayBuf);
}
```

For more information, refer to Thread Security and Access Rights, http://msdn.microsoft.com/en-us/library/ms686769(VS.85).aspx

Registering an SNMP Agent Application

In addition to SNMP manager operations, the WinSNMP API version 2.0 also supports SNMP agent operations. To register a WinSNMP application as an SNMP agent, the application can call the **SnmpListen** function. This function informs the Microsoft WinSNMP implementation that an SNMP entity will be acting in the role of an SNMP agent. The application can also call **SnmpListen** to inform the implementation when it will no longer be acting as an agent. If an application calls the **SnmpListen** function and passes the value SNMPAPI_ON in the *lStatus* parameter, the following actions occur:

- The entity that will be functioning in an SNMP agent role binds to its assigned port, and "listens" for incoming SNMP message requests.
- The agent uses application-specific logic to process each SNMP request.
- The agent forms appropriate responses to each request.
- The agent transmits the response to the requesting entity by calling the **SnmpSendMsg** function.

When the agent calls **SnmpSendMsg**, it specifies the address of the agent in the *srcEntity* parameter, and the address of the remote manager entity in the *dstEntity* parameter. (These values are the reverse of the values the agent entity received in these parameters when it called the **SnmpRecvMsg** function to retrieve an SNMP request.)

For the Microsoft Windows Server 2003, Microsoft recommends performing the following tasks:

- Refer to the Microsoft Windows Resource Kits Web site.(http://www.microsoft.com/) and refer to "Simple Network Management Protocol." Follow the SNMP distributed security model to organize SNMP communities by functional organization.

- The default Security tab settings are one community name, public, and **Accept SNMP packets from any host**. These settings should be changed to a specific community name of our choice and **Accept SNMP packets from these hosts**, with a list of hosts. The settings should be monitored and updated on an ongoing basis.
- Take advantage of SNMP security checking by configuring authentication traps on all SNMP agents.
- If it is desired to monitor specific components, such as Dynamic Host Configuration Protocol (DHCP) or Windows Internet Name Service (WINS), it should be verified that these services have been successfully installed and configured.

Microsoft also recommends that the SNMP service is implemented with the following checklist:

- Obtain, install, and configure the SNMP management software such as Castle Rock's SNMPc.
- Gather information required to implement SNNP on our network. Requirements include contact persons (administrator), physical computer location, configured SNMP community names, and IP or IPX addresses, or computer names of SNMP management systems on our network.
- Install SNMP on the computer.
- Configure SNMP agent properties.
- If there is an additional TCP/IP service in the network, such as a bridge or router, you should consult RFC 1213 for additional configuration information before proceeding.
- Configure trap destinations.
- Configure SNMP security properties.

When the SNMP service is installed, or selected from the list of installed services, a new window should appear. This window is broken up into three tabs: `Agent, Traps`, and `Security`. In the `Agent` tab, you should configure the Contact (`sysContact`), Location (`sysLocation`), and Service (`sysServices`). The latter is defined by RFC 1213 as follows:

```
sysServices OBJECT–TYPE

SYNTAX INTEGER (0. .127)

ACCESS read–only

STATUS mandatory

DESCRIPTION

"A value which indicates the set of services that this entity
primarily offers.
```

The value is a sum. This sum initially takes the value zero. Then, for each layer L, in the range 1 through 7, that this node performs transactions for, 2^{L-1} is added to the sum. For example, a node which performs primarily routing functions would have a value of 4 (2^{3-1}).In contrast, a node which is a host offering application services would have a value of 72 ($2^{4-1} + 2^{7-1}$). Note that in the context of the Internet suite of protocols. values should be calculated accordingly:

layer functionality

1. physical (e.g.,repeaters)

2. datalink/sUbnetwork (e.g., bridges)

3. internet (e.g.,IP gateways)

4. end–to–end (e.g., IP hosts)

7. applications (e.g. , mail relays)

For systems including OSI protocols, layers 5 and 6 may also be counted."
::= { system 7 }

The Agent tab provides a checkbox for each of the seven ISO layers `sysServices` represents. The `DESCRIPTION` text in the RFC gives a brief definition for each layer. If you so desire, you can check each service that is offered by Windows.

Next, select the Traps tab; this allows us to configure the community in which the SNMP agent sends traps. In the "Community Name" box, enter the case–sensitive community name of your choice. Click the "Add" button to the left and then add up to five trap destinations for this community name. The trap destinations can be IPX addresses, IP addresses, or DNS names.

Now, click the Security tab. The top of this tab gives you the option to send authentication–error traps. It's a good idea to check this box, since it can help us detect intruders. The "Accepted Community Names" box lists all the community names to which the agent will respond. Click "Add" and enter your community name of choice. Configuring these communities is important, since someone with the correct community string can invalidate our system. If you leave this box blank, the agent will respond to all requests. The bottom half of the Security menu allows us to specify whether the agent will accept SNMP packets from any host or only from a specified list. To create a list, which is strongly recommended, click “Only Accept SNMP Packets from These Hosts" and then use the "Add" button to add the host names or addresses of our monitoring stations. The options for the hosts are the same as for trap destinations; IPX addresses, IP addresses, and DNS names are acceptable.

Finally, click "OK" to save your changes and update the Windows registry. If at any time you make a mistake, click "Cancel." This aborts the configuration process; no changes will be made to your registry.

8.14 SNMPv3

The essential characteristics of SNMPv3 are:

- It allows SNMPv1, SNMPv2, and SNMPv3 to coexist in a single management entity
- Addition of security features for SNMP management
- The vast amount of SNMP documentation is organized into a document architecture
- In SNMPv3 managers and agents are now referred to as SNMP entities

The following is the main list of RFCs that define SNMPv3.

- RFC 2570 Introduction to SNMPv3
- RFC 2571 Architecture for SNMP Frameworks
- RFC 2572 Message Processing and Dispatching
- RFC 2573 SNMP Applications
- RFC 2574 User–based Security Model
- RFC 2575 View–based Access Control Model
- RFC 2576 Coexistence Between SNMP Versions

8.14.1 Documentation Overview

Figure 8.22 shows the set of documents that fit within the SNMP architecture.

Document Roadmap

One or more documents may be written to describe how sets of documents taken together form specific Frameworks. The configuration of document sets might change over time, so the "road map" should be maintained in a document separate from the standards documents themselves. An example of such a roadmap is "Introduction to Version 3 of the Internet–standard Network Management Framework" [RFC 2570].

Applicability Statement

SNMP is used in networks that vary widely in size and complexity, by organizations that vary widely in their requirements of management. Some models will be designed to address specific problems of management, such as message security. One or more documents may be written to describe the environments to which certain versions of SNMP or models within SNMP would be appropriately applied, and those to which a given model might be inappropriately applied.

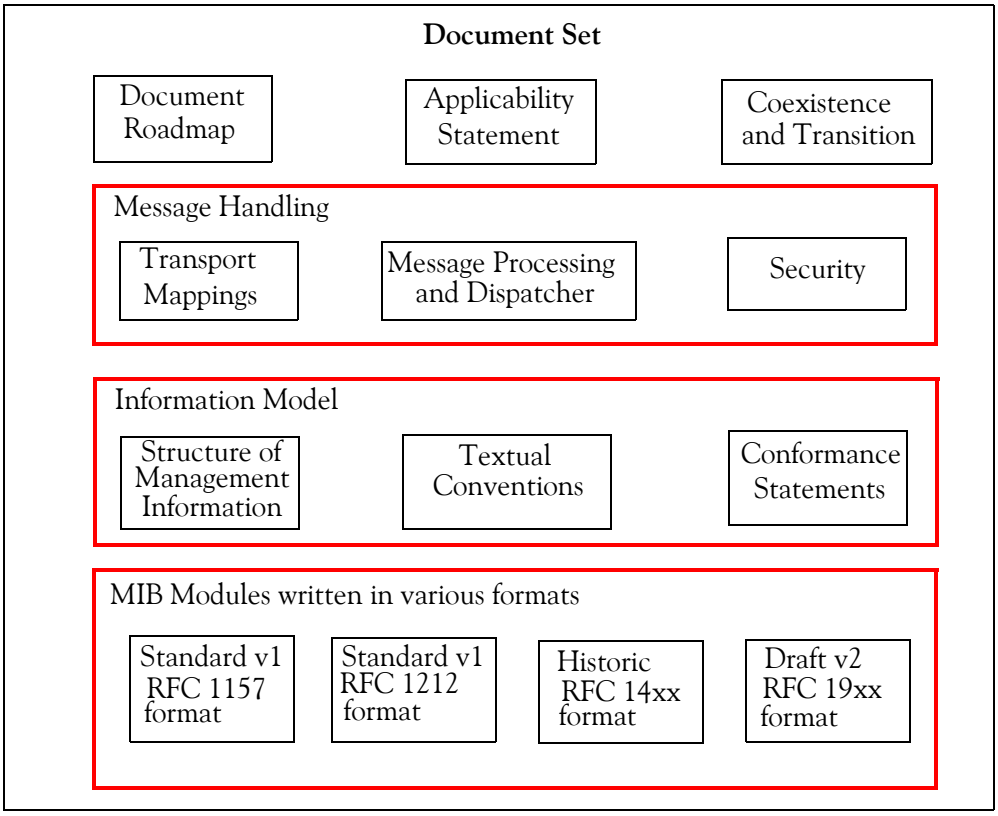


Figure 8.22. Set of documents within the SNMP architecture

Coexistence and Transition

The purpose of an evolutionary architecture is to permit new models to replace or supplement existing models. The interactions between models could result in incompatibilities, security "holes", and other undesirable effects. The purpose of Coexistence documents is to detail recognized anomalies and to describe required and recommended behaviors for resolving the interactions between models within the architecture. Coexistence documents may be prepared separately from model definition documents, to describe and resolve interaction anomalies between a model definition and one or more other model definitions. Additionally, recommendations for transitions between models may also be described, either in a coexistence document or in a separate document. One such coexistence document is [SNMP–COEX], "Coexistence between Version 1, Version 2, and Version 3 of the Internet–standard Network Management Framework".

Transport Mappings

SNMP messages are sent over various transports. It is the purpose of Transport Mapping documents to define how the mapping between SNMP and the transport is done.

Message Processing

A Message Processing Model document defines a message format, which is typically identified by

a version field in an SNMP message header. The document may also define a MIB module for use in message processing and for instrumentation of version–specific interactions. An SNMP engine, to be discussed on Page 8–68, includes one or more Message Processing Models, and thus may support sending and receiving multiple versions of SNMP messages.

Security

Some environments require secure protocol interactions. Security is normally applied at two different stages:

- In the transmission/receipt of messages
- In the processing of the contents of messages.

For purposes of this document, "security" refers to message–level security; "access control" refers to the security applied to protocol operations.

Authentication, encryption, and timeliness checking are common functions of message level security. SNMPv3 encrypts messages using the CBC – DES encryption.*

A security document describes a Security Model, the threats against which the model protects, the goals of the Security Model, the protocols which it uses to meet those goals, and it may define a MIB module to describe the data used during processing, and to allow the remote configuration of message–level security parameters, such as keys.

An SNMP engine, discussed on Page 8–68, may support multiple Security Models concurrently.

Access Control

During processing, it may be required to control access to managed objects for operations. An Access Control Model defines mechanisms to determine whether access to a managed object should be allowed. An Access Control Model may define a MIB module used during processing and to allow the remote configuration of access control policies.

---

* *Cipher Block Chaining (CBC) is the most commonly used mode of operation for a block cipher. Prior to encryption, each block of plaintext is XOR–ed with the prior block of ciphertext. After decryption, the output of the cipher must then be XOR–ed with the previous ciphertext to recover the original plaintext. The first block of plaintext is XOR–ed with an initialization vector which is usually a block of random bits transmitted in the clear.*

The most important symmetric (meaning the same key is used for both encryption and decryption) algorithms are block ciphers. The general operation of all block ciphers is the same – a given number of bits of plaintext (a block) is encrypted into a block of ciphertext of the same size. Thus, all block ciphers have a natural block size – the number of bits they encrypt in a single operation.

Data Encryption Standard (DES) is a type of Substitution–Permutation Network (SPN) cipher. DES uses a 56–bit key which can be broken using brute–force methods, that is, a trivial but very general problem–solving technique, that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

Protocol Operations

SNMP messages encapsulate an SNMP Protocol Data Unit (PDU). SNMP PDUs define the operations performed by the receiving SNMP engine. It is the purpose of a Protocol Operations document to define the operations of the protocol with respect to the processing of the PDUs. Every PDU belongs to one or more of the PDU classes defined below:

- **Read Class**
  The Read Class contains protocol operations that retrieve management information. For example, RFC 1905 defines the following protocol operations for the Read Class: `GetRequest`–PDU, `GetNextRequest`–PDU, and `GetBulkRequest`–PDU.

- **Write Class**
  The Write Class contains protocol operations which attempt to modify management information. For example, RFC 1905 defines the protocol operation for the Write Class: `SetRequest`–PDU.

- **Response Class**
  The Response Class contains protocol operations which are sent in response to a previous request. For example, RFC 1905 defines the Response Class: `Response`–PDU, `Report`–PDU.

- **Notification Class**
  The Notification Class contains protocol operations which send a notification to a notification receiver application. For example, RFC 1905 defines the operations for the Notification Class: `Trapv2`–PDU, `InformRequest`–PDU.

- **Internal Class**
  The Internal Class contains protocol operations which are exchanged internally between SNMP engines. For example, RFC 1905 defines the following operations for the Internal Class: `Report`–PDU.

The preceding five classifications are based on the functional properties of a PDU. It is also useful to classify PDUs based on whether a response is expected:

- **Confirmed Class**
  The Confirmed Class contains all protocol operations which cause the receiving SNMP engine to send back a response. For example, RFC 1905 defines the operations for the Confirmed Class: `GetRequest`–PDU, `GetNextRequest`–PDU, `GetBulkRequest`–PDU, `SetRequest`–PDU, and `InformRequest`–PDU.

- **Unconfirmed Class**
  The Unconfirmed Class contains all protocol operations which are not acknowledged. For example, RFC 1905 defines the following operations for the Unconfirmed Class: `Report`–PDU, `Trapv2`–PDU, and `GetResponse`–PDU. An application document defines which Protocol Operations are supported by the application.

Applications

An SNMP entity normally includes a number of applications. Applications use the services of an SNMP engine to accomplish specific tasks. They coordinate the processing of management information operations, and may use SNMP messages to communicate with other SNMP entities.

Applications documents describe the purpose of an application, the services required of the associated SNMP engine, and the protocol operations and informational model that the application uses to perform management operations.

An application document defines which set of documents are used to specifically define the structure of management information, textual conventions, conformance requirements, and operations supported by the application.

Structure of Management Information

Management information is viewed as a collection of managed objects, residing in a virtual information store, termed the Management Information Base (MIB). Collections of related objects are defined in MIB modules. It is the purpose of a Structure of Management Information document to establish the notation for defining objects, modules, and other elements of managed information.

Textual Conventions

When designing a MIB module, it is often useful to define new types similar to those defined in the SMI, but with more precise semantics, or which have special semantics associated with them. These newly defined types are termed textual conventions, and may be defined in separate documents, or within a MIB module.

Conformance Statements

It may be useful to define the acceptable lower–bounds of implementation, along with the actual level of implementation achieved. It is the purpose of the Conformance Statements document to define the notation used for these purposes.

Management Information Base Modules

MIB documents describe collections of managed objects which instrument some aspect of a managed node.

SNMP Instrumentation MIBs

An SNMP MIB document may define a collection of managed objects which instrument the SNMP protocol itself. In addition, MIB modules may be defined within the documents which describe portions of the SNMP architecture, such as the documents for Message processing Models, Security Models, etc. for the purpose of instrumenting those Models, and for the purpose of allowing remote configuration of the Model.

SNMP Framework Documents

This architecture is designed to allow an orderly evolution of portions of SNMP Frameworks. Throughout the rest of this document, the term "subsystem" refers to an abstract and incomplete

specification of a portion of a Framework, that is further refined by a model specification. A "model" describes a specific design of a subsystem, defining additional constraints and rules for conformance to the model. A model is sufficiently detailed to make it possible to implement the specification. An "implementation" is an instantiation of a subsystem, conforming to one or more specific models.

SNMP version 1 (SNMPv1), is the original Internet–standard Network Management Framework, as described in RFCs 1155, 1157, and 1212.

SNMP version 2 (SNMPv2), is the SNMPv2 Framework as derived from the SNMPv1 Framework. It is described in STD 58, RFCs 2578, 2579, 2580, and RFCs 1905–1907. SNMPv2 has no message definition.

The Community–based SNMP version 2 (SNMPv2c), is an experimental SNMP Framework which supplements the SNMPv2 Framework, as described in RFC 1901. It adds the SNMPv2c message format, which is similar to the SNMPv1 message format.

SNMP version 3 (SNMPv3), is an extensible SNMP Framework which supplements the SNMPv2 Framework, by supporting the following:

- A new SNMP message format
- Security for Messages,
- Access Control
- Remote configuration of SNMP parameters

Other SNMP Frameworks, i.e., other configurations of implemented subsystems, are expected to also be consistent with this architecture.

8.14.2 Elements of the Architecture

This subsection describes the various elements of the architecture and how they are named. There are three kinds of naming:

- the naming of entities
- the naming of identities
- the naming of management information.

This architecture also defines some names for other constructs that are used in the documentation.

The Naming of Entities

An SNMP entity is an implementation of this architecture. Each such SNMP entity consists of an SNMP engine and one or more associated applications. Figure 8.23 shows details about an SNMP entity and the components within it.

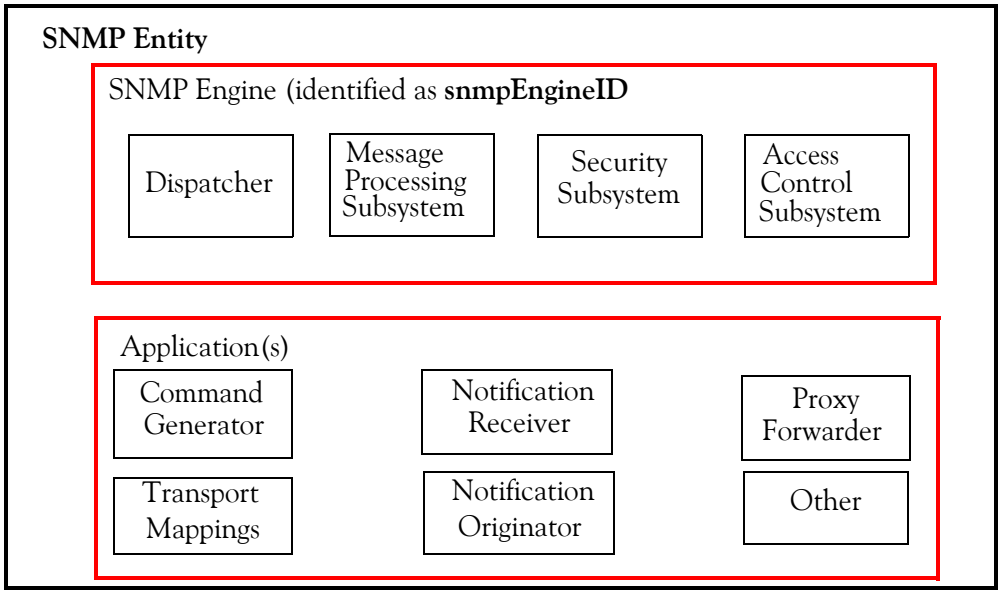


Figure 8.23. SNMPv3 entity and its components

SNMP engine

As shown in Figure 8.23, an SNMP engine is part of the SNMP Entity* which provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. There is a one–to–one association between an SNMP engine and the SNMP entity which contains it. As shown in Figure 8.23, the SNMP engine contains:

- a Dispatcher,
- a Message Processing Subsystem,
- a Security Subsystem, and
- an Access Control Subsystem.

♦ **snmpEngineID**

Within an administrative domain, an `snmpEngineID` is the unique and unambiguous identifier of an SNMP engine. Since there is a one–to–one association between SNMP engines and SNMP entities, it also uniquely and unambiguously identifies the SNMP entity within that administrative domain. Note that it is possible for SNMP entities in different administrative domains to have the same value for `snmpEngineID`. Federation of administrative domains may necessitate assignment of new values.

* *In SNMPv3, managers and agents are referred to as SNMP entities, and each entity consists of an SNMP engine and one or more SNMP applications. As stated on Page 8–70, in SNMPv3, the SNMP Manager and SNMP Agent havedifferent meanings.*

♦ **Dispatcher**

There is only one Dispatcher in an SNMP engine. It allows for concurrent support of multiple versions of SNMP messages in the SNMP engine. It does so by:

- ♥ sending and receiving SNMP messages to/from the network
- ♥ determining the version of an SNMP message and interacting with the corresponding Message Processing Model
- ♥ providing an abstract interface to SNMP applications for delivery of a PDU to an application.
- ♥ providing an abstract interface for SNMP applications that allows them to send a PDU to a remote SNMP entity.

♦ **Message Processing Subsystem**

The Message Processing Subsystem is responsible for preparing messages for sending, and extracting data from received messages. The Message Processing Subsystem potentially contains multiple Message Processing Models as shown in the next figure. One or more Message Processing Models may be present.

Each Message Processing Model defines the format of a particular version of an SNMP message and coordinates the preparation and extraction of each such version–specific message format.

♦ **Security Subsystem**

The Security Subsystem provides security services such as the authentication and privacy of messages and potentially contains multiple Security Models. One or more Security Models may be present.

A Security Model specifies the threats against which it protects, the goals of its services, and the security protocols used to provide security services such as authentication and privacy.

A Security Protocol specifies the mechanisms, procedures, and MIB objects used to provide a security service such as authentication or privacy.

♦ **Access Control Subsystem**

The Access Control Subsystem provides authorization services by means of one or more Access Control Models. An Access Control Model defines a particular access decision function in order to support decisions regarding access rights.

Applications

The Applications part in Figure 8.23 contains several types of applications, including:

- command generators, which monitor and manipulate management data

- command responders, which provide access to management data
- notification originators, which initiate asynchronous messages
- notification receivers, which process asynchronous messages, and
- proxy forwarders, which forward messages between entities.

These applications make use of the services provided by the SNMP engine.

♦ **SNMP Manager**

An SNMP entity containing one or more command generator and/or notification receiver applications, along with their associated SNMP engine, is traditionally called an SNMP manager.

♦ **SNMP Agent**

An SNMP entity containing one or more command responder and/or notification originator applications (along with their associated SNMP engine) has traditionally been called an SNMP agent.

♦ **Command generator**

Generates `get`, `get–next`, `get–bulk`, and `set` requests and processes the responses. This application is implemented by a Network Management Station (NMS), so it can issue queries and set requests against entities on routers, switches, Unix hosts, etc.

♦ **Command responder**

Responds to `get`, `get–next`, `get–bulk`, and `set` requests. For SNMPv3, this application is implemented by an entity on a Cisco router or Unix host. For SNMPv1 and SNMPv2, the command responder is implemented by the SNMP agent.

♦ **Notification originator**

Generates SNMP traps and notifications. This application is implemented by an entity on a router or Unix host. (For Versions 1 and 2, the notification originator is part of an SNMP agent.)

♦ **Notification receiver**

Receives traps and inform messages. This application is implemented by an NMS.

♦ **Proxy forwarder**

Facilitates message–passing between entities.

SNMPv3 Textual Conventions

SNMPv3 defines a number of additional textual conventions, outlined below.

`SnmpEngineID`

An administratively unique identifier for an SNMP engine. Objects of this type are for identification, not for addressing, even though an address can be used in the generation of a specific value. RFC 2571 provides a detailed discussion of how SnmpEngineIDs are created.

`SnmpSecurityModel`

An SNMP security Model (SNMPv1, SNMPv2, or USM), where USM stands for **User–based Security Model**, which is the security method used in SNMPv3. It is defined in RFC 3414.

`SnmpMessageProcessingModel`

A Message Processing Model used by the Message Processing Subsystem.

`SnmpSecurityLevel`

The level of security at which SNMP messages can be sent, or the level of security at which operations are being processed. Possible values are `noAuthNoPriv` (without authentication and without privacy), `authNoPriv` (with authentication but without privacy), and `authPriv` (with authentication and with privacy). These three values are ordered such that `noAuthNoPriv` is less than `authNopriv` and `authNopriv` is less than `authPriv`.

`SnmpAdminString`

An octet string containing administrative information, preferably in human–readable form. The string can be up to 255 bytes in length.

`SnmpTagValue`

An octet string containing a tag value. Tag values are preferably in human–readable form. According to RFC 2573, valid tags include acme, router, and host.

`SnmpTagList`

An octet string containing a list of tag values. Tag values are in human–readable form. According to RFC 2573, examples of a tag list are the empty string, acme router, and host manager Station.

`KeyChange`

An object used to change authentication and privacy keys.

8.14.3 The View–based Access Control Model (VACM)

In SNMPv3, access control has been more secure and more flexible with the introduction of VACM. The VACM is described in RFC 2575.

The VACM determines the access rights of a group, representing zero or more `securityNames` which have the same access rights. For a particular context, identified by `contextName`, to which a group, identified by `groupName`, has access using a particular `securityModel` and `securityLevel`, that group's access rights are given by a read–view, a write–view and a notify–view.

The *read–view* represents the set of object instances authorized for the group when reading objects. Reading objects occurs when processing a retrieval operation (when handling Read Class PDUs).

The *write–view* represents the set of object instances authorized for the group when writing objects. Writing objects occurs when processing a write operation (when handling Write Class PDUs).

The *notify–view* represents the set of object instances authorized for the group when sending objects in a notification, such as when sending a notification (when sending Notification Class PDUs).

The procedures followed by an Access Control module that implements the View–based Access Control Model when checking access rights as requested by an application (for example a Command Responder or a Notification Originator application) are described below. The abstract service primitive is as follows:

```
statusInformation = -- success or errorIndication
isAccessAllowed (
securityModel -- Security Model in use
securityName -- principal who wants access
securityLevel -- Level of Security
viewType -- read, write, or notify view
contextName -- context containing variableName
variableName -- OID for the managed object
)
```

The abstract data elements are:

```
statusInformation – one of the following:
accessAllowed – a MIB view was found and access is granted.
notInView – a MIB view was found but access is denied. The vari-
ableName is not in the configured MIB view for the specified
viewType (e.g., in the relevant entry in the vacmAccessTable).
noSuchView – no MIB view found because no view has been config-
ured for specified viewType (e.g., in the relevant entry in the
vacmAccessTable).
noSuchContext – no MIB view found because of no entry in the vac-
mContextTable for specified contextName.
```

noGroupName – no MIB view found because no entry has been configured in the vacmSecurityToGroupTable for the specified combination of securityModel and securityName.
noAccessEntry – no MIB view found because no entry has been configured in the vacmAccessTable for the specified combination of contextName, groupName (from vacmSecurityToGroupTable), securityModel and securityLevel.
otherError – failure, an undefined error occurred.
securityModel – Security Model under which access is requested.
securityName – the principal on whose behalf access is requested.
securityLevel – Level of Security under which access is requested.
viewType – view to be checked (read, write or notify).
contextName – context in which access is requested.
variableName – object instance to which access is requested.

Figure 8.24 shows how the decision for access control is made by the VACM and how the decision for `isAccessAllowed` is made

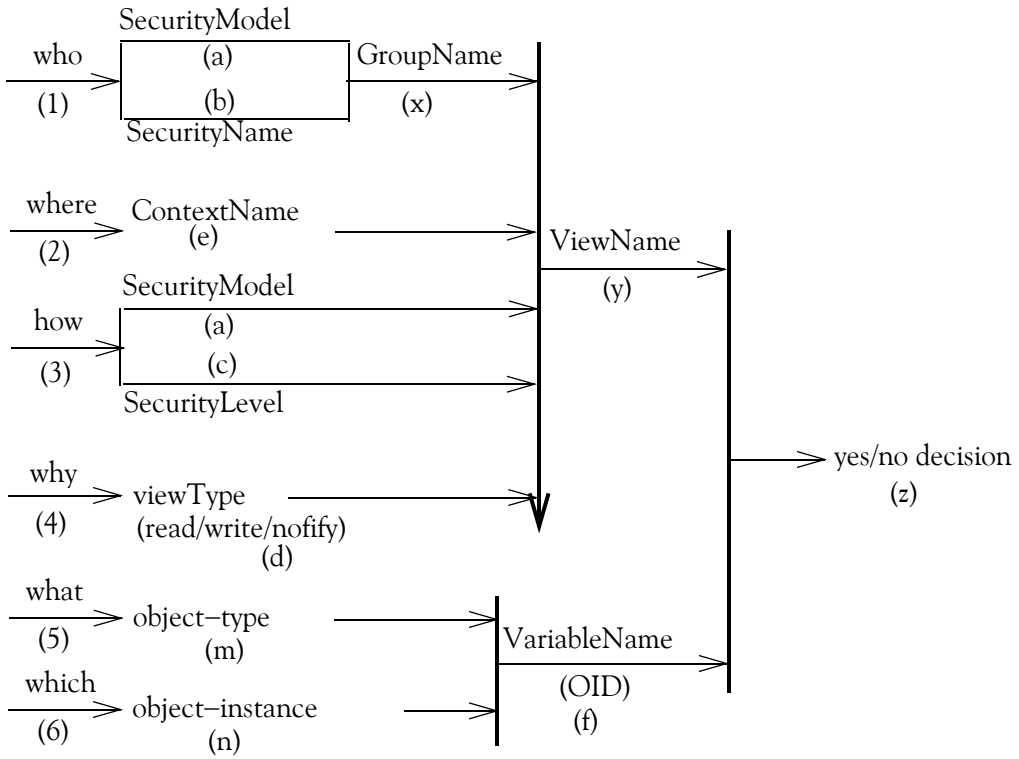


Figure 8.24. The VACM Process

1. Inputs to the `isAccessAllowed` service are:

```
(a) securityModel-- Security Model in use
(b) securityName -- principal who wants to access
(c) securityLevel -- Level of Security
(d) viewType -- read, write, or notify view
(e) contextName -- context containing variableName
(f) variableName -- OID for the managed object -- this is made up of:
                                                  - object-type (m)
                                                  - object-instance (n)
```

2. The partial "who" (1), represented by the `securityModel (a)` and the `securityName (b),` are used as the indices (a,b) into the `vacmSecurityToGroupTable` to find a single entry that produces a group, represented by `groupName (x).`

3. The "where" (2), represented by the `contextName` (e), the "who", represented by the `groupName (x)` from the previous step, and the "how" (3), represented by `securityModel (a)` and `securityLevel (c)`, are used as indices (e,x,a,c) into the `vacmAccessTable` to find a single entry that contains three MIB views.

4. The "why" (4), represented by the `viewType` (d), is used to select the proper MIB view, represented by a `viewName (y)`, from the `vacmAccessEntry` selected in the previous step. This viewName (y) is an index into the `vacmViewTreeFamilyTable` and selects the set of entries that define the variableNames which are included in or excluded from the MIB view identified by the viewName (y).

5. The "what" (5) type of management data and "which" (6) particular instance, represented by the `variableName (f)`, is then checked to be in the MIB view or not, e.g., the yes/no decision (z).

The procedure below is followed by an Access Control module that implements the View–based Access Control Model (VACM) whenever it receives an `isAccessAllowed` request.

1. The `vacmContextTable` is consulted for information about the SNMP context identified by the `contextName`. If information about this SNMP context is absent from the table, then an errorIndication (`noSuchContext`) is returned to the calling module.

2. The `vacmSecurityToGroupTable` is consulted for mapping the `securityModel` and `securityName` to a `groupName`. If the information about this combination is absent from the table, then an `errorIndication` (`noGroupName`) is returned to the calling module.

3. The `vacmAccessTable` is consulted for information about the `groupName`, `contextName`, `securityModel` and `securityLevel`. If information about this combination is absent from the table, then an `errorIndication` (`noAccessEntry`) is returned to the calling module.

4.

a. If the viewType is "read", then the read view is used for checking access rights.

b. If the viewType is "write", then the write view is used for checking access rights.

c. If the viewType is "notify", then the notify view is used for checking access rights.

If the view to be used is the empty view (zero length `viewName`) then an `errorIndication` (`noSuchView`) is returned to the calling module.

5.

a. If there is no view configured for the specified viewType, then an `errorIndication` (`noSuchView`) is returned to the calling module.

b. If the specified `variableName` (object instance) is not in the MIB view (see DESCRIPTION clause for `vacmViewTreeFamilyTable` in section 4), then an errorIndication (`notInView`) is returned to the calling module.

c. The specified `variableName` is in the MIB view. A `statusInformation` of success (`accessAllowed`) is returned to the calling module.

The following example shows how to configure SNMPv3 on a Cisco router. As stated above, we first need to define a view. The line below creates a view called `exampleview` and allows access to the internet subtree where `included` is used to mandate that the specified subtree must be included in the `exampleview`.

router(config)**#snmp–server view exampleview internet included**

We can exclude a subtree using excluded in our command. Next, we create a group that uses this view. The following command creates a group called `readonly; v3` means that SNMPv3 should be used. The `auth` keyword specifies that the entity should authenticate packets without encrypting them; `read exampleview` indicates that our defined view must appear whenever any member of the `readonly` group access the router.

router(config)**#snmp–server group readonly v3 auth read exampleview**

Now, we will create a user. The following command creates a user called `anderson`, who belongs to the `readonly` group. `auth md5` specifies that the router should use *Message Digest 5* (MD5)* to authenticate the user. The final item on the command line is the user's password which cannot exceed 64 characters.

router(config)**#snmp–server user anderson readonly v3 auth md5 hispassword**

The above command uses a password as the only encryption. However, other information included in SNMP packets are sent without encryption and can therefore be read by anyone who

* *MD5 is an algorithm where a password is repeated until it generates a sequence of 16 octets. SHA–1 is another such algorithm where a password is repeated until it generates a sequence of 20 octets.*

has a packet sniffer* and access to our network. If we want to encrypt the packets also, we can use a command like the one below which may contain information that we don't want available to the public.

router(config)**#snmp–server user anderson readonly v3 auth md5 hispassword\priv des56 passphrase**

The additional keywords on this command specify privacy (i.e., encryption for all SNMP packets), use of the Data Encryption Standard (DES)† 56–bit encryption, and a `passphrase` to use when encrypting packets.

8.15 Host Management

Host management is also very important in network management. The Host Resources MIB defines the following seven groups:

