

COMPARISON OF COMPUTER COMMUNICATION TECHNIQUES

109624

by

Pınar TÜFEKÇİ

T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ

109624

October, 2001

İZMİR

COMPARISON OF COMPUTER COMMUNICATION TECHNIQUES

**A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of
Dokuz Eylül University
In Partial Fulfillment of the Requirements for
the Degree of Master of Science in Electrical and Electronics Engineering**

**by
Pınar TÜFEKÇİ**

**October, 2001
İZMİR**


M.Sc. THESIS EXAMINATION RESULT FORM

We certify that we have read the thesis, entitled “**COMPARISON OF COMPUTER COMMUNICATION TECHNIQUES**” completed by **PINAR TÜFEKÇİ** under supervision of **Assist.Prof. Dr. ZAFER DİCLE** and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.



Assist.Prof. Dr. Z. Dicle

Supervisor



Assoc.Prof. Dr. Y. Çebi

Committee Member



Prof. Dr. M. Gündüzalp

Committee Member

Approved by the
Graduate School of Natural and Applied Sciences



Prof.Dr.Cahit Helvacı

Director

ACKNOWLEDGMENTS

I would like to express my gratitude and endless appreciation to my supervisor Ass. Prof. Dr. Zafer Dicle for his continued academic and moral support. I especially would like to thank to Ass. Prof. Dr. Zafer Dicle for giving me many chances for completing my thesis.

I would, also, like to thank my family and husband who support me.



Pınar TÜFEKÇİ

ABSTRACT

One of the today's advantage almost in every kind of business is computer networking. If we ask why today, because computer networking will not really be a competitive advantage in the future: it will be a necessity. The ability to link computers and data has created new business opportunities especially in projects where large amounts of data must be processed.

In this project, the process of establishing a physical connection between the machines on the network and installing the drivers and services necessary to enable network communication was examined. In order to use networks we need a set of rules which all of the networks's member agree on, that is a protocol. The purpose of a network is to exchange information among computers and protocols are the rules by which computers communicate. The computing community has settled on several standards and specifications that define the various components of network architecture. Computers can communicate through cables, light and radio waves. Transmission media enable computers to send and receive messages.

There are the obvious advantages of a computer network: Multiple real time usage which allows more than one person to work in the system at a time. In addition to above advantage with the recent proliferation of the internet, the subject of computer networks has received great attention.

ÖZET

Bugün bütün iş ve bilim dünyasında yer alan en büyük avantajlardan biri, bilgisayarların bir ağ yapısı içinde yer almasıdır. Bu iş çevrelerinin sadece rekabet edebilecek bir avantajı değil gelecekte olmazsa olmazlarından biri haline dönüşecektir. Bilgisayarlar ve veriler arasında fiziksel bağlantılar kurmak özellikle büyük çapta veri işleyen projelerde yeni fırsat ortamları yaratılmasına da neden olmuştur.

Bu projede, temel olarak bilgisayar ağı içinde bulunan makineler arasında fiziksel bir noktanın oluşturulması ve bu fiziksel noktaya sürücü ve gerekli servis elemanlarının ilave edilmesiyle nasıl ağ haberleşmesinin etkin kılındığı araştırılmıştır. Bilgisayar ağlarını etkin durumda kullanmak için, ağa bağlı tüm bilgisayarların üzerinde anlaştığı ve adına da protokol denilen bir dizi kurallar bütününe ihtiyaç duyulur. Bir ağ yapısının amacı bilgisayarlar arasında bilgi alış-verişini bilgisayarların haberleşme metodu olan protokoller vasıtasıyla yapmaktır. Bilgi iletişim topluluğu çeşitli standartlar ve ağ mimarisinin çeşitli birimlerinin belirttiği özellikler üzerine kurulmuştur. Ağa bağlı bilgisayarlar kablolar, ı ışık ve radyo dalgaları vasıtasıyla haberleşirler. Ağ içindeki iletim ortamı bilgisayarların mesaj alış verişini sağlar.

Bir bilgisayar ağının getirdiği en büyük avantajlar: Bir kerede sistem içersinde birden fazla insanın çoklu ve gerçek ortamda bilgi kullanımı. Ek olarak internetin önem kazanması, dünya üzerinde etkin ve popüler duruma gelmesi ile birlikte bilgisayar ağları kavramı daha önce olduğundan daha büyük bir değer kazanmıştır.

CONTENTS

CONTENTS	IV
LIST OF FIGURES	XIV
LIST OF TABLES	XVIII

Chapter One INTRODUCTION

1. INTRODUCTION.....	1
----------------------	---

Chapter Two NETWORKING TERMS AND CONCEPTS

2.1 Networking Concepts and Components.....	2
2.2 Models of Network Computing.....	6
2.2.1 Centralized Computing.....	6
2.2.2 Distributed Computing.....	7
2.2.3 Collaborative Computing.....	8
2.3 Compare a Client/Server Network with a Peer-to-Peer Network.....	10
2.3.1 Client/Server-Based Networking.....	10
2.3.2 Peer-to-Peer Networking.....	13
2.4 Local and Wide Area Networks.....	13
2.4.1 Local Area Networks (LANs)	14
2.4.2 Wide Area Networks (WANs)	14
2.5 Intranets and Internets.....	15
2.6 Network Services.....	15

2.6.1 Basic Connectivity Services.....	16
2.6.2 Redirector Service.....	16
2.6.3 Server Service.....	17
2.6.4 File Services.....	17
2.6.5 File Transfer Services.....	20
2.6.6 Printing Services.....	22
2.6.7 Application Services.....	23
2.6.8 Database Services.....	24
2.6.9 Messaging/Communication Services.....	25
2.6.9.1 Email.....	26
2.6.9.2 Voice Mail.....	26
2.6.9.3 Fax Services.....	26
2.6.10 Groupware.....	26
2.6.11 Directory Services.....	27
2.6.12 Security Services.....	28

Chapter Three

NETWORKING STANDARDS

3.1 Standards.....	29
3.1.1 Standards Organisations and the ISO.....	29
3.2 The OSI Reference Model.....	30
3.2.1 How Peer OSI Layers Communicate.....	32
3.2.2 Protocol Stacks.....	33
3.3 Conceptualising the Layers of the OSI Model.....	34
3.3.1 OSI Physical Layer Concepts.....	34
3.3.2 OSI Data Link Layer Concepts.....	35
3.3.2.1 Hardware Access at the Data Link Layer.....	35
3.3.2.2 Addressing at the Data Link Layer.....	36
3.3.2.3 Error and Flow Control at the Data Link Layer.....	37
3.3.3 OSI Network Layer Concepts.....	37
3.3.3.1 Network Layer Addressing.....	38

3.3.3.2 Delivering Packets.....	39
3.3.3.3 Connection-Oriented and Connectionless Modes.....	40
3.3.3.4 Gateway Services.....	42
3.3.4 OSI Transport Layer Concepts.....	42
3.3.4.1 Transport Layer Connection Services.....	43
3.3.5 OSI Session Layer Concepts.....	43
3.3.6 OSI Presentation Layer Concepts.....	44
3.3.7 OSI Application Layer Concepts.....	45
3.4 Comparing TCP/IP to the OSI Reference Model.....	46
3.5 Standards that Utilize Multiple Levels of the OSI Model.....	49
3.5.1 Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP).....	50
3.6 The IEEE 802 Family.....	53
3.7 NDIS and ODI.....	56

Chapter Four

NETWORK TRANSMISSION MEDIA

4.1 Introduction.....	58
4.2 Transmission Frequencies.....	58
4.3 Transmission Media Characteristics.....	60
4.3.1 Cost.....	60
4.3.2 Installation Requirements.....	61
4.3.3 Bandwidth.....	61
4.3.4 Band Usage (Baseband or Broadband)	61
4.3.4.1 Frequency-Division Multiplexing.....	62
4.3.4.2 Time-Division Multiplexing.....	63
4.3.5 Attenuation.....	64
4.3.6 Electromagnetic Interference.....	64
4.4 Guided Transmission Media.....	64
4.4.1 Coaxial Cable.....	65
4.4.1.1 Types of Coaxial Cable.....	65
4.4.1.1.1 Thinnet.....	66

4.4.1.1.2 Thicknet.....	66
4.4.1.2 Coaxial Characteristics.....	66
4.4.1.2.1 Installations.....	67
4.4.1.2.2 Cost.....	68
4.4.1.2.3 Capacity.....	68
4.4.1.2.4 EMI Characteristics.....	68
4.4.1.3 Connectors for Coaxial Cable.....	68
4.4.2 Twisted-Pair Cable.....	70
4.4.2.1 Shielded Twisted-Pair (STP) Cable.....	71
4.4.2.1.1 Cost.....	72
4.4.2.1.2 Installation.....	72
4.4.2.1.3 Capacity.....	72
4.4.2.1.4 Attenuation.....	73
4.4.2.1.5 EMI Characteristics.....	73
4.4.2.2 Unshielded Twisted-Pair (UTP) Cable.....	73
4.4.2.2.1 Cost.....	74
4.4.2.2.2 Installation.....	74
4.4.2.2.3 Capacity.....	75
4.4.2.2.4 Attenuation.....	75
4.4.2.2.5 EMI Characteristics.....	75
4.4.3 Fiber Optic Cable.....	75
4.4.3.1 Fiber Optic Characteristics.....	76
4.4.3.1.1 Cost.....	77
4.4.3.1.2 Installation.....	77
4.4.3.1.3 Capacity.....	77
4.4.3.1.4 Attenuation.....	77
4.4.3.1.5 EMI Characteristics.....	77
4.4.4 Summary of Cable Characteristics.....	78
4.5 Wireless Transmission.....	79
4.5.1 Reasons for Wireless Networks.....	79
4.5.2 Wireless Communications with LANs.....	80
4.5.2.1 Infrared Transmission.....	80

4.5.2.2 Laser Transmission.....	81
4.5.2.3 Narrow-Band Radio Transmission.....	81
4.5.2.4 Spread-Spectrum Radio Transmission.....	81
4.5.2.5 Microwave.....	83
4.5.2.5.1 Terrestrial Microwave.....	84
4.5.2.5.2 Satellite Microwave.....	86
4.5.3 Comparisons of Different Wireless Transmission.....	87

Chapter Five

NETWORK TOPOLOGIES AND ARCHITECTURES

5.1 Network Topologies.....	88
5.1.1 Bus Topologies.....	89
5.1.2 Ring Topologies.....	90
5.1.3 Star Topologies.....	91
5.1.4 Mesh Topology.....	91
5.2 Network Architectures.....	92
5.2.1 Ethernet.....	92
5.2.1.1 Ethernet Cabling.....	94
5.2.1.2 10BASE2.....	95
5.2.1.3 10BASE5.....	97
5.2.1.4 10BASE-T.....	98
5.2.1.5 10BASE-FL.....	100
5.2.1.6 100VG-AnyLAN.....	101
5.2.1.7 100BASE-X.....	102
5.2.2 Token Ring.....	102
5.2.2.1 Token Ring Cabling.....	103
5.2.3 Asynchronous Transfer Mode (ATM).....	104
5.2.4 ARCNet.....	106
5.2.5 FDDI.....	107

1. Содержание

Chapter Six

NETWORK ADAPTER CARDS

6.1 Network Adapter cards.....	108
6.2 Defining the Workings of a Network Adapter Card.....	108
6.3 Preparing and Sending Data.....	109
6.4 How a Network Card Works.....	110
6.4.1 Signals.....	111
6.4.1.1 Analog Signals.....	111
6.4.1.2 Digital signals.....	113
6.4.2 Clocking.....	113

Chapter Seven

CONNECTIVITY DEVICES

7.1 Introduction.....	114
7.2 Modems.....	114
7.3 Repeaters.....	115
7.4 Hubs.....	116
7.4.1 Passive Hubs.....	117
7.4.2 Active Hubs.....	117
7.5 Switches.....	118
7.6 Bridges.....	118
7.7 Routing.....	121
7.7.1 Routers.....	122
7.7.2 Brouters.....	125
7.8 Gateways.....	125

Chapter Eight

TRANSPORT PROTOCOLS

8.1 Introduciton.....	126
-----------------------	-----

8.2 Packets and Protocols.....	126
8.3 Protocols and Protocol Layers.....	128
8.3.1 TCP/IP – Internet Protocols.....	129
8.3.1.1 General TCP/IP Transport Protocols.....	130
8.3.1.1.1 Addressing in TCP/IP.....	130
8.3.1.1.2 Internet Protocol (IP)	132
8.3.1.1.3 Transmission Control Protocol (TCP)	132
8.3.1.1.4 User Datagram Protocol (UDP)	133
8.3.1.1.5 Address Resolution Protocol (ARP)	134
8.3.1.1.6 Internet Control Message Protocol (ICMP)	134
8.3.1.2 TCP/IP Services.....	135
8.3.1.2.1 Dynamic Host Configuration Protocol (DHCP)	135
8.3.1.2.2 Domain Name System (DNS)	135
8.3.1.2.3 Windows Internet Naming Services (WINS)	135
8.3.1.2.4 File Transfer Protocol (FTP)	136
8.3.1.2.5 Simple Mail Transfer Protocol (SMTP)	136
8.3.1.2.6 Remote Terminal Emulation (TELNET)	136
8.3.1.2.7 Network File System (NFS)	137
8.3.1.3 TCP/IP Routing Protocols.....	137
8.3.1.3.1 Routing Information Protocol (RIP)	137
8.3.1.3.2 Open Shortest Path First (OSPF)	138
8.3.2 NetWare IPX/SPX.....	138
8.3.2.1 General IPX/SPX Transport Protocols.....	139
8.3.2.1.1 Addressing in IPX.....	139
8.3.2.1.2 IPX.....	140
8.3.2.1.3 SPX.....	140
8.3.2.1.4 Frame Type.....	141
8.3.2.2 IPX/SPX Services.....	142
8.3.2.2.1 Service Advertising Protocol (SAP)	142
8.3.2.2.2 NetWare Core Protocol (NCP)	142
8.3.2.3 IPX/SPX Routing.....	142
8.3.2.3.1 Router Information Protocol (RIP)	142

8.3.2.3.2 NetWare Link Services Protocol (NLSP)	143
8.3.3 NetBEUI.....	143
8.3.4 Apple Talk.....	143
8.3.5 Data Link Control (DLC)	145
8.4 NetBIOS Names.....	145
8.4.1 NetBIOS Background	145
8.4.2 Assigning NetBIOS Names.....	146

Chapter Nine

DISASTER RECOVERY

9.1 Introduction.....	147
9.2 Protecting Data.....	147
9.2.1 Backup.....	147
9.2.2 Uninterruptible Power Supply.....	150
9.3 Recovering From System Failure.....	151
9.3.1 Implementing a Fault-Tolerant Design.....	151
9.3.2 Using RAID.....	151
9.3.2.1 RAID 0.....	153
9.3.2.2 RAID 1.....	153
9.3.2.3 RAID 5.....	154
9.3.2.4 Choosing a RAID Level.....	156
9.3.2.5 Disk Duplexing.....	157
9.4 Other Fault-Tolerance Mechanisms.....	158

Chapter Ten

NETWORK MANAGEMENT

10.1 Introduction.....	159
10.2 Resource Sharing Basics.....	160
10.2.1 Resources.....	160
10.2.2 Sharing.....	160

10.2.3 Users.....	161
10.2.4 Groups.....	161
10.2.5 Security.....	161
10.3 General Network Administrative Models.....	162
10.3.1 Workgroup Model.....	162
10.3.1.1 Windows 95.....	163
10.3.1.2 Windows NT.....	163
10.3.2 Bindery-Based Model.....	164
10.3.3 Domain Model.....	165
10.3.4 Directory Services Model.....	166
10.4 Managing User Accounts and Groups Using Windows NT.....	169
10.4.1 User Accounts.....	169
10.4.2 Groups.....	170
10.4.2.1 Global Groups.....	170
10.4.2.2 Local Groups.....	171
10.4.2.3 Security Groups.....	171
10.4.2.4 Distribution Groups.....	171
10.4.2.5 Built-in Global and Local Groups in Windows NT.....	171
10.4.3 Permissions.....	173
10.4.4 Rights.....	173
10.5 Additional Administrative Tasks.....	173
10.5.1 Auditing.....	174
10.5.2 Handling Data Encryption.....	174
10.5.3 Handling Virus Protection.....	175
10.5.4 Security Equipment.....	175

Chapter Eleven

MONITORING THE NETWORK

11.1 Introduction.....	176
11.2 Monitoring Network Trends.....	176
11.3 Keeping Records.....	177

11.4 Monitoring Performance.....178

 11.4.1 Simple Network Management Protocol (SNMP)178

 11.4.2 Windows NT Performance Monitor.....179

 11.4.3 Windows 95 System Monitor.....180

11.5 Monitoring Network Traffic.....181

11.6 Logging events.....182

Chapter Twelve

CONCLUSIONS

CONCLUSIONS.....184

REFERENCES.....186



LIST OF FIGURES

	Page
Figure 2.1 The simplest network.....	2
Figure 2.2 The various components involved in a network.....	5
Figure 2.3 In centralized computing all the processing is done by a central computer.....	7
Figure 2.4 Distributed computing.....	8
Figure 2.5 File Server	11
Figure 2.6 Print Server	11
Figure 2.7 Application Server	12
Figure 2.8 The WAN or the link up of LAN's is often shown as a cloud.....	15
Figure 2.9 The dialog box on a Windows 95 machine that shows a redirector being installed.....	17
Figure 2.10 A file server stores files for users on other network machines.....	20
Figure 2.11 Print services manage access to a shared printer, making it accessible to users at other network machines.....	22
Figure 2.12 An application server runs all or part of an application on behalf of a client and then transmits the result to the client for further processing.....	23
Figure 2.13 Master-driven and locally driven database replications.....	25
Figure 2.14 Directory services tells clients the location of resources on the network.....	27
Figure 3.1 The OSI model has seven layers.....	31
Figure 3.2 Each layer, except the Physical Layer, adds a header to the frame as it travels down the OSI layers and removes it as it travels up the OSI layers.....	33
Figure 3.3 TCP/IP in comparison to the OSI Reference Model.....	47
Figure 3.4 The five layers of the TCP/IP Reference Model.....	49
Figure 3.5 The relationship between SLIP, PPP and the OSI model.....	50