```
host OBJECT IDENTIFIER :: = { mib–2 25 }

hrSystem OBJECT IDENTIFIER :: = { host 1 }

hrStorage OBJECT IDENTIFIER :: = { host 2 }

hrDevice OBJECT IDENTIFIER :: = { host 3 }

hrSWRun OBJECT IDENTIFIER :: = { host 4 }

hrSWRunPerfOBJECT IDENTIFIER :: = { host 5 }

hrSWInstalledOBJECT IDENTIFIER :: = { host 6 }
```

The `host` object identifier is 1.3.6.1.2.1.25 (*iso.org.dod.intemet.mgmt.mib–2.host*). The remaining six groups define various objects that provide information about the system.

The `hrSystem` (1.3.6.1.2.1.25.1) group defines objects that pertain to the system itself. These objects include uptime, system date, system users, and system processes.

The `hrStorage` (1.3.6.1.2.1.25.2) and `hrDevice` (1.3.6.1.2.1.25.3) groups define objects pertaining to system storage and file systems, such as total system memory, disk utilization, and CPU non–idle percentage. They are particularly helpful, since they can be used to manage the disk partitions on our host. They can also be used to check for errors on a given disk device.

The `hrSWRun` (1.3.6.1.2.1.25.4), `hrSWRunPerf` (1.3.6.1.2.1.25.5), and `hrSWInstalled` (1.3.6.1.2.1.25.6) groups define objects that represent various aspects of software running or installed on the system. From these groups, we can determine what operating system is running on the host, as well as what programs the host is currently running. The `hrSWInstalled`

* *Packet sniffer is a management tool that can capture the packets going across a transmission medium.*
† *The Data Encryption Standard (DES) and the International Data Encryption Algorithm (IDEA) are two standard algorithms that implement secret key cryptography. DES uses a 56–bit key and IDEA uses a 128–bit key.*

group can be used to track which software packages are installed.

8.16 SNMP Implementations

Implementations of the SNMPv3 specifications are being developed by various vendors and research departments. A partial list in alphabetical order is provided below. The Microsoft implementation WinSNMP is discussed in Section 8.13.

- **AdventNet**

  AdventNet Java SNMP API is a development environment comprising of SNMP stack/SNMP library for building SNMP management applications which supports all three versions of SNMP, SNMPv1, SNMPv2c, SNMPv3

- **AGENT SNMP v1, v2C, v3**

  SNMP++v3 and AGENT++v3 are C++ APIs allowing the development of SNMP managers and agents respectively. Both APIs support SNMP v1, v2c and v3. The v3 support includes MD5 and SHA authentication as well as DES and IDEA privacy.

- **Applied SNMP, LLC**

  A software and systems engineering organization offering network management products and services, with special expertise in SNMP and Microsoft Windows platforms.

- **Castle Rock Computing**

  SNMPc from **Castle Rock Computing** provides both real time network status and statistics and historical distributed SNMP information over the web for a network. Recently announced the release of the SNMPc 7.1 Network Management System. SNMPc 7.1 which supports a larger number of remote users and remote polling agents in the base system and provides expanded polling capabilities.

- **Cisco Systems**

  With a wide array of SNMP management features, Cisco Systems provides truly useful management functionality across an extensive range of media and protocols. As a leader in SNMP–based management, Cisco continues to expand its management capabilities to incorporate new protocols and features important to those protocols.

- **DMH Software**

  Provides real–time, Portable, Embedded SNMP Agent Software (SNMPv1, SNMPv2C and SNMPv3), MIB Compiler, HTTP/WEB Server. Includes a SMIv2 MIB–Compiler for rapid MIB development.

- **DPS Telecom**

  Offers a complete line of Network Alarm Management Products including SNMP.

- **IBM**

  IBM has developed a complete multi–lingual SNMPv1/v2c/v3 stackwith sample code for a Command Generator, a Command Responder, Notification Originator, and Notification Receiver. The code is written in ANSI C. The code also supports the DPI (RFC 1592). In addition the code contains a WinSNMP API library that allows an application to transparently talk to SNMPv1/v2c/v3 targets.

  The eNetwork Communications Server Version 2 Release 7 contains an agent and an SNMP management command line interface based on the IBM Research code. IBM also has a Java implementation for SNMPv1/v2c/v3. It is used in the following products on the SNMP manager side: Nways Manager for AIX version 1.2.2, Nways Manager for HP–UX Version 1.2, Nways Workgroup Manager for Windows NT version 1.1.2.

- **InterWorking Labs, Inc.**

  Recently announced SilverCreek SL SNMP APIs as well as new, expanded, encryption capabilities for enhanced SNMP security.

- **MG–SOFT Corporation**

  MG–SOFT MIB Browser Professional Edition with MIB Compiler runs ion Microsoft Windows operating systems (Windows ME, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008). A version for Linux operating systems is also available.

- **MIMIC SNMP Agent Simulator**

  Creates a network of up to 20,000 SNMP–manageable devices per 64–bit Intel–based PC (Itanium, Xeon), AMD–based PC (AMD64) or Sun Sparc, or 10,000 per 32–bit Intel–based PC (x86), AMD–based PC (E86) or Sun Sparc. With support for any SNMP–based device you can run a large variety of device configurations with your SNMP management application.

  MIMIC simulated devices respond to SNMPv1, SNMPv2C and SNMPv3 queries on any of its configured IP (or IPv6) addresses. It appears to the SNMP Network Management Application as if it is talking to actual devices. Each device has its own IP addresses, independent read and write SNMPv1 community strings or SNMPv3 USM and VACM parameters, and notion of uptime. Devices can be configured at run–time, both on an individual and collective basis.

- **ModLink Networks**

  Develops embedded SNMP technology for both simple and enterprise–wide **network** devices.

- **MultiPort Corporation**

  MultiPort Corporation is now offering their SNMPv3 solution – called EZMP3 for the Easy to Use SNMPv3 Solution. It supports SNMPv1, SNMPv2c and SNMPv3 in an easy to use, highly portable agent. The product includes full support for MIB–II, contains an advanced

MIB Compiler to facilitate the creation of new MIBs and we can offer support with our extensive library of 'off–the–shelf' MIB's. EZMP3 also includes support for MD5 and SHA Authentication as well as DES Encryption Services.

- **Netaphor Software Inc.**

  Netaphor Software Inc. is now selling the Cyberons for Java SNMP Manager Toolkit v2.0 which supports SNMPv1, SNMPv2c and SNMPv3. Additional details may be found at the Netaphor website.

- **Net–SNMP**

  The NET SNMP project has added SNMPv3 support to their will known NET SNMP package (formerly known as UCD SNMP). They also offer access to a test agent for interoperability tests.

- **SimpleSoft**

  SimpleSoft's Automated SNMP Agent Tester, SimpleTester (version 3.0), now supports SNMPv3, in addition to SNMPv1 and SNMPv2c. The Multiple SNMP Agent Simulator, SimpleAgentPro, will support SNMPv3 noAuth/noPriv later this year.

- **SNMP Research**

  SNMP Research has complete implementations of SNMPv3 in all of its agent and management products.

- **TechnischeUniversität of Braunschweig**

  Software engineers at the Technical University of Braunschweig have implemented SNMPv3 patches for tcpdump as well as noAuth/noPriv SNMPv3 support for the Scotty network management package. Interoperability (noAuth/noPriv) was tested against the SNMPv3 implementation from SNMP Research to ensure that the packet decoder/encoder work as expected.

- **Université du Quebéc a Montréal**

  Software engineers at the University of Quebec in Montreal have implemented a modular SNMP engine based on the abstract service interfaces (ASIs). The implementation is written in Java. All security features are implemented. This implementation is running on the Internet for the purpose of remote testing.

- **Westhawk Ltd**

  The Westhawk lightweight SNMP stack in Java, which comes with Java applet, application and servlet examples, provides manager functionality for SNMPv1, SNMPv2c and SNMPv3 (authentication and privacy). It is capable of sending and receiving traps, but has no other agent functionality. Source code and documentation is included. The stack is free and commercial support is available.

8.17 Summary

- SNMP provides a method of managing network hosts such as workstation or server computers, routers, bridges, and hubs from a centrally–located computer running network management software.
- The standards for SNMP and other protocols such as TCP/IP, are published in a series of documents called Requests for Comments (RFCs).
- SNMP Version 1 (SNMPv1) is the standard version of the SNMP protocol. It is defined in RFC 1157 and it is a full Internet Engineering Task Force (IETF) standard. Security in SNMPv1 is based on the so–called communities which are just passwords.
- SNMP Version 2 (SNMPv2) was developed to provide the security functions that SNMP lacked. It is defined in RFCs 1905, 1906, and 1907.
- SNMP Version 3 (SNMPv3) was developed to provide the best possible security in SNMP management. It is defined in RFCs 2571, 2572, 2573, 2574, and 2575.
- A managed device is a piece of equipment with an SNMP agent (software) built into it.
- Managed objects are the operating characteristics of managed devices.
- A single operating characteristic such as a UDP session on a single managed device is referred to as object instance.
- A Management Information Base (MIB) is a database of managed objects accessed by network management protocols.
- SNMP contains two standard MIBs. The first, MIB I, established in RFC 1156, was defined to manage the TCP/IP–based internet. MIB II, defined in RFC 1213, is basically an update to MIB I. MIB–II refers to the current definition. SNMPv2 includes MIB–II and adds some new objects.
- MIB objects are managed objects that are categorized in accordance to the job they perform, and are placed in the Management Information Base (MIB).
- An object identifier is a series of integers based on nodes in the tree, and separated by dots (.). Thus, iso(1).org(3).dod(6).internet(1) in object identifier form is represented as 1.3.6.1 or in textual form as *iso.org.dod.internet*.
- In SNMP, the request operations follow a lexicographic order.
- The Structure of Management Information (SMI) is a standard that uses the Abstract Systems Notation One (ASN.1). SMI specifies the syntax for data types such as object identifiers, counters, rows, tables, octet strings, network addresses, and other SNMP elements so that SNMP is machine independent.

- The two main branches beyond the Internet root are the Management and Private MIBs. Industry–standard MIBs go through the management branch to become *iso.org.dod.internet.mgmt.mib* with the object identifier 1.3.6.1.2.1. Private MIBs become *iso.org.dod.internet.private* or 1.3.6.1.4.
- Traps are unsolicited messages sent from an agent to an NMS.
- SNMPv1 uses the operations `Get, Getnext, Set,` and `Trap`
- SNMPv2 uses the operations `Get, Getnext, Set, Trap, GetBulk,` and `Inform`.
- All private enterprise number assignments for individuals, institutions, and organizations are managed by the Internet Assigned Numbers Authority (IANA).
- Notification in SMIv2 is equivalent to trap in SMIv1. In SMIv1, the trap is formally specified an ASN.1 macro TRAP–TYPE. In SMIv2, notification is specified by an ASN.1 macro NOTIFICATION–TYPE.
- SNMPv2 provides an `inform` operation to allow for NMS–to–NMS communication. When an `inform` is sent from one NMS to another, the receiving NMS sends a response to the sending NMS to acknowledge receipt of the message. We can use an SNMP `inform` to send SNMPv2 traps from an agent to an NMS. In this case, the agent will be notified by the NMS that the trap has been received.
- The `report` operation was intended for SNMPv2 but it was never implemented. However, it is used in SNMPv3 to enable SNMP engines to communicate with each other and report problems with processing SNMP messages.
- In SNMPv3, the engine is composed of four pieces: the Dispatcher, the Message Processing Subsystem, the Security Subsystem, and the Access Control Subsystem.
- The Dispatcher's job is to send and receive messages. It tries to determine the version of each received message (i.e., v1, v2, or v3) and, if the version is supported, hands the message off to the Message Processing Subsystem. The Dispatcher also sends SNMP messages to other entities.
- The Message Processing Subsystem prepares messages to be sent and extracts data from received messages. A message processing system can contain multiple message processing modules. For example, a subsystem can have modules for processing SNMPvI, SNMPv2, and SNMPv3 requests. It may also contain a module for other processing models that are yet to be defined.
- The Security Subsystem provides authentication and privacy services. Authentication uses either community strings (SNMP Versions 1 and 2) or SNMPv3 user–based authentication. User–based authentication uses the MD5 or SHA algorithms to authenticate users without sending a password in the clear. The privacy service uses the DES algorithm to encrypt and decrypt SNMP messages.

- The Access Control Subsystem is responsible for controlling access to MIB objects. We can control what objects a user can access as well what operations he/she is allowed to perform on those objects. For example, we might want to limit a user's read–write access to certain parts of the mib–2 tree, while allowing read–only access to the entire tree.
- In SNMPv3, the command generator generates `get, get–next, get–bulk,` and `set` requests and processes the responses. This application is implemented by a Network Management Station (NMS), so it can issue queries and set requests against entities on routers, switches, Unix hosts, etc.
- In SNMPv3, the command responder responds to `get, get–next, get–bulk,` and `set` requests. For SNMPv3, this application is implemented by an entity such as a Cisco router or Unix host. (For SNMPv1 and SNMPv2, the command responder is implemented by the SNMP agent.)
- In SNMPv3, the notification originator generates SNMP traps and notifications. This application is implemented by an entity on a router or Unix host. (For Versions 1 and 2, the notification originator is part of an SNMP agent.)
- In SNMPv3, the notification receiver receives traps and inform messages. This application is implemented by an NMS.
- In SNMPv3, the proxy forwarder facilitates message–passing between entities.

8.18 Exercises

True/False

1. SNMP's predecessor, the Simple Gateway Management Protocol (SGMP), was developed to manage internet routers only. _____

2. A manager (NMS) and an agent communicate via UDP. _____

3. A managed device is a piece of equipment with an SNMP agent built into it. _____

4. Managed objects is another name for managed devices. _____

5. Each MIB object has a numerical object identifier and an associated textual name. _____

6. The Directory(1) subtree in the SMIv1 Object Tree defines a standard set of Internet directory objects. _____

7. All private enterprise number assignments for individuals, institutions, and organizations are managed by the Internet Assigned Numbers Authority (IANA). _____

8. The NOTIFICATION–TYPE trap is defined in SNMPv3. _____

9. The notation – – is an operator used for an SMI definition.

10. A variable binding (VarBind) is a managed object that has a value associated with it. _____

Multiple Choice

11. MIBs are programmed by _____

    A. ISO

    B. vendors

    C. ASN.1

    D. IEEE

12. Most managed objects are _____ objects

    A. scalar

    B. tabular

    C. NMSs

    D. agent

13. In SNMPv1, traps have _____

    A. a different PDU than those of the `get` and `set` PDUs

    B. the same PDU as those of the `get` and `set` PDUs

C. a different IP than those of the `get` and `set` IPs

D. the same IP as those of the `get` and `set` IPs

14. The SNMPv2 `inform` operation _____

A. was never implemented in SNMPv2

B. is used in SNMPv1 but was never implemented in SNMPv2 or SNMPv3

C. allows agent–to–agent communications

D. allows NMS–to–NMS communications

15. The SNMPv2 `report` operation _____

A. was never implemented in SNMPv2 but it is used in SNMPv3

B. is used in SNMPv1 but was never implemented in SNMPv2 or SNMPv3

C. reports problems from one agent to another

D. none of the above

16. The essential characteristics of SNMPv3 are _____

A. It allows SNMPv1, SNMPv2, and SNMPv3 to coexist in a single management entity

B. Addition of security features for SNMP management

C. The vast amount of SNMP documentation is organized into a document architecture

D. all of the above

17. In SNMPv3 the notification receiver _____

A. facilitates message–passing between entities

B. receives traps and inform messages

C. generates traps and notifications

D. none of the above

18. In SNMPv3 the notification originator _____

A. facilitates message–passing between entities

B. receives traps and inform messages

C. generates traps and notifications

D. none of the above

19. In SNMPv3 the command responder _____

A. facilitates message–passing between entities

B. receives traps and inform messages

C. responds to `get, get–next, get–bulk,` and `set` requests

D. none of the above

20. In SNMPv3 the command generator _____

A. facilitates message–passing between entities

B. Generates `get, get–next, get–bulk,` and `set` requests

C. receives traps and inform messages

D. none of the above

8.19 Answers to End–of–Chapter Exercises

True/False

1. T Refer to page 8–1

2. T Refer to page 8–4

3. T Refer to page 8–6

4. F Refer to page 8–7

5. T Refer to page 8–10

6. F Refer to page 8–10

7. T Refer to page 8–23

8. F Refer to page 8–28

9. F Refer to page 8–32

10. T Refer to page 8–36

Multiple Choice

11. B Refer to page 8–12

12. B Refer to page 8–26

13. A Refer to Table 8.6, page 8–42

14. D Refer to page 8–46

15. A Refer to page 8–46

16. D Refer to page 8–62

17. B Refer to page 8–70

18. C Refer to page 8–70

19. C Refer to page 8–70

20. B Refer to page 8–70

Chapter 9

Introduction to Remote Monitoring (RMON)

This chapter is an introduction to the Remote Monitoring (RMON). SNMP and RMON are closely related network standards that allow us to capture real time information across the entire network. Both are written in accordance with Management Information Base (MIB) guidelines and thus are platform independent.

9.1 RMON Overview

RMON is a standard MIB that is separate but closely related to SNMP. Like SNMP, RMON is an open standard administered by the Internet Engineering Task Force (IETF). The RMON standard is an SNMP MIB definition described in RFC 1757. RMON1, or simply RMON is defined in RFC 2819. An enhanced version, referred to as RMON2, is defined in RFC 2021. RMON1 provides the Network Management Station (NMS) with packet–level statistics about the entire LAN, MAN, or WAN. RMON2 improves RMON1 by providing network and application level statistics.

RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs) and interconnecting T–1/E–1 and T–2/E–3 lines from a central site. RMON specifically defines the information that any network monitoring system will be able to provide. The basic differences between RMON and SNMP are:

- RMON is instrument–based, in that it uses specialized hardware (probes) to operate.
- RMON proactively (acting in advance) sends data instead of waiting to be polled, making it bandwidth–efficient and more responsive to network events.
- RMON is capable of collecting more detailed data.

RMON instrumentation provides a powerful monitoring system but at a considerably larger monetary expense. Accordingly, RMON probes are normally installed on critical links such as network backbones and servers.

RMON system can configured to provide such data as:

- Information regarding network utilization
- Historical information for network trend and statistical analysis
- Information describing communications between systems and the quantity of data exchanged

9.2 How RMON Works

Figure 9.1 shows a typical RMON configuration. Like SNMP, a typical RMON configuration consists of a central Network Management Station (NMS) and a remote monitoring device, called an RMON agent.

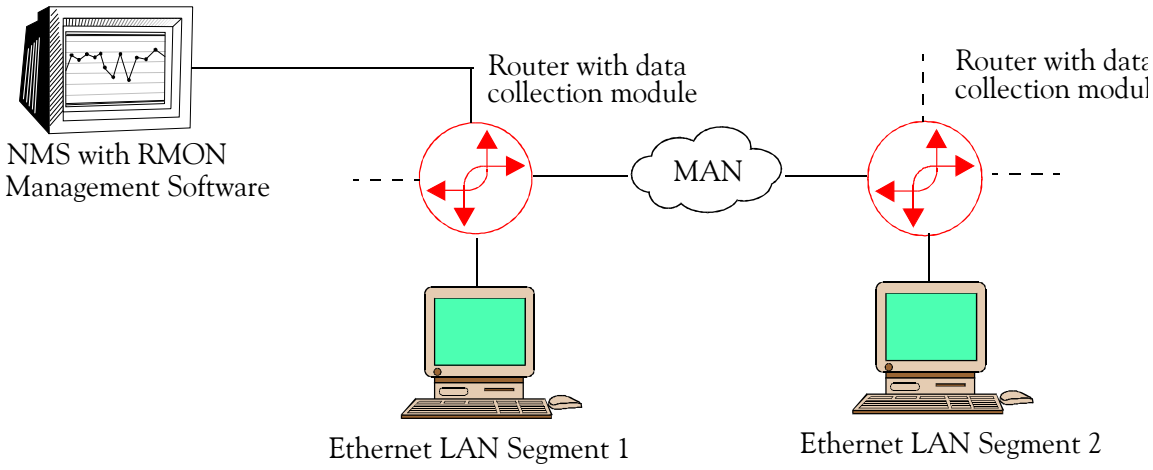


Figure 9.1. Typical RMON Configuration

The NMS can be a Windows–based or UNIX–based workstation or PC running a network management application that performs tasks as gathering statistics by monitoring packets of data on an Ehernet segment, and storing information in accordance with the RMON specification. From the NMS we can issue SNMP commands requesting information from the RMON agent. The RMON agent sends the requested information to the NMS which then processes and displays this information on a console.

NIKSUN, www.niksun.com, has introduced the NetVCR Solution, a system that performs monitoring and analysis and supports critical RMON I and II groups. The RMON MIBs generated by NetVCR allow network management systems to remotely access RMON data collected by NetVCR's recording interfaces. The user can set alarm thresholds on the NetVCR appliance.

The Bay Networks Implementation of RMON is shown in Figure 9.2. It consists of a BayStack AN or BayStack ANH base module, the Data Collection Module (DCM), the Data Collection Module MiddleWare (DCMMW), the DCM Flash memory module, and the RMON agent.

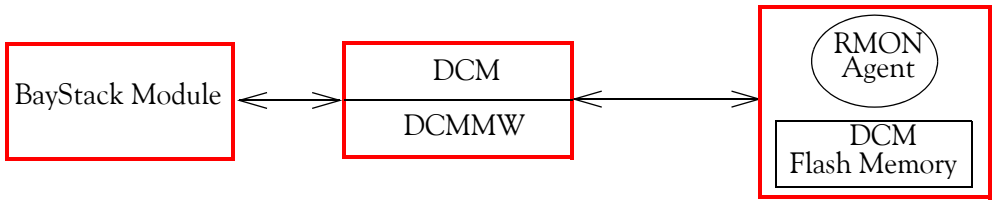


Figure 9.2. Bay Networks RMON Architecture

The RMON agent is software that resides on a Data Collection Module (DCM) within a Bay Networks BayStack AN or ANH router on a remote network. As packets travel across the network, the RMON agent continuously collects and analyzes Ethernet data in real time on a remote LAN segment and stores the data locally in the Ethernet DCM according to the RMON MIB specification, defined in RFC 1757. We can have multiple RMON agents running in different segments of the network, usually one per subnet.

As shown in Figure 9.2, the Ethernet DCM physically connects to the BayStack AN or BayStack ANH base module. The Ethernet DCM contains a Flash memory module for its own boot image and configuration file. The Ethernet DCM runs the RMON agent software that

- Gathers statistics by monitoring packets on an Ethernet segment
- Stores the information according to the RMON MIB specification. in compliance with RFC 1757

To communicate with the RMON agent software on the Ethernet DCM, the BayStack AN or BayStack ANH uses a software subsystem, called the DCMMW. This software subsystem enables and configures an installed Ethernet DCM, and allows us to modify the Ethernet DCM configuration, boot the Ethernet DCM, disable the Ethernet DCM using the NMS. We can use an SNMP–based network management application that supports RMON to view RMON statistics.

9.3 RMON Goals

RMON became a standard in 1992 with the release of RMON1 for Ethernet. The RMON2 standard, the current version, was completed in early 1997. While RMON1 operates only at the data–link layer of the seven–layer OSI reference model, RMON2 adds the capability to collect data at higher layers, giving it more reporting capability. The ability to monitor upper layer events has been a boon to the popularity of RMON. For example, RMON2 can report what is happening with TCP traffic as opposed to IP on a multiprotocol LAN segment.

Network administrators have used network analyzers to proactively monitor network usage and troubleshoot network–related problems. To ensure accurate reading of network traffic data, the first network analyzers had to be physically attached to the target network to avoid missing important information that might be filtered by bridges or routers. To improve remote monitoring and troubleshooting of network traffic, subsequent network analyzers were enhanced to relay network traffic data to centralized consoles.

The user community with the help of the Internet Engineering Task Force (IETF) defined a standard monitoring specification that allows various network monitors and console systems to exchange network monitoring data. This RMON specification defines a set of statistics and functions that can be exchanged between RMON–compliant console managers and network probes. RMON offers network administrators more freedom in selecting network monitoring probes and consoles whose features meet their particular networking needs.

RMON probes replace expensive network analyzer devices that must be physically attached to the

approximate area of a network problem. RMON probes come in different forms, depending on the size and type of device to be monitored:

- An RMON MIB that uses the monitored device's hardware (called an embedded agent)
- A specialized card module inserted into a slot within the monitored device
- A purpose–built probe externally attached to one or more monitored devices
- A dedicated PC attached to one or more monitored devices

Implementing specialized network hardware that are remotely located with a monitored device offers significant advantages. This is because RMON probes can yield a more detailed set of measurement data than that of an SNMP agent. The dedicated hardware is used as a real–time sensor that can gather and analyze data for possible upload to the NMS.

This and the next two sections are extracted from RFC 1757 to provide the basic RMON goals, control of RMON devices and conventions. Section 5 of this RFC provides definitions but the content is very lengthy and therefore it is not included here. These definitions are very similar to those of the SNMP.

- **Offline Operation**

  With RMON it is not necessary that a management station is in constant contact with its remote monitoring devices. RMON allows a probe to perform diagnostics and to collect statistics continuously, even when communication with the management station is not in effect. The probe will attempt to notify the management station when an abnormal condition occurs. However, if communications between management station and probe is not continuous, information will be continuously accumulated and communicated to the management station conveniently and efficiently at a later time.

- **Proactive Monitoring**

  With RMON, a remote monitoring device (probe) has the resources to perform diagnostics and to log network performance. Thus, the probe can notify the management station of a failure and can store historical statistical information about the failure. This historical information can be played back by the management station in an attempt to perform further diagnostics to isolate the cause of the problem.

- **Problem Detection and Reporting**

  The probe can be configured to recognize conditions, most notably error conditions, and continuously to check for them. When one of these conditions occurs, the event may be logged, and management stations may be notified in several ways.

- **Value Added Data**

  Since a remote monitoring device represents a network resource dedicated exclusively to network management functions, and because it is located directly on the monitored portion of the

network, the remote network monitoring device has the opportunity to add significant value to the data it collects. For instance, by highlighting those hosts on the network that generate the most traffic or errors, the probe can give the management station precisely the information it needs to solve a series of problems.

- **Multiple Managers**

  An organization may have multiple management stations for different units of the organization, for different functions (e.g. engineering and operations), and in an attempt to provide disaster recovery. Because environments with multiple management stations are common, the remote network monitoring device has to deal with more than own management station, potentially using its resources concurrently.

9.3.1 Textual Conventions

Two data types were introduced as a textual convention in RFC 1757. This RFC defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP–based networks. In particular, it defines objects for managing remote network monitoring devices.

These textual conventions enhance the readability of the specification and can ease comparison with other specifications if appropriate. It should be noted that the introduction of the these textual conventions has no effect on either the syntax nor the semantics of any managed objects. The use of these is merely an artifact of the explanatory method used. Objects defined in terms of one of these methods are always encoded by means of the rules that define the primitive type. Hence, no changes to the SMI or the SNMP are necessary to accommodate these textual conventions which are adopted merely for the convenience of readers and writers in pursuit of the elusive goal of clear, concise, and unambiguous MIB documents. The data types are: `OwnerString` and `EntryStatus`.

9.3.2 Structure of MIB Defined in RFC 1757

The objects are arranged into the following groups:

```
- ethernet statistics
- history control
- ethernet history
- alarm
- host
- hostTopN
- matrix
- filter
- packet capture
- event
```

These groups are the basic unit of conformance. If a remote monitoring device implements a group, then it must implement all objects in that group. For example, a managed agent that implements the host group must implement the `hostControlTable`, the `hostTable`, and the `hostTimeTable`. All groups in this MIB are optional. Implementations of this MIB must also implement the system and interfaces group of MIB–II. MIB–II may also mandate the implementation of additional groups. These groups are defined to provide a means of assigning object identifiers, and to provide a method for managed agents to know which objects they must implement.

9.3.3 The Ethernet Statistics Group

The ethernet statistics group contains statistics measured by the probe for each monitored Ethernet interface on this device. This group consists of the `etherStatsTable`. In the future other groups will be defined for other media types including Token Ring and FDDI. These groups should follow the same model as the ethernet statistics group.

9.3.4 The History Control Group

The history control group controls the periodic statistical sampling of data from various types of networks. This group consists of the `historyControlTable`.

9.3.5 The Ethernet History Group

The ethernet history group records periodic statistical samples from an ethernet network and stores them for later retrieval. This group consists of the `etherHistoryTable`. In the future, other groups will be defined for other media types including Token Ring and FDDI.

9.3.6 The Alarm Group

The alarm group periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. A hysteresis mechanism is implemented to limit the generation of alarms. This group consists of the `alarmTable` and requires the implementation of the event group.

9.3.7 The Host Group

The host group contains statistics associated with each host discovered on the network. This group discovers hosts on the network by keeping a list of source and destination MAC Addresses seen in good packets promiscuously received from the network. This group consists of the `hostControlTable`, the `hostTable`, and the `hostTimeTable`.

9.3.8 The HostTopN Group

The `hostTopN` group is used to prepare reports that describe the hosts that top a list ordered by

one of their statistics. The available statistics are samples of one of their base statistics over an interval specified by the management station. Thus, these statistics are rate based. The management station also selects how many such hosts are reported. This group consists of the `hostTopNControlTable` and the `hostTopNTable`, and requires the implementation of the host group.

9.3.9 The Matrix Group

The matrix group stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its tables. This group consists of the `matrixControlTable`, the `matrixSDTable`, and the `matrixDSTable`.

9.3.10 The Filter Group

The filter group allows packets to be matched by a filter equation. These matched packets form a data stream that may be captured or may generate events. This group consists of the `filterTable` and the `channelTable`.

9.3.11 The Packet Capture Group

The Packet Capture group allows packets to be captured after they flow through a channel. This group consists of the `bufferControlTable` and the `captureBufferTable`, and requires the implementation of the filter group.

9.3.12 The Event Group

The event group controls the generation and notification of events from this device. This group consists of the `eventTable` and the `logTable`.

9.4 Control of RMON Devices

Due to the complex nature of the available functions in these devices, the functions often need user configuration. In many cases, the function requires parameters to be set up for a data collection operation. The operation can proceed only after these parameters are fully set up.

Many functional groups in this MIB have one or more tables in which to set up control parameters, and one or more data tables in which to place the results of the operation. The control tables are typically read–write in nature, while the data tables are typically read–only. Because the parameters in the control table often describe resulting data in the data table, many of the parameters can be modified only when the control entry is invalid. Thus, the method for modifying these parameters is to invalidate the control entry, causing its deletion and the deletion of any associated data entries, and then create a new control entry with the proper parameters. Deleting the control entry also gives a convenient method for reclaiming the resources used by the associated data.

Some objects in this MIB provide a mechanism to execute an action on the remote monitoring device. These objects may execute an action as a result of a change in the state of the object. For those objects in this MIB, a request to set an object to the same value as it currently holds would thus cause no action to occur.

To facilitate control by multiple managers, resources have to be shared among the managers. These resources are typically the memory and computation resources that a function requires.

9.4.1 Resource Sharing Among Multiple Management Stations

When multiple management stations wish to use functions that compete for a finite amount of resources on a device, a method to facilitate this sharing of resources is required. Potential conflicts include:

- Two management stations wish to simultaneously use resources that together would exceed the capability of the device.
- A management station uses a significant amount of resources for a long period of time.
- A management station uses resources and then crashes, forgetting to free the resources so others may use them.

A mechanism is provided for each management station initiated function in this MIB to avoid these conflicts and to help resolve them when they occur. Each function has a label identifying the initiator (owner) of the function. This label is set by the initiator to provide for the following possibilities:

- A management station may recognize resources it owns and no longer needs.
- A network operator can find the management station that owns the resource and negotiate for it to be freed.
- A network operator may decide to unilaterally free resources another network operator has reserved.
- Upon initialization, a management station may recognize resources it had reserved in the past. With this information it may free the resources if it no longer needs them.

Management stations and probes should support any format of the owner string dictated by the local policy of the organization. It is suggested that this name contain one or more of the following: IP address, management station name, network manager's name, location, or phone number. This information will help users to share the resources more effectively.

There is often default functionality that the device or the administrator of the probe (often the network administrator) wishes to set up. The resources associated with this functionality are then owned by the device itself or by the network administrator, and are intended to be long–lived. In this case, the device or the administrator will set the relevant owner object to a string starting

with “monitor”. Indiscriminate modification of the monitor–owned configuration by network management stations is discouraged. In fact, a network management station should only modify these objects under the direction of the administrator of the probe.

Resources on a probe are scarce and are typically allocated when control rows are created by an application. Since many applications may be using a probe simultaneously, indiscriminate allocation of resources to particular applications is very likely to cause resource shortages in the probe.

When a network management station wishes to utilize a function in a monitor, it is encouraged to first scan the control table of that function to find an instance with similar parameters to share. This is especially true for those instances owned by the monitor, which can be assumed to change infrequently. If a management station decides to share an instance owned by another management station, it should understand that the management station that owns the instance may indiscriminately modify or delete it.

It should be noted that a management application should have the most trust in a monitor–owned row because it should be changed very infrequently. A row owned by the management application is less long–lived because a network administrator is more likely to re– assign resources from a row that is in use by one user than from a monitor–owned row that is potentially in use by many users. A row owned by another application would be even less long–lived because the other application may delete or modify that row completely at its discretion.

9.4.2 Row Addition Among Multiple Management Stations

The addition of new rows is achieved using the method described in RFC 1212. In this MIB, rows are often added to a table in order to configure a function. This configuration usually involves parameters that control the operation of the function. The agent must check these parameters to make sure they are appropriate given restrictions defined in this MIB as well as any implementation specific restrictions such as lack of resources. The agent implementor may be confused as to when to check these parameters and when to signal to the management station that the parameters are invalid. There are two opportunities:

- When the management station sets each parameter object.
- When the management station sets the entry status object to valid.

If the latter is chosen, it would be unclear to the management station which of the several parameters was invalid and caused the `badValue` error to be emitted. Thus, wherever possible, the implementor should choose the former as it will provide more information to the management station.

A problem can arise when multiple management stations attempt to set configuration information simultaneously using SNMP. When this involves the addition of a new conceptual row in the same control table, the managers may collide, attempting to create the same entry. To guard against these collisions, each such control entry contains a status object with special semantics that help to arbitrate among the managers. If an attempt is made with the row addition mecha-

nism to create such a status object and that object already exists, an error is returned. When more than one manager simultaneously attempts to create the same conceptual row, only the first will succeed. The others will receive an error.

When a manager wishes to create a new control entry, it needs to choose an index for that row. It may choose this index in a variety of ways, hopefully minimizing the chances that the index is in use by another manager. If the index is in use, the mechanism mentioned previously will guard against collisions. Examples of schemes to choose index values include random selection or scanning the control table looking for the first unused index. Because index values may be any valid value in the range and they are chosen by the manager, the agent must allow a row to be created with any unused index value if it has the resources to create a new row.

Some tables in this MIB reference other tables within this MIB. When creating or deleting entries in these tables, it is generally allowable for dangling references to exist. There is no defined order for creating or deleting entries in these tables.

9.5 Conventions

The following conventions are used throughout the RMON MIB and its companion documents.

- **Good Packets**

  Good packets are error–free packets that have a valid frame length. For example, on Ethernet, good packets are error–free packets that are between 64 octets long and 1518 octets long. They follow the form defined in IEEE 802.3 section 3.2.

- **Bad Packets**

  Bad packets are packets that have proper framing and are therefore recognized as packets, but contain errors within the packet or have an invalid length. For example, on Ethernet, bad packets have a valid preamble and System Function Description (SFD), but have a bad CRC, or are either shorter than 64 octets or longer than 1518 octets.

Most RMON providers implement enough of the RMON specification (usually the first seven groups) to support these data link and traffic flow analysis functions. A fully instrumented RMON probe offers additional packet capture capabilities that allow it to be used as a data collection mechanism for more extensive network analysis and accounting applications. RMON groups eight and nine deliver the information needed to support sophisticated protocol analyzer and network accounting functions such as:

- Packet traps to provide network alarms
- Packet capture for network traffic decoding and analysis
- Source data to support network accounting/billing applications

As mentioned earlier, RMON can be supported by hardware monitoring devices (known as

"probes") or through software or some combination. For example, Cisco's line of LAN switches includes software in each switch that can trap information as traffic flows through and record it in its MIB. A software agent can gather the information for presentation to the network administrator with a graphical user interface. A number of vendors provide products with various kinds of RMON support.

RMON collects nine kinds of information, including packets sent, bytes sent, packets dropped, statistics by host, by conversations between two sets of addresses, and certain kinds of events that have occurred. A network administrator can find out how much bandwidth or traffic each user is imposing on the network and what Web sites are being accessed. Alarms can be set in order to be aware of impending problems.

RMON and Switched Networking

The movement toward RMON–based network management is closely linked to the rise of switched networking. While LAN switching is on the rise as the way to improve network performance, it poses special problems for conventional SNMP management methods. In a network formed using hubs, a LAN analyzer has full visibility because the medium is shared by all nodes. But a switched LAN is not a shared medium; so to maintain the same level of visibility, the analyzer would have to be placed on each switched port. A prudent solution is to incorporate the probe part of the analyzer directly into the switch's hardware. This is the function of an RMON probe.

9.6 Expanded MIB–II Tree and RMON Group

Figure 9.3 shows an expanded MIB–II tree. This is the same as the tree of Figure 8.15 except that we have added *rmon(16)*.

The RMON group is node 16 under MIB–II {mib–2 16} and all RMON groups under {mib–2 16} are shown in Figure 9.3. The entire RMON group consists of nine Ethernet RMON1 groups, one token ring extension group and ten RMON2 groups. RMON1 is defined in RFC 1513 and RMON2 is defined in RFC 2021. RMON1 operates at the Link layer of the OSI model whereas RMON2 operates in the upper five (Network through Application) of the OSI model.

9.7 RMON1

RMON1 is specified by RFC 1757 for Ethernet LANs and by RFC 1513 for Extensions to Token ring LANs.

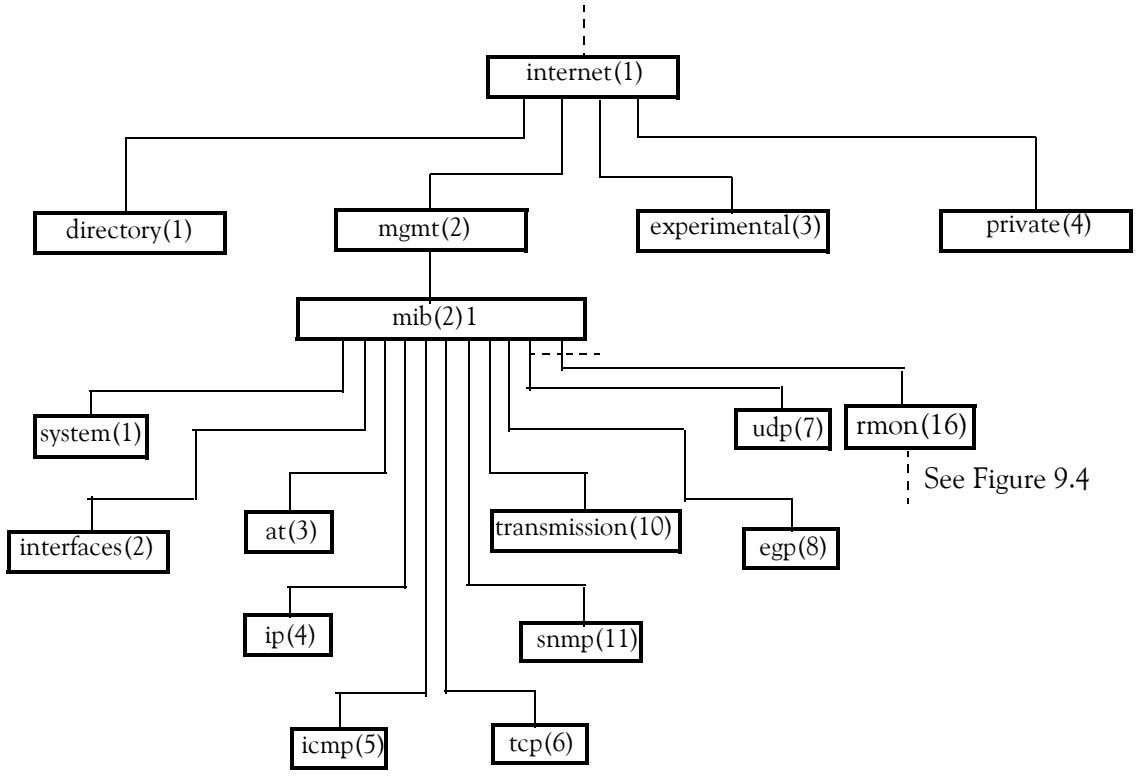


Figure 9.3. Expanded MIB–II tree

9.7.1 RMON1 Ethernet Groups

The RMON1 MIB defines the following 10 groups:

```
rmon OBJECT IDENTIFIER ::= { mib-2 16 }
statisticsOBJECT IDENTIFIER ::= { rmon 1 }
historyOBJECT IDENTIFIER ::= { rmon 2 }
alarmOBJECT IDENTIFIER ::= { rmon 3 }
hostsOBJECT IDENTIFIER ::= { rmon 4 }
hostTopNOBJECT IDENTIFIER ::= { rmon 5 }
matrixOBJECT IDENTIFIER ::= { rmon 6 }
filterOBJECT IDENTIFIER ::= { rmon 7 }
captureOBJECT IDENTIFIER ::= { rmon 8 }
eventOBJECT IDENTIFIER ::= { rmon 9 }
```

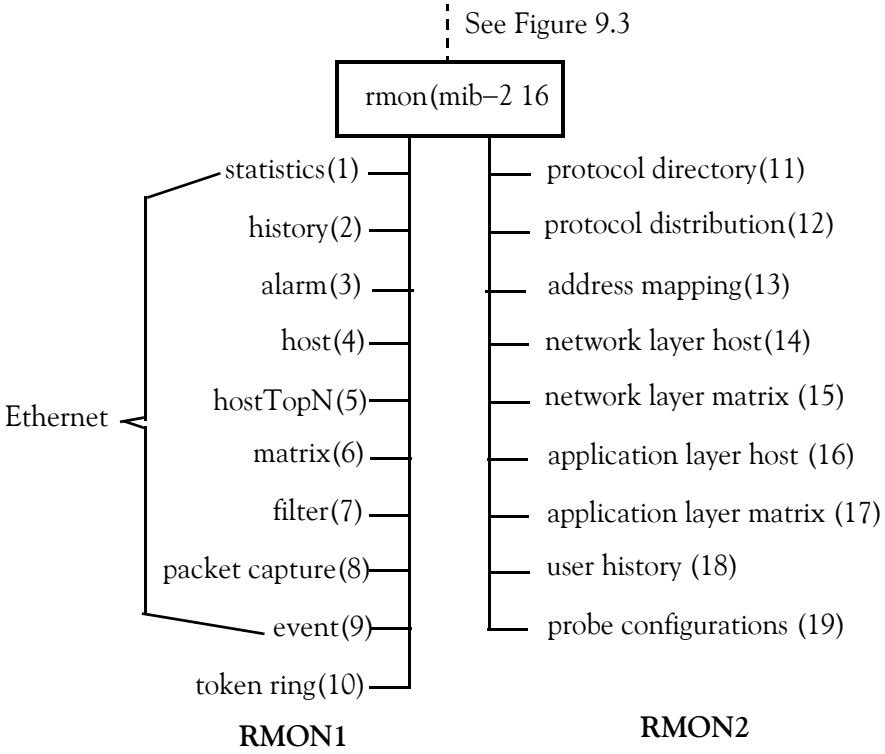


Figure 9.4. The Entire RMON Group

RMONl provides packet–level statistics about an entire LAN or WAN. The rmon object identifier is 1.3.6.1.2.1.16 (*iso.org.dod.internet.mgmt.mib–2.rmon*). RMONl is made up of nine Ethernet groups and a Token ring network which will be discussed in the next subsection.

`statistics` (1.3.6.1.2.1.16.1) Contains statistics about all the Ethernet interfaces monitored by the probe.

`history` (1.3.6.1.2.1.16.2) Records periodic statistical samples from the statistics group
`alarm` (1.3.6.1.2.1.16.3) Allows a user to configure a polling interval and a threshold for any object the RMON probe records.

`hosts` (1.3.6.1.2.1.16.4) Records traffic statistics for each host on the network.

`hostTopN` (1.3.6.1.2.1.16.5) Contains host statistics used to generate reports on hosts that top a list ordered by a parameter in the host table.

`matrix` (1.3.6.1.2.1.16.6) Stores error and utilization information for sets of two addresses

`filter` (1.3.6.1.2.1.16.7) Matches packets based on a filter equation; when a packet matches the filter, it may be captured or an event may be generated.

`capture` (1.3.6.1.2.1.16.8) Allows packets to be captured if they match a filter in the filter group.

`event` (1.3.6.1.2.1.16.9) Controls the definition of RMON events.

9.7.2 RMON1 Token Ring

The Remote Network Monitoring MIB, RFC 1271, defines a framework for remote monitoring functions implemented on a network probe. That MIB defines objects broken down into nine functional groups. Some of those functional groups, the statistics and the history groups, have a view of the data–link layer that is specific to the media type and require specific objects to be defined for each media type. RFC 1271 defined those specific objects necessary for Ethernet. RFC 1513 includes four groups that define those specific objects necessary for Token Ring LANs. In addition, it defines some additional monitoring functions specifically for Token Ring. These are defined in the Ring Station Group, the Ring Station Order Group, the Ring Station Configuration Group, and the Source Routing Statistics Group.

The Token Ring Statistics Groups

The Token Ring statistics groups contain current utilization and error statistics. The statistics are broken down into two groups, the Token Ring Mac–Layer Statistics Group and the Token Ring Promiscuous Statistics Group. The Token Ring Mac–Layer Statistics Group collects information from Mac Layer, including error reports for the ring and ring utilization of the Mac Layer. The Token Ring Promiscuous Statistics Group collects utilization statistics from data packets collected promiscuously.

The Token Ring History Groups

The Token Ring History Groups contain historical utilization and error statistics. The statistics are broken down into two groups, the Token Ring Mac–Layer History Group and the Token Ring Promiscuous History Group. The Token Ring Mac–Layer History Group collects information from Mac Layer, including error reports for the ring and ring utilization of the Mac Layer. The Token Ring Promiscuous History Group collects utilization statistics from data packets collected promiscuously.

The Token Ring Station Group

The Token Ring Station Group contains statistics and status information associated with each Token Ring station on the local ring. In addition, this group provides status information for each ring being monitored.

The Token Ring Station Order Group

The Token Ring Station Order Group provides the order of the stations on monitored rings.

The Token Ring Station Config Group

The Token Ring Station Config Group manages token ring stations through active means. Any station on a monitored ring may be removed or have configuration information downloaded from it.

The Token Ring Source Routing Group

The Token Ring Source Routing Group contains utilization statistics derived from source routing information optionally present in token ring packets.

9.8 RMON2

RMON2 enhances RMON1 by providing network through application–level statistical gathering. RFC 2021 provides updated information on what enhancements this version of RMON brings to network monitoring.

The RMON2 MIB defines the following 10 groups.