Figure 3.6 The relationship between the IEEE 802 standards and the OSI model...	53
Figure 4.1 High frequency and low frequency waves.....	59
Figure 4.2 Baseband and Broadband transmission modes.....	62
Figure 4.3 Frequency-division multiplexing.....	63
Figure 4.4 Time division multiplexing streams data depending on the data's allocated time slots.....	63
Figure 4.5 The structure of coaxial cable consists of four major components.....	65
Figure 4.6 Coaxial cable wiring configuration.....	67
Figure 4.7 Thinnet is connected using BNC T-connectors.....	69
Figure 4.8 Connectors and cabling for Thicknet.....	70
Figure 4.9 Twisted-pair cabling.....	70
Figure 4.10 A shielded twisted-pair cable.....	72
Figure 4.11 A multipair UTP cable.....	73
Figure 4.12 A fiber-optic cable.....	76
Figure 4.13 Frequency hopping transmits data over various frequencies for specific periods of time.....	82
Figure 4.14 Direct sequence modulation.....	83
Figure 4.15 Terrestrial and satellite microwave links.....	84
Figure 5.1 Bus, Star, Ring and Mesh Network Topologies.....	88
Figure 5.2 A bus topology.....	89
Figure 5.3 Bus topology.....	89
Figure 5.4 BNC T Connector.....	90
Figure 5.5 A ring topology.....	90
Figure 5.6 A star topology.....	91
Figure 5.7 A mesh topology.....	92
Figure 5.8 A sample of part of an Ethernet II frame.....	94
Figure 5.9 The 10BASE2 cabling.....	95
Figure 5.10 T connector and a BNC connector.....	96
Figure 5.11 Two segments using 10BASE2 cabling.....	97
Figure 5.12 Components of a Thicknet network.....	98
Figure 5.13 A 10BASE-T network wired in a star topology.....	99
Figure 5.14 Cascaded star topology.....	101

Figure 5.15	Operation of a token-ring.....	103
Figure 5.16	An example of a token-ring cabling.....	104
Figure 5.17	The relationship of ATM to the OSI reference model.....	105
Figure 5.18	A FDDI network.....	107
Figure 6.1	An example of a network adapter card.....	109
Figure 6.2	An example of an analog signal.....	112
Figure 6.3	These two analog waveforms differ in frequency.....	112
Figure 6.4	These two waveforms differ in amplitude.....	112
Figure 6.5	An example of digital signal.....	113
Figure 7.1	A repeater regenerates a weak signal.....	116
Figure 7.2	Using a repeater to extend an Ethernet LAN.....	116
Figure 7.3	A network wired to a central hub.....	117
Figure 7.4	Separating signals on a LAN segment with a bridge.....	119
Figure 7.5	A complex network with bridges.....	122
Figure 7.6	An internetwork: A series of networks separated by routers.....	123
Figure 7.7	Gateways convert protocol information to dissimilar environments.....	125
Figure 8.1	The network adapter card checks whether the destination address matches the PC's address.....	127
Figure 8.2	TCP/IP or the "Internet Protocol Suite"	129
Figure 8.3	The NetWare protocol architecture.....	138
Figure 8.4	The Apple Talk protocol suite.....	144
Figure 9.1	An ideal backup scheme implements a schedule of different backup types.....	149
Figure 9.2	A large UPS can service numerous components at once.....	150
Figure 9.3	Data striping arranges data in different sequence accross drives.....	152
Figure 9.4	In disk mirroring, two hard drives use the same disk channel.....	153
Figure 9.5	In this example, if Disk 2 fails, the system can reconstruct the information on it using the parity data.....	155
Figure 9.6	Different RAID levels offer their own unique capabilities.....	154
Figure 9.7	Disk duplexing simultaneously writes data to two disks located on diferent controller cards.....	157
Figure 10.1	A workgroup does not rely on a centralised user account database....	162

Figure 10.2 A Bindery-based network has a centralised user account database. Client machines run no services.....	165
Figure 10.3 Directory Services has a distributed hierarchical database.....	168
Figure 10.4 A directory auditing window in Windows NT.....	174
Figure 11.1 A Windows NT Performance Monitor chart.....	179
Figure 11.2 Windows NT Server's Network Monitor main screen.....	181
Figure 11.3 The Event Viewer main screen	183



LIST OF TABLES

	Page
Table 2.1 Employee Information.....	12
Table 4.1 Thinnet Cable Classifications.....	66
Table 4.2 Comparisons of Guided Transmission Media.....	78
Table 4.3 Comparisons of Wireless Transmission.....	87
Table 8.1 Classes and Addresses.....	131



CHAPTER ONE

INTRODUCTION

This thesis concentrates on the computer communication techniques for building computer networks. In this context a network is simply: 'a selection of computing equipment that is connected together so as to allow inter-communication'. In computer communication the techniques can be explained in the following.

Chapter 2 introduces you to some of the basic terms and concepts used when discussing networking. This chapter explains three different computing models used by various systems throughout the world and two main types of network models and then covers how networks are classified based on various factors. The chapter goes on to describe the various services that a network can offer. Chapter 3 explores some of standards. The chapter is exploring the Open Systems Interconnection (OSI) reference model and the other industry standards. These standards include the SLIP, PPP, the IEEE 802 standards, NDIS, and ODI. Chapter 4 discusses some of the most common network transmission media. Chapter 5 describes network topologies and architectures. Chapter 6 examines the role of the network adapter card also known as a network interface card (NIC). Because a network adapter card is the most common mechanism for attaching PCs to a network. Chapter 7 explains some of the other more common devices used to transmit data in a network. Chapter 8 examines a variety of actual transport protocols and protocol suites, such as TCP/IP and IPX/SPX. Chapter 9 discusses how the use of fault-tolerant disk configurations and a backup strategy can help reduce the danger of lost time and data. Chapter 10 deals with the process of implementing resource sharing, with the main focus being the administration of a Microsoft network. Chapter 11 presents various programs or mechanisms that can be used to monitor and record information about the network. The explanation of what these different mechanisms are and when you would utilise them is addressed in this chapter.

CHAPTER TWO

NETWORKING TERMS AND CONCEPTS

2.1 Networking Concepts and Components

This chapter begins with a definition of networking. It then moves on to cover three different computing models used by various systems throughout the world. The discussion next turns to the two main types of network models and then covers how networks are classified based on various factors. The chapter goes on to describe the various services that a network can offer.

A network is a collection of machines that have been linked together physically and on which software components have been added to facilitate communication and sharing of information. By this definition, a network might be as simple as the computers shown in Figure 2.1. Computer, NIC and network cables are the three elements of a network. A more complicated network may involve more network devices such as Hubs and repeaters etc. However, computers, NICs and network cables are necessary to build a network (Glen Berg, 1998).

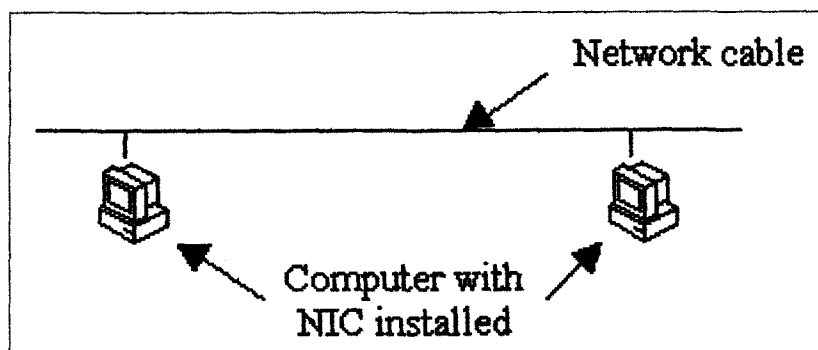


Figure 2.1 The simplest network

Network Interface Card (NIC), sometimes refers to as Network Adapter. NIC is plugged into the slot of the computer and provides the physical connection between the network cable and the computer.

Suppose NIC A is plugged into computer A, while NIC B is plugged into computer B. If a user of computer A wants to send a message to a user of computer B. The message goes to the NIC A first. After that, NIC A converts the message to small packets that can be transmitted via the network cable. After NIC B receives the packets from NIC A, it reassembles them and converts the data back to a format that can be understood by the computer has NIC B installed. This mechanism makes the communication possible between two computers.

Networking is the concept of sharing resources and services. A network of computers is a group of interconnected systems sharing resources and interacting using a shared communications link. A network, therefore, is a set of interconnected systems with something to share. The shared resource can be data, a printer, a fax modem, or a service such as a database or an email system. The individual systems must be connected through a pathway (called the transmission medium) that is used to transmit the resource or service between the computers. All systems on the pathway must follow a set of common communication rules for data to arrive at its intended destination and for the sending and receiving systems to understand each other. The rules governing computer communication are called protocols.

All networks must have the following:

- ◆ A resource to share (resource)
- ◆ A pathway to transfer data (transmission medium)
- ◆ A set of rules governing how to communicate (protocols)

In general, all networks have certain components, functions and features in common. These includes:

- ◆ **Servers:** Computers that provide shared resources to network users.

- ◆ **Clients:** Computers that access shared network resources provided by a server.
- ◆ **Media:** The way that computers are connected.
- ◆ **Shared data:** Files provided by servers across the network.
- ◆ **Shared printers and other peripherals:** Other resources provided by servers.
- ◆ **Resources:** Files, printers or other items to be used by network users.

Having a transmission pathway does not always guarantee communication. When two entities communicate, they do not merely exchange information; rather, they must understand the information they receive from each other. The goal of computer networking, therefore, is not simply to exchange data but to understand and use data received from other entities on the network.

An analogy is people speaking. Just because two people can speak, it does not mean they automatically can understand each other. These two people might speak different languages or interpret words differently. One person might use sign language, while the other uses spoken language. As in human communication, even though you have two entities who "speak," there is no guarantee they will be able to understand each other. Just because two computers are sharing resources, it does not necessarily mean they can communicate.

Because computers can be used in different ways and can be located at different distances from each other, enabling computers to communicate often can be a daunting task that draws on a wide variety of technologies.

The two main reasons for using computer networking are to provide services and to reduce equipment costs. Networks enable computers to share their resources by offering services to other computers and users on a network. The following are specific reasons for networking PCs:

- ◆ **Sharing files**
- ◆ **Sharing printers and other devices**

- ◆ Enabling centralized administration and security of the resources within the system
- ◆ Supporting network applications such as electronic mail and database services

Figure 2.2 shows the main hardware and software components required to enable communication between these two machines. The components shown in Figure 2.2 are defined here:

- ◆ **OS:** This is the operating system; more specifically, this is the user interface that you use to connect to other computers on the network.
- ◆ **RDR:** The RDR, or redirector, intercepts requests for resource access and, if required, passes the request to the network. The redirector (or client) can talk only to a server that understands what it is talking about, or that has a common frame of reference.
- ◆ **SVR:** The server component receives and services the requests from a redirector.
- ◆ **Protocol:** The requests from the redirector and the responses from the server are encapsulated in a transport protocol. The protocol (such as TCP/IP) then finds the other computer and moves the data to the target machine.
- ◆ **Network Card:** The protocol works with the Network Card to physically move the data to the other computer.

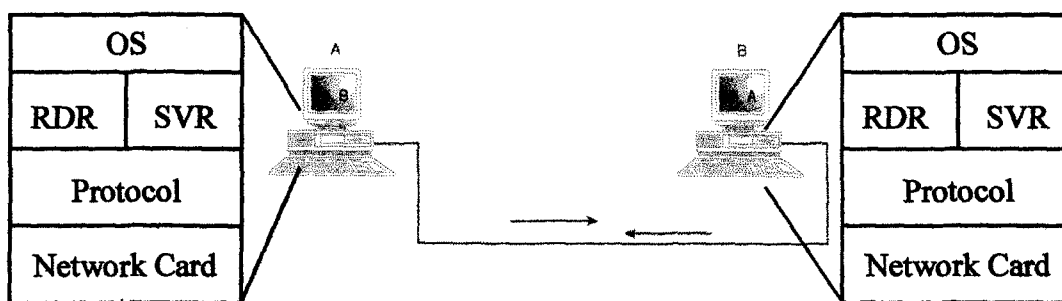


Figure 2.2 The various components involved in a network

2.2 Models of Network Computing

After you have the necessary prerequisites for network communication, a structure must be put in place that organizes how communication and sharing occurs. Three methods of organization, or models, generally are recognized. The following are the three models for network computing:

- ◆ Centralized computing
- ◆ Distributed computing
- ◆ Collaborative or cooperative computing

2.2.1 Centralized Computing

The first computers were large, expensive, and difficult to manage. Originally, these large mainframe computers were not networked as you are familiar with today. Jobs were entered into the system by reading commands from card decks. The computer executed one job at a time and generated a printout when the job was complete. Terminals, which came later, provided the user with a new mechanism to interact with the centralized computer. These terminals, however, were merely input/output devices that had no independent processing power. All processing still took place on the central mainframe, hence the name centralized computing. Networks, therefore, served little purpose other than to deliver commands to and get results from the powerful centralized processing device. To this day, large mainframe systems are still being operated around the world, most often by governments and large corporations. An example of centralized computing to which everyone can relate is using an ATM machine. ATMs function as terminals. All processing is done on the mainframe computer to which the ATMs are connected. In summary, the centralized computing model involves the following:

- ◆ All processing takes place in the central mainframe computer.
- ◆ Terminals are connected to the central computer and function only as input/output devices.

This early computing model worked well in large organizations that could justify the need for these expensive computing devices.

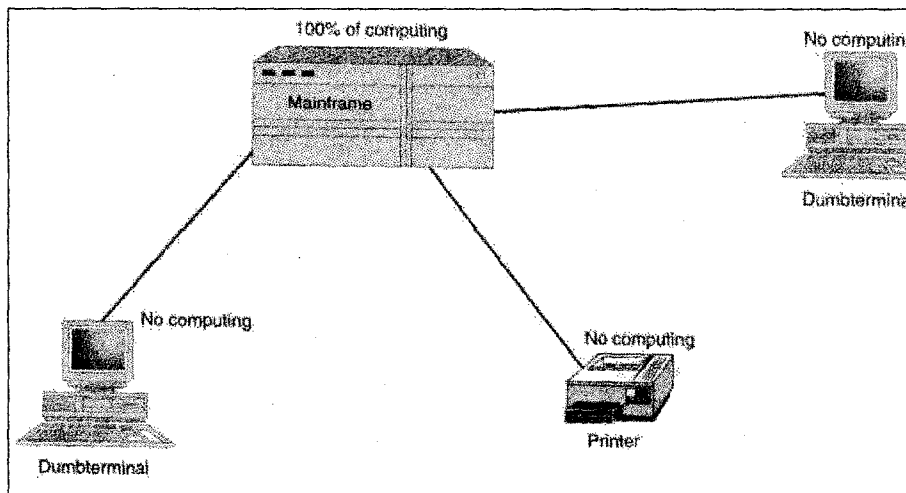


Figure 2.3 In centralised computing all the processing is done by a central computer

2.2.2 Distributed Computing

As personal computers (PCs) were introduced to organizations, a new model of distributed computing emerged. Instead of concentrating computing at a central device, PCs made it possible to give each worker an independent, individual computer. Each PC could receive input and could process information locally, without the aid of another computer.

This means that groups who previously had found the cost of a mainframe environment to be prohibitive were now able to gain the benefits of computing at a far lower cost than that of a mainframe. These PCs, however, did not have the computing power of a mainframe. Thus, in most instances, a company's mainframe could not be replaced by a PC.

An analogy might help clarify the difference between the two computing models. A mainframe, which uses a centralized computing model, is like a bus. A bus is a large, powerful vehicle used to transport many people at once. Everyone goes to one

location to be transported. In the same way, everyone must work through or at a mainframe computer. A personal PC, which uses distributed computing, is like a motorcycle. It transports one person at a time. Each person can use his own motorcycle to go somewhere without worrying about the other users. PCs enable individuals to work at their own computers rather than through a single large computer (Glen Berg, 1998).

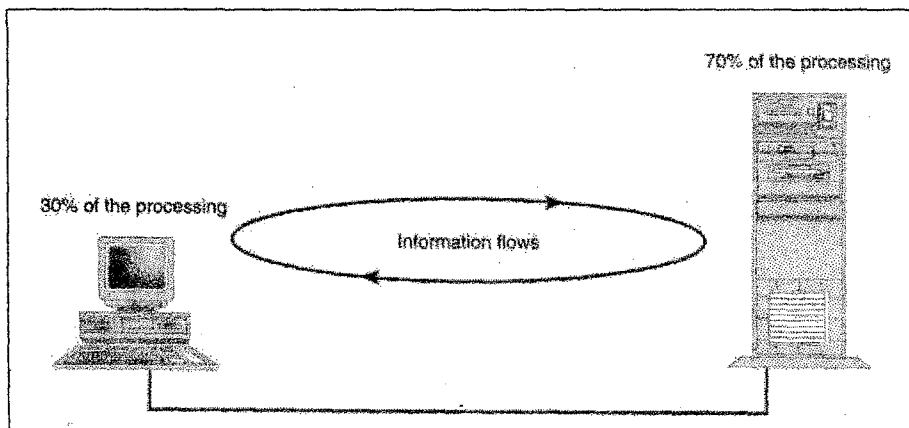


Figure 2.4 Distributed computing

In summary, distributed computing involves the following:

- ◆ Multiple computers capable of processing independently
- ◆ Task completion by the local computer or other computers on the network

Distributed computing was a major step forward in how businesses leveraged their hardware resources. It provided smaller businesses with their own computational capabilities, enabling them to perform less-complex computing tasks on the smaller, relatively inexpensive machines.

2.2.3 Collaborative Computing

Also called cooperative computing, collaborative computing enables computers in a distributed computing environment to share processing power in addition to data, resources, and services. In a collaborative computing environment, one computer might borrow processing power by running a program on another computer on the

network. Or, processes might be designed so they can run on two or more computers. Collaborative computing cannot take place without a network to enable the various computers to communicate.

Collaborative computing basically is a messaging system to help a team and workgroup numbers to work more efficiently and effectively. Collaborative computing has following advantages:

- ◆ Make it easy to share information.
- ◆ Provide tools for automating group processes.
- ◆ Help users keep track of schedules for people and resources.
- ◆ Help organise and track tasks.

A person browsing the Internet is an example of collaborative Computing. On the Internet, Web servers actively use resources to give your computer information about how a Web page should look, including its colours, its font sizes, and what graphics should display. Your computer uses its processing power to interpret this information and to display it in the format intended by the designer. Another example of collaborative computing is Microsoft server based products such as Exchange Server or SQL Server. For both of these products, requests originate from intelligent client software (which uses the processor power of the workstation it is running on) but then are serviced from server software running on a Windows NT server. The server then processes the request using its own resources and passes the results back to the client. Processor and memory resources on both the client and the server are utilized in the completion of the task (Glen Berg, 1998).

In the future, you can expect collaborative computing to provide even greater amounts of computing power. This might happen through a new capability of computers to detect which PCs are idle on the network and to harness the CPU power or RAM of the idle PCs for use in processing.