```
rmon OBJECT IDENTIFIER ::= { mib-2 16 }
protocolDirOBJECT IDENTIFIER ::= { rmon 11 }
protocolDistOBJECT IDENTIFIER ::= { rmon 12 }
addressMapOBJECT IDENTIFIER ::= { rmon 13 }
n1HostOBJECT IDENTIFIER ::= { rmon 14 }
n1MatrixOBJECT IDENTIFIER ::= { rmon 15 }
a1HostOBJECT IDENTIFIER ::= { rmon 16 }
a1MatrixOBJECT IDENTIFIER ::= { rmon 17 }
usrHistoryOBJECT IDENTIFIER ::= { rmon 18 }
probeConfigOBJECT IDENTIFIER ::= { rmon 19 }
```

These groups perform the following functions:

`protocolDir (1.3.6.1.2.1.16.11)` Performs inventory of protocols

`protocolDist (1.3.6.1.2.1.16.12)` Maintains statistics on octets and pockets

`addressMap (1.3.6.1.2.1.16.13)` Provides address translation to network address on each interface

`n1Host (1.3.6.1.2.1.16.14)` Measures traffic from and to each network address.

`n1Matrix (1.3.6.1.2.1.16.15)` Provides information on the conversation between pairs of hosts in both directions.

`a1Host (1.3.6.1.2.1.16.16)` Computes traffic by protocol units

`a1Matrix (1.3.6.1.2.1.16.17)` Generates a report on the top N protocol conversations

`usrHistory (1.3.6.1.2.1.16.18)` Collects user–specified historical data on alarms and statistics

`probeConfig (1.3.6.1.2.1.16.19)` Provides configuration of probe parameters.

9.9 Cisco's RMON

The recently announced software enhancements to the Catalyst™ workgroup switch make it the industry's first LAN switch to support embedded RMON software. Cisco has teamed with Frontier Software to produce the industry's most advanced traffic analysis and troubleshooting capabilities for switched networks in this newest release (3.0) of Catalyst. With its embedded RMON software, Catalyst now provides network administrators enhanced visibility of their switched network traffic and offers them more powerful and cost–effective ways to troubleshoot and tune switched network performance.

Complementing Catalyst's enhanced monitoring capabilities is NETScout Manager, a Graphical User Interface (GUI)–based RMON console manager. Its powerful RMON filtering and monitoring functions help network administrators manage the complex information available from the RMON Management Information Base (MIB). A collection of tools provides extensive graphing, alarm, logging, and reporting capabilities.

9.9.1 Cisco's RMON Switches, Bridges, and Routers

Although LAN switching is being embraced as a cost–effective means of improving network performance, it has also brought its own set of management problems to network administrators. Since most LAN switches behave like bridges or routers, network managers must reassess the way they monitor the traffic on a LAN. Using conventional methods, a network administrator would be forced to deploy a network analyzer to each switched LAN segment to maintain the same coverage obtained from one LAN analyzer on a shared network.

Figure 9.5 shows how a typical RMON configuration could grow without bounds. Obviously, as our network grows and we keep adding devices with probes, our configuration becomes very expensive and less effective.

Cisco offers a unique solution by integrating monitoring functions into its LAN switching platform. Because of the Catalyst switch's multiprocessor design (one processor dedicated exclusively for management), it can simultaneously perform as both a LAN switch and a multi–segment RMON network probe.

To provide both network monitoring and switching performance optimally, Catalyst can be configured to collect network traffic data in two ways. In standard RMON mode, Catalyst can collect and forward comprehensive network traffic information from multiple Ethernet segments simultaneously. This allows the network administrator to obtain all the information necessary to help tune or troubleshoot a switched LAN. The benefit of concurrently collecting multiple traffic feeds is obvious for network administrators who attach workgroup servers to dedicated Ethernet seg-

ments to improve network performance. If network administrators need to troubleshoot client/server applications, the task is greatly simplified through Catalyst's ability to simultaneously record traffic from both the server's and the client's segments.

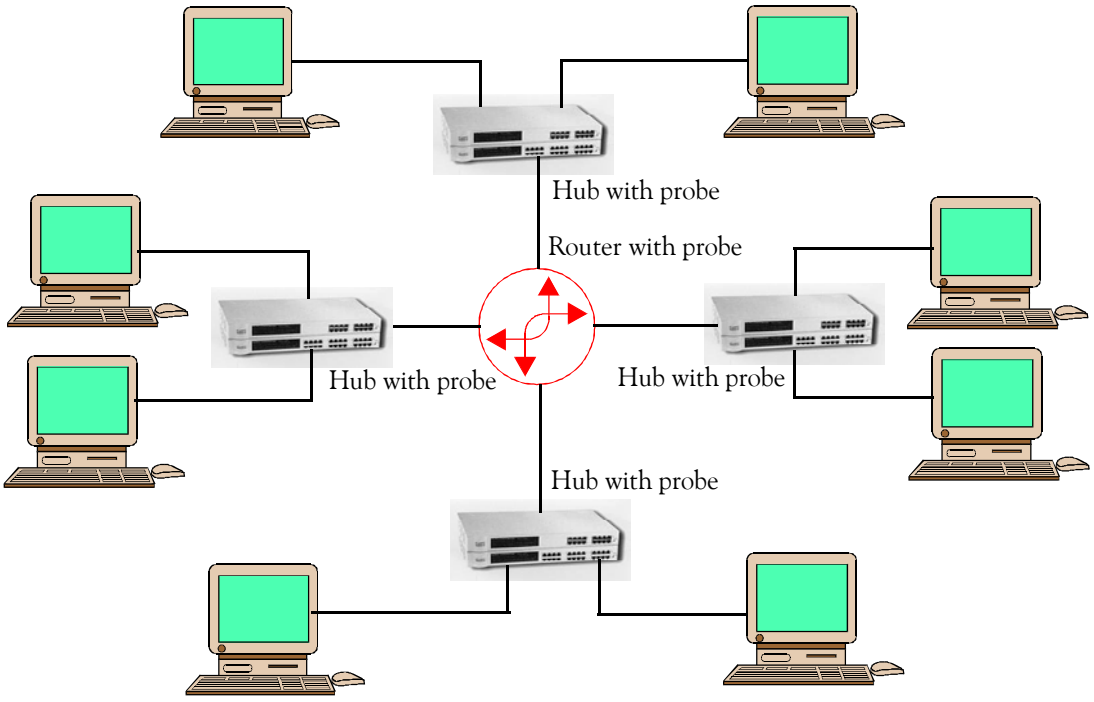


Figure 9.5. Typical RMON Configuration that could grow without bounds

Cisco's Catalyst supports a secondary monitoring mode that provides more focused coverage across all of its eight switched Ethernet segments. Called *Roving RMON**, this mode allows the network administrator to monitor either of two RMON groups across all eight Catalyst Ethernet segments. Roving RMON can be used to collect historical network traffic data (like total switched data including packets, octets, and errors) per port or even per station. The network manager can use this data for various tasks such as capacity planning analysis or network accounting and billing.

Catalyst's Roving RMON also has a unique, user–definable trap feature that lets it reconfigure itself in case it detects specific network events. Network administrators can preconfigure the Catalyst to look out for potentially threatening conditions such as excessive collisions, corrupted packets, or even excessive traffic from a specific station. If the switch detects one of these predefined conditions, it sends an alert (trap) to the network management console and simultaneously initializes a fully configured RMON probe to monitor traffic on the offending network segment. With this function, network administrators can detect and collect troubleshooting data

* *Roving RMON simply means that for limited environments, where all groups cannot be supported on all interfaces simultaneously, we may choose which groups should be activated based on certain automatic threshold criteria or by our selection.*

automatically, thereby extending their management capability while also helping to recognize and rectify network problems before they affect users.

9.9.2 User Friendly Interface to RMON

The usefulness of a comprehensive switching and monitoring platform is only as valuable as the accessibility of the information available to the network administrator. The ability to centrally configure, control, and manage these RMON agents with an easy–to–use, GUI–based console becomes a necessity as more RMON–capable systems are deployed throughout the network. Leveraging configuration and monitoring functions with semi–automated network traffic recording, configurable alarms, and accounting functions further simplifies network administrators' duties while improving their ability to maintain reliable, trouble–free networks. The following paragraphs describe some of the features needed in an RMON GUI.

Easy to Use and Understand Statistics

The console monitor should present RMON data in a format that is easy to view and understand. The network administrator should be able to create customizable "views" of the RMON traffic information coming from specific segments attached to the network analyzer. With customizable views, network administrators can troubleshoot their network applications more effectively by selecting specific elements from the RMON MIB.

Filter and Configuration Tools

Since the RMON MIB can monitor virtually all network traffic, it is also important that the monitor console has the necessary tools to easily manage the myriad bits of information that can be collected from a LAN segment. These tools should let the administrator select specific information provided by the RMON MIB, such as data–link statistics, traffic history, host traffic, and host matrix information. If the RMON agent also supports packet capture for protocol analysis, the console monitor should provide the tools to display the various protocol layers contained in the packet.

Protocol filter tools should support popular protocols (like TCP/IP, XNS, Novell IPX, or AppleTalk) and should let the administrator view higher–level services as well (like NFS, SNMP, Apple ARP, and DEC LAT, to name a few). Console monitors with comprehensive filter tools can help network administrators save configuration and troubleshooting time. Flexibility in defining custom filters also ensures the long–term value of the console monitor as new systems and protocols are introduced to the network.

Alarm Functions and Automated Data Capture

The RMON console's ability to automatically capture network traffic data and provide alarms is also valuable to the network administrator for network diagnosis and troubleshooting. A well–designed RMON console should allow the network administrator to define alarm conditions from any of the elements available in the RMON MIB. This level of flexibility helps the administrator

address virtually any potential network troubleshooting problem. For example, an event–logging feature, working in conjunction with the RMON alarm, could help track the frequency and timing of network events while also providing information that could help the network administrator track down the cause–and–effect relationships of network–related problems.

To help network administrators track and troubleshoot protocol–related network problems, both the RMON probe and the console should also provide the tools to automatically capture network packet data for offline analysis. The console manager should let the network administrator limit packet captures by using predefined or user–defined filters to help tailor the RMON probe functionality to meet specific troubleshooting needs.

Graphing, Accounting, and Reporting Tools

Finally, since fully instrumented RMON probes provide data to track network usage, a full–featured console manager should offer graphing, reporting, and accounting tools that help the network administrator track the growth and usage of the network. Graphing functions are useful for measuring and representing network traffic or server utilization over extended time periods. These graphs can show interesting trends in growth of network or server usage. Similarly, network administrators can use network accounting tools to show network resource usage by functional department. Reporting tools can help organize accounting data so that network administrators can produce usage information for budgeting or departmental billing purposes.

NETScout RAMON Console Management

The NETScout RMON console provides an easy–to–use GUI for monitoring RMON statistics and protocol analysis information. NETScout also provides extensive tools that simplify data collection, analysis and reporting. Applications include:

- GUI RMON monitor (browser)
- Simplified, user–definable RMON configuration and control tools
- Sophisticated RMON filter editor (Domain Manager)
- Protocol monitor and analyzer
- Traffic monitor
- Alarm manager (Watchdog) and automated data capture
- RMON graphics
- Report generator
- Event logger and database

These tools allow the administrator to monitor traffic, set thresholds, and capture data on any set of network traffic for any segment. They collect information about all nine RMON groups to isolate and determine problem conditions on the network.

NETScout is available on a variety of platforms including SunNet Manager, HP OpenView, IBM NetView 6000, and PC Windows. NETScout Manager can run as a complementary application to Cisco's network management applications (CiscoWorks™, Workgroup Director™), third–party network management applications (SunNet Manager, HP OpenView), or as a standalone application.

Table 9.1 lists Cisco's Catalyst features.

TABLE 9.1 Cisco's Catalyst Features

Feature	Catalyst
RMON Probe	
Instrumentation of all nine RMON groups (including packet capture and filtering)	Yes
RMON functionality without compromising switching performance	Yes
Simultaneously collect full RMON information for multiple segments	Four–segment capture without degradation
Means of monitoring all switched segments simultaneously	Roving RMON
RMON Console	
Easy–to–use, GUI–based interface	Yes
Preconfigured, user–definable filters for RMON data collection	Yes
Automated RMON console alarms	Yes
Semi–automated packet data capture	Yes
GUI–based protocol decode capability	Yes for 14 protocols
Graphing functions for network trend analysis	Yes
Network usage reporting functions	Yes
RMON console across a variety of management platforms	Yes; Sun, HP 9000/700, IBM RS/6000, and PC Windows

9.10 Viewing and Analyzing Statistics Using Optivity

Bay Networks Optivity Network Management System is a comprehensive network management solution. Its key features include fault management, performance analysis, reporting, and access level security. Optivity Network Management System is based on a client/server architecture that supports today's popular operating systems. It provides powerful visualization and drill–down capabilities that allow network managers to troubleshoot and isolate network problems, and it offers core service capabilities that provide a strong foundation for fault, topology, and statistics gathering for the Bay Networks family of products. Optivity Network Management System applications are engineered to be network–driven to support new hardware, helping network managers to quickly incorporate new equipment under a single management system.

9.10.1 Using Optivity Analysis with RMON

Optivity Analysis consists of a set of graphical network management applications based on RMON. These Optivity applications offer powerful RMON–based tools that work together to keep a network working optimally.

With Optivity, each RMON tool is a complete application. After the tool requests and receives information from the NMS, it processes the information and displays a graphical summary of network traffic. Each tool is configurable, so we can obtain exactly the type of information we need.

In Optivity Analysis, RMON tools represent an intelligent implementation of the RMON MIB groups. Table 9.2 provides a summary of RMON–based tools and lists the corresponding RMON MIB groups that may use to collect and present traffic statistics in graph form.

For detailed information about how to install, configure, and customize the RMON–based tools with RMON, and updated products, contact Bay Networks, www.baynetworks.com.

9.10.2 Using Optivity LAN with RMON

Optivity LAN offers two tools that we can use to monitor network statistics collected by the Ethernet Data Collection Module (DCM): *Threshold Manager* and *Fault Correlator*. These tools allow us to set thresholds on integer–based RMON objects and display trap information when the threshold is exceeded.

Threshold Manager Tool

After we establish a level of performance that we consider normal for our network, we can set up our system to generate responses whenever our network performance becomes abnormal.

In addition to generating fault information, we can set thresholds that initiate alarms whenever specified unfavorable network conditions occur. Whenever a threshold is met or exceeded, the specified event occurs and the alarm is triggered. The Optivity application allows us to set thresholds specific to a slot or port. With Threshold Manager, we can perform the following tasks:

- Display thresholds
- Add, delete, and modify thresholds
- Define custom thresholds on any MIB object (RMON only)
- Save and load thresholds to and from a file
- Save thresholds to nonvolatile random–access memory (N VRAM) (RMON only)

TABLE 9.2 Optivity Analysis RMON–based tools

Tool Name	Purpose	Possible Uses	Special Features	RMON MIB Group
Segment Statistics	Displays and records information from RMON statistics group. This information includes raw packet counts and bandwidth utilization.	Plan bandwidth–intensive tasks Baseline individual segment traffic characteristics	Ability to view multiple sessions Automatic utilization calculation based on available bandwidth History collection	Ethernet Statistics
Host Statistics	Displays traffic summaries for each host on a selected segment. Provides a HostTopN filter that allows us to concentrate on only the most active hosts on the network.	Determine which hosts are generating specific types of traffic	Filter for viewing TopN hosts Hotlink[a] packet capture	HostTable and HostTopN
Host Matrix	Presents statistics on conversations between host pairs on a selected segment.	Isolate sources of broadcasts, errors, etc. Locate work groups for segmentation	Sparse matrix[b] display Quick view of graphic coding of information Level 3 support for conversations by protocol Hotlink capture	Matrix
Filter/Capture	Define channels and filters Activate channels for captures	Capture packets for analysis of a specific problem or to provide selective traffic statistics	Flexible channel and filter editors Realtime display of counters Automatic capture activation form other tools	Filter and Packet Capture

TABLE 9.2 Optivity Analysis RMON–based tools

DecodeMan	Decode and display captured packet content	Troubleshoot problems by pipointing the source	Full seven–layer decode Quick search index Quick configuration of RMON probes for standalone operation	Filter and Packet Capture
Alarm Editor	View thresholds for segment Run Learning Tool locally	Modify individual normative models Run Learning Tool with local configuration for specific segment	Editing of individual thresholds and hysteresis values interactively.	Ancillary to Alarm and Events
Alarm Monitor	Continually monitor all segments	Proactive maintenance	Monitors all segments at once Quick filter by segment or alarm type Hotlink to Filter/ Capture and DecodeMan	Alarms and Events
Learning Tool	Automatically "learn" normal network behavior on all segments	Create normative model comprising threshold values for all segments	Learns automatically Flexible sample Builds model statically	Ancillary to Alarm and Events

a. *A hotlink is a connection made between application programs so that when changes are made to the data in one file, the changes appear instantly in the other. Hotlinks can be made in Windows and Macintosh.*

b. *A sparse matrix has most of the entries set to zero. This can be used with advantage in computations and saves memory and computing time.*

Fault Correlator Tool

After the alarm thresholds on RMON variables using the Threshold Manager have been set, the networks administrator can use the Fault Correlator tool to decode the traps that are sent to the network management station.

The Fault Correlator generates fault reports and calculates the current state of network objects and devices. It generates fault reports by reducing network faults and traps into network problems. Optivity automatically stores this information in the Optivity fault database.

When the management station is booted, the system starts Fault Correlator. Fault Correlator automatically assigns a health status to all network devices and builds an internal model of the network using information from the SuperAgent's domain database and incoming traps.

When a network device or other application receives a trap, the Fault Correlator uses the network model to determine which devices are related to the event. It determines the severity of the event by comparing the trap to the predefined fault and stated rules.

9.11 Summary

- RMON is a standard MIB that is separate but closely related to SNMP. Like SNMP, RMON is an open standard administered by the Internet Engineering Task Force (IETF). The RMON standard is an SNMP MIB definition described in RFC 1757. RMON1, or simply RMON is defined in RFC 2819. An enhanced version, referred to as RMON2, is defined in RFC 2021. RMON1 provides the Network Management Station (NMS) with packet–level statistics about the entire LAN, MAN, or WAN. RMON2 improves RMON1 by providing network–and–application level statistics.
- The basic differences between RMON and SNMP are:
- RMON is instrument–based, in that it uses specialized hardware (probes) to operate.
- RMON proactively (acting in advance) sends data instead of waiting to be polled, making it bandwidth–efficient and more responsive to network events.
- RMON is capable of collecting more detailed data.
- RMON instrumentation provides a powerful monitoring system but at a considerably larger monetary expense. Accordingly, RMON probes are normally installed on critical links such as network backbones and servers.
- RMON system can configured to provide such data as:
- Information regarding network utilization
- Historical information for network trend and statistical analysis
- Information describing communications between systems and the quantity of data exchanged
- RMONs have replaced expensive network analyzer devices that must be physically attached to the approximate area of a network problem. RMON probes come in different forms, depending on the size and type of device to be monitored:
- A RMON MIB that uses the monitored device's hardware (called an embedded agent)
- A specialized card module inserted into a slot within the monitored device
- A purpose–built probe externally attached to one or more monitored devices
- A dedicated PC attached to one or more monitored devices

The basic RMON goals are:

- Offline Operation
- Proactive Monitoring
- Problem Detection and Reporting
- Value Added Data

- Multiple Managers
- The RMON textual conventions and structure of MIB are defined in RFC 1757. The objects are arranged into the following groups:

- ethernet statistics
- history control
- ethernet history
- alarm
- host
- hostTopN
- matrix
- filter
- packet capture - event.

- Good packets are error–free packets that have a valid frame length.
- Bad packets are packets that have proper framing and are therefore recognized as packets, but contain errors within the packet or have an invalid length.
- The RMON group is node 16 under MIB–II (mib–2 16) and all RMON groups under mib–2 16 are shown in Figure 9.3. The entire RMON group consists of nine Ethernet RMON1 groups, one token ring extension group and ten RMON2 groups. RMON1 is defined in RFC 1513 and RMON2 is defined in RFC 2021. RMON1 operates at the Link layer of the OSI model whereas RMON2 operates in layers 3 through 7 of the OSI model.

9.12 Exercises

True/False

1. RMON is capable of collecting more detailed data than SNMP. _____

2. RMON1 operates only at the Data–link layer of the seven–layer OSI reference model. _____

3. RMON definitions are entirely different than those of the SNMP. _____

4. On an Ethernet LAN `good packets` are error–free packets that are between 32 and 64 octets long. _____

5. The group `statistics` (1.3.6.1.2.1.16.1) that is specified in RMON1 contains statistics about all the Ethernet interfaces monitored by the probe. _____

6. The group `nlHost` (1.3.6.1.2.1.16.14) that is specified in RMON2 provides information on the conversation between pair of hosts in both directions. _____

7. NETScout Manager is a Graphical User Interface (GUI) RMON console manager that enhances Cisco's Catalyst. _____

8. Optivity Analysis is a set of graphical network management based on RMON. _____

9. The Threshold Manager Tool is a tool that can be used with Bay Networks' Optivity LAN. _____

10. The Fault Correlator Tool is another tool that can be used with Bay Networks's Optivity LAN. _____

Multiple Choice

11. RMON2 operates at _____ layers of the OSI reference model.

A. all seven

B. the Network and Transport

C. the Presentation and Application

D. the upper five (Network through Application)

12. On an Ethernet LAN `bad packets` are packets that _____

A. have improper framing

B. are not recognized as packets

C. have proper framing and are therefore recognized as packets, but contain errors within the packet or have an invalid length.

D. none of the above

13. The group `hosts` (1.3.6.1.2.1.16.4) that is specified in RMON1 _____

A. records traffic statistics for each host on the network.

B. contains host statistics used to generate reports on hosts that top a list ordered by a parameter in the host table.

C. records periodic statistical samples from the statistics group.

D. none of the above

14. The Token Ring _____ Group contains statistics and status information associated with each Token Ring station on a local ring.

A. Ring Station Order

B. Ring Station

C. Ring Station Config Group

D. Source Routing

15. The group `a1Matrix` (1.3.6.1.2.1.16.17) that is specified in RMON2 _____

A. computes traffic by protocol units.

B. generates a report on the top N protocol conversations.

C. provides user–specified historical data on alarms and statistics.

D. none of the above

16. Cisco's NETScout is available on several platforms including _____

A. HP OpenView.

B. IBM NetView.

C. PC windows.

D. all of the above

17. With Bay Networks' Threshold Manager Tool we can _____

A. display thresholds.

B. save and load thresholds to and from a file.

C. add, delete, and modify thresholds.

D. all of the above

18. With Bay Networks's Fault Correlator Tool we can _____.

A. decode the traps that are sent to the NMS

B. generate fault reports.

C. calculate the current state of network objects and devices.

D. all of the above

19. We can use the Optivity Analysis RMON–based _____ tool to display and record raw packet counts and bandwidth utilization.

A. Host Statistics

B. Segment Statistics

C. Host Matrix

D. Filter/Capture

20. We can use the Optivity Analysis RMON–based _____ tool to monitor all segments continuously.

A. Learning Tool

B. Alarm Editor

C. Alarm Monitor

D. Segment Statistics

9.13 Answers to End–of–Chapter Exercises

True/False

1. T – Refer to page 9–1

2. T – Refer to page 9–3

3. F – Refer to page 9–4

4. F – Refer to page 9–10

5. T – Refer to page 9–13

6. F – Refer to page 9–15

7. T – Refer to page 9–16

8. T – Refer to page 9–21

9. T – Refer to page 9–21

10. T – Refer to page 9–23

Multiple Choice

11. D – Refer to page 9–11

12. C – Refer to page 9–10

13. A – Refer to page 9–13

14. B – Refer to page 9–14

15. B – Refer to page 9–15

16. D – Refer to page 9–20

17. D – Refer to page 9–21

18. D – Refer to page 9–23

19. B – Refer to Table 9.2, page 9–22

20. C – Refer to Table 9.2, page 9–23

Appendix A

Optimization of Cable Connections

This topic is known as network analysis. It is discussed in detail in a branch of mathematics called *operations research* that is concerned with financial and engineering economic problems. We will illustrate network analysis with a simple and yet practical example.

A.1 Network Analysis

A *network*, as defined in this appendix, is a set of points referred to as *nodes* and a set of lines referred to as *branches*. Thus, Figure A.1 is a network with 5 nodes *A, B, C, D* and *E*, and 6 branches, *AB, AC, AD, BD, BE,* and *CD*.

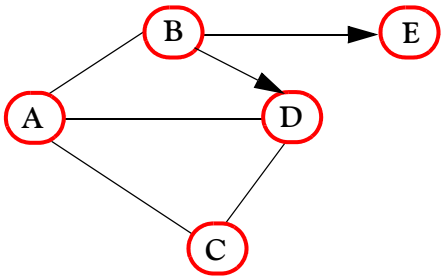


Figure A.1. A typical network

Branches can be either *directed* (or *oriented*), if they have a direction assigned to them, that is, one-way, or two-way. If no direction is assigned, they are considered to be two-way. Thus, the branches *BD* and *BE* in Figure A.1, are directed but the others are not.

A network is said to be *connected*, if there is a path (branch) connecting each pair of nodes. Thus, the network shown in Figure A.1 is connected. The network of Figure A.2 is also connected.

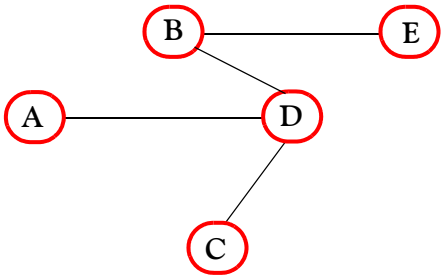


Figure A.2. A network which is connected

However, the network of Figure A.3 is not connected since the branch DC is removed.

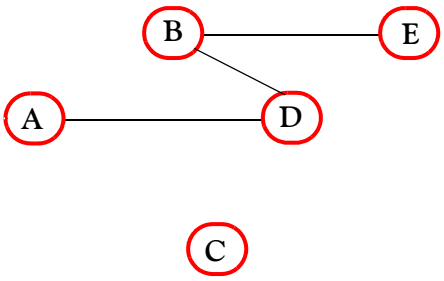


Figure A.3. A network which is not connected

A *tree* is a *connected network* which has *n* branches and *n+1* nodes. For example, the network of Figure A.4 is a tree network.

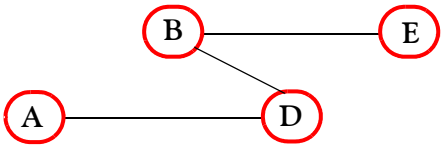


Figure A.4. A tree network

Network analysis is a method that is used to solve *minimum span problems*. In such problems, we seek to find a tree which contains all nodes, and the sum of the costs (shortest total distance) is a minimum.

Example A.1

Figure A.5 represents a network for a project that requires fiber optic cable to be installed to link 7 towns where a large corporation maintains facilities. The towns are the nodes, the branches indicate possible paths, and the numbers beside the branches, show the distance (not to scale) between towns in kilometers. Find the minimal spanning tree, that is, the least amount of fiber optic cable required to link each town.

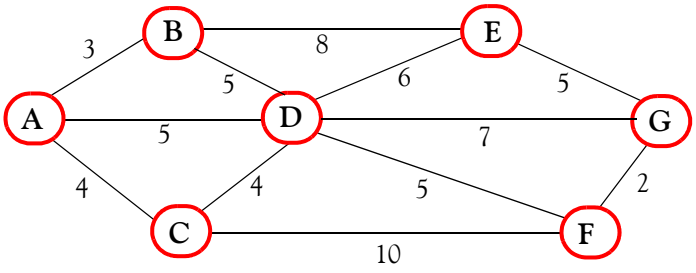


Figure A.5. Network for Example A.1

Solution:

For convenience, we redraw the given network with dotted lines as shown in Figure A.6, and we arbitrarily choose *A* as the starting node.

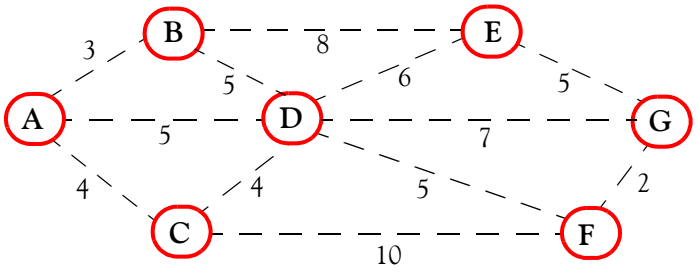


Figure A.6. Network of Example 14.5 with no connections

We observe that there are 3 branches associated with node *A*, i.e., *AB*, *AD*, and *AC*. By inspection, or from the expression

$$\min\{AB = 3, AD = 5, AC = 4\} = AB = 3 \tag{A.1}$$

we find that branch *AB* is the shortest. We accept this branch as the first branch of the minimum span tree, and we draw a solid line from Node *A* to Node *B* as shown in Figure A.7.

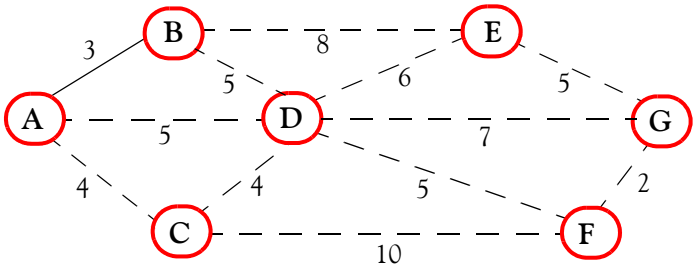


Figure A.7. Network of Example A.1 with first connection

Next, we consider all branches associated with Nodes *A* and *B*. We find that the minimum of these is

$$\min\{AD = 5, AC = 4, BD = 5, BE = 8\} = AC = 4 \tag{A.2}$$

and thus, *AC* is connected to the network as shown in Figure A.8.

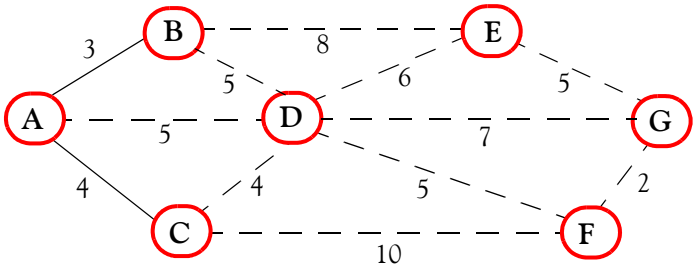


Figure A.8. Network of Example A.1 with the second connection

We continue by considering all branches associated with Nodes *A*, *B* and *C*, and we find that the shortest is

$$\min\{AD = 5, BE = 8, BD = 5, CD = 4, CF = 10\} = CD = 4 \qquad (A.3)$$

and we add branch *CD* to the network shown in Figure 14.16. The dotted lines *AD* and *BD* have been removed since we no longer need to consider branch *AD* and *BD*, because Nodes *B* and *D* are already connected; otherwise, we will not have a tree network.

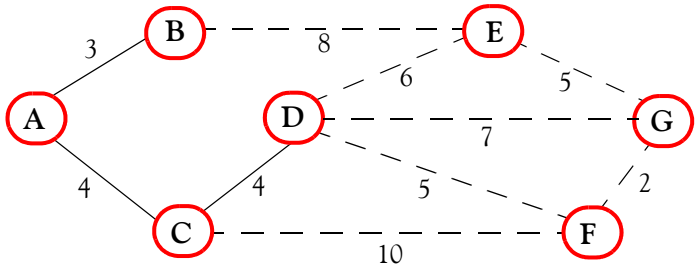


Figure A.9. Network of Example A.1 with the third connection

Next, considering all branches associated with Nodes *B*, *C*, and *D* and we find that the shortest is

$$\min\{BE = 8, DE = 6, DG = 7, DF = 5, CF = 10\} = DF = 5 \qquad (A.4)$$

and the network now is connected as shown in Figure A.10.

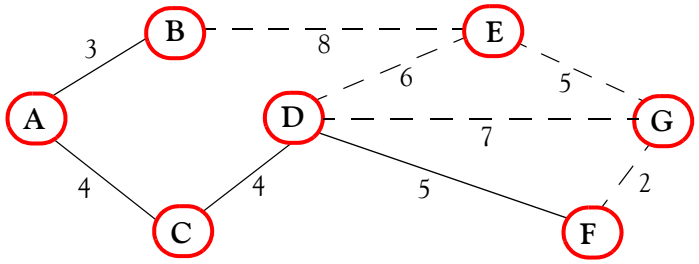


Figure A.10. Network of Example A.1 with the fourth connection

Continuing, we obtain

$$\min\{BE = 8, DE = 6, DG = 7\} = DE = 6 \qquad (A.5)$$

and the network is connected as shown in Figure A.11.

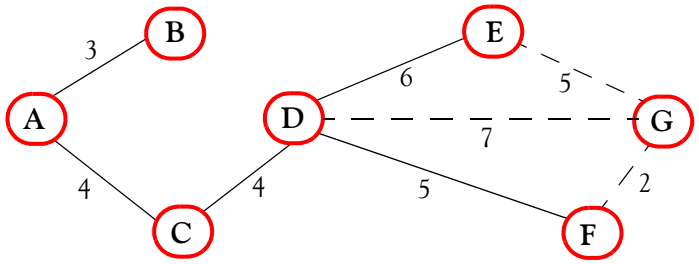


Figure A.11. Network of Example A.1 with the fifth connection

The last step is to determine the shortest branch to Node G. We find that

$$\min\{EG = 5, DG = 7, FG = 2\} = FG = 2 \tag{A.6}$$

and the complete minimum span tree is shown in Figure A.12.

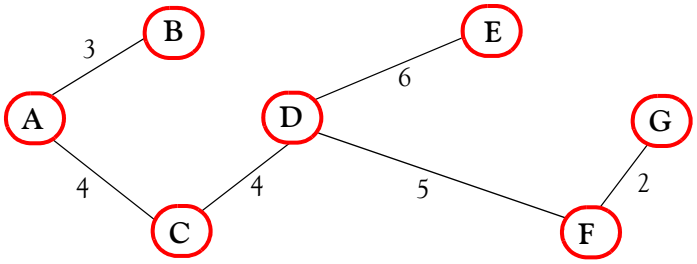


Figure A.12. Network of Example 14.5 with all connections

Figure A.12 shows that the minimum distance is $3 + 4 + 4 + 6 + 5 + 2 = 24$ kilometers.

A.2 Exercise

Repeat Example A.1 for the network below.

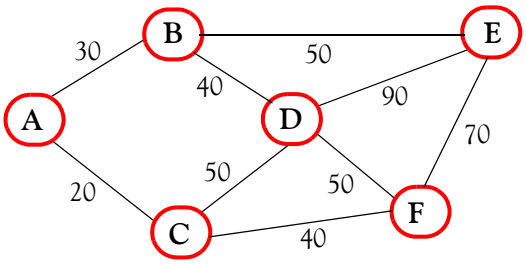


Figure A.13. Line graph for the exercise

Answer:

A→C = 20, A→B = 30, B→D = 40, C→F = 40, B→E = 50

Therefore, minimum length of cable is 20+30+40+40+50=180 Km

Appendix B

Binary Information and Standard Codes

This appendix is a review of the binary information representation, and the standard codes used for information processing systems, communications systems, and associated equipment. It provides the basic concepts to illustrate how networking devices work and communicate with others.

B.1 Binary Messages

Networking devices such as servers, client computers, routers, hubs, switches, and firewalls operate with signals that exhibit two discrete variations. These variations are represented by the absence of a pulse, also known as off pulse, and the presence of a signal, also known as on pulse. It is convenient to denote an off pulse as 0 (zero) and the on pulse as 1 (one). These zeros and ones are known as *bits* (*b*inary dig*its*). A file that consists of bits is known as a *binary file*. When a binary file is transmitted from one device to another, this process is referred to as binary transmission. A typical binary transmission is shown in Figure B.1.

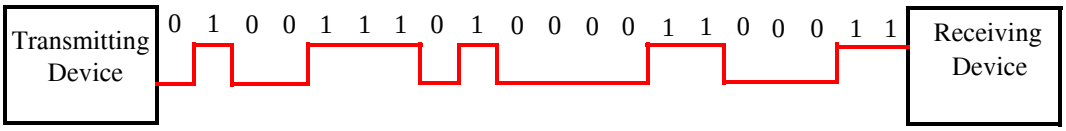


Figure B.1. Binary transmission

When a device is said to be operating at, say 100 Mbps (Million bits per second), this means that the device is capable of processing 100 million pulses (zeros and ones) per second.

A *byte* (or *octet*) is a group of eight bits. Because computers operate at very high speeds, it is convenient to speak of *binary words*. These are the number of bytes that a device can handle in each clock cycle.

A *computer clock* is an electronic circuit in a computer that generates a steady stream of timing pulses— the digital signals that synchronize every operation. The system clock signal is precisely set by a quartz crystal, typically at a specific frequency between 1 and 50 megahertz or megacycles. The clock rate of a computer is one of the prime determinants of its overall processing speed, and it can go as high as the other components of the computer allow. Also called system clock. The clock consists a square waveform as shown in Figure B.2.

When we say that Intel's Pentium is a 32-bit processor, it means that it can process 32 bits or 4 bytes per clock cycle. Likewise, Intel's Itanium is a 64-bit processor, meaning that it can process 64 bits or 8 bytes per clock cycle.

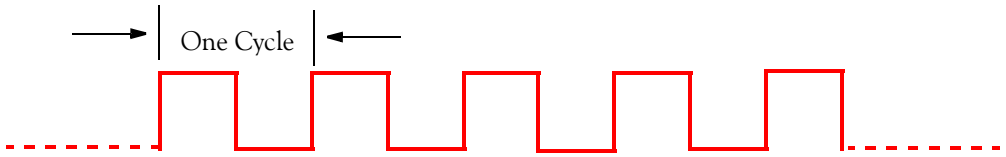


Figure B.2. The waveform of a typical computer clock

B.2 The American Standard Code for Information Interchange (ASCII)

ASCII is a standard seven-bit code that was proposed by the American National Standards Institute (ANSI). This coded character set is the accepted standard for interchange of information. It consists of 128 decimal numbers ranging from 0 through 127. These numbers are assigned to numbers, letters, punctuation marks, and the most special characters. The standard 7-bit character representation with b_7 the high-order bit b_1 the low-order bit is shown in Figure B.3.

BIT NUMBERS →								0_0	0_0	0_1	0_1	1_0	1_0	1_1	1_1
b_7	b_6	b_5	b_4	b_3	b_2	b_1	COLUMN → / ROW ↓	0	1	2	3	4	5	6	7
			0	0	0	0	0	NUL	DLE	SP	0	@	P	`	p
			0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
			0	0	1	0	2	STX	DC2	"	2	B	R	b	r
			0	0	1	1	3	ETX	DC3	#	3	C	S	c	s
			0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
			0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
			0	1	1	0	6	ACK	SYN	&	6	F	V	f	v
			0	1	1	1	7	BEL	ETB	'	7	G	W	g	w
			1	0	0	0	8	BS	CAN	(	8	H	X	h	x
			1	0	0	1	9	HT	EM	)	9	I	Y	i	y
			1	0	1	0	10	LF	SUB	*	:	J	Z	j	z
			1	0	1	1	11	VT	ESC	+	;	K	[	k	{
			1	1	0	0	12	FF	FS	,	<	L	\	l	|
			1	1	0	1	13	CR	GS	-	=	M	]	m	}
			1	1	1	0	14	SO	RS	.	>	N	^	n	~
			1	1	1	1	15	SI	US	/	?	O	_	o	DEL

Figure B.3. The Standard ASCII Code

As an example, the bit representation of the letter *j* is

b_7	b_6	b_5	b_4	b_3	b_2	b_1
1	1	0	1	0	1	0

The following is a description of the first 32 ASCII characters, often referred to as *control codes*.
NUL - A character code with a null value; literally, a character meaning "nothing." Although it is real in the sense of being recognizable, occupying space internally in the computer, and being sent or received as a character, a NUL character displays nothing, takes no space on the screen or on paper, and causes no specific action when sent to a printer. In ASCII, NUL is represented by the character code 0. It can be addressed like a physical output device (such as a printer) but that discards any information sent to it.

SOH – Start of Heading

STX – Start of Text

ETX - Marks the end of a text file. End-of-text does not necessarily mean end of transmission; other information, such as error-checking or transmission-control characters, can be included at the end of the file. In ASCII, end-of-text is represented by the decimal value 3 (hexadecimal 03).

EOT – End of Transmission (Not the same as ETB)

ENQ - Enquiry - A control code transmitted from one station to request a response from the receiving station.

ACK – Acknowledgement – A message sent by the receiving unit to the sending station or computer indicating either that the unit is ready to receive transmission or that a transmission was received without error.

BEL – Bell – Causes teletype machines to ring a bell. Causes a beep in many common terminals and terminal emulation programs.

BS – Backspace – Moves the cursor (or print head) move backwards (left) one space.
TAB – Horizontal Tab – Moves the cursor (or print head) right to the next tab stop. The spacing of tab stops is dependent on the device, but is often either 8 or 10.

LF – Linefeed – Tells a computer or printer to advance one line below the current line without moving the position of the cursor or print head.

VT – Vertical Tab

FF – Form Feed – Advances paper to the top of the next page (if the output device is a printer).

CR – Carriage Return – Tells a printer to return to the beginning of the current line. It is similar to the return on a typewriter but does not automatically advance to the beginning of a new line. For example, a carriage-return character alone, received at the end of the words “This is a sample line of text” would cause the cursor or printer to return to the first letter of the word “This.” In the ASCII character set, the CR character has the decimal value of 13 (hexadecimal 0D).

SO – Shift Out – Switches output device to alternate character set.

SI – Shift In – Switches output device back to default character set.

DLE – Data Link Escape

DC1 – Device Control 1

DC2 – Device Control 2

DC3 – Device Control 3

DC4 – Device Control 4

NAK – Negative Acknowledgement – A control code, ASCII character 21 (hexadecimal 15H), transmitted to a sending station or computer by the receiving unit as a signal that transmitted information has arrived incorrectly.

SYN – Synchronous – A character used in synchronous (timed) communications that enables the sending and receiving devices to maintain the same timing.

ETB – End of Transmission Block) – Not the same as EOT

CAN – Cancel

EM – End of Medium

SUB – Substitute

ESC – Escape – Usually indicates the beginning of an escape sequence (a string of characters that give instructions to a device such as a printer). It is represented internally as character code 27 (hexadecimal 1B).

FS – File Separator

GS – Group Separator

RS – Record Separator

US – Unit Separator

DEL – Delete

B.3 The Extended Binary Coded Decimal Interchange Code (EBCDIC)

The EBCDIC also known as *Extended ASCII Character Set* consists of 128 additional decimal numbers, that is, 256 decimal numbers. The range from 128 through 255 represents additional special, mathematical, graphic, and foreign characters. Software engineers write source code files consisting of alpha numerics, that is, alphabet characters and numbers, as well as other symbols. Eventually this code must be translated to machine language, that is, bits or bytes. This translation is performed by *compilers* which are special software applications and the files created are known as *executable* or *binary* files. An executable file is generally written with a short name followed by the *.exe* extension. Likewise, a binary file is identified with the *.bin* extension. Typical compilers are C++, Java, and others.

Appendix C

Common Number Systems and Conversions

This appendix is a review of the decimal, binary, octal, and hexadecimal numbers, their representation, and conversion from one base to another. The conversion procedures are illustrated with several examples.

C.1 Decimal, Binary, Octal, and Hexadecimal Systems

The familiar decimal number system has base or radix 10. It referred to as base ten because it uses ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. These digits are referred to as the *coefficients* of the decimal system. Thus, in the decimal system the coefficients are multiplied by the appropriate powers of 10 to form a number. For example, the decimal number 58, 392.46 is interpreted as:

$$\begin{aligned} 58,392.46 &= 50,000 + 8,000 + 300 + 90 + 2 + 0.4 + 0.06 \\ &= 5\times 10^{4} + 8\times 10^{3} + 3\times 10^{2} + 9\times 10^{1} + 2\times 10^{0} + 4\times 10^{-1} + 6\times 10^{-2} \end{aligned}$$

In general, any number may be represented by a series of coefficients as:

$$A_nA_{n-1}A_{n-2}\ldots\ldots A_2A_1A_0.A_{-1}A_{-2}\ldots\ldots A_{-n}$$

In the decimal system, the A_k coefficients are the ten coefficients (zero through nine), and the subscript value *k* denotes the power of ten by which the coefficient must be multiplied. Thus, the last expression above can also be written as

$$A_n\cdot 10^{n} + A_{n-1}\cdot 10^{n-1} + A_{n-2}\cdot 10^{n-2} + \ldots + A_2\cdot 10^{2} + A_1\cdot 10^{1} + A_0\cdot 10^{0} + A_{-1}\cdot 10^{-1} + \ldots + A_{-n}\cdot 10^{-n}$$

Digital computers use the binary (base 2) system which has only two coefficients, *0* and *1*. In the binary system each coefficient A_k is multiplied by 2^k. In general, a number of base *r* with coefficients A_k is expressed as

$$A_n\cdot r^{n} + A_{n-1}\cdot r^{n-1} + A_{n-2}\cdot r^{n-2} + \ldots + A_2\cdot r^{2} + A_1\cdot r^{1} + A_0\cdot r^{0} + A_{-1}\cdot r^{-1} + \ldots + A_{-n}\cdot r^{-n} \qquad (C.1)$$

The number 110010.01 could be interpreted as a binary, or decimal or any other base number since the coefficients *0* and *1* are valid in any number with base 2 or above. Therefore, it is a common practice to enclose the number in parenthesis and write a subscript representing the base of the number. Thus, if the number 110010.01 is binary, it is denoted as

$$(110010.01)_2$$

But if it is a decimal number, it should be denoted as

$$(110010.01)_{10}$$

Two other numbers of interest are the *octal* (base 8) and *hexadecimal* (base 16).

The octal system uses the coefficients 0 through 7. Thus, the number 5467.42 can be either an octal number or a decimal number. Accordingly, if it is an octal number, it must be denoted as

$$(5467.42)_8$$

But if it is a decimal number, it must be denoted as

$$(5467.42)_{10}$$

The hexadecimal number system uses the numbers 0 through 9 and the letters *A, B, C, D, E*, and *F*. These letters correspond to the decimal numbers *10, 11, 12, 13, 14*, and *15* respectively. Table C.1 shows the first 16 numbers of the decimal, binary, octal, and hexadecimal systems.

TABLE C.1 The first 16 decimal, binary, octal, and hexadecimal numbers.

Decimal (Base 10)	Binary (Base 2)	Octal (Base 8)	Hexadecimal (Base 16)
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F

C.2 Binary, Octal, and Hexadecimal to Decimal Conversions

A number in base r other than *base 10*, can be converted to its decimal equivalent using the following steps:

1. Express the given number in the form of (C.1).

2. Add the terms following the rules of decimal addition.

Example C.1

Convert the binary number $(1101.101)_2$ to its decimal equivalent.

Solution:

$$(1101.101)_2 = 1\times 2^3 + 1\times 2^2 + 0\times 2^1 + 1\times 2^0 + 1\times 2^{-1} + 0\times 2^{-2} + 1\times 2^{-3}$$
$$= 8 + 4 + 0 + 1 + 0.5 + 0 + 0.125 = (13.625)_{10}$$

Example C.2

Convert the octal number $(540.6)_8$ to its decimal equivalent.

Solution:

$$(540.6)_8 = 5\times 8^2 + 4\times 8^1 + 0\times 8^0 + 6\times 8^{-1}$$
$$= 5\times 64 + 4\times 8 + 0\times 1 + 6\times 8^{-1} = (352.75)_{10}$$

Example C.3

Convert the hexadecimal number $(DB0.A)_{16}$ to its decimal equivalent.

Solution:

$$(DB0.A)_{16} = D\times 16^2 + B\times 16^1 + 0\times 16^0 + A\times 16^{-1}$$
$$= 13\times 256 + 11\times 16 + 0\times 1 + 10\times 16^{-1} = (3,504.625)_{10}$$

We have learned how to convert any number of any base other than base *10* to its equivalent decimal. Now we will learn how to convert a decimal number to another base number. The procedure is as follows:

- An integer decimal number can be converted to any other base, say r, by repeatedly dividing the given decimal number by r until the quotient becomes zero. The first remainder obtained becomes the least significant digit, and the last remainder becomes the most significant digit of the base r number.
- A fractional decimal number can be converted to any other base, say r, by repeatedly multiplying the given decimal number by r until a number with zero fractional part is obtained. This, how-

ever, may not be always possible, i.e., the conversion may be endless as some examples to follow will show.

- A mixed (integer and fractional) decimal number can be converted to any other base number, say r, by first converting the integer part, then converting the fractional part, and finally combining these two parts.

Example C.4

Convert the decimal number $(39)_{10}$ to its binary equivalent.

Solution:

$$\begin{aligned}
39/2 &= \text{Quotient } 19 + \text{Remainder } 1 \text{ (lsb)}\\
19/2 &= \text{Quotient } 9 + \text{Remainder } 1\\
9/2 &= \text{Quotient } 4 + \text{Remainder } 1\\
4/2 &= \text{Quotient } 2 + \text{Remainder } 0\\
2/2 &= \text{Quotient } 1 + \text{Remainder } 0\\
1/2 &= \text{Quotient } 0 + \text{Remainder } 1 \text{ (msb)}
\end{aligned}$$

In the last step above, the quotient is 0; therefore, the conversion is completed and thus we have

$$(39)_{10} = (100111)_2$$

Example C.5

Convert the decimal number $(0.39654)_{10}$ to its binary equivalent.

Solution:

$$\begin{aligned}
0.39654 \times 2 &= 0.79308 = \mathbf{0} \text{ (msb of binary number)} + 0.79308\\
0.79308 \times 2 &= 1.58616 = \mathbf{1} \text{ (next binary digit)} + 0.58616\\
0.58616 \times 2 &= 1.17232 = \mathbf{1} + 0.17232\\
0.17232 \times 2 &= 0.34464 = \mathbf{0} + 0.34464\\
&\text{and so on}
\end{aligned}$$

We observe that, for this example, the conversion is endless; this is because the given fractional decimal number is not an exact sum of negative powers of *2*.

Therefore, for this example,

$$(0.39654)_{10} = (0.0110\ldots)_2$$

Example C.6

Convert the decimal number $(0.84375)_{10}$ to its binary equivalent.

Solution:

$$0.84375 \times 2 = 1.6875 = \mathbf{1}\ (\text{msb of binary number}) + 0.6875$$
$$0.6875 \times 2 = 1.375 = \mathbf{1}\ (\text{next binary digit}) + 0.375$$
$$0.375 \times 2 = 0.75 = \mathbf{0} + 0.75$$
$$0.75 \times 2 = 1.5 = \mathbf{1} + 0.5$$
$$0.5 \times 2 = 1.0 = \mathbf{1}\ (\text{lsb}) + 0.0$$

Since the fractional part of the last step above is 0, the conversion is complete and thus

$$(0.84375)_{10} = (0.11011)_2$$

For this example, the conversion is exact; this is because

$$(0.84375)_{10} = (0.11011)_2 = 1 \times 2^{-1} + 1 \times 2^{-2} + 0 \times 2^{-3} + 1 \times 2^{-4} + 1 \times 2^{-5}$$

Example C.7

Convert the decimal number $(39.84375)_{10}$ to its binary equivalent.

Solution:

Here, we first convert the integer part, i.e., 39 to its equivalent binary, then we convert the fractional part to its equivalent binary, and finally we combine the two parts to form the entire binary number. Thus, from Example C.4,

$$(39)_{10} = (100111)_2$$

and from Example C.6,

$$(0.84375)_{10} = (0.11011)_2$$

Therefore,

$$(39.84375)_{10} = (100111.11011)_2$$

Conversion from *decimal–to–octal* is accomplished by repeated division by 8 for the integer part, and by repeated multiplication by 8 for the fractional part.

Example C.8

Convert the decimal number $(345.158)_{10}$ to its octal equivalent.

Solution:

We first convert the integer part, next the fractional part, and then we combine these.
Integer part conversion:

$$345/8 = \text{Quotient } 43 + \text{Remainder } 1\ (\text{lsb})$$
$$43/8 = \text{Quotient } 5 + \text{Remainder } 3$$
$$5/8 = \text{Quotient } 0 + \text{Remainder } 5\ (\text{msb})$$

Fractional part conversion:

$$0.158 \times 8 = 1.264 = \mathbf{1}\ (\text{msb of fractional part}) + 0.264$$
$$0.264 \times 8 = 2.112 = \mathbf{2}\ (\text{next octal digit}) + 0.112$$
and so on

We observe that the fractional part conversion is endless; therefore,

$$(345.158)_{10} = (531.12\ldots)_8$$

Conversion from *decimal–to–hexadecimal* is accomplished by repeated division by 16 for the integer part, and by repeated multiplication by 16 for the fractional part.

Example C.9

Convert the decimal number $(389.125)_{10}$ to its hexadecimal equivalent.

Solution:

As before, we first convert the integer part, next the fractional part, and then we combine these.

Integer part conversion:

$$389/16 = \text{Quotient } 24 + \text{Remainder } 5\ (\text{lsb})$$
$$24/16 = \text{Quotient } 1 + \text{Remainder } 8$$
$$1/16 = \text{Quotient } 0 + \text{Remainder } 1\ (\text{msb})$$

Fractional part conversion:

$$0.125 \times 16 = 2.0 = \mathbf{2}\ (\text{msb of fractional part}) + 0.0$$

We observe that the conversion of this example is exact; therefore,

$$(389.125)_{10} = (185.2)_{16}$$

C.3 Binary-Octal-Hexadecimal Conversions

Since $2^3 = 8$ and $2^4 = 16$, it follows that each octal digit corresponds to three binary digits and each hexadecimal digit corresponds to four binary digits. Accordingly, to perform binary–to–octal conversion, we partition the binary number into groups of three digits each starting from the binary point and proceeding to the left for the integer part and to the right of the binary point for the fractional part.

Example C.10

Convert the binary number $(10110001101011.1111)_2$ to its octal equivalent.

Solution:

Since leading zeros (zeros to the left of the integer part of the number) and zeros added to the right of the last digit of the fractional part of the number do not alter the value of the number, we

partition the number in groups of three digits by inserting a zero to the left of the number (i.e. a leading zero), and two zeros to the right of the given number, and then we assign the equivalent octal value to each group as shown below.

$$\begin{array}{ccccccccc} 010 & 110 & 001 & 101 & 011 & . & 111 & 100 \\ 2 & 6 & 1 & 5 & 3 & & 7 & 4 \end{array}$$

Therefore,

$$(10110001101011.1111)_2 = (26153.74)_8$$

Conversion from octal–to–binary is accomplished in the reverse procedure, i.e. each octal digit is converted to its binary equivalent as it is shown in the following example.

Example C.11

Convert the octal number $(673.124)_8$ to its binary equivalent.

Solution:

Here, we replace each octal digit by its binary equivalent, i.e.,

$$\begin{array}{rccccccccc} (673.124)_8 = & 110 & 111 & 011 & . & 001 & 010 & 100 \\ & 6 & 7 & 3 & . & 1 & 2 & 4 \end{array}$$

Therefore,

$$(673.124)_8 = (110111011.001010100)_2$$

Conversion from binary–to–hexadecimal or hexadecimal–to–binary is performed similarly except that the binary number is divided into groups of four digits for the binary–to–hexadecimal conversion, or replacing each hexadecimal digit to its four digit binary equivalent in the hexadecimal–to–binary conversion.

Example C.12

Convert the binary number $(10110001101011.111101)_2$ to its hexadecimal equivalent.

Solution:

For this example, we insert two leading zeros to the left of the integer part and two zeros to the right of the decimal part, we partition the given binary number in groups of four digits, and we assign the equivalent hexadecimal digit to each binary group, that is,

$$\begin{array}{ccccccccc} 0010 & 1100 & 0110 & 1011 & . & 1111 & 0100 \\ 2 & C & 6 & B & . & F & 4 \end{array}$$

Therefore,

$$(10110001101011.111101)_2 = (2C6B.F4)_{16}$$

Example C.13

Convert the hexadecimal number $(306.D)_{16}$ to its binary equivalent.

Solution:

3	0	6	.	D
0011	0000	0110	.	1101

Therefore,

$$(306.D)_{16} = (1100000110.1101)_2$$

Appendix D

RSA Encryption

This appendix discusses the RSA Encryption, a public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up–to–date implementations.

D.1 How RSA Encryption Works

Let p and q be two large prime numbers, and let the prime number e, an exponent, be a coprime* to the product

$$(p-1)(q-1) \tag{D.1}$$

The product pq and the exponent e are referred to as *public key*, meaning that they can be made public, but the individual numbers p and q must be kept secret.

Now, let M denote a message (value) to be encrypted. The encryption function X is defined as

$$X = M^{e} (\text{mod } pq) \tag{D.2}$$

where *mod* is the modulus† of the product pq.

The decryption function Y is defined as

$$M = X^{d} (\text{mod } pq) \tag{D.3}$$

where M is the message to be decrypted, and d is a prime secret exponent found from the relation

$$d = \frac{a \cdot (p-1)(q-1) + 1}{e} \tag{D.4}$$

where a is an arbitrary odd number, not necessarily a prime number.

---

* *Two integers a and b are said to be* ***coprime*** *or* ***relatively prime*** *if they have no common factor other than 1 or, equivalently, if their greatest common divisor is 1.*

† *Modulus refers to a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value — the modulus. For example, in a 12–hour clock the modulus is 12, and if the current time is 11 AM, 3 hours later the time will be 2 PM, not 14 AM, and this is denoted as* $x = \text{mod}(14, 12) = 2$, *i.e., 2 PM.*

D.2 An Example

We wish to encrypt the value $M = 41$.

1. We begin by choosing the prime numbers $p = 59$, and $q = 47$. These are secret values.

2. We compute their product, that is $pq = 59 \times 47 = 2773$. This is referred to as the first public key.

3. We compute the product $(p-1)(q-1) = 58 \times 46 = 2668$, and we choose the secret exponent $e = 31$ observing that the value of e is a coprime to the value of $(p-1)(q-1)$.

4. Using the encryption function in equation (D.2), we obtain

$$\mathbf{X = M^{e} (\mathrm{mod}\ pq) = 41^{31} (\mathbf{mod}\ 2773)}$$

5. This expression is the same as

$$\mathbf{X = mod(41^{31}, 2773)}$$

but the value of $\mathbf{41^{31}}$ is too large to be evaluated by Excel or MATLAB. Therefore, we express it as

$$\mathbf{41^{31} = 41^{16+8+4+2+1} = 41^{16} \cdot 41^{8} \cdot 41^{4} \cdot 41^{2} \cdot 41^{1}}$$

and thus

$$X = \mathbf{41^{1} \cdot 41^{2} \cdot 41^{4} \cdot 41^{8} \cdot 41^{16}}\ \mathrm{mod}(2773)^{*}$$

Then,

$$\mathrm{mod}(41, 2773) = 41$$

$$\mathrm{mod}(41^{2}, 2773) = 1681$$

$$\mathrm{mod}(41^{4}, 2773) = 74$$

$$\mathrm{mod}(41^{8}, 2773) = 2703$$

$$\mathrm{mod}(41^{16}, 2773) = \mathrm{mod}(2703^{2}, 2773) = 2127$$

and

$$X = 41^{31} (\mathrm{mod}\ 2773) = 2127 \cdot 2703 \cdot 74 \cdot 1681 \cdot 41\ \mathrm{mod}(2773)$$

from which

* *The notations* mod(A, B) *and* Amod(B) *are equivalent.*

$$\begin{aligned} \mathrm{mod}(2127 \cdot 2703, 2773) &= 852 \\ \mathrm{mod}(852 \cdot 74, 2773) &= 2042 \\ \mathrm{mod}(2042 \cdot 1681, 2773) &= 2401 \\ \mathrm{mod}(2401 \cdot 41, 2773) &= 1386 \end{aligned}$$

and thus

$$X = 1386$$

6. For the decryption, the procedure is as follows:

In equation (D.4), we choose $a = 15$. Then,

$$d = \frac{a \cdot (p-1)(q-1)+1}{e} = \frac{15 \cdot 58 \cdot 46 + 1}{31} = 1291$$

and the message M is found from equation (D.3), i.e.,

$$\mathbf{M} = \mathbf{X}^{\mathbf{d}} (\mathrm{mod}\ pq) = 1386^{1291} (\mathrm{mod}\ 2773)$$

but this value is extremely large to be calculated by Excel or MATLAB. Therefore, let us express the exponent ***d*** as

$$d = 1291 = 1 + 2 + 8 + 256 + 1024$$

and thus

$$1386^{1291} = 1386^{1} \cdot 1386^{2} \cdot 1386^{8} \cdot 1386^{256} \cdot 1386^{1024}$$

Next, using Excel, we form the table below.

$$\begin{aligned} 1386^{1} (\mathrm{mod}\ 943) &= \mathrm{mod}(1386^{1}, 943) = 1386 \\ 1386^{2} (\mathrm{mod}\ 2773) &= \mathrm{mod}(1386^{2}, 2773) = 2080 \\ 1386^{4} (\mathrm{mod}\ 2773) &= \mathrm{mod}(2080^{2}, 2773) = 520 \\ 1386^{8} (\mathrm{mod}\ 2773) &= \mathrm{mod}(520^{2}, 2773) = 1419 \\ 1386^{16} (\mathrm{mod}\ 2773) &= \mathrm{mod}(1419^{2}, 2773) = 363 \\ 1386^{32} (\mathrm{mod}\ 2773) &= \mathrm{mod}(363^{2}, 2773) = 1438 \\ 1386^{64} (\mathrm{mod}\ 2773) &= \mathrm{mod}(1438^{2}, 2773) = 1959 \\ 1386^{128} (\mathrm{mod}\ 2773) &= \mathrm{mod}(1959^{2}, 2773) = 2622 \\ 1386^{256} (\mathrm{mod}\ 2773) &= \mathrm{mod}(2622^{2}, 2773) = 617 \\ 1386^{512} (\mathrm{mod}\ 2773) &= \mathrm{mod}(617^{2}, 2773) = 788 \\ 1386^{1024} (\mathrm{mod}\ 2773) &= \mathrm{mod}(788^{2}, 2773) = 2565 \end{aligned}$$

From rows 11, 9, 4, 2, and 1 above

$$1386^{1291}(\text{mod } 2773) = 2565 \cdot 617 \cdot 1419 \cdot 2080 \cdot 1386 \ (\text{mod } 2773)$$

and we compute the partial products below.

$$\begin{aligned} \text{mod}(2565 \cdot 617, 2773) &= 1995 \\ \text{mod}(1995 \cdot 1419, 2773) &= 2445 \\ \text{mod}(2445 \cdot 2080, 2773) &= 2691 \\ \text{mod}(2671 \cdot 1386, 2773) &= \mathbf{41} \end{aligned}$$

and we observe that the last value, i.e. 41, is the encrypted value $M = 41$

For this example, we chose small prime numbers so hat the computations could be performed with Excel or MATLAB. But in a real–world RSA encryption, the prime numbers are very large. A direct computation such as $783^{2896}\text{mod}(3124)$ will display a number 2 pages long.

Appendix E

Glossary of Computer / Internet Related Terms

10Base2 A standard for networking computers at 10 Mbps over RG–58 coaxial cable. 10Base2 uses the CSMA/CD method of networking in a linear bus configuration. 10Base2 was developed as an alternative to 10Base5 as the RG–8 cabling used by 10Base5 is rigid and difficult to work with and also requires external transceivers which are expensive. 10Base2 is also known as Thin Ethernet and Thin Net.

10Base5 A standard for networking computers at 10 Mbps over RG–8 or RG–11 coaxial cable. 10Base5 uses the CSMA/CD method of networking in a linear bus configuration. 10Base5 is the original Ethernet standard using external transceivers and a vampire clamp that fastens directly into the cable. The transceiver connects to a drop cable which is connected to a workstation network interface card via a 15–pin DIX connector. 10Base5 is also known as Thick Ethernet and Thick Net.

10BaseT A standard for networking computers at 10 Mbps over category 5 or category 3 unshielded twisted pair cable. 10BaseT uses the CSMA/CD method of networking and – equipment allowing – can co–exist with a 100BaseT Network. When installing a new network it is recommended that we use category 5 cable to allow the network to be upgraded to 100BaseT in the future without replacing the cabling.

10BaseFL A standard for networking computers at 10 Mbps over fibre optic cable. 10BaseFL uses the CSMA/CD method of networking.

100BaseFX A standard for networking computers at 100 Mbps over fibre optic cable. 100BaseFX uses the CSMA/CD method of networking.

100BaseT A standard for networking computers at 100 Mbps over category 5 unshielded twisted pair cable. 100BaseT uses the CSMA/CD method of networking and – equipment allowing – can co–exist with a 10BaseT Network.

32 Bit Refers to hardware or software that is capable of addressing instructions containing 32 bits per instruction.

3D API Three Dimensional Application Programming Interface – refers to any API that supports the creation of standard 3D objects, lights, cameras, perspectives, and so on. Such APIs include 3D Studio MAX and Microsoft's Reality Lab.

3D Sound When we hear things in the physical world, our ears pick up a variety of audible clues that tell us such things as "a truck is approaching me rapidly, from behind and to the left, and it's remarkably near." Until recently, however, most computer–generated sound was merely stereophonic. Sounds could appear from the left or right, but they had no real depth. The latest 3D sound techniques, including A3D from Aureal and Creative Labs' Environmental Audio, use tech-

niques to trick our ears into positioning sounds in three dimensions. Many 3D audio techniques require a specially designed sound card to work.

404 Error Is the error message we get when an Internet address we have tried to reach can't be located. It is usually seen in this format "404, URL Not Found".

56K Line A digital phone–line connection capable of carrying 56,000 bps. At this speed, a Megabyte will take about 3 minutes to transfer. This is twice as fast as a 28.8 Kbps modem. The figure is derived from the data capacity of a normal single channel digital telephone line (4 kHz) and the 16–bit encoding used to change analog signals to digital (4000 times 16 = 64000), minus the 8000 bit/s used for signalling and supervision.

64 Bit Refers to hardware or software that is capable of addressing instructions containing 64 bits per instruction.

802.1 A standard created by the IEEE responsible for maintaining what is now known as the spanning tree algorithm. The spanning tree algorithm is used by transparent bridges. They use this algorithm to detect other bridges on the network, remove loops, and to detect when another bridge fails.

802.2 A standard created by the IEEE that defines the standards for the Logical Link Control sublayer of the Data Link layer of the OSI Model.

802.3 Is a standard created by the IEEE that defines the CSMA/CD form of networking. Ethernet, which uses the CSMA/CD method of networking is defined by the 802.3 standard.

802.4 A standard created by the IEEE that defines Token–passing bus network systems. Almost all modern token–passing networks are rings, not bus types. This standard never really took off, and we will very rarely see it used.

802.5 A standard created by the IEEE that defines IBM's Token Ring network standard. This standard uses a logical ring topology running at 4 or 16 megabits.

802.6 A standard created by IEEE that defines standards for MANs. The main purpose of this standard is to define Distributed Queue Dual Bus (DQDB), a network with two physical channels.

802.7 A standard created by the IEEE that defines the Broadband Technology Advisory Group.

802.8 A standard created by the IEEE that defines the Fiber Optic Technical Advisory Group.

802.9 A standard created by the IEEE that defines Integrated Data and Voice Networks.

802.10 A standard created by the IEEE that defines network security issues.

802.11 A standard created by the IEEE that defines wireless network access protocols. See also Wireless Application Protocol (WAP).

802.12 Is a standard created by the IEEE that defines Hewlett–Packard's own 100–megabit stan-

dard for the next generation of networks. This new network type is called 100VG–AnyLAN.

AARP See AppleTalk Address Resolution Protocol.

Abend Short for abnormal end. The abnormal termination or a program or process through user input or program failure.

Abort The abnormal termination or a program or process through user input or program failure.

Accelerated Graphics Port A bus specification designed by Intel to allow affordable 3D graphics cards to provide high quality graphics by providing the graphic card fast access to the CPU.

Acceptable User Policy A set of rules and regulations for content and conduct permitted on a site or network. Acceptable User Policies are often stated for ISPs, networks, organizations, and universities.

Access Control List A list that contains user and group security identifiers (SIDs) for a server, with the associated privileges of each user and group. Each object, such as a file or folder, has an access control list associated with it.

Access Number The telephone number used by a subscriber to dial into an Internet Service Provider or online service.

Access Provider A company that provides Internet access, E–mail accounts and/or an online account to access their computer system. Also known as an Internet Service Provider.

Access Speed Refers to the average amount of time it takes for a storage device (Floppy, Hard or CD drive) to find any particular piece of data on a disk.

Account Policy The set of rules indicating how passwords and account lockout are managed in Windows NT. Account policy is managed by using the Account Policy dialog box in User Manager or User Manager for Domains.

ACK When a computer sends a block of data to another over a network, the receiving computer sends an acknowledgment code back to indicate that the transfer was successful. If there were errors detected in the transmission, the receiving computer would send a negative acknowledgment (NAK).

ACL See: Access Control List

Acoustic Coupler A type of modem which converts digital signals into sound for transmission through a telephone mouthpiece, and reception through a telephone ear speaker. Acoustic couplers generally have cups for the telephone handset.

Active Channels An Active Channel is what Microsoft calls a Web site that has been enabled for push delivery to Internet Explorer 4.x and 5.x browsers. To create a channel, developers write and upload Channel Definition Format (CDF) file to their Web site. New content is delivered to users automatically when the site is updated. Developers and subscribers can control the update frequency and other channel characteristics. Most Active Channels use Dynamic HTML (DHTML)

and other effects to spice up content and make it more interactive.

Active Directory A directory service from Microsoft Corporation, that integrates with the user organization's DNS structure. Active Directory is included in Windows 2000 and beyond.

Active Matrix Display A type of liquid crystal display where each display element or pixel includes an active component such as a transistor to maintain its state between scans. Active Matrix Displays were first used to provide better picture quality on laptop computers and are now widely used with desktop computers as well.

Active Partition A primary partition on the first hard disk in a computer that has been marked active by a partitioning program, such as Fdisk or Disk Manager. A computer loads its operating system from the active partition.

Active Server Pages A scripting environment for Microsoft Internet Information Server which allows the combination of HTML, scripts and reusable ActiveX server components to create dynamic web pages. Active server pages have the .asp file extension.

Active Window The top or front window in a multiple window environment. If our Windows 95/ 98/2000 or NT color scheme is set to default, the title bar of the active window will be blue while inactive windows' tile bars will be grey.

ActiveX Microsoft's answer to Java. ActiveX is a stripped down implementation of OLE designed to run over slow Internet links.

Address Book A feature of E–mail client applications that stores names and E–mail addresses in an accessible format.

Address Harvester A program that searches web pages and/or filters newsgroup traffic looking for valid E–mail addresses. Some address harvesters are benign, used only for compiling address directories. Most are run by miscreants compiling address lists to send unrequested advertising E–mails more commonly known as spam.

Address Resolution In order to communicate, computers on a network must know each other's MAC Address. Address resolution is the process of mapping a networked computer's IP address to its hardware address.

Address Resolution Protocol In order to communicate, computers on a network must know each other's MAC Address. Address resolution is the process of mapping a networked computer's IP address to its hardware address. Address Resolution Protocol is responsible for obtaining MAC addresses of TCP/IP hosts on broadcast based networks.

Address Verification System VISA® /MasterCard® headquarters introduced a new regulation requiring all businesses who manually key in the majority of their credit card transactions to have a special fraud prevention feature on their credit card processing equipment. This feature is referred to as an Address Verification System (it checks to see that the billing address given by the customer matches the credit card). If we opt not to use AVS, VISA® and MasterCard® will not

support our transactions and will charge us an additional 1.25% on those sales.

ADN See Advanced Digital Network

ADSL See Asymmetric Digital Subscriber Line

Advanced Digital Network A 56 Kbps dedicated leased–line.

Advanced Interactive Executive IBM's proprietary version of the UNIX operating system.

Advanced Power Management A feature available on all of today's computers, monitors and many peripherals., APM as the name suggests, controls the powering down of equipment usually in two stages. The first stage places the equipment into a powered down state where the equipment receives just enough power to make it instantly accessible on demand. The second stage actually turns off power to the main components of the equipment so that they will last longer. Equipment capable of being managed by APM is often referred to as "green"(we may have heard the term "green monitor").

Advanced Research Projects Agency Network The precursor to the Internet. Developed in the late 60's and early 70's by the US Department of Defense as an experiment in Wide Area Networking that would survive a nuclear war.

AFK An abbreviation of 'Away From Keyboard' universally used in online chat rooms to signify that the user is not currently in front of the computer.

Agent An agent is a type of software program that is instructed to go out onto the Internet and perform a specific function on behalf of a user. The most common type of agents are programs called spiders and worms, which roam the Internet, collecting and indexing its content and creating their own searchable databases of the content found. New and custom uses for agents are being developed that will let users do such things as search online music sites to compare prices for a specific CD title.

AGP See Accelerated Graphics Port

AI See Artificial Intelligence

AIX See Advanced Interactive Executive

Algorithm A detailed sequence of actions performed to accomplish a task of some kind. Named after an Iranian mathematician, Al–Khawarizmi.

Alias A name, usually short and easy to remember/type, that is translated into another name, usually long and difficult to remember/type. Aliases are used heavily in every area of computing and on the Internet.

Aliasing Jagged steps visible in images along angled object edges, due to sharp tonal contrasts between pixels.

Alpha Testing Testing of software at the developer's site by customers. Alpha testing is usually

carried out when a software package is first fully functional so that customers can suggest changes and report bugs which are usually plentiful at this stage.

American National Standards Institute The organization responsible for approving US standards for computers and communications.

American Standard Code for Information Interchange ASCII is the default world–wide standard for the code numbers used by computers to represent all the upper and lower–case Latin letters, numbers, punctuation and special characters. There are 128 standard ASCII codes each of which can be represented by a 7 digit binary number: 0000000 through 1111111.

Amplitude The measurement of the difference in magnitude of waves in an analog transmission. AM radio is amplitude modulation. FM is frequency modulation. In AM radio it is the difference in magnitude or height of a radio wave that is used, while in FM it is the frequency or closeness of the waves to each other that is used.

Analog The system of transmitting information in alternating waves. Information is read by measuring wavelengths over time. Analog is quickly being superseded by digital transmission.

Anchor An HTML tag that marks a specific point in an HTML document as either the source or destination of a hypertext link. This allows us to create links from one hypertext document to another, as well as to different sections within the same document. The destination marker uses the <A NAME> tag which is frequently used to navigate a long document with many sections. Anchors that point to <A NAME> markers use the <A HREF> tag.

Animated GIF A variation of the GIF image format, often used on World–Wide Web pages to provide moving icons and banners.

Animation The creation of artificial moving images.

Annoyware A slang term used to describe shareware that reminds us frequently that we are using an unregistered version of the software product.

Anonymous FTP See FTP

Anonymous Login Convention Standard username (anonymous) and password (guest) which allows anonymous users to login to FTP sites and gain access to files and folders in the public domain (Unprotected).

ANSI See American National Standards Institute

Answer Files Answer files are text files that contain stylized responses to the queries posed by Microsoft® setup programs during installation. We can use an answer file, in conjunction with a network installation startup disk, to fully automate the installation of Microsoft software on a single computer (in other words, perform an unattended installation). The default name for an answer file is Unattend.txt, but we can use any file name we want for our answer files.

Anti–aliasing A technique applied by graphics editing software on image files to make diagonal

edges appear smoother by setting pixels near the contrasting edge to an intermediate colour of the contrasting colours.

API See Application Program Interface

APM See Advanced Power Management

Applet A small Java program that can be embedded in an HTML page. Applets differ from full–fledged Java applications in that they are not allowed to access certain resources on the local computer, such as files and serial devices (modems, printers, etc.), and are prohibited from communicating with most other computers across a network. The current rule is that an applet can only make an Internet connection to the computer from which the applet was sent.

AppleTalk A routable network protocol developed by Apple Computer, Inc. This protocol was used in Macintosh computers. Apple computers are now using the TCP/IP protocol

AppleTalk Address Resolution Protocol. The Address Resolution Protocol was used with AppleTalk networks. It allowed the upper–layer protocols to use MAC addresses instead of logical addresses. See also Address Resolution Protocol (ARP).

AppleTalk Remote Access A protocol (and product) that provided system–level support for dial–in (modem) connections to an AppleTalk network. With AppleTalk Remote Access (ARA), we can call our desktop Mac from a PowerBook and remotely access all the available services – files, printers, servers, e–mail, etc.

Application Software that lets users do relatively complex tasks, as well as create and modify documents. Common application types include word processors, spreadsheets, database managers, and presentation graphics programs.

Application Layer The top layer of the OSI model. The application layer handles issues like resource allocation. The application layer is responsible for communicating between the application accessing network resources and the presentation layer.

Application Program Interface An Application Program Interface is an interface between an operating system and application programs (software packages) that specifies how the two communicate with each other and provides a common set of controls to access a computers resources.

Application Server A server that processes information for a client computer. The application the client runs is stored on the client. Requests are sent to the server to be processed and the results are returned to the client. This way, little information is processed by the client and nearly everything is done by the server.

Application Services A network service that allows servers to provide application services in a client/server relationship. A client computer runs a small front–end application that sends all queries and requests to a server for processing. The server than processes the requests and returns the results to the client. Application services manages the entire transaction.

ARA See AppleTalk Remote Access

Archie A tool for finding files stored on Anonymous FTP sites. We need to know the exact file name or a substring of it.

Archive A file containing one or usually more files that are compressed to save storage space. Archives are generally created to backup important information, to save disk space, for software distribution or to limit the time and use of bandwidth when transporting files across media.

Archiving The process of backing up data so that it is not lost in the case of a hard disk failure. Files have an archive attribute that is removed when a file has been backed up and then replaced when a file has been changed. This enables backup software to know which files need to be backed up and removes the need of having to duplicate all files every time a backup is performed.

ARCNet See Attached Resource Computer Network

ARP See Address Resolution protocol

ARPANet See: Advanced Research Projects Agency Network

Artificial Intelligence The field of computer science concerned with the attempt to model aspects of human thought into computers. It is also sometimes defined as trying to solve by computer any problem that a human can solve faster.

ASCII See American Standard Code for Information Interchange

a/s/l An abbreviation for Age/Sex/Location used commonly in chat rooms.

ASP See Active Server Pages

Asset Management The process that a large organization uses to collect and maintain a comprehensive list of all items it owns such as hardware and software. This data is used in connection with the financial aspects of ownership such as calculating the total cost of ownership, depreciation, licensing, maintenance, and insurance.

Asymmetric Digital Subscriber Line A method for moving data over regular phone lines. An ADSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. An ADSL circuit must be configured to connect two specific locations, similar to a leased line. A commonly discussed configuration of ADSL would allow a subscriber to receive data (download) at speeds of up to 1.544 megabits (not megabytes) per second, and to send (upload) data at speeds of 128 Kbps. Thus the "Asymmetric" part of the acronym. Another commonly discussed configuration would be symmetrical: 384 Kbps in both directions. In theory ADSL allows download speeds of up to 9 megabits per second and upload speeds of up to 640 Kbps. ADSL is often discussed as an alternative to ISDN, allowing higher speeds in cases where the connection is always to the same place.

Asynchronous Communication Two–way communication in which there is a time delay between when a message is sent and when it is received. Examples include electronic mail and voice mail systems. Synchronous communication takes place in the same time frame such as a telephone conversation.

Asynchronous Transfer Mode A packet switching model for fast long distance communications that uses fixed packet size and allows for intelligent decisions on routing, handling, prioritization, and costing. This allows for special handling and routing for data that must be reassembled quickly and accurately, such as live Video.

ATM See Asynchronous Transfer Mode

Attached Resource Computer Network ARCNet is a relatively old network type which was created in 1977 by the Datapoint Corporation. ARCNET uses token passing in combination with a star or bus topology to transmit data at 2.5 Mbps. ARCNet was designed to be a simple, inexpensive, and reliable topology. ARCNet can be a good solution for small LANs.

Attenuation The fading of an electrical signal over a distance. This is caused by resistance, impedance, and electrical noise.

AUI Connector Attachment Unit Interface or AUI, is actually a renamed DIX connector. When Xerox had to release its patents and trademarks to the public domain after turning over Ethernet to the 802.3 committee, DIX was renamed. Companies did not like the connector named after three rival companies. (Digital, Intel, Xerox)

AUP See Acceptable User Policy

Authentication The verification of the identity of a person or process.

Avatar A digital representation of a person in a virtual environment (2D & 3D chat rooms and VRML worlds for example). An individual may choose a symbol to represent himself in the form of a cartoon character or other visual representation.

AVS See Address Verification System

B Short for Byte

B2B Business to Business. A mode of conducting business between two or more companies over the Internet, rather than more traditional modes such as telephone, mail, fax and face to face.

Backbone A high–speed line or series of connections that forms a major pathway within a network. The term is relative more to a small network which will more likely be much smaller than many non–backbone lines in a large network.

Backdoor An unofficial means of gaining access to a computer system, a program, or data, usually undocumented and known only to person who created it. Backdoors can be useful if the usual way of access is blocked, but they compromise security. The term backdoor is also commonly used to refer to alternative means of accessing password protected websites through programming oversites.

Backup The action of copying important data to a second location or onto removable media to protect against data loss though equipment failure and unforeseen events. The end product (i.e. the backed up data) is also known as a backup.

Bandwidth The capacity of the transmission medium stated in bits per second or as a frequency. The bandwidth of optical fiber is in the gigabit or billion bits per second range, while ethernet coaxial cable is in the megabit or million bits per second range.

Banner Ad An image file of any size displayed on a website encouraging the viewer to click on it in order to load the advertisers webpage promoting their product or service.

Basic Input Output System The BIOS is a program which is stored in Read Only Memory on a computer's motherboard. The BIOS contains instructions for performing the Power On Self Test as well as information about the computer setup which it retains while the power is turned off.

Baseband System A baseband system is one that transmits signals without converting them to multiple frequencies thus limiting the systems bandwidth. Ethernet–based networks are an example of a baseband system and lack the multiple frequency capabilities of a broadband system.

BAT DOS Filename extension for a batch file.

Batch File DOS file that allows the execution of multiple commands by typing one word. Each command must be issued on a new line in the batch file. To initiate the commands all one would have to do is type the name of the batch file at a command prompt.

Baud In common usage the baud rate of a modem is how many bits it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value – for example a 1200 bit–per–second modem actually runs at 300 baud, but it moves 4 bits per baud (4 x 300 = 1200 bits per second). The term was derived from the name of J.M.E. Baudot, a French pioneer in the field of printing telegraphy.

Baud Rate See Baud

bbl An abbreviation for Be Back Later commonly used in chat rooms.

BBS See Bulletin Board System

Beaconing The continuous signalling of an error condition over a Token ring network. This condition alerts other computers and routing equipment that an error exists on the "beaconing" computer.

Best Effort Attempt The term for data that is routed using a connectionless transfer method. As there is no connection setup or error checking, the transfer is considered a Best Effort Attempt.

Beta A version of an application or software package that is made available prior to it's accepted completion for the purposes of testing. Beta testing is carried out after Alpha Testing and involves ironing out any bugs or issues that a programmer has missed just prior to release.

Beta Testing See Beta

bfn An abbreviation for Bye For Now commonly used in chat rooms.

BGI See Binary Gateway Interface

Binary The digital numbering system where only zeroes and ones are used.

Binary File A file that contains more than plain text (i.e., photos, sounds, spreadsheet, etc.) In contrast to an ASCII file which only contains plain text.

Binary Gateway Interface Provides a method of running a program from a Web server. Similar to a Common Gateway Interface (CGI). BGI uses a binary DLL which is loaded into memory when the server starts. While more efficient than CGI, BGI must be compiled and is not as easily portable to other environments.

Binary Hexadecimal A method for converting non–text files (non–ASCII) into ASCII. This is needed because Internet e–mail can only handle ASCII.

Binary Number System See Binary

Bindings Associations between a network service and a protocol, or between a protocol and a network adapter.

Binhex See: Binary Hexadecimal

BIOS See Basic Input Output System

Bit The smallest unit of information that a computer can process. Each bit is either a one(1) or a zero(0). Computers usually work with chunks of bits rather than one bit at a time; the smallest chunk a computer works with is a byte which is 8 bits.

Bit Depth The number of bits used to represent each pixel in an image, determining its color or tonal range. True colour is called 24 bit and contains more than 24 million colours.

Bitmap Generally used to describe an illustration or font file as being created by a predefined number of pixels. The screen we are looking at has its size set at 640 x 480 bits or higher. To produce a picture a bit map maps a particular color to every different location in the picture. The top left of our screen is (0,0) and the bottom right would be (640,480).

BITNET A network of educational sites separate from the Internet, but e–mail is freely exchanged between BITNET and the Internet. Listservs® , the most popular form of e–mail discussion groups, originated on BITNET. BITNET machines are usually mainframes running the VMS operating system, and the network is probably the only international network that is shrinking.

Bits Per Second A measurement of how fast data is moved from one place to another. A 28.8 modem can move 28,800 bits per second.

Black Point A movable reference point that defines the darkest area in an image, causing all other areas to be adjusted accordingly. This is used so that images can be made smaller. i.e. all areas darker than the black point will be mapped as a single colour (black.)

Blue Screen is displayed by Windows when it encounters a STOP error that it cannot recover from. A blue screen contains information about the type of error that occurred, a list of loaded

drivers, and a processor stack dump. In Windows 9X it is called a GPF (General Protection Fault) screen.

BNC Connector Short for Bayonet Neill–Concelman (for the inventors Paul Neill and Carl Concelman). A twist–and–lock connector for coaxial cable, BNC connectors are used for electronic equipment and for wiring LANs.

Bookmark A clickable link stored on a drop down menu that takes us to a page on the Internet. It is a method of "saving" a web sites location. Bookmarking a web site allows us to easily return to that page at a later time with a simple click of the mouse rather than remembering and typing out long and sometimes cryptic URLs. Many web sites have a "links" section or page which is made up of a collection of bookmarks.

Boolean See Boolean Logic

Boolean Logic A system used frequently in search engines and directories for searching and retrieving information using and combining terms using separators such as AND, OR, and NOT to sort data.

Boolean Search See Boolean Logic

Boot Loader A program that is used to load a computer's operating system.

Boot Partition The partition that contains the operating system files. The boot partition contains the folder that the operating system files are installed on. The Boot Partition must also be the active partition.

Boot Sequence The operating system boot sequence consists of a series of steps, beginning with powering on the computer and ending with completion of the logon process. The boot sequence steps vary according to the hardware platform we are using.

Booting The act of starting up a computer via the power switch, which loads the system software into memory. Restarting the computer via a keystroke combination or shutdown button is called re–booting or warm booting.

Bot Short for robot. A program designed to search the Internet looking for information. A common use of bots is the variously named spiders, worms, and crawlers that support search engines by following links from site to site and within a site to dig out information to be indexed by the search engine.

Bottleneck The component in the system that is slowing system performance. In a networking environment, the bottleneck is the part of the system that is performing at peak capacity while other components in the system are not working at peak capacity. In other words, if it weren't for the limiting component, the rest of the system could go faster.

Bounce The return of an e–mail message because of an error in its address or a fault in the online postal systems.

Bounded Media Refers to any network or communication that travels over a physical connection

of some type. They are referred to as bounded media because the signal travels through a physical media shielded on the outside (bounded) by some material.

bps See Bits Per Second

Bps Bytes Per Second. A measure of the transfer rate of information across media.

brb An abbreviation for Be Right Back commonly used in chat rooms.

Bridge A device similar to a router or a dedicated computer used to connect two different networks of the same type. It uses data link layer address (i.e., physical addresses) to determine if packets should be passed between the networks. A bridge's biggest weakness is its susceptibility to produce broadcast storms. i.e a broadcast message is sent to all hosts so if we have two or more bridges on our network they will continue to pass the message through each other causing the entire network to fail.

Broadband See Broadband System

Broadband System A broadband system is one that is capable of transmitting many different signals at the same time without interference between the signals. For local area networks, a broadband system is one that handles multiple channels of local area network traffic. A good example of a Broadband system is cable television.

Broadcast A packet whose special address results in its being heard by all hosts on a computer network.

Broadcast Storm Occurs when a broadcast message is sent to all hosts. If we have two or more bridges on our network they will continue to pass the message through each other causing the entire network to fail.

Broken Link A link in the form of clickable text or a clickable image which no longer takes us to the destination it is supposed to. This can occur for several reasons, the server hosting the web site is temporarily unavailable, or the web site has moved and is no longer on the server or the HTML code for the link is incorrect.

Browser A Client program (software) that is used to look at various kinds of Internet resources like the one we are using now to view this glossary.

Browsing 1.The process of viewing a list of computers and their available shared resources, or viewing a list of files and folders on a local or network connected drive. 2. Using an internet browser to navigate from page to page on the internet.

btw Shorthand for 'By The Way' used in an online forum or on a chat server to save time.

Bug A mistake, or unexpected occurrence, in a piece of software or hardware.

Bulletin Board System A computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. There are many thousands (millions?) of BBS's

around the world, most are very small, running on a single IBM clone PC with 1 or 2 phone lines. Some are very large and the line between a BBS and a system like CompuServe gets crossed at some point, but it is not clearly drawn.

Bus An electronic pathway. In networks, a configuration (topology) with a single linear cable, terminated at each end, to which computers and devices are connected. There are no loops or branches in the cable.

Bus Mastering Allows an add–on card in a computer to operate without the Central Processing Unit being involved. For example, a disk controller can read and write to a hard disk by itself without involving the CPU. Normally the CPU itself handles the transaction while putting other processes on hold. Bus Mastering greatly helps multi–tasking operating systems.

Bus Topology A bus topology is a network configuration in which all devices on a network are connected via one primary trunk cable. The bus topology is a passive technology that requires no special equipment to amplify or regenerate a signal, although amplification can be used to extend the signal. The bus topology is typically used with a contention based network. When a device wants to transmit across the bus, it has to determine whether the media is in use. If no other device is transmitting, the signal is sent. Each device receives the signal and then determines whether its address matches that of the recipient. Messages that weren't addressed to the device are disregarded.

Byte A set of Bits that represent a single character. Usually there are 8 Bits in a Byte, sometimes more, depending on how the measurement is being made.

C–band Satellite uplink/downlink frequency operating on the lower end of the microwave spectrum, shared with terrestrial microwave services.

C2 Secure Environment A designation in a range of security levels identified in the computer security specifications developed by the National Computer Security Association.

Cable Television Use of a broadband coaxial or fiber optic cable to deliver multiple video signals directly to TV sets utilizing multiplexing. Current systems can deliver signals in both directions.