In summary, collaborative computing involves the following:

- ◆ Multiple computers cooperating to perform a task

- ◆ Software designed to take advantage of the collaborative environment

2.3 Compare a Client/Server Network with a Peer-to-Peer Network

Networks generally fall into one of two broad network categories:

- ◆ Client/server networks
- ◆ Peer-to-peer networks

2.3.1 Client/Server-Based Networking

A client/server network consists of a group of user-oriented PCs (called clients) that issue requests to a server. The client PC is responsible for issuing requests for services to be rendered. The server's function on the network is to service these requests. Servers generally are higher-performance systems that are optimised to provide network services to other PCs. The server machine often has a faster CPU, more memory, and more disk space than a typical client machine.

Eating at a restaurant is analogous to a client/server model. You, the customer, are a client. You issue requests for meals, drinks, and dessert. The waiter is the server. It is the waiter's job to service those requests. The client/server model is a network in which the role of the client is to issue requests and the role of the server is to service requests.

An example of a client/server system is Microsoft Exchange Server. Your PC is responsible for constructing and displaying email messages, to name a couple of the possible tasks. The Exchange server is responsible for delivering outgoing email and for receiving email intended for you.

Some examples of client/server-based networks are Novell NetWare, Windows NT Server, and Banyan Vines. Some common server types include file and print servers, application servers, and mail servers, fax servers:

◆ **File and Print Servers:** File and print servers manage user access and use of file and printer resources. A computer provides storage space and print service for the other computers in a network.

Suppose we have several computers in a network. Computer A has a directory c:\ww that is network shared. Because other computers such as computer B and computer F in the network can also access this shared directory, computer A is called file server. In a Microsoft's operating system such as Windows 95 or Windows NT, you can use Windows Explorer to share a directory or map a shared directory to a local driver.

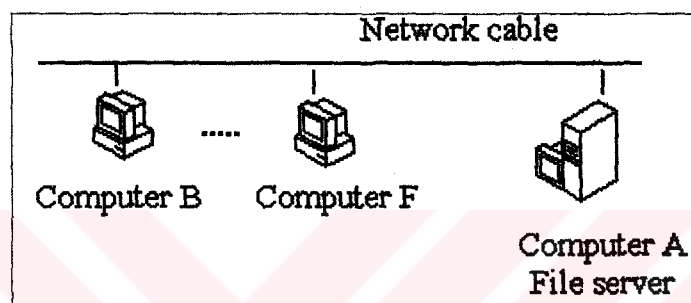


Figure 2.5 File Server

A printer is connected to computer A. Computer A shares this printer and provides printing service to other computers in the network. If any of the computer in the network such as computer B or computer F can print documents in this printer via computer A's printing service, computer A is called a printer server.

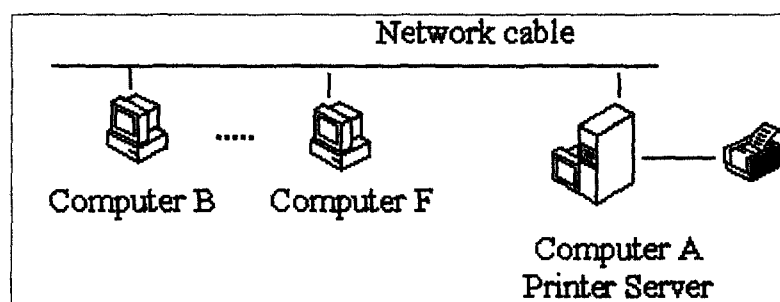


Figure 2.6 Print Server

♦ **Application Server:** An application server is a computer provides back-end data processing for other computers in the network. SQL Server and Exchange Server are examples of an application server. Compared to a file server, which saves the file directly, an application server executes data processing. Sometimes it is difficult to distinguish a file server with an application especially in the database area. Most database applications such as Oracle, Sybase, Informix, Ingress and Microsoft's SQL Server for Windows NT Server meet the requirement of application server because they provide back-end data processing.

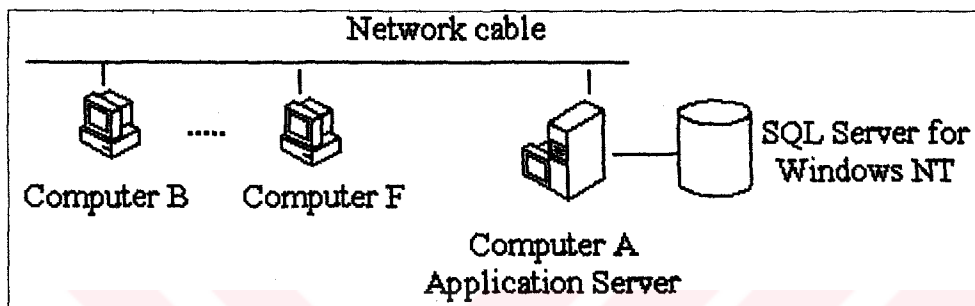


Figure 2.7 Application Server

We install SQL server for Windows NT in computer A and install the client tools of SQL Server in computer B and computer F. We create an employee table (Table 2.1) in computer A via the SQL server.

Table 2.1 Employee information

Name	Age	Sex
Wang Wei	30	Male
Li Bo	27	Female
Bill Gates	44	Male

Now computer B wants to list all the employees whose age is bigger than 28, it sends the following SQL statement to computer A. Select Name from employee where age > 28. After computer A receives this request, it executes the data processing and returns the result: "Wang Wei" and "Bill Gates" to the computer B.

- ◆ **Mail Servers:** Mail servers manage electronic messaging between network users.
- ◆ **Fax Servers:** Fax servers manage fax traffic into and out of the network, by sharing one or more fax modem boards.

2.3.2 Peer-to-Peer Networking

A peer-to-peer network consists of a group of PCs that operate as equals. Each PC is called a peer. The peers share resources (such as files and printers) just like in a server-based network, although no specialized or dedicated server machines exist. In short, each PC can act as a client or a server. No one machine is set up with a higher powered set of devices, nor is any one PC set up simply to provide one service (such as storing files). Small networks-usually with fewer than 10 machines-can work well in this configuration. In larger networks, companies usually move to a server-based network because many clients requesting to use a shared resource can put too much strain on one client's PC. Examples of peer-to-peer networks include Windows for Workgroups, Windows 95 and Windows NT Workstation.

Many actual network environments consist of a combination of server-based and peer-to-peer networking models. In the real world, companies often grow from a peer-to-peer network into a client/server-based network.

2.4 Local And Wide Area Networks

Networks come in all shapes and sizes. Network administrators often classify networks according to geographical size. Networks of similar size have many similar characteristics. The following are the most common size classifications:

- ◆ **Local area networks (LANs):** LAN is a network that covers a relatively limited area, such as an office or a building.
- ◆ **Wide area networks (WANs):** WAN is a network that connects geographically separated areas.

2.4.1 Local Area Networks (LANs)

A local area network (LAN) is a group of computers and network communication devices interconnected within a geographically limited area, such as a building or a campus. LANs are characterized by the following:

- ◆ They transfer data at high speeds (higher bandwidth).
- ◆ They exist in a limited geographical area.
- ◆ Connectivity and resources, especially the transmission media, usually are managed by the company running the LAN.

2.4.2 Wide Area Networks (WANs)

A wide area network (WAN) interconnects LANs. This interconnection often is represented by a line going into a cloud. This is because the company running the network typically has only a general idea of the path that the data will take on its journey to the other LAN segment. All the company knows is that the data enters the cloud on one side and exits the other side. A WAN can be located entirely within a state or a country, or it can be interconnected around the world. WANs are characterized by the following:

- ◆ They exist in an unlimited geographical area.
- ◆ They usually interconnect multiple LANs.
- ◆ They often transfer data at lower speeds (lower bandwidth).
- ◆ Connectivity and resources, especially the transmission media, usually are managed by a third-party carrier such as a telephone or cable company.

WANs can be further classified into two categories: enterprise WANs and global WANs. An enterprise WAN connects the widely separated computer resources of a single organization. An organization with computer operations at several distant sites can employ an enterprise WAN to interconnect the sites. An enterprise WAN can combine private and commercial network services, but it is dedicated to the needs of a particular organization. A global WAN interconnects networks of several corporations or organizations (Glen Berg, 1998).

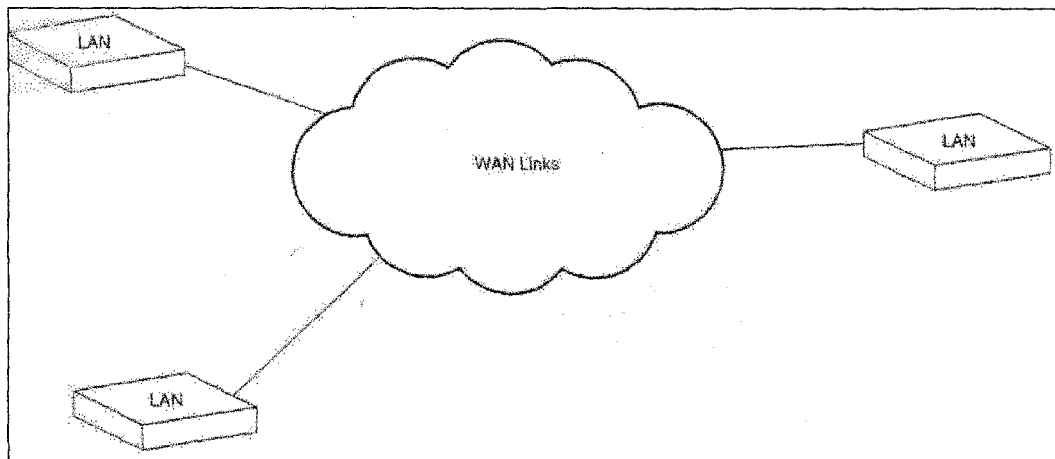


Figure 2.8 The WAN or the link up of LAN's is often shown as a cloud

2.5 Intranets and Internets

In recent years, two new terms have been introduced: Internet and intranet. A company that has a LAN has a network of computers. As a LAN grows, it develops into an internetwork of computers, referred to as an Internet.