Cache A section of memory used to temporarily store files from a hard disk thus giving the responsible application quick access to the data.

Caching A process in which frequently accessed data is kept in memory, rather than constantly having to be read from the place where it is stored.

CAD See Computer Aided Design

CAE See Computer Aided Engineering

Capacity Planning The process of determining current usage of server and/or network resources, as well as tracking utilization over time, in order to predict future usage and the additional hardware that will be required to meet the projected levels of utilization.

Carrier Sense Multiple Access On modern contention–based networks, devices listen for other signals on the media before transmitting. Collisions are not totally eliminated, but they are kept down to manageable levels. This is known as Carrier Sense Multiple Access. There are two types of CSMA, CSMA/CD and CSMA/CA.

Carrier Sense Multiple Access/Collision Avoidance A system where devices on a network listen for other signals on the media before transmitting. Collisions are not totally eliminated, but they are kept down to manageable levels. This is known as Carrier Sense Multiple Access. With CSMA/CA a device listens to the media to see if it is clear for transmission and if so, sends a request to send message to the network server.

Carrier Sense Multiple Access/Collision Detection A system where devices on a network listen for other signals on the media before transmitting. Collisions are not totally eliminated, but they are kept down to manageable levels. This is known as Carrier Sense Multiple Access. With CSMA/CD a device listens to the media to see if it is clear for transmission and then sends its transmission when the line is clear. This does not eliminate collisions as two devices often begin sending at the same time.

Cascading Style Sheets A technique built into version 4.0 browsers that support styles for pages. For example, we can set up styles for fonts and page layouts that will apply automatically to pages developed under a particular style.

Case–dependent See Case–sensitive

Case–sensitive Usually referring to a login name or password meaning that the name or password must be entered in the upper–case and/or lower–case order that it was created in order to gain access.

Cathode Ray Tube An electronic screen or monitor connected to a computer to display data.

CATV Community Access Television now known as Cable Television.

CCD See Charge–coupled Device

CDFS See Compact Disk Filing System

CD–i See Compact Disk – interactive

CD–R See Compact Disk – Recordable

CD–RW See Compact Disk – Rewritable

CD–ROM An optical data storage medium using the same physical format as audio compact discs, readable by a computer with a CD–ROM drive. CD–ROM drives are rated with a speed factor relative to music CDs (1x). 50x drives are common today.

Central Processing Unit The CPU is the largest electronic chip(s) in any computer. This is the brain of the computer where almost all information processing is carried out.

Centralized Computing A network that stores and processes all information on a Server. No processing or file storage is done by the clients. This allows for easy backup, high security and low cost but provides slower network access and fewer options. See also: Collaborative, Distributed.

Centralized Networks See Centralized Computing.

Certificate Authority An issuer of Security Certificates used in SSL connections.

CGA See Colour Graphics Adapter

CGI See Common Gateway Interface

cgi–bin The most common name of a directory on a web server in which CGI programs are stored. The "bin" part of "cgi–bin" is a shorthand version of "binary", because once upon a time, most programs were referred to as "binaries". In real life, most programs found in cgi–bin directories are text files – scripts that are executed by binaries located elsewhere on the same machine.

Chain Letter A form of spam which asks us to distribute the letter to many other people. They are against the policies of most Internet service providers, and almost always are hoaxes. Many of them promise quick ways to make money, usually on the basis of pyramid or Ponzi schemes, which are illegal. Some make pie–in–the–sky promises, for example, that Bill Gates will give everyone $1000 for just helping test his new mail distribution scheme. Many of them prey on our sympathy and tell stories of a sick child who has asked that word be spread about the illness by chain letters.

Channel In communication, a signal path or section of an electromagnetic spectrum which is uniquely assigned for a particular use.

Charge–coupled Device An integrated (built–in), micro–electrical light sensing component built into image capturing devices such as scanners.

Charset Short for character set. Different character sets are used for different purposes such as the different characters (Letters) used by different languages.

Chat Describes the way people communicate online in real time. The term "chat" is actually a misnomer. Typically, people in online chat sessions type messages to each other using their keyboards. The messages then appears on the screens of all participants. Chat sessions can involve two or more people.

Chat Room An electronic space, typically a website or a section of an online service, where people can go to communicate online in real time. Chat rooms are often organized around specific interests, such as small business owners, gardening, etc.

Checksum The unique value generated from a Cyclic Redundancy Check algorithm.

Chip A thin silicon wafer on which electronic components are deposited in the form of integrated circuits; the basis of digital systems.

Chipset A collection of integrated circuits on a circuit board that are designed to be used together for some specific purpose. A chipset is usually made up of 1 – 3 main chips.

Circuit Switching A dedicated connection made between two communicating devices on a network. Advantages of this method are no congestion (because the link is dedicated) and almost no channel–access delay. Disadvantages are inefficient use of media and a possible long wait to establish a connection. An example of circuit switching is the telephone system.

Click The act of depressing a button on a mouse or other pointing device.

Click–through A click–through is registered whenever a viewer clicks on a banner ad. This measurement is important to determine whether an online advertisement is successfully creating traffic for the advertisers website.

Click–through Rate The percentage of times an online advertisement is clicked on, based on the number of times it's viewed. If a banner ad is seen by 1000 site visitors and 50 of them actually click on the ad, the banner ad has a click–though rate of 5%. (50/1000) x 100.

Clickable Image Any image that has instructions embedded in it so that clicking on it initiates some kind of action or result. On a web page, a clickable image is any image that has an URL embedded in it.

Client A client is a computer that is capable of accessing resources on other computers (servers) across a network. Some computers are configured with both client and server software.

Client–Server Architecture See Client/Server Relationship

Client/Server Relationship A client application is one that resides on a user's computer, but sends requests to a remote system to execute a designated procedure using arguments supplied by the user. The computer that initiates the request is the client and the computer responding to the request is the server. Many network services follow a client and server protocol.

Client Service for Netware A Windows NT Workstation service that enables a Windows NT Workstation computer to access files and print queues on NetWare 3. x and 4. x servers.

Clipboard A temporary memory area, used to transfer information within a document being edited or between documents or between programs. The fundamental operations are "cut" which moves data from a document to the clipboard, "copy" which copies it to the clipboard, and "paste" which inserts the clipboard contents into the current document in place of the current selection.

Clipping The conversion of all tones lighter than a specified grey level to white, or darker than a specified grey level to black, causing loss of detail. This also applies to individual channels in a color image. Clipping is used heavily on graphics destined for the web as the image size is greatly reduced meaning faster download times and less use of bandwidth.

CMOS (Complementary Metal Oxide Semiconductor) A semiconductor fabrication technology using a combination of n– and p– doped semiconductor material to achieve low power dissipation. The idea is that any path through a gate through which current can flow includes both n– and p– type transistors. Only one type is turned on in any stable state so there is no static power dissipation and current only flows when a gates switches in order to charge the parasitic capaci-

tance. A CMOS is utilized by most mainboards to store configuration information about a computer while the power is switched off.

CMS See Colour Management System

CMYK (Cyan, Magenta, Yellow, Key) A system for describing colours by giving the amount of each secondary colour (cyan, magenta, yellow), along with the "key" (black). The CMYK system is used for printing. For mixing of pigments, it is better to use the secondary colours, since they mix subtractively instead of additively. The secondary colours of light are cyan, magenta and yellow, which correspond to the primary colours of pigment (blue, red and yellow). In addition, although black could be obtained by mixing these three in equal proportions, in four–colour printing it always has its own ink. This gives the CMYK model. The K stands for "Key' or 'blacK,' so as not to cause confusion with the B in {RGB}.

Coax See Coaxial Cable.

Coaxial Cable A networking cable with a solid central conductor surrounded by insulator, in turn surrounded by a cylindrical shield woven from fine wires. It is used to carry high frequency signals such as video or radio. The shield is usually connected to electrical ground to reduce electrical interference.

Codec (Coder/decoder) An electronic device used to combine the circuits needed to convert digital signals to and from analog signals.

Cold Boot The process of restarting an operating system which includes turning the power of the computer off and then back on.

Collaborative Computing A network that allows each of the client computers to cooperate and process the same information. This way tasks are completed faster than if they only ran on one computer.

Collision A collision occurs on a network when two computers transmit data at exactly the same time causing that data to collide and corrupt.

Collision Detection A method in which computers transmit data over a network as soon as they have data to send and then check to see whether their transmission has suffered a collision with another computer's data. If a collision is detected then the data must be resent.

Co–location Most often used to refer to having a server that belongs to one person or group physically located on an Internet–connected network that belongs to another person or group. Usually this is done because the server owner wants their machine to be on a high–speed Internet connection and/or they do not want the security risks of having the server on their own network.

Colour Graphics Adapter One of IBM's earliest hardware video display standards formerly used in IBM PCs. The standard is now obsolete.

Colour Management System Software that ensures color uniformity across input and output devices so that final printed results match originals. The characteristics or profiles of devices are

normally established by reference to standard colour targets.
Com Port See Communication Port

COMDEX (COMPuting and Data Storage EXhibition) A computer show that is held twice yearly, once in the spring (in Atlanta) and once in autumn (in Las Vegas). Comdex is a major show during which new releases of software and hardware are made.

Command A string of characters that instruct a program to perform a specific action. Most commands take switches which either modify the action performed or supply it with input. Commands may be typed by the user or read from a file by a command interpreter. It is also common to refer to menu items as commands.

Command Interpreter A program which reads textual commands from the user or from a file and executes them.

Commerce Server A Web server that contains the software necessary for processing customer orders via the Web, including shopping cart programs, dynamic inventory databases, and online payment systems. Commerce servers are usually also secure servers.

Common Gateway Interface A set of rules that describe how a Web Server communicates with another piece of software on the same machine, and how the other piece of software (the "CGI program") talks to the web server. Any piece of software can be a CGI program if it handles input and output according to the CGI standard. Usually a CGI program is a small program that takes data from a web server and does something with it, like putting the content of a form into an e–mail message, or turning the data into a database query. we can often see that a CGI program is being used by seeing "cgi–bin" in a URL, but not always.

Communication Port A port used to connect serial devices such as mice and modems to computers and other electronic devices.

Communications Servers Communications servers are set up to handle remote users dialing into a network. The communications server applications are normally located on separate servers for security. It is much easier to secure a server that only does one thing than try to secure a server that internal users also access.

Compact Disc A 4.72 inch disc developed by Sony and Phillips that can store still and/or moving images in monochrome and/or color; stereo or two separate sound tracks integrated with and/or separate from the images; and digital program and information files on the same disc. One disc can store up to 640MB of uncompressed data.

Compact Disk Filing System Enables access to compact disc directory structure and file retrieval. It is only used on CD–ROM devices.

Compact Disk – interactive An embedded application on a CD–ROM that allows limited interaction with films, games and educational applications.

Compact Disk – Recordable A write–once version of a CD–ROM. They can only be written to by a CD–R or CD–RW drive. CD–Rs can hold about 640 megabytes of data. They are very dura-

ble and can be read by normal CD–ROM drives, but once data has been written it cannot be altered.

Compact Disk – Rewritable A version of a CD–ROM that allow data to be rewritten to it multiple times. CD–RWs can hold about 640 megabytes of data. They are very durable and can be read by normal CD–ROM drives. They can only be written to by a CD–RW drive.

Compiler A piece of software that converts a program from its source language into another programming language.

Complete Trust Domain Model A decentralized domain model that consists of two or more domains that contain both user accounts and shared resources. In the complete trust domain model, a two–way trust relationship must be established between each and every domain. Because of the excessive number of trusts required for this model, the complete trust domain model is not often implemented.

Compress To decrease the size of a file or files using a complex algorithm. The file is not usable until it has been uncompressed. Files are compressed to save space on storage media when they are not needed and also to transport them over a network or the internet faster. The most common type of compressed file is the zip file.

Compression see Compress

Compression Ratio The size that a file or group of files have been compressed down to in relation to their uncompressed size.

Computers Powerful tools that can be programmed to manipulate symbols. Computers can perform complex and repetitive procedures quickly, precisely and reliably and can quickly store and retrieve large amounts of data. They are also great for playing games.

Computer Aided Design The part of CAE concerning the drawing or physical layout steps of engineering design.

Computer Aided Engineering using computers to help with all phases of engineering design work. Like CAD, but also involving the conceptual and analytical design steps.

Computer Browser Service This Windows NT service is responsible for the process of building a list of available network servers, called a browse list. The Computer Browser service is also responsible for determining the role a computer will play in the browser hierarchy: domain master browser, master browser, backup browser, or potential browser.

Computer Conferencing The use of computers which are linked through modems and telephone lines (or other means) to each other. Computer users are allowed to freely or systematically interact to share ideas and concepts. With video projection equipment, large groups can view the conferencing process.

Computer Name A unique name that is used to identify a particular computer on the network. No two computers on the same internetwork should have the same computer name.

Computer Policy A collection of Registry settings created with a System Policy Editor that specify a local computer's configuration. A computer policy enforces the specified configuration on all users of a particular Windows NT (or Windows 95/98/2000/Me) computer.

Computer Virus See Virus

Concentrator A communications device that multiplexes low–speed communications lines onto one high–speed line, more "intelligent" than a multiplexer because it can store and forward transmissions.

Configuration 1. The components that make up a computer system (which model and what peripherals). 2. The physical arrangement of those components (what's placed and where). 3. The software settings that enable two computer components to talk to each other (as in configuring communications software to work with a modem).

Congestion What we get when the load of a data communication path exceeds its recommended capacity.

Connection–Oriented Service A data transfer service of the LLC Sublayer of the OSI Model. The opposite of unacknowledged connectionless service. It uses a sliding–window flow control and acknowledgments for error checking to transfer data reliably between computers on a network.

Connector The part of a cable that plugs into a port or interface to connect one device to another.

Contention–Based Networking A system that allows any device on a network to transmit whenever it needs to. The advantages of this system are that it allows equal access to the network media, but at the expense of possible collisions. On modern contention–based networks, devices listen for other signals on the media before transmitting. Collisions are not totally eliminated, but they are kept down to manageable levels. This is known as Carrier Sense Multiple Access, or CSMA.

Control Panel is a group of mini applications that are used to configure a Windows® computer.

Cookie The most common meaning of "Cookie" on the Internet refers to a piece of information sent by a Web Server to a Web Browser that the Browser software is expected to save and to send back to the Server whenever the browser makes additional requests from the Server. Depending on the type of Cookie used, and the Browser's settings, the Browser may accept or not accept the Cookie, and may save the Cookie for either a short time or a long time. Cookies might contain information such as login or registration information, online "shopping cart" information, user preferences, etc. When a Server receives a request from a Browser that includes a Cookie, the Server is able to use the information stored in the Cookie. For example, the Server might customize what is sent back to the user, or keep a log of particular user's requests. Cookies are usually set to expire after a predetermined amount of time and are usually saved in memory until the Browser software is closed down, at which time they may be saved to disk if their "expire time" has not

been reached. Cookies do not read our hard drive and send our life story to the CIA, but they can be used to gather more information about a user than would be possible without them.

Coprocessor Any computer processor which assists the main processor (CPU) by performing certain special functions, usually much faster than the main processor could perform them. The co–processor often decodes instructions in parallel with the main processor and executes only those instructions intended for it.

Cost Per Action Any advertisement pricing formula in which advertisers pay not for number of impressions but when visitors perform a certain action in response to the ad, such as filling out a registration form, entering a contest or making a purchase.

Cost Per Click A form of CPA pricing. Advertisers pay each time a viewer clicks on their ad.

Cost Per Thousand When referring to banner ads, the CPM is the cost per thousand impressions. This equals how much an advertiser pays for 1,000 page views, or impressions, of its banner. It is called CPM as M is the roman numeral for 1000.

Country Code Most countries in the world that are connected to the Internet have been assigned two–letter country codes by the international standard ISO 3166. These two letter codes are appended to the end of domain addresses for the country.

CPA See Cost Per Action

CPC See Cost Per Click

CPM See Cost Per Thousand

CPS Characters per second. Measure of speed of printers and other output devices.

CPU See Central Processing Unit

Cracker A person who attempts to break into a network or computer system, often with the intent to steal material or perform malicious destruction of files or just to show it can be done.

Cramming The practice by some phone companies of adding false charges to phone bills for calls that were never made.

Crash A sudden, drastic system failure (the term originally described what happened when the air gap of a hard disk collapses). A disk crash that involves the read/write heads dropping onto the surface of the disks and scraping off the oxide may also be referred to as a "head crash", whereas the term "system crash" usually, though not always, implies that the operating system or other software was at fault.

Crawler See Spider

CRC See Cyclic Redundancy Check

Cross–platform Refers to software (or anything else) that will work on more that one operating system and/or hardware configuration.

Cross Talk What happens when a signal from one cable is leaked into another by an electrical field. An electrical field is created whenever an electrical signal is sent through a wire. If two wires are close enough together and do not have enough shielding, the signal may leak and cause noise on the other wire.

CRT See Cathode Ray Tube

Cryptography The process of securing private information that is passed through public networks by mathematically scrambling (encrypting) it in a way that makes it unreadable to anyone except the person or persons holding the mathematical "key" that can unscramble (decrypt) it. The two most common types of cryptography are "same–key" and "public–key." In same–key cryptography, a message is encrypted and decrypted using the same key, which is passed along from one party to another in a separate transmission. A more secure method is public–key cryptography which uses a pair of different keys (one public, one private) that have a particular relationship to one another, such that any message encrypted with one key can only be decrypted with the other key and vice versa.

CSMA See: Carrier Sense Multiple Access

CSMA/CA See Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD See Carrier Sense Multiple Access/Collision Detection

CSNW See Client Service for Netware

CSS See Cascading Style Sheets

CTR See Click–through Rate

cul An abbreviation for 'See You Later' commonly used in chat rooms.

Cursor A visually distinct usually flashing mark on a display indicating where newly typed text will be inserted. The cursor moves as text is typed and, in most modern editors, can be moved around within a document by the user to change the insertion point.

cXML
A new set of document type definitions (DTD) for the XML specification. cXML works as a meta–language that defines necessary information about a product. It will be used to standardize the exchange of catalog content and to define request/response processes for secure electronic transactions over the Internet. The processes includes purchase orders, change orders, acknowledgments, status updates, ship notifications, and payment transactions.

Cyberbunny Someone who knows absolutely nothing about computers and advises people who know absolutely nothing about computers.

Cyberpunk This term was originally a cultural sub–genre of science fiction taking place in a not–so–distant, dystopian, over–industrialized society. Cyberpunk grew out of the work of William Gibson and Bruce Sterling and has evolved into a cultural label encompassing many different kinds of human, machine, and punk attitudes. It includes clothing and lifestyle choices as well.

Cyberspace Term originated by author William Gibson in his novel Neuromancer the word Cyberspace is currently used to describe the whole range of information resources available through computer networks.

Cybersquatting The act of registering a company name as a domain name by someone outside the company in hopes of selling it to the company for a profit. Anti–cybersquatting legislation has been introduced to make it illegal.

Cyclic Redundancy Check A method of detecting errors in the transmission of data. Before data is sent, a CRC number is calculated by running the data through an algorithm and producing a unique number. At the receiving end of the transmission, the data is run through the same algorithm again to produce the number. If the numbers match, the data was sent error free.

Cylinder The set of tracks on a multi–headed hard disk that may be accessed without head movement. That is, the collection of disk tracks which are the same distance from the spindle about which the disks rotate. Each such group forms the shape of a cylinder. Placing data that is likely to be accessed together in cylinders reduces the access rate significantly as head movement (seeking) is slow compared to disk rotation and switching between heads.

DAT 1. Digital Audio Tape. The most common type of tape used for backing up important computer data. DAT records data digitally (zeros & ones) thus minimizing quality loss. 2. File extension commonly used for database files.

Data A term loosely used to describe any information stored in a electronic fashion whether it is in storage, in memory, or in transit over network media.

Data Link Layer The second layer of the OSI model. The main purpose of this layer is to provide a reliable method of transmitting data across physical media. The data link layer breaks the input data into frames, transmits the frames sequentially, and processes the acknowledged frames sent back by the receiver. It adds a header and trailer to the frames it creates. These allow the destination device to see when a frame begins or ends on the physical media. The data link layer is broken down into two sublayers. The Logical Link Control Sublayer and the Media Access Control Sublayer.

Data Projector A device for taking the information that we would normally see on a computer monitor and projecting it onto to a larger movie screen. By projecting our work instead of displaying it on a monitor, we can show projects we've developed on a computer to a larger group of people.

Database A file created by a database manager that contains a collection of information organized into records, each of which contains labeled categories called fields.

Database Services A network service that is responsible for maintaining distributed databases which are multi homed in entirety or in part. Database services are responsible for replicating the database and making sure that all information is current on all copies of the database.

Datagram A segment of a file that has been broken into smaller pieces in order to be transported

over a network medium. This is done so that the data being transferred is in portions that are the same size or smaller than the maximum packet size stipulated by each network end system and intermediate device. It also means the data is small enough to be stored in memory.

Daughtercard See Daughterboard

Daughterboard A circuit board that attaches to (rides piggyback on) another circuit board, such as the motherboard. For example, we can often add a daughtercard containing additional memory to an graphics accelerator card.

Datagram Packet Switching A connectionless method of packet switching. Each piece of information is tagged with the destination address so no dedicated connection is needed. Every piece of data is routed individually through the network to its destination. At the destination device, the data is pieced back together by using a Packet Assembler/Disassembler (PAD).

Datagram Switching Methods of data transfer where data is broken down into smaller pieces (datagrams) and then sent over the network media using different methods of switching.

Data Link Layer The second layer of the OSI model. Its purpose being the reliable transmission of data across physical media. It breaks input data into frames, transmits the frames sequentially, and processes the acknowledged frames sent back by the receiver. The Data Link layer is divided into two sublayers, the Media Access Control (MAC) sublayer and the Logical Link Control (LLC) sublayer.

DDS See Digital Data Storage.

De Facto Standard Protocol Latin for existing in fact, indicates a protocol controlled by the entire industry, and is thus also known as an industry standard. Anyone can use a de facto standard free of charge. Changes to these standards are sometimes very hard to make, as we must convince the rest of the industry that the changes are needed.

De Jure Standard Protocol Latin for according to law, indicates a protocol designed by one company or organization. Normally this organization maintains control of the protocol and is responsible for any additions or changes.

Decompression The expansion of files that have been compressed to minimize storage space or to expedite delivery over slow media.

Dedicated Line A telephone or data line that is always available and always connected. For example, a leased telephone line can be dedicated for computer data communications. This line is not used by other computers or individuals, is available 24 hours a day, and is never disconnected.

Default Computer Policy A computer policy that applies to all computers that don't have an individual computer policy.

Default Gateway A TCP/IP configuration setting that specifies the IP address of the router on the local network segment.

Default User Policy A user policy that applies to all users that don't have an individual user policy.

Default User Profile is a user profile folder created during the operating system installation process. The settings in the Default User profile are applied, by default, to new user profiles as they are created. The Default User profile can be modified by using Registry Editors or by using Windows Explorer.

Demand Paging A process used by a Memory Manager that involves reading pages of memory from the paging file into RAM, and writing pages of memory from RAM into the paging file as required by the operating system.

Demodulation A process of converting analog signals sent over a telephone line into digital form so that they can be processed by a receiving computer, or more widely in telecommunications, any time analog signals are digitized.

Desktop The screen that is displayed after Windows boots and we log on. The desktop replaces the Program Manager interface from earlier versions of Windows and Windows NT.

Desktop Computer A desktop computer is a personal computer that can fit on an end user's desk and perform business computing tasks. Also, especially if linked to a network of other computers, it may be referred to as a workstation.

Desktop Publishing Refers to designing, proofing and publishing printed media on our computer. The whole process is carried out on our desktop.

Desktop Operating System An operating system that is designed to be used by an individual user on his or her desktop computer. A desktop operating system is not designed to be used on a network server.

Deterministic Network A network that determines transmission order of devices on the network. This ensures that no collisions occur as devices may only transmit when they have permission to do so. There are two types, token passing and polling.

Device Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, a mouse, and modems.

Device Driver Software to control a hardware component or peripheral device of a computer, such as a hard drive, modem or printer.

DHCP See Dynamic Host Configuration Protocol

dHTML See Dynamic Hypertext Markup Language

Dialog Box A window that displays additional options or questions when a command is chosen in an operating system or software package.

Dial–Up Networking A Windows service that enables a computer to use its modem to make a network connection over a telephone line to another computer.

Digerati The digital version of literati, it is a reference to a vague cloud of people seen to be knowledgeable, hip, or otherwise in–the–know in regards to the digital revolution.

Digital Data or voltages consisting of discrete steps or levels, as opposed to continuously variable analog data.

Digital Data Storage A format for storing and backing up computer data on tape that evolved from the digital audio tape (DAT) technology. The DDS format of data storage uses DAT cartridges (it uses a 4 mm tape). There are four types of DDS drives:

DDS–1, which can store up to 2 gigabytes of uncompressed data on a 120–minute cartridge.

DDS–2, which can store up to 8 gigabytes of uncompressed data on a 120–minute cartridge.

DDS–3, which can store up to 24 gigabytes of uncompressed data on a 125–minute cartridge.

DDS–4, which can store up to 40 gigabytes of uncompressed data on a 125–minute cartridge.

Digital Signature A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for e–commerce and are a key component of most authentication schemes.

Digitizer Any device that converts a picture into data that can be stored, manipulated, printed or displayed on a computer.

DIP Switches See Dual Interface Poll Switches

Direct Memory Access Direct memory access, or DMA, enables internal hardware devices in computers to work directly with memory. Normally the Central Processing Unit must be involved any time devices need to move data into or out of memory. If a device uses a DMA channel, it can handle communications directly with memory without the help of the CPU.

Directory A folder or group of folders. In computer terminology, the terms directory and folder are almost synonymous. The two terms are used interchangeably through–out computer terminology documentation and the Windows user interface. For a clear differentiation, the root directory of a hard drive contains all the folders and files saved to it. A folder may contain other folders as well as files.

Directory Name Service A TCP/IP based name resolution service. It is used to resolve a host name or a Fully Qualified Domain Name (FQDN) to its associated IP address.

Directory Replication This is replication designed to copy logon scripts from a central location, usually the PDC (Primary Domain Controller), to all domain controllers, thus enabling all users to execute their own logon scripts no matter which domain controller validates their logon. Replication involves copying subfolders and their files from the source folder on the source server to the destination folder on all computers on the network that are configured as replication destinations.

Directory Services A network service that stores information about all the objects available on a network. An object being anything that requires information to be stored like printers, users and shared resources.

Dish An earthbound parabolic antenna used for receiving satellite signals.

Disk A revolving platter on which data and programs are stored.

Disk Drive A device into which a floppy disk is placed for storing and retrieving data.

Disk Duplexing is a fault tolerance method that involves duplication of a partition from one hard disk onto a second hard disk. In disk duplexing, each hard disk must be on a different hard disk controller.

Disk Mirroring A fault tolerance method that involves duplication of a partition from one hard disk onto a second hard disk. In disk mirroring, each hard disk can be on the same or a different hard disk controller.

Distributed Computing A network where clients do their own processing and use a server for storage.

Distributed Databases These are databases that are replicated completely or in part to one or more locations to distribute load.

Distributed Networks See Distributed Computing. See also Centralized, Collaborative.

DIX Connector A network cable connector type that is not used often anymore but was widely used when thick Ethernet was popular. DIX is a 15–pin connector with two rows of pins. A cable was attached to the NIC through this connector and was attached to the thick Ethernet cable by use of a "vampire tap". The tap had to be drilled into the cable and tightened down. DIX stands for the three companies that invented it: Digital, Intel, and Xerox.

DMA See Direct Memory Access

DNS See Directory Name Service

Domain A logical grouping of networked computers in which one or more of the computers has shared resources, such as a shared folder or a shared printer, and in which all of the computers share a common central domain Directory Services database that contains user account and security information.

Domain Controller is a computer that maintains a copy of the domain Directory Services database (also called the SAM).

Domain Master Browser A computer that maintains a list of available network servers located on all subnets in the domain. Additionally, the domain master browser maintains a list of available workgroups and domains on the internetwork. The domain master browser is the primary domain controller. See also Computer Browser service.

Domain Name A domain name is a unique name, up to fifteen characters in length, assigned to identify the domain on the network. A domain name must be different than all other domain names, workgroup names, and computer names on the network.

DOS Disk Operating System. The operating system used on IBM personal computers and compatible machines. It comes in many flavours the most common of which is Microsoft's MS DOS.

Dot Matrix Printer A type of printer that produces characters and illustrations by striking pins against an ink ribbon to print closely spaced dots in the appropriate shape. Dot–matrix printers are relatively expensive and do not produce high–quality output; however, they can print to multi–page forms (that is, carbon copies), something laser and ink–jet printers cannot do.

Downlink The communications link between a satellite and an earthbound receiving station or dish.

Download To transfer a file from a remote computer through a network connection or modem to the hard drive of the user's computer.

Downtime The time between which a computer, or system, does not work because of hardware or system software failure and the time it is brought back into operation.

dpi Dots Per Inch. A measure of the resolution of a printer, scanner, or monitor. It refers to the number of dots in a one–inch line. The more dots per inch, the higher the resolution.

Driver A piece of software that tells the computer how to operate an external or added device, such as a printer, hard disk, CD–ROM drive, scanner or modem. For instance, we can't print unless we have a printer driver. Hard disk drivers are invisible files that are loaded into memory when we start the computer, while scanner drivers are usually plug–ins accessed from within a particular application.

DS–0 Digital Service, level 0. The designation for the smallest channel subdivision within the digital signal hierarchy. DS–0 can be a single voice communication channel or a 56 Kbps data channel. Normal long distance voice calls use one DS–0 to establish the connection. Technically a DS–0 only exists as a 64 Kbps sub–channel of a DS–1 circuit. Only 56 Kbps of the channel are available for use by data or voice because 8 Kbps are lost to synchronization and signaling.

DS–1 Digital Service, level 1. A bidirectional digital transmission link operating at the North American standard of 1.544 Mbps which usually contains 24 DS–0 transmission signals. Typically used to interconnect PBX switches and to provide wideband channels for compressed video and high speed computer data links. Also referred to as T–1.

DS–2 Digital Service, level 2. A bidirectional digital transmission link operating at 6.312 Mbps which usually carries 96 DS–0 transmission signals or 4 DS–1 signals.

DS–3 Digital Service, level 3. A bidirectional digital transmission link operating at 44.736 Mbps which is capable of carrying 672 DS–0 transmission signals or 28 DS–1 signals. Commonly referred to as 45 Mbps or T–3.

DTP See Desktop Publishing

Dual Boot The capability of a computer to permit a user to select from more than one operating system during the boot process. (Only one operating system can be selected and run at a time.)

Dual Interface Poll Switches Dual Interface Poll switches allow for either an ON or OFF setting with any number of switches. DIP switches commonly allow us to change the configuration of a circuit board to suit our particular computer.

Dump The process of copying all information from RAM into a file. Most operating systems do this when they are about to crash to save information and to allow us to diagnose the cause of the crash.

DUN See Dial–Up Networking.

Dvorak Keyboard A data input device designed for speed typing. Unlike the traditional QWERTY keyboard, the Dvorak keyboard was designed so that the most commonly typed letters are contained in the middle row of keys. Common letter combinations are also positioned in order that they can be typed quickly. It is estimated that in an average eight–hour day, a typist's hands travel 16 miles on a QWERTY keyboard, but only 1 mile on a Dvorak keyboard. The Dvorak keyboard was designed by August Dvorak and William Dealy in the 1930s.

Dynamic Host Configuration Protocol A protocol used to dynamically assign IP addresses to client computers on a network. DHCP Relay Agent is a Windows NT Server service that forwards client computers' DHCP requests to a DHCP server on another subnet.

Dynamic Hypertext Markup Language An extension of HTML that gives greater control over the layout of page elements and the ability to have Web pages that change and interact with the user without having to communicate with the server. The three components of dHTML pages are HTML, JavaScript, and cascading style sheets.

Dynamic Routing In dynamic routing, a router automatically builds and updates its routing table. In a dynamic routing environment, administrators don't have to manually configure the routing table on each individual router. As changes are made to the network, dynamic routers automatically adjust their routing tables to reflect these changes. Periodically, each dynamic router on the network broadcasts packets containing the contents of its routing table. Dynamic routers that receive these packets add the routing table information received to their own routing tables. In this way, dynamic routers are able to recognize other routers as they are added to and removed from the network.

E– (prefix) A prefix meaning electronic for current jargon terms, such as e–commerce, e–business, and so on.

E–Commerce The processing of transactions, such as buying and selling, through electronic communication. E–commerce often refers to transactions occurring on the Internet, such as credit card purchases of products advertised on Web sites.

E–lecture (Electronic lecture) A textual lecture delivered via electronic mail to networked individual computers.

E–mail (Electronic Mail) Messages, usually text, sent from one computer to another via the internet or between Mail Servers via direct modem connections. E–mail can also be sent automatically to a large number of addresses on a Mailing List.

E–zine A regular publication on some particular topic distributed in digital form, chiefly via e–mail and also via the Web and on CD–ROMs.

Easter Egg A hidden, undocumented program sequence built into a program that only activates when we press the right keys. They are often funny, and they are often used to introduce the team that developed the program. If we are using Netscape, typing about:mozilla into the URL window will give us an example.

EB See Exabyte

EDI See Electronic Document Interchange

EE–PROM See Electronically Erasable Programmable Read Only Memory

EFT See Electronic Funds Transfer

EISA See Extended Industry Standard Architecture

Electron Gun Three radiation–emitting elements inside a traditional computer monitor. The gun fires electron beams on command from the video board.The electrons are guided magnetically toward a set of phosphor dots on the face of the tube. A mask, or grid, between the gun and the tube face assures the beams from the gun hit only the phosphor dots towards which they're aimed thus creating an image on the monitor.

Electronic Document Interchange The process of exchanging standardized document forms between computer systems for business use. This involves conversion of a transmitted document into a format readable by the receiving computer.

Electronic Funds Transfer The process of transferring money initiated through electronic terminal, automated teller machine, computer, telephone, or magnetic tape. In the late 1990s, this increasingly included transfers initiated via the Web. The term also applies to credit card and automated bill payments.

Electronically Erasable Programmable Read Only Memory A type of memory where changes can be made to an integrated circuit electronically byte by byte under software control. EE–PROM uses a special ultraviolet light device so that data or instructions on an integrated circuit can be erased and new data can be recorded in its place.

Emoticon The use of simple keystrokes, found on any keyboard, to express emotions, thoughts and actions. They can be thought of as the computer users body language. They are commonly found in E–mail, USENET, newsgroups, chat rooms, and mailing lists. For example :–) is a wink.

EMF See Enhanced Meta File

Emulation The function of a software program that enables it to perform activities equivalent to those performed by a separate, different hardware or software unit.

Encoding File transfer formatting that enables encrypted, compressed or binary files to be transferred without corruption or loss of data.

Encryption A way of coding information in a file or e–mail message so that if it is intercepted by a third party as it travels over a network it cannot be read.
End Systems The source and destination devices of any transmission on a network.

End–User Ultimate user of a product or service.

Enhanced Meta File An EMF is an intermediate print job format that can be created very quickly by the graphic device driver interface. Using an EMF enables Operating Systems to process the print job in the background while the foreground process continues.

Error Checking See CRC

Error Control A method of detecting errors in the transmission of data. Before data is sent, Error control is implemented using cyclic redundancy checks (CRCs) and checksums.

Ethernet A very common method of networking computers in a LAN. Ethernet will handle about 10,000,000 bits–per–second and can be used with almost any kind of computer.

Event Viewer A tool that enables an administrator to view and/or archive the operating system, application, and security event logs.

Exabyte is a billion gigabytes (1,152,921,504,606,846,976 bytes).

Executable File Refers to a file that is a program. Executables in DOS and Windows usually have an .exe or a .com extension. In UNIX and Macintosh environments, executable files can have any name.

Expanded Memory In a computer, internal random access memory that has been added over and above the memory originally installed in the computer.

Extended Industry Standard Architecture A computer bus architecture designed by a group of industry leaders who were not happy with the idea of paying IBM to use MCA. EISA overcomes the speed limitations of ISA while maintaining backward compatibility. EISA slots are deeper than ISA enabling ISA cards to use shallower connectors and EISA cards to use deeper connectors. EISA runs at 8 MHz and transmits at up to 32 bits. EISA was the first bus architecture to introduce bus mastering.

Extended Partition A disk partition that can be sub–divided into one or more logical drives. An extended partition can't be the active partition.

External Viewer An external viewer is an additional piece of software that "helps" a software package interpret and display specific file types that it doesn't have the built–in ability to interpret or display itself.

Extranet An extranet is a network that allows a company to share information with other businesses and customers. Extranets transmit information over the Internet and require a user to have a user name and password to access information on internal company servers.

Facsimile Machine A device that transmits and receives – via a voice telephone line – images of graphic designs, photographs and pages of text either printed or handwritten. Also known as a FAX machine.

FAT See File Allocation Table

FAQ See Frequently Asked Questions

Fault Tolerance Refers to the ability of a computer or operating system to continue operations when a severe error or failure occurs, such as the loss of a hard disk or a power outage.

FAX Machine See Facsimile Machine

FDDI See Fiber Distributed Data Interface

Fiber Distributed Data Interface A standard for transmitting data on optical fiber cables at a rate of around 2 Mbps per second. One segment can measure up to 2 kilometers.

Fiber Optic Cable Insulated glass core cable which used light pulses rather than electricity to transmit messages.

Fiber Optics A transmission technology that uses light as an information carrier and has enormous bandwidth capacity. Fiber optic transmission systems utilize light emitting diodes (LEDs) or laser light sources to transport light pulses over thin fibers made of glass or plastic to transmit video, audio or data signals. Each fiber can carry from 90 to 150 megabits of digital information per second or 1,000 voice channels. A fiber optic system offers the advantages of clarity of transmission, speed, accuracy, security and volume.

Field A separately identifiable group of characters within one record or file.

File A single document or collection of code that is stored on media as one entity or item.

File Allocation Table A 16 bit type of file system that is used by several operating systems. The maximum size of a FAT(16) partition is 2GB. (Also known as FAT16).

File Attributes Markers assigned to files that describe properties of the file and limit access to the file. File attributes include: Archive, Compress, Hidden, Read–only, and System.

File Compression See Compression

File Extension The portion of a filename that comes after the period denoting the type of file. e.g. .exe and .com are executable files while .doc would be a document file.
File Naming Convention The method used to denote the structure of a file name. e.g. MS–DOS 8.3 format has up to eight characters before the period and three after. The three characters after the period are usually reserved for file type specification.

File Permissions We can assign files various levels of permission, specifying who can access them, and what type of access they can have.

File Server A computer that allows other computers access to its storage media to save and retrieve files. All processing is carried out on the client computers.

File Services Functions that are available on a computer or across a network that allow the manipulation of information stored in containers called files.

File System is an overall architecture for naming, storing, and retrieving files on a disk.

File Transfer Transferring files electronically across a network from one computer to another computer located in the same room or on the other side of the world.

File Transfer Protocol The most common protocol used to move files between two Internet sites. FTP allows login to another Internet site for the purpose of retrieving and/or sending files. There are many Internet sites that have established publicly accessible repositories of material that can be obtained using FTP, by logging in using the account name anonymous, thus these sites are called anonymous FTP servers.

File Storage The storage of data on media such as hard disks, CD–ROMS and magnetic tape.
File Migration Moving data from one form of file storage media to another. When we move files from our hard disk to a CD–ROM to save hard disk space we have migrated the files.

File Update Synchronization A network service that keeps track of different versions of the same file. If two clients open a file at the same time and then try to save the changes that each have made, one file will overwrite the other. File update synchronization co–ordinates this problem so all changes are applied to the file regardless of how many versions are open.

Filename A string of characters and/or numerals that are assigned to data to uniquely identify it from other data. The data is stored in a container called a file.

Filter A piece of software that an application uses for file–format conversion or special effects. PageMaker, for example, has a filter that lets it import Microsoft Word files, while Photoshop has dozens of filters for special effects (such as image blurring). Filters can be part of the main application or external programs called plug–ins.

Finger An Internet tool for locating people on other Internet sites. Finger is also sometimes used to give access to non–personal information, but the most common use is to see if a person in online at a particular Internet site.

Firewall A firewall is a combination of hardware and software that many companies or organizations have in place between their internal networks and the Internet. A firewall allows only specific kinds of messages from the Internet to flow in and out of the internal network. This protects the internal network from intruders or hackers who might try to use the Internet to break into those systems.

Flame Originally, flame meant to carry forth in a passionate manner in the spirit of honorable

debate. Flames most often involved the use of flowery language and flaming well, was an art form. More recently flame has come to refer to any kind of derogatory comment no matter how witless or crude.

Flame War an online discussion that degenerates into a series of personal attacks against the debaters, rather than a discussion of their positions. A heated exchange.

Flaming See Flame

Flash A bandwidth–friendly and browser–independent animation technology that uses geometrical formulas (rather than patterns of dots) to represent images. As long as different browsers are equipped with the necessary plug–ins, Flash animations will look the same when viewed by any of them.

Flatbed Scanner Any scanning device that incorporates a flat transparent plate, on which original images are placed for scanning. The scanning process is linear rather than rotational.

Floating–point Error An error that occurs mainly in accounting programs because the programmer of the software did not allow enough decimal places in his code to allow a particular calculation or on rare occasions a fault in the CPU.

Floating–point Processor A special chip that handles sophisticated calculations, such as those used in spreadsheets, CAD, and scientific programs.

Flow Control Not all network devices run at the same speed. For this reason, there needs to be a method to control the amount of data sent to another device so that device will be able to handle it. This is called flow control and there are two methods of handling it. The sliding window method and the stop and wait method.

Folder Of storage media a folder is a virtual container used to organize files and other folders.

Font Refers to the style of typeface. This page is formatted using the Goudy Old Style font.

Footprint The part of the earth's surface where a particular satellite's signal can be picked up at a particular time. A footprint can cover one–third of the globe, but is usually less.

Format Preparation of a disk for use. The disk is checked for errors and formatted so that data can be recorded and retrieved. Formatting a used disk erases any previously stored information.

FQDN See Fully Qualified Domain Name

Fragmentation A condition where parts of a file are stored in different locations on a disk. When a file is fragmented, the drive's read/write head has to jump from place to place to read the data; if many files are fragmented, it can slow the drive's performance.

Frame(s) A technique used in web pages to divide the page into multiple windows, where each window is called a frame and can contain its own separate page. The advantage of frames is that one window can be scrolled or changed while other windows remain fixed for such purposes as keeping a menu in view all the time. The disadvantage is that not all browsers support it.

Frame Relay A packet switching standard based on the older X.25 protocol that achieves greater speeds with fast, reliable networks. It lowers overhead by reducing the accounting and checking procedures used in X.25.

Frame Type (also called a frame format) is an accepted, standardized structure for transmitting data packets over a network.

Freeware Software that is available to download and use for free.

Frequency The number of recurrences of a phenomenon during a specified period of time. In communications, the number of wavelengths of light or electricity or the number of times the signal repeats the same cycle in a second. The measurement of electrical frequency is Hertz.

Frequently Asked Questions Documents that list and answer the most common questions on a particular subject. Frequently Asked Questions are usually written by people who have tired of answering the same questions over and over.

Front–End A small application that runs on a client computer and sends and receives information from a database situated on a server. When a user on the client computer needs information from the database, an instruction is sent from the client to the server telling it to search for that information. The server then sorts through the database, locates the information and sends it back to the client.

FTP See File Transfer Protocol

Full Duplex A communication channel over which both transmission and reception are possible in two directions at the same time; e.g., a four wire circuit.

Fully Qualified Domain Name A term for the way computers are named and referenced on the Internet. The format for an FQDN is: server_name.domain_name.root_domain_name. For example, a server named online in the allhere domain in the .com root domain has a Fully Qualified Domain Name of online.allhere.com. Fully qualified domain names always use lower case characters.

Function Keys Specialized keys on a computer keyboard for performing specific tasks within application software. On most operating systems the F1 function key will bring up a help menu.

<g> An abbreviation for 'Grin' commonly used in chat rooms. Used either to show that we are amused or to say, "Don't take what I said too seriously." The latter usage can prevent misunderstandings.

Ga An abbreviation for 'Go Ahead' commonly used in chat rooms to signify that a person is through typing.

Gamma Correction The correction of tonal ranges in an image, normally by the adjustment of tone curves.

Gateway Refers to hardware or software that bridges the gap between two otherwise incompatible applications or networks so that data can be transferred among different computers. Gateways are

common with e–mail that gets sent back and forth between Internet sites and commercial online services that have their own internal e–mail systems.

Gateway Service for Netware A Windows NT server service that, when installed and configured on a computer, provides all of the functionality of Client Service for NetWare(CSNW). Additionally, GSNW enables the Server computer to transparently share resources (files, folders, and printers) located on a NetWare server to client computers of the Windows NT Server computer. GSNW accomplishes this by converting the Server Message Blocks (SMBs) from the client computers of the Windows NT Server computer into NetWare Core Protocol (NCP) requests that are recognized by the NetWare server.

Gauge A measure of a cables thickness. It is measured by the Radio–Grade measurement, or RG number. The higher the RG number, the thinner the central conductor core; the lower the number, the thicker the core. So, 18–gauge wire is thicker than 24–gauge wire.

Gb See Gigabit

GB See Gigabyte

Geo–synchronous In reference to satellites or space vehicles which appear to be stationery over one point above the earth (usually at the equator), which are actually travelling at the same speed as the earth's rotation, permitting the use of earth receiving stations without expensive tracking equipment.

GIF (Graphic Interchange Format) A common format for image files, especially suitable for images containing large areas of the same color. GIF format files of simple images are often smaller than the same file would be if stored in JPEG format, but GIF format does not store photographic images as well as JPEG (although this is changing as new technologies allow GIFs to be stored in up to 32 bit colour).

Gigabit 1,024 megabits (Mb), or 1,073,741,824 bits.

Gigabyte 1,024 megabytes (MB), or 1,073,741,824 bytes.

GMT Greenwich Mean Time, often used as a standard time zone. In e–mail headers, we will often see references to the hours offset from GMT. For example, Eastern Standard Time is GMT minus 5 hours because of the 5 hour difference between Greenwich, England and the Eastern US.

gmta An abbreviation for 'Great Minds Think Alike' commonly used in chat rooms.

Gopher A widely successful method of making menus of material available over the Internet. Gopher is a Client and Server style program, which requires that the user have a Gopher Client program. Although Gopher spread rapidly across the globe in only a couple of years, it has been largely supplanted by Hypertext. There are still thousands of Gopher Servers on the Internet and we can expect they will remain for a while.

Graphical User Interface The graphical visual representation of the working environment that presents the elements of our computer as objects on a desktop. GUIs allow us to press buttons

instead of typing commands at the command line and they give us a much closer representation of the end product.

Greyscale Refers to an image that contains only black, grey and white pixels and utilizing grey tones in place of colour.

Group Dependencies Groups of services or drivers that must be running before a given service (or driver) can start.
Group Policy A policy that applies to a group of users. Group policies apply to all users that are members of a group (that has a group policy), and that do not have individual user policies.

GSNW See Gateway Service for Netware

GUI See Graphical User Interface

Hacker A person who gains access to secured or password protected networks via dial–up connection or via the internet. There are a few professionals who earn their living this way but for some strange reason many teenagers consider it cool to attempt to break into protected areas.

Half Duplex A communications system, circuit or component capable of transmitting in two directions alternatively, not simultaneously.

Handle A unique name given to a person utilizing Internet Relay Chat. Their 'Handle' is what they are known as for the duration that a session is established from their computer to an IRC server.

Handshaking The process computers and modems go through in order to establish a connection and agree on the speed and protocols for data transmission.

Hard Drive The main device a computer uses to permanently store and retrieve information. These drives are sealed boxes typically found inside the computer. Also called a "hard disk."

Hardcopy Printed or filmed output, such as paper, which can be read by someone other than the person at a computer screen. Information that can't be distributed with out the use of some electronic device is known as softcopy.

Hardware Any physical device located within or connected to a computer. In order to use programs (Software) we require a hardware platform that the programs can utilize.

Hardware Compatibility List A list of hardware that is supported by an operating system. This list can usually be found at the operating system manufacturer's website.

Hardware Configuration The devices we have within and connected to our computer and the way in which they must be set up in order for them to work together.
HCL See Hardware Compatibility List

HDTV High Definition Television. Regular NTSC signals have 525 lines of resolution. HDTV has 1125 lines of resolution. The difference between a professional photographer's work and an Instamatic. Having over five times the video information than that of a conventional NTSC–type

TV set. In spite of its obvious advantages, it does require extraordinary bandwidth on the frequency spectrum to transmit five times the capacity of a conventional TV signal. HDTV receivers are estimated to be 30% more expensive than today's most costly TV sets.

Headend A cable systems site that houses the equipment needed to receive, process and originate signals for a cable system.

Header The portion of a packet of transmitted information, preceding the actual data, containing source and destination addresses, error checking and other fields. A header is also the part of an electronic mail message that precedes the body of a message and contains, among other things, the message originator, date and time.

Hertz A unit of frequency measurement equivalent to one cycle per second. Named in honor of Heinrich Hertz, first to detect such waves in 1883.

Hex See: Hexadecimal

Hexadecimal Base 16 arithmetic. Conventionally, the 16 digits are represented by the digits 0 through 9 and the letters A through F. The letter A, for example, represents the decimal number 10. A byte (8 bits of data) is often represented by two hexadecimal numbers. The hexadecimal values can range from 00 to FF or from decimal 0 to 255. Hexadecimal values are often differentiated from decimal by either following them with the letter h or preceding them with an angle bracket, for example 33h or >0B. Hexadecimal numbers have many applications in computer programming, and they are frequently used in RGB color coding for web pages.

High Performance File System The file system used by OS/2. Windows NT used to support HPFS, but HPFS support was dropped for NT version 4.0.

Hit As used in reference to the World Wide Web, "hit" means a single request from a web browser for a single item from a web server; thus in order for a web browser to display a page that contains 3 graphics, 4 "hits" would occur at the server: 1 for the HTML page, and one for each of the 3 graphics. Hits are often used as a very rough measure of load on a server, e.g. "Our server has been getting 300,000 hits per month." Because each hit can represent anything from a request for a tiny document (or even a request for a missing document) all the way to a request that requires some significant extra processing (such as a complex search request), the actual load on a machine from 1 hit is almost impossible to define.

Hive A group of Registry keys and values that are stored in a single file.

Home Page (or Homepage) Several meanings. Originally, the web page that our browser is set to use when it starts up. The more common meaning refers to the main web page for a business, organization, person or simply the main page out of a collection of web pages, e.g. "Check out Dirk's new Home Page." Another use of the term refers to practically any web page as a "homepage," e.g. "That web site has 65 homepages and none of them are interesting."

Hop A message or data packet travels a path from source to destination crossing many routers along the way. The link from source to router, router to router and router to destination is defined

as a hop.

Hop Count The number of routers that a data packet travels across +1 to get to its destination. We must add one to the router count as the packet makes one final hop from the last router to the destination computer.

Host A host is a computer that is connected to a TCP/IP network, such as the Internet.

HP Hewlett Packard

HPFS See High Performance File System

HTML See Hypertext Markup Language

HTTP See Hypertext Transfer Protocol

Hub A device that connects the cables from computers and other devices such as printers in an ethernet local area network. Traditionally, hubs are used for star topology networks, but they are often used with other configurations to make it easy to add and remove computers without bringing down the network. Smart hubs or switching hubs are often used to improve performance by managing traffic.

Hyperlink A link in a web page that takes us to another location or resource when activated. Hyperlinks usually appear as underlined text and printed in a contrasting color, but they may also appear as graphics, such as buttons to click. Hyperlinks may link to another place in the same page, to a different page, to play an audio or video file, to download a file, to set up a message to an e–mail address, to search a database, to read Usenet newsgroups, and to link to other Internet resources.

Hypertext Generally, any text that contains links to other documents – words or phrases in the document that can be chosen by a reader and which cause another document to be retrieved and displayed.

Hypertext Markup Language The coding language used to create Hypertext documents for use on the World Wide Web. HTML looks a lot like old–fashioned typesetting code, where we surround a block of text with codes that indicate how it should appear, additionally, in HTML we can specify that a block of text, or a word, is linked to another file on the Internet. HTML files are meant to be viewed using a World Wide Web Client Program, such as Netscape or Mosaic.

Hypertext Transfer Protocol The protocol for moving hypertext files across the Internet. Requires an HTTP client program on one end, and an HTTP server program on the other end. HTTP is the most important protocol used on the World Wide Web (WWW).

Hz See Hertz

I/O Input/Output

I/O Address Input/Output address. A hexadecimal number that is assigned to a piece of hardware in a computer and then given to the software driver for that piece of equipment so that they

can communicate.

I/O Operations Instructions provided by a program for inputting data into internal memory and outputting information.

IAB See Internet Architecture Board

IANA See Internet Assigned Number Authority

IBM International Business Machines

Icon A graphical symbol, usually representing a file, folder, disk or tool. Icons are usually either 16x16 pixels or 32x32 pixels in dimension.

IDE See Integrated Drive Electronics

IEEE See Institute of Electrical and Electronics Engineers

IEEE 802.2 The IEEE standard defining the Logical Link Control sublayer which is the upper portion of the data link layer for local area networks.

IETF See Internet Engineering Task Force

iirc An abbreviation for 'If I Remember Correctly' commonly used in chat rooms.

IIS See Internet Information Server

Image Map A graphic divided into regions or "hotspots". When a particular region is clicked with a mouse, it calls up a web page that has been associated with that particular region.

IMAP See Internet Message Access Protocol

IMHO Shorthand for 'In My Humble Opinion' added to a comment written in an online forum. IMHO indicates that the writer is aware that they are expressing a debatable view, probably on a subject already under discussion.

Impedance Opposition to current flow in an alternating current (AC). It is measured in ohms. While DC travels through the core of a wire, AC travels on the surface.

Import To bring data into a document from another document, often generated by a different application.

Impression With regards to Internet advertising, an impression is one viewer looking at one banner ad. By collecting impression information an advertiser can ascertain how many people have seen his ad, how many have clicked on it and can judge the effectiveness of the ad by comparing these figures.

Inactive Window In a multiple window environment (when we run more than one program on a computer each program is represented in a separate window.) any window that is behind the active window and whose title bar is greyed out.

Industry Standard Architecture The ISA bus was designed by IBM and used in the IBM PC. Due

to the need for compatible devices, IBM decided to make ISA an open standard, allowing third–party manufacturers to produce hardware without paying IBM for the use of the standard. This bus was originally designed to transfer 8 megabits per second. It was later enhanced to allow 8–bit add–on cards and 16–bit add–on cards to use the same slot and still benefit from their designed architecture speed.

Information Technology Encompasses all matters concerned with the use and furtherance of computer science and technology as well as the design, development, installation and implementation of information systems and applications.

Infrastructure This term can be either narrowly or broadly defined. In a narrow sense, it refers to "the underlying structure of technical facilities and institutional arrangements that supports communication via telecommunication, broadcasting, film, audio and video recording, cable, print and mail." In a much broader sense, it can be defined as "not only the tangible capital assets, but the human capital necessary to realize the potential of any technical system."

Institute of Electrical and Electronics Engineers The world's largest technical professional society, based in the USA. Founded in 1884 by a handful of practitioners of the new electrical engineering discipline, today's Institute has more than 320,000 members who participate in its activities in 147 countries. The IEEE sponsors technical conferences, symposia and local meetings worldwide, publishes nearly 25% of the world's technical papers in electrical, electronics and computer engineering and computer science, provides educational programs for its members and promotes standardization. Areas covered include aerospace, computers and communications, biomedical technology, electric power and consumer electronics.

Integrated Drive Electronics A standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices.

Integrated Services Digital Network A way to move more data over existing regular phone lines. ISDN is rapidly becoming available to much of the USA and in most markets it is priced very comparably to standard analog phone circuits. It can provide speeds of roughly 128,000 bits–per–second over regular phone lines. In practice, most people will be limited to 56,000 or 64,000 bits–per–second.

Interchange A standard format for sharing or transferring data electronically between parties that do not share a common application. Usually a format that is platform–independent is agreed upon as a standard.

Interface Something that connects two separate entities. For example, a user interface is the part of a program that connects the computer with a human operator (user). There are also interfaces to connect programs, to connect devices, and to connect programs to devices. An interface can be a program or a device, such as an electrical connector.

Intermediate Device Any device or system on a network that data must pass through between end systems.

Intermediate System See Intermediate Device

Internet The vast collection of inter–connected networks that all use the TCP/IP protocol and that evolved from the ARPANET of the late 60's and early 70's.

internet Any time we connect 2 or more networks together, we have an internet – as in inter–national or inter–state.

Internet Architecture Board The Internet Architecture Board is the technical advisory group of the Internet Society responsible for setting Internet standards, publishing RFCs, and overseeing the Internet standards process. The IAB governs the Internet Engineering Task Force, the Internet Assigned Number Authority and the Internet Research Task Force.

Internet Assigned Number Authority The arm of the Internet Architecture Board responsible for overseeing and coordinating the assignment of every unique protocol identifier used on the Internet.

Internet Engineering Task Force This Task Force is concerned with developing solutions to technical problems and needs as they arise on the Internet and with developing Internet standards and protocols. The IETF is governed by the IAB who are in turn responsible to ISOC.

Internet Information Server A Microsoft® Server service that provides World Wide Web (WWW), File Transfer Protocol (FTP), and Gopher publishing services on the World Wide Web.

Internet Mail Access Protocol See Internet Message Access Protocol

Internet Message Access Protocol A mail protocol that provides management of received messages on a remote server. The user can review headers, create or delete folders/mailboxes and messages, and search contents remotely without downloading. It includes more functions than the similar POP protocol.

Internet Protocol Address Sometimes called a dotted quad. A unique number consisting of 4 parts separated by dots, e.g. 165.113.245.2. Every machine that is on the Internet has a unique IP number – if a machine does not have an IP number, it is not really on the Internet. Most machines also have one or more Domain Names that are easier for people to remember.

Internet Relay Chat A huge multi–user live chat facility. There are a number of major IRC servers around the world which are linked to each other. Anyone can create a channel and anything that anyone types in a given channel is seen by all others in the channel. Private channels can (and are) created for multi–person conference calls.

Internet Research Task Force The arm of the Internet Architecture Board responsible for coordinating all TCP/IP related research projects.

Internet Service Provider An institution that provides access to the Internet in some form, usually for money.

Internet Society Was created in 1992 and is a global organization responsible for the internetworking technologies and applications of the Internet. Though its principal purpose is to encourage the development and availability of the Internet, it is in turn responsible for the further devel-

opment of the standards and protocols that allow the Internet to function.

Internet Telephony The conversion of analog speech signals used on current telephone systems into digital data, allowing calls to be sent over the Internet, bypassing long distance charges. While the Internet was first devised as a way of transmitting data, it is now being used to make voice calls. Internet telephony is projected to explode as the cost of Internet connections plummet.

Internetwork An interconnection of two or more networks, usually local area networks enabling data can pass between computers on the different networks as though they were on one network. This requires some kind of router or gateway.

Interoperability The ability of different hardware and/or software systems to communicate with each other in order to accomplish a particular task. This can be accomplished through adherence to certain standards or the provision of specialized technical accommodations.

Interpreter A Computer language processor that converts high–level program instructions into machine language (code) one instruction statement at a time. Compare with compiler.

Interrupt Request An IRQ is a unique number between two and fifteen that is assigned to a hardware peripheral in a computer. No two devices in the computer should have the same interrupt, unless the devices are capable of (and correctly configured to) share an interrupt.

Intranet A TCP/IP internetwork that is not connected to the Internet. For example, a company's multi–city internetwork can be called an intranetwork as long as it is not connected to the Internet.

IP Address See Internet Protocol Address

IRC See Internet Relay Chat

IRQ See Interrupt Request

IRTF See Internet Research Task Force

ISA See Industry Standard Architecture

ISDN See Integrated Services Digital Network

ISOC See Internet Society

ISP See Internet Service Provider

Java A network–oriented programming language invented by Sun Microsystems that will run on almost any platform. It is specifically designed for writing programs that can be safely downloaded to our computer through the Internet and immediately run without fear of viruses or other harm to our computer or files. Using small Java programs (called "Applets"), Web pages can include functions such as animations, calculators, and other fancy tricks. We can expect to see a huge variety of features added to the Web using Java, since we can write a Java program to do almost anything a regular computer program can do, and then include that Java program in a Web page.

Java Development Kit A software development package from Sun Microsystems that implements the basic set of tools needed to write, test and debug Java applications and applets.

Java Script A scripting language that allows dynamic behavior to be specified within HTML documents.

JDK See Java Development Kit

Joint Photographic Experts Group The organization responsible for designing and maintaining the JPEG image format.

Joystick An input device consisting of a small flat box with an embedded hand held stick that pivots about one end and transmits its angle in two dimensions to a computer. Joysticks are used to control games, and have one or more push–buttons whose state can also be read by a computer. Most I/O interface cards for PCs have a joystick port.

JPEG Most commonly mentioned as a format for image files. JPEG format is preferred to the GIF format for photographic images as opposed to line art or simple logo art.

Jumpers Small metal pairs of pins that stick out of circuit boards. We change their configuration by putting small plastic covers with metal internal connectors over them. By doing this, we are actually completing the circuit between the two pins. A jumper with the plastic cover on it is considered "closed," and one without is considered "open."

Kb See Kilobit

KB See Kilobyte

Kermit A common terminal emulation program and file transfer protocol that can be used across dialup and Telnet connections. It is much slower than xmodem, ymodem, and zmodem in most implementations, but it has the advantage of being able to transfer 8–bit files across a 7–bit telnet connection, which the others will not do. It was developed at Columbia U and is widely used in academia, probably because it is free. It was named for the frog.

Kernel The core component of an operating system.

Kernel Mode Refers to a highly privileged mode of operation given to software in an operating system. "Highly privileged" means that all code that runs in kernel mode can access the hardware directly, and can access any memory address. A program that runs in kernel mode is always resident in memory. It can't be written to the paging file.

Key A component of the Windows® Registry that is similar to a folder in a file system. A key can contain other keys and value entries.

Keyword Specified words entered into text search engines to locate information on a particular subject.

Kilobit 1,024 bits.

Kilobyte 1,024 bytes.

Ku–band The most popular format for satellite uplink and downlink reception. Operating on a higher microwave frequency than C–band, used exclusively for satellite communication.

LAN See Local Area Network

Laser Printer Although a number of devices employ laser technology to print images, this normally refers to desktop printers, which use the dry toner, xerographic printing process.

Laserdisc A 12–inch optical disk that's similar to an audio CD but holds visual images (such as high–quality movies) as well as CD quality sound. Also called a videodisc.

LCD See Liquid Crystal Display

LDAP See Lightweight Directory Access Protocol

Leased–line Refers to a phone line that is rented for exclusive 24–hour, 7–days–a–week use from our location to another location. The highest speed data connections require a leased line.

Light Pen Input device consisting of a light–sensitive photoelectric cell that reads bar codes.

Lightweight Directory Access Protocol A protocol for accessing information directories such as organizations, individuals, phone numbers, and addresses. It is based on the X.500 directory protocols, but it is simpler, and unlike X.500, it supports TCP/IP for Internet usage.

Line–of–Sight Signals that can only be received from transmission points which can be seen from a specific communications tower, since the signals cannot bend around the curvature of the earth or through hills, valleys and heavy trees. AM and FM signals are not line–of sight, while TV signals on microwave are line–of–sight.

Line Printer Daemon A print server software used in TCP/IP printing. LPD is supported by many operating systems, including Windows XP and UNIX.

Links Clickable text on the Internet or in multimedia that take us somewhere else. The alphabetical toolbars above and below are made up of links that take us to the corresponding pages of this glossary.

Liquid Crystal Display Utilized in many laptop and portable computers, it uses a clear liquid chemical trapped in tiny pockets between two pieces of glass. Each pocket of liquid is covered both front and back by thin wires. When current is applied to the wires, a chemical reaction turns the chemical a dark color, thereby blocking light. The point of blocked light is called a pixel.

List Administrator A person who manages a mailing list, adds and deletes members, and tends to the general administrative details of maintaining the list. The list administrator sometimes moderates the discussion and intervenes when there are disputes or flame wars.
Listserv® The most common kind of mail list, "Listserv" is a registered trademark of L–Soft international, Inc. Listservs originated on BITNET but they are now common on the Internet.

LLC Sublayer See Logical Link Control Sublayer

Local Area Network A computer network limited to the immediate area, usually the same build-

ing or floor of a building.

Local Group A group that can be created in the domain Directory Services database on a domain controller or in the SAM on any non–domain controller. Local groups are primarily used to control access to resources. In a typical configuration, a local group is assigned permissions to a specific resource, such as a shared folder or a shared printer. Individual user accounts and global groups are then made members of this local group. The result is that all members of the local group then have permissions to the resource. Using local groups simplifies the administration of network resources, because permissions can be assigned once, to a local group, instead of separately to each user account.

Local System Any computer equipment that we can access without information traveling across media such as the Internet or network cable is known as the local system.

LocalTalk A specification for the type of network cabling, connectors, and adapters developed by Apple Computer, Inc. for use with Macintosh computers.

Logical Drive A disk partition (or multiple partitions) that has been formatted with a file system and assigned a drive letter.

Logical Link Control Sublayer The second sublayer of the Data Link layer. It is responsible for establishing and maintaining data link connections between network devices. It is also responsible for any flow control and error correction found in this layer.

Logging On The process of supplying a user name and password, and having that user name and password authenticated by an operating system or networked computer.

Login The act of entering into a computer system, network or secure access area on the internet

Login Name The account name used to access a computer system usually requiring that a password must also be supplied.

Logoff The act of leaving and breaking communications with a computer system, network or secure access area on the internet.

Logon The act of entering into a computer system, network or secure access area on the internet.

Logon Hours The assigned hours that a user can log on to a server domain controller. The logon hours configuration only affects the user's ability to access the domain controller. It does not affect a user's ability to log on to a Workstation computer or to a non–domain controller.

Logon Script A batch file that is run when a user logs on to a server.

LOL An abbreviation for laughing out loud, LOL is used in various forms of online communications such as e–mail messages or postings to newsgroups or BBSs. LOL usually appears in brackets like this <LOL> and denotes a humorous reaction to something.

LPD See Line Printer Daemon

Lurker Slang term for someone that logs into BBS, IRC or Newsgroups without participating in

the discussions. Also known as a watcher.
MAC Address See Media Access Control Address

MAC Sublayer See Media Access Control Sublayer

Macro Virus A virus contained in and spread by a macro language program that supplements a word processed document or spread sheet. These are by far the most common type of viruses now, and they can easily be spread in attachments to e–mail. Never open an e–mail attachment without running anti–virus software first.

Mail Merge The merging of database information (such as names and addresses) with a letter template in a word processor, in order to create personalized letters.

Mailing List A system that allows people to send e–mail to one address, whereupon their message is copied and sent to all of the other subscribers to the mailing list. In this way, people who have many different kinds of e–mail access can participate in discussions together.

Mail Servers These are servers specifically set up to handle clients' E–mail needs. Some E–mail systems are capable of running from a standard file server, but as they increasingly support groupware and other applications, they need more hardware. The easiest solution is to place the E–mail server applications on their own file server.

Mailbox A folder on a mail server in which one client's E–mail is stored as the E–mail is received it is placed in the mailbox. When the client connects to the mail server his/her E–mail is downloaded from the mailbox onto the client computer.

Mail list See Mailing List

Mainboard See Motherboard

Mainframe A large capacity, powerful computer that is used by many users. All processing and file storage is carried out on the mainframe allowing all hosts to be very low powered (Dumb Terminals) as the hosts only need enough equipment to produce an image on a monitor and accept input from an input device. This is the most cost effective form of networking in terms of price and maintenance and also the safest in terms of security and viruses.

MAN See Metropolitan Area Network

Management Information Systems Computer based processing or manual procedures within an organization to provide useful and timely information to support decision–making on all levels of management.
Mandatory User Profile A user profile that, when assigned to a user, can't be modified by the user. A user can make changes to desk–top and work environment settings during a single logon session, but these changes are not saved to the mandatory profile when the user logs off. Each time the user logs on, the user's desktop and work environment settings revert to those contained in the mandatory user profile.

MAPI See Message Application Programming Interface

Master Browser The computer on the subnet that builds and maintains the browse list for that subnet. The master browser distributes this browse list to backup browsers on the subnet and to the domain master browser.