In the 1990s, graphical utilities (or browsers) were developed to view information on a server. Today, the two most popular forms of this utility are Microsoft's Internet Explorer and Netscape's Navigator. These browsers are used to navigate the Internet. This terminology initially led to much confusion in the industry because an Internet is a connection of LANs, and the Internet is the connection of servers on various LANs that is available to various browser utilities. To avoid this confusion, the term intranet was coined. This term describes an internetwork of computers on a LAN for a single organization; the term Internet describes the network of computers you can connect to using a browser-essentially, an internetwork of LANs available to the public (Glen Berg, 1998).

2.6 Network Services

Network services are the basic reason we connect computers. Services are what a company wants to have performed or provided. Based on the services a company

wants to utilize, the company purchases a specific program and operating system. This section describes some of the most common services available on computer networks (Glen Berg, 1998).

2.6.1 Basic Connectivity Services

The PCs in a network must have special system software that enables them to function in a networking environment. The first network operating systems really were add-on packages that supplied the networking software for existing operating systems such as MS-DOS or OS/2. More recent operating systems, such as Windows 95 and Windows NT, come with the networking components built in.

An analogy might help you differentiate fully integrated systems from add-ons. A box can hold goods, but it is not specifically designed to go anywhere. You can place a set of logs on the ground to act as rollers for the box, thus providing a mechanism for transporting or moving the box. This is similar to how old network systems used to work. Newer operating systems are like trucks. A truck is designed from the ground up with a chassis that supports a box to move goods. The box and the mechanism for transportation (the chassis) are integrated from the beginning; they are designed to operate with each other.

Client and server machines require specific software components. A computer that is strictly a server often cannot provide any client functionality. On a Novell server or a Banyan server, for example, a user cannot use the server for word processing. This is not always the case, however; Microsoft's NT Server and UNIX servers can run client programs.

2.6.2 Redirector Service

A network client must have a software component called a redirector. In a typical standalone PC, I/O requests pass along the local bus to the local CPU. The redirector intercepts I/O requests within the client machine and checks whether the request is

directed toward a service on another computer. If it is, the redirector directs the request toward the appropriate network entity. The redirector enables the client machine to send information out of the computer, provided that a transmission pathway exists.

In some operating environments, the redirector is called the requester. The workstation service acts as a redirector on Windows NT systems. In the field, people often refer to a redirector as a client. To connect a Windows 95 machine to a Windows NT machine, for example, it often is said, "Install the Microsoft Client for Microsoft Networks." If you want this Windows 95 machine to connect to a Novell server, you might say, "Install a Novell Client on the Windows 95 machine."

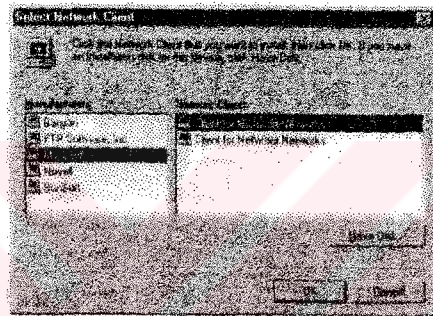


Figure 2.9 The dialog box on a Windows 95 machine that shows a redirector being installed

2.6.3 Server Service

A network server machine must have a component that accepts I/O requests from clients on the network and that fulfils those requests by routing the requested data back across the network to the client machine. In Windows NT, the server service performs the role of fulfilling client requests.

2.6.4 File Services

File services enable networked computers to share files with each other. This capability was one of the primary reasons networking of personal computers initially

came about. File services include all network functions dealing with the storage, retrieval, or movement of data files. File services enable users to read, write, and manage files and data. This includes moving files between computers and archiving files and data.

File services are an important part of client/server and peer-to-peer networks. Computers providing files services are referred to as file servers. Two types of servers exist: dedicated and non-dedicated. Dedicated servers do nothing but fulfil requests to network clients. These servers commonly are found in client/server environments. Non-dedicated servers do double duty. They enable a user to go onto the machine acting as a file server and request the use of files from other machines; at the same time, they give files to users who request them from other computers on the network. Non-dedicated file servers often are found in peer-to-peer networks. An example of a non-dedicated server is a Windows 95 machine that accesses files from other computers on the network and that provides access to its hard drive for other computers. Dedicated file servers have the following benefits:

- ◆ Files are stored in a specific place where they can be reliably archived.
- ◆ Central file servers can be managed more efficiently because there is a single point of storage:
 - ◆ Central file servers can contain expensive high-performance hardware that expedites file services and makes file servers more reliable.
 - ◆ The cost of specialized file server technology is shared by a large number of users.
 - ◆ Centralized networks are more scalable.

The following drawbacks, however, should be considered with regard to centralized file services:

- ◆ When all data is stored on a single server, a single point of failure exists. If the server fails, all data becomes unavailable.
- ◆ Because all clients contend for file services from a single source, average file-access times might be slower with a centralized file server than when files are stored on individual local hard drives.

Centralised file services generally are best for organizations that want to achieve the highest levels of centralized control for their data. In a peer-to-peer network environment, most computers can share their files and applications with other computers, provided that a service is installed on the machine allowing them to do this. The sharing of services must be established for each individual computer, and each user must have the skills required to manage the networking services on her PC. Because services are being provided by many different computers, users must be aware of which computers are providing which services. Clearly, the skills and responsibility required in this situation are greater than for centralized file services. This is in contrast to a client/server model, in which the network often has one or more dedicated people to manage the servers.

The following are advantages of distributed file storage:

- ◆ No single point of failure exists. When a computer fails, only the files stored on that computer become unavailable.
- ◆ Individuals typically experience faster access to files located on their local machines than to files on centralized file servers.
- ◆ No specialized server hardware is required. File services can be provided with standard PCs.

The following are disadvantages related to distributed file storage:

- ◆ It is more difficult to manage the file service because there is not a single file location.
- ◆ File services provided by peers typically are not as fast or as flexible as file services provided by a central file server specifically designed for that purpose.

Organisations tend to choose peer-to-peer networking for two reasons. The first reason is a desire to network with their current stock of PCs without the expense of a centralised server. Another reason is that a peer-to-peer network is an informal networking approach that fits the working style of many organisations. Microsoft implements peer-to-peer networking components in Windows for Workgroups, Windows 95, and Windows NT Workstation. All of these operating systems are

capable of sharing and accessing network resources without the aid of a centralised server. These systems are not optimised for file and printer sharing, however; this sort of network structure is recommended only for smaller networks with limited security concerns.

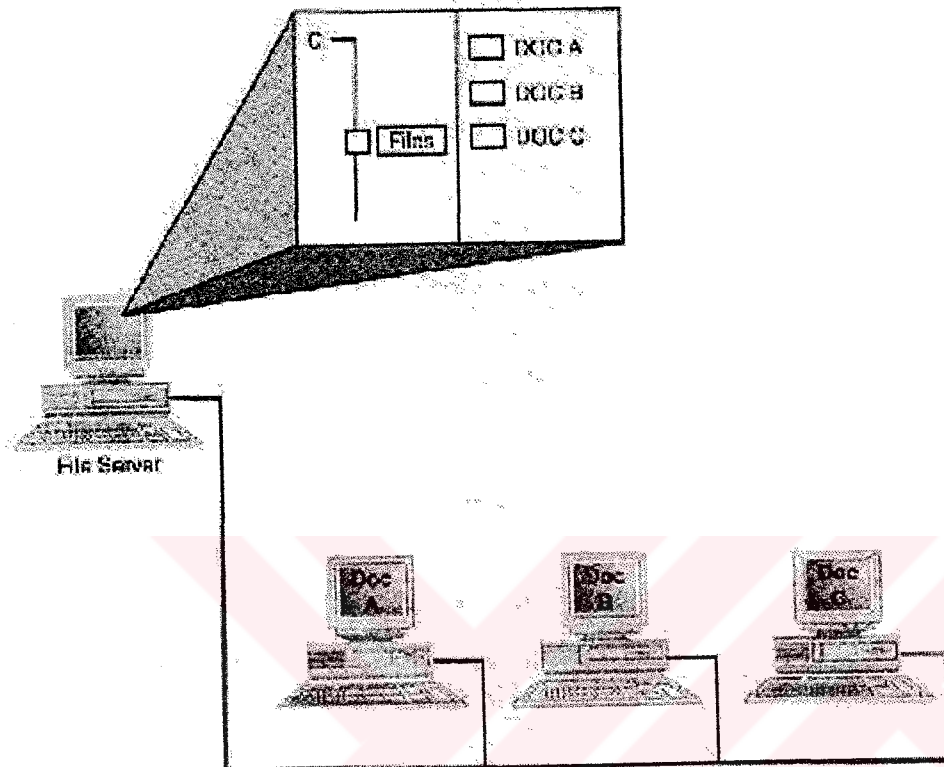


Figure 2.10 A file server stores files for users on other network machines

2.6.5 File Transfer Services

Without a network, the options are limited for transferring data between computers. You can, of course, exchange files on floppy disks. This process is called sneaker-net because it consists of networking by physically running around and hand-delivering floppy disks from desk to desk. Otherwise, you can use communication software to dial up another computer and transfer files using a modem or a direct serial connection. With a network, users have constant access to high-speed data transfer without leaving their desks or dialling another computer. Making a file accessible on a network is as easy as moving it into a shared directory.