Math Coprocessor A secondary processing chip that is added to a computer that works with the CPU to solve floating–point calculations.

Matrix A Method of organizing information into a 3–Dimensional structure by giving it vertical and horizontal cross–points.

Maximum Password Age The maximum number of days a user may use the same password.

Mb See Megabit

MB See Megabyte

Mbps See Megabits per second

MCA See MicroChannel Architecture

Media Physical connection between the devices on a network.

Media Access Control Address Every device on a network has a hard–coded address attached to it. An example of this for an Ethernet card would be 00–AA–00–59–65–71.

Media Access Control Sublayer The first sublayer of the Data Link layer. It is responsible for physical addressing and access to the network media. Only one device at a time may transmit on any type of media. If multiple devices attempt to transmit, they will scramble each other's signal.The three ways it controls access to media are Addressing, Contention and Deterministic network management.

Medium The material used to support the transmission of data. Examples include twisted–pair wire, coaxial cable, optical fiber, or microwave.

Megabit 1,024 kilobits, or 1,048,576 bits.

Megabits per second A measurement of data transmission speed that is used to describe WAN links and other network connections.

Megabyte 1,024 kilobytes, or 1,048,576 bytes.

Megahertz A million cycles (occurrences, alterations, pulses or wavelengths) per second. Used to describe the speed at which a computer's processor (or CPU) operates.

Member Server A server computer that is not installed as a domain controller, and that has joined an existing server domain.

Memory In general, another word for dynamic RAM, the chips where the computers store system software, programs, and data we are currently using. Other kinds of computer memory we may encounter are parameter RAM (PRAM), video RAM (VRAM), and static RAM (SRAM). Most computer memory is volatile, that is, its contents are lost when the computer shuts down.

Memory Dump Refers to the process of an operating system copying the contents of RAM into a file (the memory.dmp file) when a STOP error or blue screen occurs.

Menu A list that drops down when a mouse button is depressed over a menu title. A menu contain a list of commands that are carried out when the menu item is clicked on or otherwise activated.

Menu Bar The horizontal bar that contains the names of available menus. The menu bar is located below the title bar at the very top of a program window.

Mesh Topology A network configuration in which all computers and devices are connected to every other computer and device with a separate dedicated physical connection between each device. The mesh topology provides the highest level of fault tolerance. A true mesh network uses separate cables to connect each device to every other device on the network, providing a straight communications path.

Message A collection of data that is ordered according to the rules of any given protocol suite, such that it is intelligible to the sending and receiving software.

Message Application Programming Interface A standard Windows interface for messaging that enables different mail programs and other mail–aware applications like word processors and spreadsheets to exchange messages and attachments with each other.

Message Services A network service that enables the sending of files with E–mails as attachments.

Message Switching A method of data transfer where data is sent from device to device in whole across a network. This is also known as store and forward. Devices must store all information as it is sent in whole. Media is used efficiently and congestion can be controlled. Priorities on information can be set so important data arrives first. This method does not work with real–time applications such as voice or video.

Meta A prefix meaning "information about". Commonly associated with Meta Tags which are located within an HTML document and contain information that makes it easier for search engines to locate relevant pages on the Internet in response to a search request.

Metropolitan Area Network A metropolitan area network or MAN is a group of Local Area Networks located within the same city that a joined by some form of connection. For example, if a college had campuses with networks in several suburbs of a city, they could be connected to create a MAN. MANs are slower than LANs but usually have fewer errors over the network.

MHz See Megahertz

Microsoft® Disk Operating System A computer operating system developed by Microsoft® .

MicroChannel Architecture A proprietary computer bus architecture designed by IBM to replace ISA. MCA operates at 16Mbps or 32Mbps and uses software to configure resource settings. MCA was not designed to be backward compatible with ISA, requiring people to buy new MCA hardware adapters.

Microwave In communications, a way of sending voice, data or video signals through the air as high frequency radio waves, to obtain high transmission capacities at lower cost than copper cable systems. Microwave systems carry analog or digital signals on a line of sight between antennas or on satellite uplinks and downlinks.

MIDI See Musical Instrument Digital Interface

MIME See Multipurpose Internet Mail Extension

Minimum Password Age The minimum number of days a user must keep the same password.

Minimum Password Length Specifies the minimum number of characters required in a user's password.

MIPS Millions of Instructions Per Second.

Mirror Generally speaking, "to mirror" is to maintain an exact copy of something. Probably the most common use of the term on the Internet refers to "mirror sites" which are web sites, or FTP sites that maintain exact copies of material originated at another location, usually in order to provide more widespread access to the resource. Another common use of the term "mirror" refers to an arrangement where information is written to more than one hard disk simultaneously, so that if one disk fails, the computer keeps on working without losing anything.

Mirror Site See Mirror

MIS See Management Information Systems

Modem (MOdulator, DEModulator) A device that we connect to our computer and to a phone line, that allows the computer to talk to other computers through the phone system. Basically, modems do for computers what a telephone does for humans.

MOO See Mud, Object Oriented

Mosaic The first WWW browser that was available for the Macintosh, Windows, and UNIX all with the same interface. Mosaic really started the popularity of the Web. The source–code to Mosaic has been licensed by several companies and there are several other pieces of software almost as good as Mosaic.

Motherboard The main circuit board of a computer. This plastic board resembles a miniature city, but its buildings are actually chips for things like the processing, RAM, and ROM, and the tiny roads connecting them are circuit traces. Also called the mainboard.

MOV A file extension commonly found on the Internet that denotes that the file is a movie or video in Apple's QuickTime format.

Moving Pictures Expert Group MPEG is an international standard for video compression and desktop movie presentation. We need a special viewing application to run the MPEG movies on our computer. Files in the MPEG format have a .mpg or .mpeg file extension.

MPEG See Moving Pictures Expert Group

MS–DOS See Microsoft® Disk Operating System

MUD See Multi–User Dungeon

Mud, Object Oriented One of several kinds of multi–user role–playing environments, so far only text–based.

Multi–User Dungeon A multi–user simulation environment. Some are purely for fun and flirting, others are used for serious software development, or education purposes and all that lies in between. A significant feature of most MUDs is that users can create things that stay after they leave and which other users can interact with in their absence, thus allowing a world to be built gradually and collectively.

Multi–User Simulated Environment A kind of MUD where there is little or no simulated violence.

Multihomed A computer is said to be multihomed when it has more than one network adapter installed in it.

Multimedia Any presentation or software program that combines several media, such as graphics, sound, video, animation, and/or text.

Multipurpose Internet Mail Extension The standard for attaching non–text files to standard Internet mail messages. Non–text files include graphics, spreadsheets, formatted word–processor documents, sound files, etc. An E–mail program is said to be MIME Compliant if it can both send and receive files using the MIME standard. When non–text files are sent using the MIME standard they are converted (encoded) into text – although the resulting text is not really readable. Generally speaking the MIME standard is a way of specifying both the type of file being sent and the method that should be used to turn it back into its original form. Besides E–mail software, the MIME standard is also universally used by Web Servers to identify the files they are sending to Web Clients, in this way new file formats can be accommodated simply by updating the Browsers' list of pairs of MIME–Types and appropriate software for handling each type.

Multiple Master Domain Model This domain model consists of two or more master domains that contain user accounts, and any number of resource domains that contain shared resources. In this model, a two–way trust is used between each of the master domains, and a one–way trust is used from each resource domain to each and every master domain. See also trust relationship, one–way trust, and two–way trust.

Multiplexer A device that is capable of dividing a single transmission medium into multiple logical channels supporting many simultaneous sessions.

Multiplexing Dividing a single transmission medium into multiple logical channels to support many simultaneous sessions. e.g. cable television.

Multiplexing Device A device that is capable of dividing a single transmission medium into multiple logical channels supporting many simultaneous sessions.

Multipoint Distribution A method of broadcasting where one origination site sends the same programming simultaneously to many different reception sites.

Multiprocessing Refers to the capability of an operating system to use more than one processor in a single computer simultaneously.

Multitasking Refers to the capability of an operating system to carry out more than one process at a time.

MUSE See Multi–User Simulated Environment

Musical Instrument Digital Interface A technology that enables a computer to record and play musical performance. The major difference between MIDI and other forms of playback is that MIDI merely gives a music score to the built–in instruments of a sound card or musical instrument and the Instruments are played 'live'. That is they reproduce sounds according to the score so there is no quality loss. Many people have a bad impression of MIDI music as the quality of the rendition is in direct proportion to the quality of the sound card it is played through. With a high quality sound card there is nothing closer to listening to a live performance.

MUX See Multiplexing Device

Narrowband Communication A form of a communication system capable of carrying only voice or relatively slow speed computer signals.

Native Software that's written specifically to run on a particular processor. For example, a program optimized for an x86 Intel processor runs in native mode on a PC, but it runs in emulation mode (which is slower) on an Apple computer. Also, the file format in which an application normally saves its documents. The native format is generally readable only by that application (other programs can sometimes translate using filters).

Navigation The process of moving around a website or multimedia presentation.

Navigation Tools These are tools that allow users to find their way around a website or multimedia presentation. They can be hypertext links, clickable buttons, icons, or image maps.

NDIS See Network Device Interface Specification

Near–Line Refers to data or services that is kept offline to save expensive disk space or resources but can be bought back online automatically when a user requests it. Examples of this are optical disk jukeboxes that store data offline and then automatically copy requested information on to a hard disk where it can be accessed. The data is removed from the hard disk after a specified amount of time.

NetBEUI A nonroutable protocol designed for use on small networks.

Netiquette The etiquette of the Internet.

Netizen Derived from the term citizen, referring to a citizen of the Internet, or someone who uses

networked resources. The term connotes civic responsibility and participation.

Netscape A WWW Browser and the name of the company that publishes it. The Netscape® browser was originally based on the Mosaic program developed at the National Center for Supercomputing Applications (NCSA). Netscape corporation also produces web server software.

Netware Novell's server operating system.

Network In general, a group of computers set up to communicate with one another. Our network can be a small system that's physically connected by cables (a LAN), or we can connect separate networks together to form larger networks (called WANs). The Internet, for example, is made up of thousands of individual networks.

Network Access Order Specifies which protocol or service an operating system will use first when it attempts to access another computer on a network.

Network Adapter An adapter card in a computer that enables the computer to connect to a network.

Network Cards Adapter cards in computers that enable the computers to connect to a network.

Network Client Administrator A Windows NT® Server tool we can use to create an installation disk set to install network clients or services on client computers. We can also use Network Client Administrator to create a network installation startup disk. A network installation startup disk, when run on a computer that needs to be set up (the target computer), causes the target computer to automatically connect to the server and to start an interactive installation/setup routine.

Network Device Driver A kernel mode driver that is designed to enable Windows NT to use a network adapter to communicate on the network.

Network Device Interface Specification Was created by Microsoft and 3Com. It is utilized by almost all companies in the PC networking community. NDIS specifies how network devices interface with the network and maps very closely to the OSI Model.

Network File System A protocol developed by Sun Microsystems which allows a computer system to access files over a network as if they were on its local hard disks. This protocol has been incorporated in products by more than two hundred companies, and is now a de facto Internet standard.

Network Interface Card An add–on card which plugs into a computer and adapts the network interface to the appropriate standard. ISA, PCI, and PCMCIA network cards are all examples of NICs.

Network Layer The third layer of the OSI model. This layer is responsible for routing information from one network device to another. The Network layer decides what path data will take if the destination device is located on another network.

Network Monitor is a server administrative tool that allows us to capture, view, and analyze network traffic (packets).

Network News Transfer Protocol The protocol used by client and server software to carry USENET postings back and forth over a TCP/IP network. If we are using any of the more common software such as Netscape, Internet Explorer, etc. to participate in newsgroups then we are benefiting from an NNTP connection.

Network Numbers These are 32–bit binary numbers that uniquely identify an NWLink IPX/SPX Compatible Transport network segment for routing purposes. Because network numbers uniquely identify a network segment, they are used by IPX routers to correctly forward data packets from one network segment to another.

Network Services These are services available to client computers over a network.

Networking Model describes how information is processed by the computers on the network. Data can be processed by clients (Collaborated), by a central server (Centralized), or by everyone (Distributed).

Newbie A newcomer to the Internet, who reveals his or her inexperience by lack of knowledge of Internet conventions, netiquette, vocabulary, and know–how.

News Server A machine that contains a number of USENET newsgroups. Also referred to an NNTP server.

Newsgroup The name for discussion groups on USENET.

Newsreader A software program that lets us subscribe to newsgroups on USENET as well as read and post messages to them.

NFS See Network File System

NIC See Network Interface Card

NNTP See Network News Transfer Protocol

NNTP Server See News Server

Node The point at which computers and telecommunications equipment are connected to a network.

Noise Electrical interference to a cable that causes irregularities in a signal that travels along it resulting in poor reception of transmitted data.

Non–Browser A computer that is not capable of maintaining a browse list either because it was configured not to do so, or because the operating system on this computer is incapable of maintaining a browse list.

NTFS 32bit File System used by Windows NT and Windows 2000.

NTFS Permissions These are permissions assigned to individual files and folders on an NTFS partition that are used to control access to these files and folders. NTFS permissions apply to local users as well as to users who connect to a shared folder over–the–network. If the NTFS permissions are more restrictive than share permissions, the NTFS permissions will be applied.

NTSC National Television Systems Committee The American engineering standard for video resolution containing 525 horizontal lines.

NWLink IPX/SPX Compatible Transport A routable transport protocol typically used in a combined Windows NT® and NetWare® environment. NWLink IPX/SPX Compatible Transport is Microsoft's® version of Novell's® IPX/SPX protocol. (IPX/SPX is the protocol used on most Novell NetWare networks.) NWLink provides protocol compatibility between Windows NT and NetWare computers. In addition to its functionality in a NetWare environment, NWLink also fully supports Microsoft networking.

Object Linking and Embedding A distributed object system and protocol from Microsoft. OLE allows an editing program to "subcontract" part of a document to another editing program and then re–import it. For example, a desk–top publishing system might send some text to a word processor or a picture to a bitmap editing program using OLE.

Object–Oriented Programming A programming technique that speeds the development of software and makes it easier to maintain through the re–use of "objects" that have behaviors, characteristics, and relationships associated with them. The objects are organized into collections (also called class libraries), which are then available for building and maintaining applications. Each object is part of a class of objects, which are united via "inheritance" and share certain characteristics and relationships.

OCR See Optical Character Recognition

ODBC (Open DataBase Connectivity) A software specification that enables ODBC–enabled applications (such as Microsoft Excel) to connect to databases (such as Microsoft SQL Server and Microsoft Access). The ODBC application in Control Panel is used to install and remove ODBC drivers for various types of databases. Additionally, this application is used to configure ODBC data sources.

Offline Not currently connected to other computers or devices. We're offline when we've logged out of the Internet, a network, BBS, or an online service. A device such as a printer is offline when it is turned off and not accessible to a computer. If we are not offline we are online.

OLE See Object Linking and Embedding

One–Way Trust When a single trust relationship exists between two domains, it is called a one–way trust. Both domains must be configured by an administrator in order to establish a trust relationship. The trusted domain should be configured first, and then the trusting domain. Members and Services on the trusted domain have access to the trusting domain but not vice versa.

On–Board Refers to functionality that has been built–in to a circuit board.

Online Actively connected to other computers or devices. We're online when we've logged on to the Internet, a network, BBS, or an online service. A device such as a printer is online when it is turned on and accessible to a computer. If we are not online we are offline.

Online Service A commercial service that provides services for a price such as e–mail, discussion forums, tech support, software libraries, news, weather reports, stock prices, plane reservations, even electronic shopping malls. To access one, we need a modem or other form of Internet connection. Popular on–line services include America Online, EarthLink, and CompuServe.

Open Systems Interconnection Model A set of rules released in 1984 by the International Standards Organization (ISO) to be used as a guide for network protocols. It consists of seven main layers and depicts the stream of information from the source application down through the network protocol as it is converted for media transport, routing and delivery to the target computer. Different hardware operates at different levels of the OSI Model. The seven layers are:

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Operating System The main software that is in use on a computer system. The operating system is responsible for booting up the computer and making all its resources available to the user and other software packages in a user friendly environment. Good examples are Windows XP, Windows Vista, and Windows NT.

Optical Character Recognition A technology that allows us to scan a printed page (with a scanner) and convert it into a text document that can be edited with a word processor or text editor.

Optical Disc Any storage disc that holds information in digital format that must be read using laser technology such as CDs, Laserdiscs and DVDs.

Optical Storage A storage technology utilizing a high–power laser beam to burn microscopic spots on a disk's surface coating. Data is represented by the presence and absence of holes in the storage locations. A much lower power laser beam is used to retrieve the data. Much more data can be stored this way than with traditional storage media and at a fraction of the cost.

OS See Operating System

OSI Model See Open Systems Interconnection Model

otoh An abbreviation for 'On The Other Hand' commonly used in chat rooms.

Packet A unit of digital data with a set number of bits, including some bits that serve as destination or "address" code. The unit, or packet, can be separated from the rest of its message components and sent through a specially switched communications network to its destination, where it

can be reunited with the other message components, regardless of which paths they took en route.

Packet Assembler/Disassembler A program or a few lines of code that disassembles data into small packets for transfer adding source and destination information to the packet or reassembles data that it has received from another PAD.

Packet Switching The method used to move data around on the Internet. In packet switching, all the data coming out of a machine is broken up into chunks, each chunk has the address of where it came from and where it is going. This enables chunks of data from many different sources to co–mingle on the same lines, and be sorted and directed to different routes by special machines along the way. This way many people can use the same lines at the same time.

PAD See Packet Assembler/Disassembler

Paging File (sometimes called a page file or a swap file) is a file used as a computer's virtual memory. Pages of memory that are not currently in use can be written to a paging file to make room for data currently needed by the processor.

PAL A European engineering standard for video resolution containing 625 horizontal lines.

Palette The set of colors used in a picture or on a computer screen. Older computers typically used only 16 colors. Modern ones use at least 256 colors, which can be coded by 8 bits of information. With advanced color cards and monitors 65.5 thousand colors (16–bit) or 16 million colors (24–bit) are used. Different web browsers and computer platforms do not necessarily use identical palettes. There is a set of 216 colors that are considered browser and platform safe, which web page designers should use, if they want screens to look essentially the same on each computer that views them.

Parallel Cable A cable used to connect peripheral devices through a computer's parallel port. A parallel cable is made up of 25 wires which can transmit information simultaneously. Its most common uses are connecting printers, scanners, external drives and connecting to other computers for data transfer.

Parallel Port A female 25 pin connector situated at the back of computers that enables the connection of peripheral devices and other computers via a parallel cable.

Parameter A word, number, or symbol that is typed after a command to further specify how the command should function. Parameters are usually typed after a forward slash (/).

Parity A check bit used to make the sum of the bits in a unit of data either even or odd (including the parity bit). A unit of data that is 8 bits long would have no parity, and a unit of data 7 bits long would have an even parity bit to make an 8 bit word. Parity is used to check a unit of data for errors during transmission over all types of media.

Parsing Refers to the process by which programming data input is broken into smaller, more distinct chunks of information that can be more easily interpreted and acted upon.

Participative Design The process of arriving at better decisions, not a process of optimization, but

rather a process of negotiation, using consensus–building methods, among those with different points of view and value systems to find a satisfying design solution. Often called dialectics.

Partition A portion of a hard disk that can be formatted with a file system, or combined with other partitions to form a larger logical drive.

Password A code used to gain access to a locked system. Good passwords contain letters and non–letters and are not simple combinations such as Pass1. A good password might be: S1n@bedt1me

Password Uniqueness Specifies how many different passwords a user must use before a previous password can be reused.

Paste To insert information from the Clipboard into a document or picture at the current cursor point. Information can be pasted multiple times.

Path A route used in finding, retrieving, and storing files on a disk, network or internetwork. The course leading from the root directory or share of a drive to a particular file.

PBX See Private Branch Exchange

PCI See Peripheral Component Interface

PCMCIA See Personal Computer Memory Card International Association

PDA see Personal Digital Assistant

PDF The file extension for Portable Document Format. A PDF file is an electronic facsimile of a printed document. PDF is designed and supported by Adobe.

Peer A computer that acts as both a client and a server.

Peer–to–Peer Networking A simple form of networking where clients on the network may also act as servers, and a large central server is not needed. Since security is hard to maintain in this type of network, the number of users must be kept low.

Peripheral A piece of hardware that is located outside the main computer. It usually refers to external hardware such as printers, and scanners sold by a third party.

Peripheral Component Interface A computer bus architecture standard that is used very widely today. PCI runs at up to 33MHz and can transfer 32 bits at a time. PCI was originally developed to speed up graphics on newer computers. PCI slots are not backward compatible with any other bus type. They use a small, condensed connector on the main board of the computer. A good feature of PCI is that it is not tied to any one type of computer. Computers based on the Intel line of processors, Digital Alphas, and Apple Macintosh computers all support and use PCI cards.

PERL See Practical Extraction and Report Language

Permissions Control access to resources, such as shares, files, folders, and printers on a networked computer.

Personal Computer Memory Card International Association The organization responsible for developing PCMCIA which is a standard format for credit–card–size expansion cards, used to add features to laptop computers, hand–held computers, and desktop computers.

Personal Digital Assistant (PDA) is a handheld computer also known as **palmtop computers**. Newer PDAs also have both color screens and audio capabilities, enabling them to be used as mobile phones, (smartphones), web browsers, or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi–Fi, or Wireless Wide–Area Networks (WWANs). Some PDAs employ touch screen technology.

Physical Layer The first layer of the OSI model. The function of this layer is the transmission of bits over the network media. It provides a physical connection for the transmission of data among the network devices and for making sure that data is read the same way on the destination device as it was sent from the source device. The Physical layer specifies the mechanical, electrical, and functional means to establish and maintain physical connections.

Ping An Internet utility used to check the connection with another site. It repeatedly bounces a signal off the remote site and shows us how long it took to complete the round trip each time. If we get no returns at all, the site is either down or unreachable. If only a portion of the signals are returned, it indicates some trouble with the connection that will slow down performance.

Pixel Picture element. Digital images are composed of touching pixels, each having a specific color or tone. The eye merges differently colored pixels into continuous tones. If we look at our display adapter setup we will see a measurement listed in pixels. 640x480 or higher.

PKUNZIP A software decompression utility for the PC. It allows us to decompress or "unzip" a file or a number of files from archive files in the ZIP file format.

PKZIP A software compression utility for the PC. It allows us to compress or "zip" a file or a number of files into one archive file in the ZIP file format.

Plug–in A piece of software that adds features to a larger piece of software. Common examples are plug–ins for the Netscape® browser and web server. Adobe Photoshop® also uses plug–ins. The idea behind plug–in's is that a small piece of software is loaded into memory by the larger program, adding a new feature, and that users need only install the few plug–ins that they need, out of a much larger pool of possibilities. Plug–ins are usually created by people other than the publishers of the software the plug–in works with.

Plug and Play A specification that makes it possible for hardware devices to be automatically recognized and configured by the operating system without user intervention.

pmfjih An abbreviation for 'Pardon Me For Jumping In Here' commonly used in chat rooms as a polite excuse to enter the discussion.

Point–to–Multipoint A teleconference or communication from one location to several receiving sites.

Point–to–Point Multilink Protocol An extension of the Point–to–Point Protocol. Point–to–Point Multilink Protocol combines the bandwidth from multiple physical connections into a single logical connection. This means that multiple modem, ISDN, or X.25 connections can be bundled together to form a single logical connection with a much higher bandwidth than a single connection can support.

Point–to–Point Protocol A newer connection protocol that was designed to overcome the limitations of the Serial Line Internet Protocol (SLIP). PPP is currently the industry standard remote connection protocol, and is recommended for use by Microsoft. PPP connections support multiple transport protocols, including: TCP/IP, NWLink IPX/SPX Compatible Transport, and NetBEUI. Additionally, PPP supports dynamic server–based IP addressing (such as DHCP). PPP supports password encryption, and the PPP connection process does not usually require a script file.

Point–to–Point Tunneling Protocol Permits a virtual private encrypted connection between two computers over an existing TCP/IP network connection. The existing TCP/IP network connection can be over a local area network or over a Dial–Up Networking TCP/IP connection (including the Internet). All standard transport protocols are supported within the Point–to–Point Tunneling Protocol connection, including NWLink IPX/SPX Compatible Transport, NetBEUI, and TCP/IP. A primary reason for choosing to use PPTP is that it supports the RAS encryption feature over standard, unencrypted TCP/IP networks, such as the Internet.

Polling System A physical network management system where a master device checks secondary devices on the network to see if they need to transmit and allots them transmission time accordingly. The order of the devices are polled in and their transmission priority can be set by an administrator. Networks that use this configuration operate in a multi point configuration. Each secondary device is directly connected to the primary controller.

POP See Post Office Protocol

POP3 Post Office Protocol version 3.0

Port (1) A place where information goes into or out of a computer, or both. E.g. the serial port on a personal computer is where a modem would be connected. (2) On the Internet port often refers to a number that is part of an URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80. Services can also listen on non–standard ports, in which case the port number must be specified in a URL when accessing the server, so we might see an URL of the form: gopher://peg.cwis.uci.edu:7000/ shows a gopher server running on a non–standard port (the standard gopher port is 70). (3) port also refers to translating a piece of software to bring it from one type of computer system to another, e.g. to translate a Windows program so that is will run on a Macintosh.

Portable Document Format See PDF

Portable Operating System Interface for Computing Environments Developed as a set of accepted standards for writing applications for use on various UNIX computers. POSIX environ-

ment applications consist of applications developed to meet the POSIX standards. These applications are sometimes referred to as POSIX–compliant applications. Windows NT provides support for POSIX–compliant applications via the POSIX subsystem. POSIX applications are source compatible across all supported hardware platforms. This means that POSIX applications must be recompiled for each hardware platform in order to be run on that platform.

Portal Usually used as a marketing term to described a Web site that is or is intended to be the first place people see when using the Web. Typically a "Portal site" has a catalog of web sites, a search engine, or both. A Portal site may also offer E–mail and other service to entice people to use that site as their main "point of entry" (hence "portal") to the Web.

Post Office Protocol The protocol used by e–mail clients to retrieve messages from a mail server. eg. E–mail address = rex@2400hrs.com When mail is sent to this address (using SMTP) the message is sent to 2400hrs.com which redirects it to its mail server (mail.2400hrs.com). The mail server places it in a folder called dirk to await collection. Dirk then uses his email client to connect to his mail server using POP which downloads all messages in the folder dirk to his computer.

Posting A single message entered into a network communications system. E.g. A single message posted to a newsgroup or message board.

POSIX See Portable Operating System Interface for Computing Environments

Potential Browser A computer that does not currently maintain or distribute a browse list, but is capable of doing so. A potential browser can become a backup browser at the direction of the master browser. See also backup browser, computer browser service, and master browser.

PPP See Point to Point Protocol.

PPTP See Point to Point Tunneling Protocol

Practical Extraction and Report Language An interpreted language for CGI scripts.

Preemptive Multitasking The operating system allocates processor time between applications. One application can be preempted by the operating system, and another application enabled to run. When multiple applications are alternately paused and then allocated processor time, they appear to run simultaneously to the user.

Presentation Layer The sixth layer of the OSI model, the Presentation layer, negotiates and establishes the format in which data is exchanged. This layer is responsible for any character set or numeric translations needed between devices. It is also responsible for data compression to reduce the amount of data transmitted, as well as encryption.

Primary Partition A disk partition that can be configured as the active partition. A primary partition can only be formatted as a single logical drive.

Print Device Refers to the physical device that produces printed output. This is what most people refer to as a printer.

Print Device Driver A kernel mode driver that formats print jobs into a RAW format. (The RAW format is ready to print, and no further processing is required.) A print device driver can also convert EMF for–matted print jobs into a RAW format.

Print Job All of the data and commands needed to print a document.

Print Monitor A software component that runs in kernel mode. A print monitor sends "ready–to–print" print jobs to a print device, either locally or across the network. Print monitors are also called port monitors.

Print Processor A kernel mode driver that manages printer device drivers and the process of converting print jobs from one format into another.
Print Queue A list of print jobs for a specific printer that are waiting to be sent to a print device.

Print Server A software program on a computer that manages print jobs and print devices. The term print server is also used to refer to a computer used primarily to manage multiple print devices and their print jobs.

Print Services These are services that allow printing to printers located over network media. These services remove the need to have many printers in an office as print services provide access from multiple computers to one or more printers. Windows 2000 even lets us access printers located anywhere in the world via an internet connection.

Printers Hardware devices that are connected to computers enabling users to produce hard copies of what is seen on the screen.

Printer Pool When a printer has multiple ports (and multiple print devices) assigned to it, this is called a printer pool. Users print to a single printer, and the printer load–balances its print jobs between the print devices assigned to it.

Private Branch Exchange A switching device owned by a customer (rather than the telephone company) to route internal calls among various extensions, to switch incoming calls to the appropriate extension and to route outgoing calls to the public telephone network access point.

Procedure In information systems, a specific sequence of steps performed to complete one or more processing activities.

Protocols Written rules used for communications. They are the languages that computers use to talk to each other over a network.

Protocol Stack Computers use protocols to talk to each other, and when information travels between computers, it moves from device to device, or layer to layer as defined by the OSI model. Each layer of the model has different protocols that define how information travels. The layered functionality of the different protocols in the OSI model is called a protocol stack.

Proxy Server A server that acts like a switchboard through a firewall to manage the various types of permitted communications with the outside world. Proxy servers may also use caching to make communications more efficient.

PSTN See Public Switched Telephone Network.

Public–domain Software that has no copyright or fee, which means we can copy, use, and even alter and sell it.

Public Switched Telephone Network The regular old–fashioned telephone system.
Query The process by which a web client requests specific information from a web server, based on a character string that is passed along.

Queue A set of computer instructions awaiting execution.

Queue–Based Printing Refers to printing that allows a client's application to spool the print job off to a network server so the application thinks the job has printed and lets the user continue to work. While the user continues to work, the network server handles sending the print job to the print device. Print queues can be given different priorities. This enables users to print more important documents quickly while lower priority jobs wait in the queue.

QuickTime A video compression system from Apple. Quicktime uses compression to make movie files a lot smaller for use on the web and in multimedia.

RAID See Redundant Array of Independent Disks

RAM See Random Access Memory

Random Access Memory The physical memory installed in a computer. When a piece of software is run on a computer, it's executable files are copied off the hard drive into RAM enabling the processor to access information quickly.

RAS See Remote Access Service

Read–Only Memory Type of memory that can be read but not altered. ROM is used primarily to store basic information about the computer that it needs to operate, startup and load an operating system.

Reduced Instruction Set Computing A relatively new microprocessor design technology which uses a smaller instruction set to control a computer's operations than the more traditional complex instruction set computing (CISC) computer design.

Redundant Array of Inexpensive Disks The system of using multiple affordable hard disks for error recovery and more efficient operation. Information is either duplicated to more than one disk (Mirroring) or spread over multiple disks (Striping).

Refresh Means to update the display with current information.

Registry A database that contains all of the information required to correctly configure an individual computer, its user accounts, and applications. Registries are unique to each computer–we should not use the Registry from one computer on another computer. The Registry is organized in a tree structure consisting of five subtrees, and their keys and value entries.

Registry Editors Tools that enable us to search and modify the Registry. There are two primary tools for editing the Registry: the Windows NT Registry Editor (regedt32.exe), and the Windows 95 Registry Editor (regedit.exe). Additionally, we can use the Windows NT System Policy Editor (poledit.exe) to modify a limited number of settings in the Registry. However, we can't use System Policy Editor to search the Registry.

Remote Access Administration An administrative tool that is primarily used to start and stop the Remote Access Service (RAS), to assign the dial–in permission to users, and to configure a call back security level for each user. Remote Access Administration can also be used to view COM port status and statistics, to disconnect users from individual ports, and to remotely manage RAS on other Windows NT computers.

Remote Access Service A service that enables dial–up network connections between a RAS server and a Dial–Up Networking client computer. RAS includes software components for both the RAS server and the Dial–Up Networking client in a single service. RAS enables users of remote computers to use the network as though they were directly connected to it. Once the dial–up connection is established, there is no difference in network functionality, except that the speed of the link is often much slower than a direct connection to the LAN.

Remote System Any other computer on the Internet or on a network to which we connect. Interactions between computers are often described using the terms "local" and "remote" systems. The local system is our computer and the remote system is the other computer.

Repeater An amplifying device used at intervals along a communications line to boost a signal so it won't be distorted by weakening. In an analog circuit, any distortion of the signal is amplified along with the signal.

Request For Comments The name of the result and the process for creating a standard on the Internet. New standards are proposed and published on line, as a Request For Comments. The Internet Engineering Task Force is a consensus–building body that facilitates discussion, and eventually a new standard is established, but the reference number/name for the standard retains the acronym RFC, e.g. the official standard for e–mail is RFC 822.

Resistance Opposition to current flow. Resistance only affects the transmission of direct current (DC), and it is measured in ohms. When more resistance is met, more electricity is lost during transmission. The resistance causes the energy to be converted to heat. Cables with small diameters have more resistance than cables with large diameters.

Resolution In general, this refers to how sharp and clear an image looks on screen or on paper, and how much detail we can see. It is usually determined by the number of dots (or pixels) per square inch (the more there are, the higher the resolution) and is used to describe printers, monitors, and scanners.

Resources Anything available to a client on a network is considered a resource. Printers, data, fax devices, other networked devices and information are resources.

Reverse Lookup A telephone or network directory service where, given the phone number or IP address, we can look up the corresponding name.

RFC See Request For Comments

RGB Red, Green, Blue. These are the primary colours as perceived by the human eye. RGB is the basis for a colour naming and picking scheme where each of these primary colours can have a quantity from 1 to 255. e.g. (0,0,0) = black and (255,255,255)=white.

Rich Text Format A file format for text files that includes formatting instructions. Also called Interchange Format. Files in the Rich Text Format have the .RTF file extension.

Ring Topology A design schematic for a ring communications network in which the messages flow in one direction from a source on the loop to a destination on the loop. Computers in between act as relay stations, but can be bypassed if one fails. Ring Topologies use the Token Passing method of network bandwidth management.

RIP See Routing Information Protocol

RISC See Reduced Instruction Set Computing

RJ–11 A type of modular jack commonly associated with telephones. It connects one to two pairs of wires with a transparent connector that plugs into our phone on one end and a wall jack on the other. We most likely have an RJ–11 jack plugged into our modem.

RJ–45 A type of modular jack that can connect up to four pairs of wires. It resembles the RJ–11 telephone jack, but is a bit larger. It is commonly used to connect twisted pair cable on a LAN.

ROFL An abbreviation for 'Rolling On the Floor Laughing' commonly used in chat rooms.

ROM See Read–Only Memory

Routable Refers to the ability of data or more specifically a protocol that can deliver information between destinations located on either side of one or more routing devices.

Router A network device that uses protocol–specific addressing information to forward packets from a source computer on one network segment across one or more routers to a destination computer on another network segment.

Routing The process of forwarding packets from a source computer on one network segment across one or more routers to a destination computer on another network segment by using protocol–specific addressing information. Devices that perform routing are called routers.

Routing Information Protocol The software that enables routers to dynamically update their routing tables.There are two versions of RIP: RIP for Internet Protocol, and RIP for NWLink IPX/SPX Compatible Transport.

RTF See Rich Text Format

rtfm An abbreviation for 'Read The F@#%ing Manual' commonly used in chat rooms.

Sampling The process of converting analog data into digital data by taking a series of samples or readings at equal time intervals.

Scanner A device that converts images (such as photographs) into digital form so that they can be stored and manipulated on computers.

Schema In computing, the organization of a relational database in its entirety, including names of all data elements and ways records are linked. In psychology, the way in which a human processes, stores and "recreates" information coming into the brain.

Screen Saver A moving picture or pattern that is displayed on the screen when no activity takes place for a specified period of time. Screen savers are so named as they were first designed to prevent static images on a monitor from etching themselves onto the screen surface. As new technologies developed to prevent this from happening, screen savers are no longer required for this purpose but are still used for their entertainment benefit and also as security while a user is away from his computer. This is achieved by requiring a password to disable the screen saver.

Scripts A type of program that consists of a set of instructions for another application or utility to carry out. A batch file is in the form of a script.

Scroll Bar The bar that appears at the right side or the bottom of a window that contains more information that can be displayed. The scroll bar is used to scroll an object or parts of a document into view when the entire object or document does not fit in the window.

SCSI See Small Computer System Interface

Search Engines A type of software that creates indexes of databases or Internet sites based on the titles of files, key words, or the full text of files. This enables files to be located by the search engine based on our search criteria. The search engines list their findings in the form or results pages.

Secure Sockets Layer A protocol designed by Netscape Communications to enable encrypted, authenticated communications across the Internet. SSL used mostly (but not exclusively) in communications between web browsers and web servers. URL's that begin with "https" indicate that an SSL connection will be used. SSL provides 3 important things: Privacy, Authentication, and Message Integrity. In an SSL connection each side of the connection must have a Security Certificate, which each side's software sends to the other. Each side then encrypts what it sends using information from both its own and the other side's Certificate, ensuring that only the intended recipient can decrypt it, and that the other side can be sure the data came from the place it claims to have come from, and that the message has not been tampered with.

Security Certificate Information (often stored as a text file) that is used by the SSL protocol to establish a secure connection. Security Certificates contain information about who it belongs to, who it was issued by, a unique serial number or other unique identification, valid dates, and an encrypted "fingerprint" that can be used to verify the contents of the certificate.In order for an SSL connection to be created both sides must have a valid Security Certificate.

Segment In network terminology, a segment refers to a network subnet that is not subdivided by a

bridge or a router. The term segment can also be used as a verb, describing the process of dividing the network into multiple subnets by using a bridge or a router.

Sequential Read A read performed (normally by the operating system) from the beginning of a file straight through to the end of the file. No random access to different parts of the file can occur during a sequential read.

Serial Cable A cable used to connect peripheral devices through a computer's serial ports. A serial cable is made up of 9 wires which can transmit information simultaneously. Its most common uses are connecting modems, mice, and connecting to other computers for data transfer. Although serial cabling only uses 9 wires, there are two types of serial connectors, 9–pin and 25–pin.

Serial Line Internet Protocol An older industry standard connection protocol developed in 1984 to support TCP/IP networking over low–speed serial interfaces in Berkeley UNIX. SLIP connections don't support NWLink IPX/SPX Compatible Transport or NetBEUI. Dynamic IP addressing is not supported. Additionally, password encryption is not supported by SLIP. A script file is usually required to automate the connection process when SLIP is used.

Serial Port A male 9–pin or 25–pin connector situated at the back of computers that enables the connection of peripheral devices and other computers via a serial cable.

Server A powerful computer on a network that provides services and resources to other computers on the network. Many computers are configured as both clients and servers, meaning that they can both access resources located on other computers across–the–network, and they can share their resources with other computers on the network. These computers are known as peers and are not to be confused with dedicated servers.

Server–Based Networking In this system, clients do not act as servers. They use a larger, central network server for their storage and/or processing. Security is easier to maintain, so server–based networks can grow large.

Server Dependencies Services and drivers that must be running before a particular service (or driver) can start.

Service A process that performs a specific function on a server or workstation and can be called by various other programs. Operating Systems provide tools to monitor and administer services.

Service Engineer A technician who maintains and repairs computers and associated peripherals.

Session Layer The fifth layer of the OSI model. This layer lets users establish connections called sessions between devices. Once a connection has been established, the Session layer manages the dialogue.

Share Name A name that uniquely identifies a shared resource on a computer, such as a shared folder or printer.

Share Permissions Control access to shared resources, such as shared folders and shared printers

on a computer. Share permissions only apply to users who access a shared resource over the network.

Shared Folder is a folder on a computer that can be accessed by other computers on the network because the folder has been configured to be shared and has been assigned a share name.

Shared Memory Address An option to I/O address allocation for internal hardware devices in computers. Shared Memory Addresses allow a hardware device and its associated software driver to use a shared RAM address in the high memory range to communicate.

Shareware Software that we can try before we buy. It's distributed through on–line services, BBSs, and user groups. We're allowed to try it out and give copies to others, but if we want to keep using it, we must pay the registration fee.

Simple Mail Transfer Protocol The main protocol used to send electronic mail on the Internet. SMTP consists of a set of rules for how a program sending mail and a program receiving mail should interact. Almost all Internet email is sent by clients and servers using SMTP.

Simple Network Management Protocol A set of standards for communication with devices connected to a TCP/IP network. Examples of these devices include routers, hubs, and switches. A device is said to be "SNMP compatible" if it can be monitored and/or controlled using SNMP messages. SNMP messages are known as "PDU's" – Protocol Data Units. Devices that are SNMP compatible contain SNMP "agent" software to receive, send, and act upon SNMP messages. Software for managing devices via SNMP are available for every kind of commonly used computer and are often bundled along with the device they are designed to manage. Some SNMP software is designed to handle a wide variety of devices.

Simplex A communication system, circuit or device capable of transmission in one direction only.

Site Organization or facility where a host is located.

Site–license The document proving that a renewable fee a location must pay a vendor, to use a fixed number of copies of copyrighted software at that location has been paid.

Sliding Window A connection–oriented method of data transfer. Sliding Window allows the two communicating devices to negotiate the number of allowable outstanding frames. Using this method, the receiving device does not need to acknowledge each frame it receives and then wait for the next; it can send one acknowledgment for a group of frames.

SLIP See Serial Line Internet Protocol

Small Computer System Interface A hardware specification for cables, adapter cards, and the devices that they manage, such as: hard disks, CD–ROMs, and scanners.

SMDS See Switched Multi megabit Data Service

SMTP See Simple Mail Transfer Protocol

Sneakernets The predecessor to the computer network. Before networking was invented, the only

way to share data between computers was to copy it onto floppy disks and carry it to the other computer.

SNMP See Simple Network Management Protocol

Sockets The logical addresses of communications access points to specific devices or programs on a host computer.

Software Programs that are loaded onto computers to perform specific tasks. Software is useless on its own as it requires a Hardware platform in order to perform its programmed tasks.

Spam (or Spamming) An inappropriate attempt to use a mailing list, or USENET or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who didn't ask for it. The term probably comes from a famous Monty Python skit which featured the word spam repeated over and over. The term may also have come from someone's low opinion of the food product with the same name, which is generally perceived as a generic content–free waste of resources. (Spam is a registered trademark of Hormel Corporation, for its processed meat product.) E.g. Mary spammed 50 USENET groups by posting the same message to each one.

Specialized Servers These are servers that have a single specialized purpose like mail servers and communications servers.

Spider A software robot that serves a search engine by exploring the net, collecting web page addresses and page contents, and following links from them to other addresses to collect still more web information. Also known as a worm or crawler.

Spreadsheet A number–related document whereby calculations and formulas are applied to the data organized in rows and columns of cells.

SQL 1. See Structured Query Language 2. Microsoft's® industrial strength database server package heavily utilized on the internet.

SSL See Secure Sockets Layer

Stand–Alone Server A server computer that is not installed as a domain controller, and that has not joined a server domain.

Star Topology A network configuration in which all computers and devices are connected by direct cables to a central hub creating the logical appearance of a star.

Static Routing A basic, no–frills IP routing. No additional software is necessary to implement static routing in multihomed computers. Static routers are not capable of automatically building a routing table. In a static routing environment, administrators must manually configure the routing table on each individual router. If the network layout changes, the network administrator must manually update the routing tables to reflect the changes.

Stop and Wait A connection–oriented method of data transfer. A green light way of handling

flow control. When the receiving device has no memory left to store incoming data, it suspends transmission. When memory is free again, it sends a signal to the transmitting device to resume.

Store and Forward See Message Switching

Stripe Set A disk configuration consisting of two to thirty two hard disks. In a stripe set, data is stored, a block at a time, evenly and sequentially among all of the disks in the set. Stripe sets are sometimes referred to as disk striping. Disk striping alludes to the process wherein a file is written, or striped, one block at a time, first to one disk, then to the next disk, and then to the next disk, and so on, until all of the data has been evenly distributed among all of the disks.

Stripe Set with Parity Similar to a stripe set, but a stripe set with parity provides a degree of fault tolerance that a stripe set cannot. In a stripe set with parity, data is not only distributed a block at a time, evenly and sequentially among all of the disks in the set, but parity information is also written across all of the disks in the set. A stripe set with parity is made up of three to thirty two hard disks. Like stripe sets, stripe sets with parity are created from identical amounts of free space on each disk that belongs to the set.

Structured Query Language A specialized programming language for sending queries to databases. Most industrial–strength and many smaller database applications can be addressed using SQL. Each specific application will have its own version of SQL implementing features unique to that application, but all SQL–capable databases support a common subset of SQL.

Style Sheet See CSS

Stylus An input device consisting of a light–sensitive photoelectric cell that, when touched to a video display screen, is used to signal the screen position to a computer.

Subfolder A subfolder is a folder that is located within another folder. Subfolders can contain other subfolders, as well as files.

Subnet Mask Specifies which portion of an IP address represents the network ID and which portion represents the host ID. A subnet mask enables TCP/IP to correctly determine whether network traffic destined for a given IP address should be transmitted on the local subnet, or whether it should be routed to a remote subnet. A subnet mask should be the same for all computers and other network devices on a given network segment. A subnet mask is a 32–bit binary number, broken into four 8–bit sections (octets), that is normally represented in a dotted decimal format. Each 8–bit section is represented by a whole number between 0 and 255. A common subnet mask is 255.255.255.0. This particular subnet mask specifies that TCP/IP will use the first three octets of an IP address as the network ID, and use the last octet as the host ID.

Switched Multi megabit Data Service A new standard for very high–speed data transfer.

Synchronous A transmission method in which the synchronizing of characters and bits is controlled by fixed timing signals generated at the sending and receiving stations. Both stations operate continuously and are maintained in a desired phase relationship. Any of several data codes may be used for transmission, so long as the codes utilizes the required line control characters.

Usually used in high speed circuits because there is less overhead than for asynchronous transmission.

Syntax Error Occurs when a user (or programmer) has put words in an order that a program does not understand.

Sysop See System Operator

System Operator Anyone responsible for the physical operations of a computer system or network resource. A System Administrator decides how often backups and maintenance should be performed and the System Operator performs those tasks.

System Partition is the active primary partition on the first hard disk in the computer. (This is usually the C: drive).

System Policy The system policy file is a collection of user, group, and computer policies. System policy restricts the user's ability to perform certain tasks on any computer on the network that the user logs on to. System policy can also be used to enforce certain mandatory display settings, such as wallpaper and color scheme. We can also create a system policy file that applies to users of Windows 95 computers. System policy gives the administrator far more configurable options than a mandatory profile. Administrators can use system policy to provide a consistent environment for a large number of users, or to enforce a specified work environment for "problem users" who demand a significant amount of administrator time.

System Policy Editor A tool that is used to edit system policy files.

Switching A method in which data is directed across a network between end systems. There are different types of switching techniques which take advantage of routers an bridges to create a virtual or physical connection between the end systems.

T–1 A leased–line connection capable of carrying data at 1,544,000 bits per second. At maximum theoretical capacity, a T–1 line could move a megabyte in less than 10 seconds. That is still not fast enough for full–screen, full–motion video, for which we need at least 10,000,000 bits per second. T–1 is the fastest speed commonly used to connect networks to the Internet.

T–3 See DS–3

Tags Formatting codes used in HTML documents. These tags indicate how the parts of a document will appear when displayed by a Web client program.

Task Manager An administrative utility that can be used to start and stop applications; to view performance statistics, such as memory and CPU usage; and to change a process's base priority.

Taskbar An bar that runs across the bottom (usually) of the Windows 95, 98, 2000, NT, Me, or XP desktops. Running applications are represented as buttons on the taskbar, the current window is shown as a depressed button, all other applications are displayed as raised buttons.

TB See Terabyte

TCP See Transmission Control Protocol

TCP/IP See Transmission Control Protocol/Internet Protocol

TechNet An invaluable knowledge base and troubleshooting resource. TechNet is published monthly by Microsoft® on multiple compact discs. TechNet includes a complete set of all Microsoft operating system Resource Kits (currently in a help file format), the entire Microsoft Knowledge Base, and supplemental compact discs full of patches, fixes, and drivers (so we don't have to spend time downloading them).

Telecommute To work at home or some other location remote from one's place of employment, making use of a computer, telephone, fax, and/or modem to receive job assignments and send in completed work.

Teleconference Simultaneous visual and/or sound interconnection that allows individuals in two or more locations to see and talk to one another in a long distance conference arrangement.

Telephone Bridge A computerized switching system which allows multi–site telephone conferencing.

Teletext A system which allows for the transmission of data via the vertical blanking interval of a television signal. The unused lines viewed as the horizontal black lines between the video. These lines are also used by networks and broadcasters to send closed–captioned programs for the hearing–impaired and test data simultaneously with the program being viewed. Digital data fed into a decoder built–in to the TV set is stored in buffer memory. When a user keys in the number of a particular page, the page is transferred to the screen and remains until a new page is requested. The advantage of teletext is that it gets essentially a "free ride" on the broadcast signal. The disadvantage is the small number of frames or pages that can be stored (100–200 pages). Also, the system is one–way, not providing two–way interactivity that fiber optics would allow.

Telnet The command and program used to login from one Internet site to another. The telnet command/program gets us to the login: prompt of another host.

Terabyte 1,024 gigabytes, or 1,099,511,627,776 bytes.

Terminal A device that allows us to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually we will use terminal software in a personal computer – the software pretends to be (emulates) a physical terminal and allows us to type commands to a computer somewhere else.

Terminal Server A special purpose computer that has places to plug in many modems on one side, and a connection to a LAN or host machine on the other side. Thus the terminal server does the work of answering the calls and passes the connections on to the appropriate node. Most terminal servers can provide PPP or SLIP services if connected to the Internet.

Terminate Stay Resident Refers to "blind" programs or portions of programs that are not visible to the user but perform either hidden tasks or monitor for an event that they will react to. On any

Microsoft® computer, we can press Ctrl+Alt+Del to see a list of the Terminate Stay Resident Programs on that machine.

TFTP See Trivial File Transfer Protocol

Thick Ethernet See 10Base5

Thick Net See 10Base5

Thin Ethernet See 10Base2

Thin Net See 10Base2

Thread The smallest unit of processing that can be scheduled by a schedule service. All applications require at least one thread.

Threshold The point at which an action begins or changes.

Title Bar The horizontal bar at the top of a window. The title bar shows the name of the window.

Token Passing A system where a small data frame is passed from device to device across a network in a predetermined order. The device that has control of the token frame has the ability to transmit data across the network. Even on large networks where contention would start to break down due to increased levels of collisions, token passing maintains an orderly network.

Token Ring One of several technologies used to allow computers on a LAN to communicate. Token Ring networks use token passing to communicate between computers.

Toolbar A collection of buttons that typically make the more common tools for an application easily accessible.

Touch Screen A system of data input where a user responds to software by touching the screen at the location that corresponds with his choice. This system is highly utilized in the retail industry.

Transmission Control Protocol A reliable, connection–oriented delivery service. Data is transmitted in segments. Connection–oriented means that a session must be established before hosts can transmit data. TCP uses byte–stream communications, which means that data is treated as a sequence of bytes with no boundaries.

Transmission Control Protocol/Internet Protocol A widely used transport protocol that provides robust capabilities for networking. TCP/IP is a fast, routable enterprise protocol. TCP/IP is the protocol used on the Internet. TCP/IP is supported by many other operating systems, including: Windows 95, Macintosh, UNIX, MS–DOS, and IBM mainframes. TCP/IP is typically the recommended protocol for large, heterogeneous networks.

Transponder Equipment on a satellite that accepts the signal sent from earth and after amplifying and changing the frequency, sends it back to earth for reception.

Transport Layer The Transport layer is the fourth layer of the OSI model. It provides a transport service between the Session layer and the Network layer. This service takes information from the

Session layer and splits it up if necessary. It then passes this information to the Network layer and checks to make sure the information arrives at the destination device successfully.

Trivial File Transfer Protocol A protocol that provides bi–directional file transfers between two TCP/IP hosts, where one is running TFTP server software and the other is running TFTP client software.

Trust Relationship An agreement between two domains that enables authenticated users in one domain to access resources in another domain. A trust relationship enables users from the trusted domain to access resources in the trusting domain.

Trusted Domain The domain that contains the user accounts of users who want to access resources in the trusting domain. The trusted domain is said to be trusted by the trusting domain. When graphically displaying a trust relationship, an arrow is used to point from the trusting domain to the trusted domain.

Trusting Domain The domain that has resources to share with users from the trusted domain. The trusting domain is said to trust the trusted domain. When graphically displaying a trust relationship, an arrow is used to point from the trusting domain to the trusted domain.

TSR See Terminate Stay Resident

Twisted Pair A pair of insulated wires that twist around each other repeatedly in a spiral pattern along the length of the wires. Twisting them rather than running them side by side reduces electromagnetic interference. Ordinary telephone cable in the house usually consists of two or three twisted pairs, with each wire coded in a different color insulation. Twisted pairs surrounded by a shielding ground layer are known as shielded twisted pair. Twisted pair is often used in Ethernet LANs.

Two–Way Trust Consists of two one–way trusts between two domains.

UDP See User Datagram Protocol

Unacknowledged Connectionless Service The fastest means of transferring data at the LLC sublayer of the Data Link Layer of the OSI Model. Although it is the most unreliable way to handle data transfers, it is commonly used as most upper layer protocols of the OSI Model handle their own error checking.

Unbounded Media Refers to transmissions that do not need a physical connection to travel from source to destination. Also known as wireless media.

UNC See Universal Naming Convention

UNICOS UNIX Cray Operating System. A version of the UNIX operating system adapted for CRAY computers.

Uniform Resource Identifier A string of characters that represents the location or address of a resource on the Internet and how that resource should be accessed. A URI is a superset of the

Uniform Resource Locator.

Uniform Resource Locator The standard way to give the address of any resource on the Internet that is part of the World Wide Web (WWW). The most common way to use a URL is to enter into a WWW browser program, such as Internet Explorer, or Netscape.

Uninterruptible Power Supply A fault–tolerance device that enables a computer to continue operations for a short period of time during a power outage. If the UPS battery runs low before power is resumed, the system is shut down safely without data damage or loss.

Universal Naming Convention An accepted method of identifying individual computers and their resources on the network. A UNC name consists of a server name and a shared resource name in the following format: \\Server_name\Share_name. Server_name represents the name of the server that the shared folder is located on. Share_name represents the name of the shared folder. A UNC name in this format can be used to connect to a network share. For example, a shared folder named Public located on a server named Server1 would have the following UNC name: \\Server1\Public.

Universal Serial Bus A new standard of serial bus architecture in PCs that allows the connection of multiple external devices to a single port using a daisy chain format. USB was designed to eventually phase out the existing Communication Port standard serial bus.

UNIX A computer operating system (the basic software running on a computer, underneath things like word processors and spreadsheets). UNIX is designed to be used by many people at the same time (it is multi–user) and has TCP/IP built–in. It is the most common operating system for servers on the Internet.

Unix to Unix Encoding A method for converting files from Binary to ASCII (text) so that they can be sent across the Internet via e–mail.

Unshielded Twisted Pair Network cable made up of multiple pairs of smaller cables that are twisted around each other. The twisted pairs have one wire that sends information and one that receives. This architecture dramatically reduces electric interference thus removing the need for further electric shielding.

Uplink A satellite antenna (earth station) which has the ability to transmit signals to a satellite. Uplink earth stations can also receive signals from a satellite in the same manner as downlink antennas. The vast majority of satellite earth stations do not have uplink capabilities, largely due to the significant expense associated with the capability.

Upload To send a file to another computer using a modem.

UPS See Uninterruptible Power Supply

URI See Uniform Resource Identifier

URL See Uniform Resource Locator

USB See Universal Serial Bus

USENET A world–wide system of discussion groups, with comments passed among hundreds of thousands of machines. Not all USENET machines are on the Internet, maybe half. USENET is completely decentralized, with over 10,000 discussion areas, called newsgroups.

User Any person that uses a client to access resources on a network.

User Account A record in the Security Accounts Manager (SAM) database that contains unique user information, such as user name, password, and logon restrictions.

User Datagram Protocol One of the protocols for data transfer that is part of the TCP/IP suite of protocols. UDP is a "stateless" protocol in that UDP makes no provision for acknowledgment of packets received.

User Id The name assigned to a user account.

User Name The name assigned to a user account.

User Policy A collection of Registry settings that restricts a user's program and network options, and/or enforces a specified configuration of the user's work environment.

User Profile A series of Registry settings and folders in the user's profile folder that define a user's work environment. The contents of a user profile include user–specific settings for: Windows NT Explorer, Notepad, Paint, HyperTerminal, Clock, Calculator, and other built–in Windows applications; screen saver, background color, background pattern, wallpaper, and other display settings; applications written to run on Windows; network drive and printer connections; and the Start menu, including program groups, applications, and recently accessed documents.

User Rights Authorize users and/or groups to perform specific tasks on a computer. User rights are not the same as permissions. User rights enable users to perform tasks; whereas permissions enable users to access objects, such as files, folders, and printers. See also permissions.

UTP See Unshielded Twisted Pair

UUCP UNIX–to–UNIX Copy Program, a program that lets us copy files between UNIX systems.

UUCP protocols are used to transfer news and Email messages through USENET.

UUENCODE See Unix to Unix Encoding

Value An individual entry in the Registry or in a program. A value cannot contain keys or other values.

VDT See Video Display Terminal

VDU See Video Display Unit

Verbose Mode Refers to running an application in such a way that the application returns the maximum amount of information and detail to the user. The verbose mode is initiated on many

applications by using the /V switch.

Veronica (Very Easy Rodent Oriented Net–wide Index to Computerized Archives) Developed at the University of Nevada, Veronica is a constantly updated database of the names of almost every menu item on thousands of gopher servers. The Veronica database can be searched from most major gopher menus.

VESA See Video Electronic Standards Association

Video Compression A coding technique used to reduce the bandwidth required for the transmission of video images by reducing redundant information within or between video frames; also called bandwidth compression, data compression or bit rate reduction.

Video Conferencing Two–way electronic voice and video communication between two or more groups or three or more individuals, who are in separate locations; may be fully interactive voice and video.

Video Display Terminal A TV like screen on which text and/or graphics can be displayed and controlled via a keyboard or a "mouse." A VDT can have a monochromatic or a colour screen.

Video Display Unit See Video Display Terminal

Video Electronic Standards Association A computer bus architecture designed as a cheaper alternative than EISA to enhance the existing ISA bus. Originally designed for video cards, it was later used for hard drive controllers and network cards. The VESA Local Bus, or VLB, could transfer 32 bits of information at a time, and ran at speeds of up to 40 MHz, depending on the system's CPU speed.

Videodisc See Laserdisc

Virtual Circuit A connection oriented method of packet switching similar to dedicated circuit switching, except the connections are virtual. This way, more than one communication can go over physical media at a time.

Virtual Device Driver is a 32–bit protected mode device driver that is used in Windows 95 and Windows for Workgroups.

Virtual Memory The physical space on a hard disk that an operating system treats as though it were RAM.

Virtual Memory Manager A kernel mode component that manages memory in an operating system environment by using demand paging.

Virtual Private Network Usually refers to a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted, so the entire network is "virtually" private. A typical example would be a company network where there are two offices in different cities. Using the Internet the two offices merge their networks into one network, but encrypt traffic that uses the Internet link.

Virtual Reality Computer simulations that use 3D graphics and devices such as the VR Head Set to allow the user to interact with the simulation.

Virtual Reality Modeling Language The specification for the design and implementation of an operating system independent programming language for the creation of environments and worlds used in virtual reality.

Virus A malicious program that searches out other programs and "infects" them by embedding a copy of itself into them. When these programs are executed, the embedded virus is executed too, thus spreading the virus. This normally happens invisibly to the user. Virii can be programmed to do anything from displaying a message on a given date to irreparably destroying all data on the computer. Today virii are becoming more and more dangerous and hard to treat as they are now aimed at the firmware BIOS' of hardware rendering computers unbootable.

VMS Digital Equipment Corporation's proprietary operating system which runs on the VAX series of computers.

VOD Video On Demand

Volume A logical drive.

Volume Set A combination of two to thirty–two partitions that are formatted as a single logical drive. A volume set does not use disk striping to store data on its partitions.

VPN See Virtual Private Network

VR See Virtual Reality

VRAM Video RAM. A type of memory dedicated to handling the image displayed on a monitor.

VRML See Virtual Reality Modeling Language

Wait State A delay of one or more clock cycles added to a processor's instruction execution time to allow it to communicate with slow external devices. The number and duration of wait states may be pre–configured or they may be controlled dynamically via certain control lines.

WAIS See Wide Area Information Servers

Wallpaper A graphical pattern displayed behind the desktop.

WAN See Wide Area Network

WAP See Wireless Application Protocol

Warm Boot To restart an operating system on a computer without actually turning the power off and back on.

Web See WWW
Web Browser Also known as a Web client program, this software allows us to access and view HTML documents. Internet Explorer, Netscape and Mosaic are examples of Web browsers.

Web Page A document created with HTML that is part of a group of hypertext documents or resources available on the World Wide Web.

Web Surfing Using a Web client program to move through the documents available on the World Wide Web.

Webmaster A person or group of people who maintain and administer a web server or site. Webmaster also refers to a standard E–mail address at most web hosts where comments and questions can be sent.

Wide Area Information Servers A commercial software package that allows the indexing of huge quantities of information, and then making those indices searchable across networks such as the Internet. A prominent feature of WAIS is that the search results are ranked (scored) according to how relevant the hits are, and that subsequent searches can find more stuff like that last batch and thus refine the search process.

Wide Area Network Any internet or network that covers an area larger than a single building or campus.

Wildcard A character (usually * or ?) that can stand for one or more unknown characters during a search.

Windows 32–bit desktop operating systems. These operating system require the least amount of hardware of all of the Microsoft® Windows operating systems.

Windows Internet Name Service A service that provides NetBIOS name resolution services to client computers. A Windows NT Server computer that has WINS installed on it is called a WINS server.

WINS See Windows Internet Name Service

Wireless Application Protocol A protocol used with small hand–held devices and utilizing small file sizes. WAP is the current buzz word as Nokia has released a phone capable of browsing WAP pages.

Wizard A utility within an application that helps us use the application to perform a particular task. For example, a "letter wizard" within a word processing application would lead us through the steps of producing letters with different types of layouts and styles.

Word Processor A program used to create and print documents that might otherwise be prepared on a typewriter. The key advantage of word processor is its ability to make changes easily, such as correcting spelling, changing margins, or adding, deleting, and relocating entire blocks of text. Once created, the document can be printed quickly and accurately and saved for later modifications.

Word Wrap A feature of word processors and most text editors where a word which would extend past the right hand margin is moved to the following line. This is more sophisticated than character wrap which only moves to the next line for the first character past the right margin and

thus will break some words in the middle. The program may actually insert a new line in the text at the point where it is wrapped or it may only display it as though it contained a new line at that point.

Workgroup is a logical grouping of networked computers in which one or more of the computers has shared resources, such as a shared folder or a shared printer. In a workgroup environment, the security and user accounts are maintained individually on each separate computer.
Workstation Any computer that is attached to a network is also known as a workstation.

World Wide Web Frequently used (incorrectly) when referring to "The Internet", WWW has two major meanings: (1) loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, Telnet, USENET, WAIS and some other tools. (2) the universe of hypertext servers (HTTP servers) which are the servers that allow text, graphics, sound files, etc. to be mixed together.

WORM (Write–Once Read–Many) Any type of storage medium to which data can be written to only a single time, but can be read from any number of times. Typically this is an optical disk whose surface is permanently etched using a laser in order to record information. WORM media types have a significantly longer shelf life than magnetic media and thus they are used when data must be preserved for a long time.

Write–Back A cache architecture in which data is only written to main memory when it is forced out of the cache.

Write–Through A cache architecture in which data is written to main memory at the same time as it is cached.

WTF (Who / What / Why The F***) An abbreviation widely used in online chat rooms to save the fingers.

WTH (Who / What / Why The Hell) An abbreviation widely used in online chat rooms to save the fingers.

WWW See World Wide Web

WYSIWYG (What You See Is What You Get) What we see on the screen will be pretty close to what we see in the finished product.

X.25 A data communications interface specification developed to describe how data passes into and out of public data communications networks. The CCITT and ISO approved protocol suite defines protocol layers 1 through 3.

X.500 A directory access protocol to enable a common standard for directories of information over a network. It never caught on as well as its designers intended. See LDAP.

XHTML eXtensible HyperText Markup Language. HTML re–written as an application of the XML language.

XML eXtensible Markup Language. A richer markup language than HTML. It is the next step in the evolution of web data formats beyond HTML.

Xmodem An early form of file transmission for dialup and telnet connections. It is slower and uses smaller blocks of data (128 bits) than Ymodem and Zmodem.
XSL eXtensible Stylesheet Language. A style sheet companion to XML.

Ymodem A common form of file transmission for dialup and telnet connections, which uses 1K blocks of data. It has two forms; single file mode and batch mode. The single file form is sometimes called 1K Xmodem, and the batch mode is sometimes called Ymodem batch. Usage is not consistent. Zmodem is newer and more reliable.

Yotabyte 1,024 zetabytes, or 1,208,925,819,614,629,174,706,176 bytes.

ZB See Zetabyte

Zetabyte 1,024 exabytes, or 1,180,591,620,717,411,303,424 bytes.

ZIF Socket (Zero Insertion Force Socket) A kind of socket for integrated circuits. A ZIF socket can be opened and closed by means of a lever or screw. When open, there the chip may be placed in the socket without any pressure at all, the socket is then closed, causing its contacts to grip the pins of the chip. Such sockets are used where chips must be inserted and removed frequently, such as in test equipment. They are more expensive and usually take up more space than conventional IC sockets.

Zip To create a compressed archive (a "zip file") from one or more files using Winzip or a compatible archiver. Its use is spreading from MS–DOS now that portable implementations of the algorithm have been written.

Zip Drive A disk drive from Iomega Corporation which takes removable 100 megabyte hard disks. Both internal and external drives are manufactured, making the drive suitable for backup, mass storage or for moving files between computers. Software is included to help with file organization. The internal SCSI model offers up to 60 MB / minute transfer rate.

Zip File See Zip

Zmodem A very common form of file transmission, which can be used across dialup and telnet connections. It can be used in batch modes (for multiple files), and it is faster than the older Xmodem and Ymodem. In some implementations, it can resume a transfer after a connection has been broken and re–established.

Zoom To show a smaller area of an image at a higher magnification (zoom in) or a larger area at a lower magnification (zoom out), similar to using a zoom lens on a camera.

References and Suggestions for Further Study

A. Internet Sources

1. *The Simple Times,* http://www.simple-times.org

2. *Cisco Systems,* http://www.cisco.com

3. *Juniper Networks,* http://www.juniper.net

4. *Nortel Networks,* http://www.nortel.com

5. *Netgear,* http://www.netgear.com

B. Texts and Handbooks

1. *Network Management*, ISBN 978-0–201–35742–4

2. *Cisco, A Beginner's Guide, ISBN 978-0-072133-39-4*

Index

D

N

S

X

Y

Z

NETWORKS
Design and Management
Second Edition

Students and working professionals will find NETWORKS - Design and Management Second Edition, to be a concise and easy-to-learn text. It provides complete, clear, and detailed information of the latest state-of-the-art networking devices, the characteristics of different types of Local Area Networks, and network management.

This text includes the following chapters and appendices:

• Basic Networking Concepts • The OSI Model and IEEE Standards • Protocols, Services, and Interfaces • Network Designs and Ethernet Networking • Buses, Network Adapters, and LAN Connection Devices • Wired and Wireless Media • Network Design and Administration • Introduction to Simple Network Management Protocol (SNMP) • Introduction to Remote Monitoring (RMON) • Optimization of Cable Connections • Binary Information and Standard Codes • Common Number Systems and Conversions • RSA Encryption • Glossary of Computer / Internet Related Terms

Each chapter contains several true/false, multiple-choice, and a few problems to reinforce the readers's knowledge on this subject.

Steven T. Karris is the founder and president of Orchard Publications. His undergraduate and graduate degrees in electrical engineering are from Christian Brothers University, Memphis, Tennessee, and Florida Institute of Technology, Melbourne, Florida. He is a registered professional engineer in California and Florida. He has over 35 years of professional engineering experience in industry. In addition, he has over 30 years of teaching experience that he acquired at several educational institutions as an adjunct professor, the most recent with UC Berkeley, California.

Orchard Publications

Visit us on the Internet
www.orchardpublications.com
or email us: info@orchardpublications.com

ISBN-13: 978-1-934404-16-4

ISBN-10: 1-934404-16-0

$70.00 U.S.A.