Another important file-management task of the network operating system (NOS) is providing and regulating access to programs and data stored on the file server's hard drive. This is known as file sharing. File sharing is another main reason companies invest in a network. Companies can save money by purchasing a single network version of an application rather than many single-user versions. Placing data files created by employees on a file server also serves several purposes including security, document control and backup.

Centralized document control can be critical for a company in which a document might need to be revised several times. In an architectural firm, for example, the design of a building might be created by using a drafting program such as AutoCAD. The architects might produce several versions of the building plan as the client comes to a decision. If the plan is stored on the individual computers of each architect, the firm might not know which is the most recent version of the plan. An older version might have the most recent date (because of a backup, for example). If the plan is saved on a file server, however, each architect can access and work on the same file.

Most networks have some form of centralized file storage. For many years, companies have used the online storage approach to file storage. In the online storage scenario, data is stored on hard disks that are accessible on demand. The files that can be accessed on a server are limited to the amount of available hard drive space. Hard drives are fast, but even with drive prices decreasing in recent years, the cost to store megabytes of data this way can still be fairly high. Hard drives also have another disadvantage. Generally, they cannot be removed for off-site storage or exchange or to build a library of files that are seldom required but must be fairly readily available.

Another common approach to file storage is offline storage, which consists of removable media that are managed manually. After data is written to a tape or an optical disk, the storage medium can be removed from the server and can be shelved. Users who require offline data might need to know which tape or optical disk to

request. Some systems provide indexes or other aids that make requesting the proper offline storage element automatic. A system operator still has to retrieve the tape or disk, however, and mount it on the server.

2.6.6 Printing Services

After file services, printing is probably the second biggest incentive for installing a LAN. The following are some of the many advantages of network print services:

- ◆ Many users can share the same printers. This capability is especially useful with expensive devices such as colour printers and plotters.
- ◆ Printers can be located anywhere, not just next to a user's PC.
- ◆ Queue-based network printing is more efficient than direct printing because the workstation can begin to work again as soon as a job is queued to the network.
- ◆ Modern printing services enable users to send facsimile (fax) transmissions through the network to a fax server.

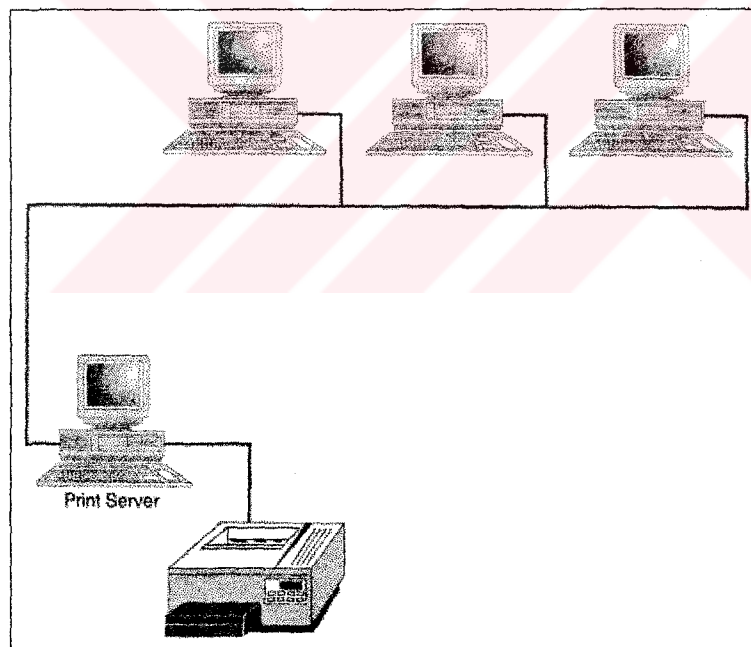


Figure 2.11 Print services manage access to a shared printer, making it accessible to users at other network machines

2.6.7 Application Services

Application services enable applications to leverage the computing power and specialized capabilities of other computers on a network. Business applications, for example, often must perform complex statistical calculations beyond the scope of most desktop PCs. Statistical software with the required capabilities might need to run on a mainframe computer or on a minicomputer. The statistical package, however, can make its capabilities available to applications on users' PCs by providing an application service.

The client PC sends the calculation request to the statistics server. When the results become available, they are returned to the client. This way, only one computer in an organization needs to have the expensive software license and processing power required to calculate the statistics, but all client PCs can benefit.

Application services enable organizations to install servers that are specialized for specific functions. Some of the more common application servers are database servers, messaging/communication servers, groupware servers, and directory servers. Application servers are an effective strategy for making a network more scalable. Additional application servers can be added as new application needs emerge.

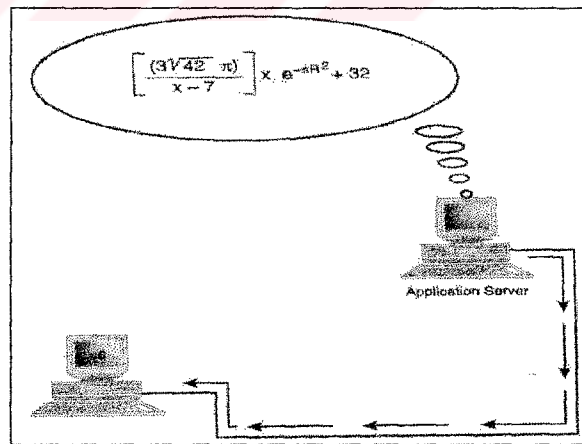


Figure 2.12 An application server runs all or part of an application on behalf of a client and then transmits the result to the client for further processing

2.6.8 Database Services

Database servers are the most common type of application servers. Because database services enable applications to be designed in separate client and server components, such applications frequently are called client/server databases.

With a client/server database, the client and server applications are designed to take advantage of the specialized capabilities of client and database systems, as described here:

- ◆ The client application manages data input from the user, generation of screen displays, some of the reporting, and data retrieval requests sent to the database server.
- ◆ The database server manages the database files; adds, deletes, and modifies records in the database; queries the database and generates the results required by the client and transmits results back to the client. The database server can service requests for multiple clients at the same time.

Database services relieve clients of most of the responsibilities for managing data. A modern database server is a sophisticated piece of software that can perform the following functions:

- ◆ Provide database security
- ◆ Optimise the performance of database operations
- ◆ Determine optimum locations for storing data without requiring clients to know where the data is located
- ◆ Service large numbers of clients by reducing the amount of time any one client spends accessing the database
- ◆ Distribute data across multiple database servers

Microsoft SQL Server and Oracle are two examples of applications that run at the server but are able to perform tasks requested by clients. Because of the way these applications were designed, both require a back-end, or server, component and a front-end or client, component.

As shown in Figure 2.13, the most popular strategies for replicating databases are the following:

- ◆ Master-driven updates. A single master server receives all updates and, in turn, updates all replicas.
- ◆ Locally driven updates. Any local server can receive an update and is responsible for distributing the change to other replicas.

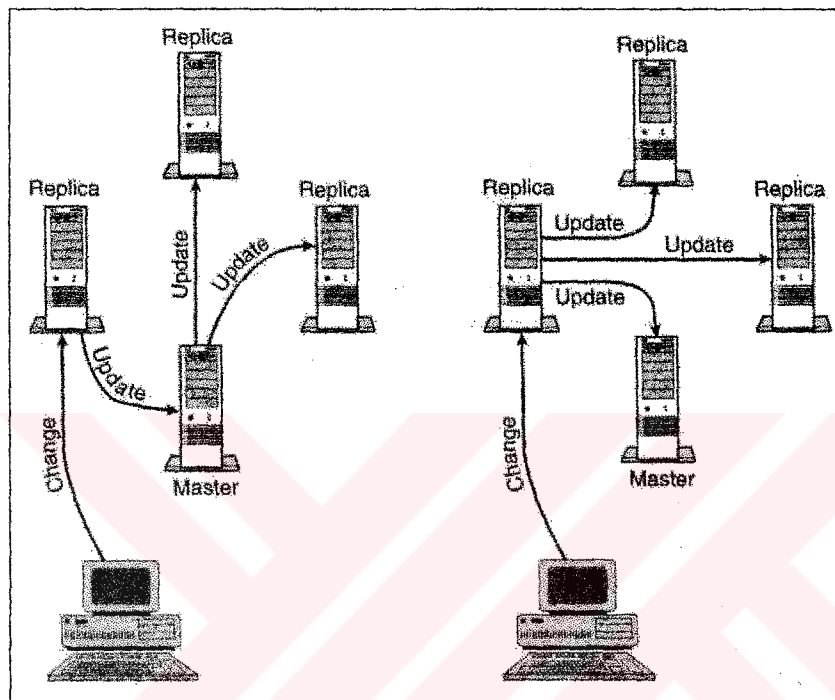


Figure 2.13 Master-driven and locally driven database replications

2.6.9 Messaging/Communication Services

Messaging/communication services generally transfer information from one place to another. This communication of information can be broken down into three sub areas:

- ◆ Email
- ◆ Voice mail
- ◆ Fax services

2.6.9.1 Email

Email systems can service any size group from a local workgroup to a corporation to the world. By installing email routing devices, you can transfer mail smoothly and efficiently among several LANs. Email also can be routed to and received from the Internet. This enables users in dozens of countries throughout the world to exchange electronic messages.

Some of the major email packages include Microsoft's Exchange Server, Novell's GroupWise, and Lotus Notes.

2.6.9.2 Voice Mail

Voice mail enables you to connect your computer to a telephone system and to incorporate telephone voicemail messages with your PC. The technical term for this is telephony. This often involves moving your voicemail messages from the phone system to the LAN and enabling the computer network to distribute this information to different clients.

2.6.9.3 Fax Services

Fax services enable you to send or receive faxes from your computer. This is similar to printing in that you can "print" the document to a fax device. Fax services, however, can take on more complicated features including the capability to send faxes to a central fax server and to receive faxes from the phone system to a central fax device. That device then delivers the fax message to your PC. This all occurs automatically.

2.6.10 Groupware

Groupware is a relatively recent technology that enables several network users to communicate and to cooperate when solving a problem through shared document

management. Interactive conferencing, screen sharing, and bulletin boards are examples of groupware applications. Groupware essentially is the capability for many users to work on one or more copies of a document together. Examples of applications with groupware features are Microsoft Exchange, Novell's GroupWise, and Lotus Notes.

2.6.11 Directory Services

Directory services, also known as the x.500 standard, provide location information for different entities on the network. Their main function is to act as an information booth, directing resource requests on the network to the location of the resource. When a client is requesting to use a printer or to find a server or even a specific application, the directory service tells the client where the resource is on the network and whether the resource is available.

This is a service that more and more networking systems are moving towards. As networking systems have developed, they have begun to include this feature. This is similar to a large company having an information desk, whereas a small company probably would not. Examples of computer systems that use directory services include Novell NetWare 4.11, Banyan VINES, Microsoft Exchange Server, and the soon-to-be-released Windows NT 5.0.

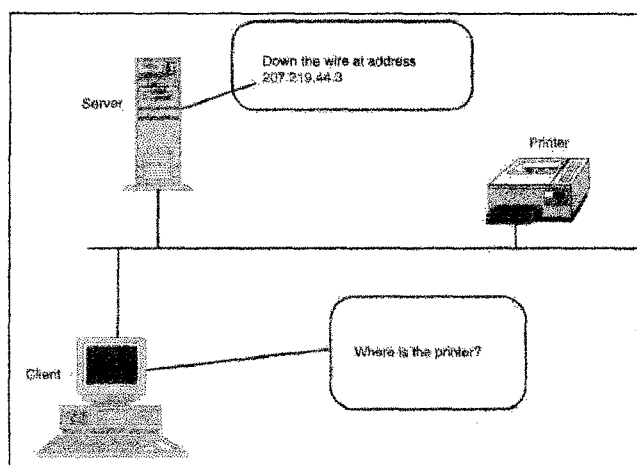


Figure 2.14 Directory services tells clients the location of resources on the network

2.6.12 Security Services

Another service provided by networks is security. Security is one of the most important elements involved in a network. When users share resources and data on a network, they should be able to control who can access the data or resource and what the user can do with it. An example of this is a file showing the financial records of a company. If this file is on a file server, it is important to be able to control who has access to the file. One step further, which is able to read and change the file also is a crucial consideration. This same example also applies to a shared printer. You might want to specify who can use the expensive colour laser printer or, more specifically, when a person can use this printer. As you can see, security is an important service on a network. Network administrators spend a great deal of time learning and setting up security.

Security services often deal with a user account database or something like the aforementioned directory services. This database of users often contains a list of names and passwords. When a person wants to access the network, he must log on to the network. Logging on is similar to trying to enter an office building with a security guard at the front door. Before you can enter the building, you must verify who you are against a list of people who are allowed access.

Security services often are intermingled with other services. Some services added to a network can utilize the security services of the system onto which they have been installed. An example of this is Microsoft Exchange Server. This messaging product can utilize the security services of an existing Windows NT Server. An example of a product that does not need to utilize an existing security system is Lotus Notes. Lotus Notes has its own independent security system.

CHAPTER THREE

NETWORKING STANDARDS

3.1 Standards

Before servers can provide services to clients, communications between the two computers must be established. Beyond the cables connecting the computers together, numerous processes operate behind the scenes to keep things running smoothly. For these processes to operate smoothly in a diverse networking environment, the computing community has settled on several standards and specifications that define the interaction and interrelation of the various components of network architecture. This chapter explores some of those standards. It begins by exploring the Open Systems Interconnection (OSI) reference model. This is an important model to learn, because all networking components and functionality are referenced within this model.

The chapter then moves from the OSI reference model to other industry standards that often encompass several areas of the OSI model at once. These standards include the TCP/IP reference model, the Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), the IEEE 802 standards, Network Driver Interface Specification (NDIS), and Open Data-Link Interface (ODI).

3.1.1 Standards Organisations and The ISO

The International Standards Organisation (ISO) is located in Geneva, Switzerland. ISO develops and publishes standards and co-ordinates the activities of all national standardisation bodies. In 1978, the ISO released a set of specifications that described a network architecture for connecting dissimilar devices. The original

document applied to systems that were open to each other because they could all use the same protocols and standards to exchange information.

In 1984, the ISO released a revision of this model and called it the Open Systems Interconnection (OSI) reference model. The 1984 revision has become an international standard and serves as a guide for networking (Glen Berg, 1998).

This model is the best known and most widely used guide to describe networking environments. Vendors design network products based on the specifications of the OSI model. It provides a description of how network hardware and software work together in a layered fashion to make communications possible. It provides a structured and consistent approach for describing, understanding, and implementing networks. The OSI Model:

- ◆ Provides general design guidelines for data-communications systems
- ◆ Provides a standard way to describe how layers of data-communications systems interact
- ◆ Divides communication problems into standard layers, facilitating the development of network products and encouraging “mix and match” interchangeability of network components
- ◆ Promotes the development of a global internetwork in which disparate systems can freely share network data and resources
- ◆ Is a tool for learning how networks function

3.2 The OSI Reference Model

The most commonly used model is the Open Systems Interconnection (OSI) reference model. The OSI model, first released in 1984 by the International Standards Organisation (ISO), provides a useful structure for defining and describing the various processes underlying networking communications.

The OSI model is an architecture that divides network communication into seven layers. Each layer covers different network activities, equipment or protocols. Figure 3.1 illustrates the layers of the OSI model. Layering specifies different functions and services at different levels: each OSI layer has well-defined networking functions and the functions of each layer communicate and work with the functions of the layers immediately above and below it.

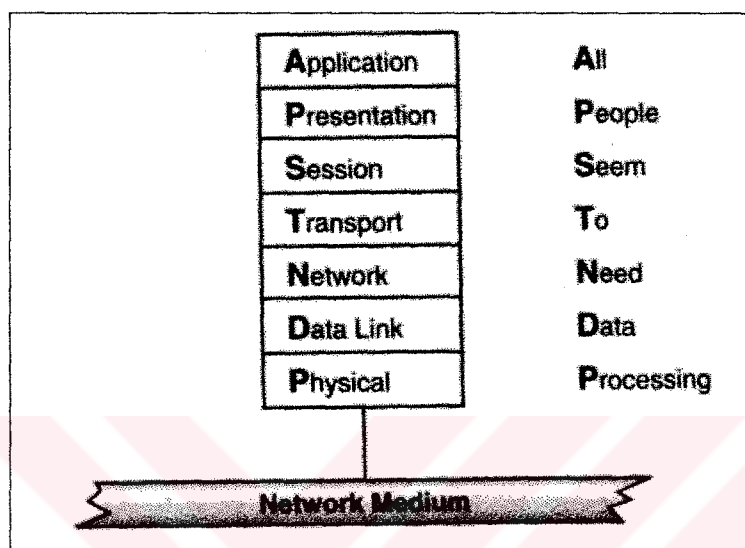


Figure 3.1 The OSI model has seven layers

Layer 1, the Physical layer, or Hardware layer, as some call it, consists of protocols that control communication on the network media. Essentially, this layer deals with how data is transferred across the transmission media. At the opposite end, Layer 7, the Application layer, interfaces the network services with the applications in use on the computer. These services, such as file and print services are discussed in Chapter 2. The five layers in between—Data Link, Network, Transport, Session, and Presentation—perform intermediate communication tasks. In essence the OSI model is a framework that describes how a function from one computer is transmitted to another computer on the network. Each layer provides some service or action that prepares the data for delivery over the network to another computer. The layers are separated from each other by boundaries called interfaces. All requests are passed from one layer, through the interface, to the next layer. Each layer builds upon the standards and activities of the layer below it (Glen Berg, 1998).

3.2.1 How Peer OSI Layers Communicate

Communication between OSI layers is both vertical within the OSI layers, and also horizontal between peer layers in another computer. This is important to understand, because it affects how data is passed within a computer, as well as between two computers.

When information is passed within the OSI model on a computer, each protocol layer adds its own information to the message being sent. This information takes the form of a header added to the beginning of the original message. The sending of a message always goes down the OSI stack, and hence headers are added from the top to the bottom.

When the message is received by the destination computer, each layer removes the header from its peer layer. Thus at each layer headers are removed (stripped) by the receiving computer after the information in the header has been utilised. Stripped headers are removed in the reverse order in which they were added. That is, the last header added by the sending computer, is the first one stripped off and read by the receiving computer. In summary, the information between the layers is passed along vertically. The information between computers is essentially horizontal, though, because each layer in one computer talks to its respective layer in the other computer.

It should probably be noted that the Physical layer does not append a header on to the information, because this layer deals with providing a transmission route between computers. An analogy to this is when one sends a courier package. To send a package, you place documents into an envelope (header no. 1). This envelope is addressed (header no. 2). The Courier Company places its documentation on the package (header no. 3). This package is then moved down the road in a vehicle (the transmission pathway). At the receiving end, the recipient strips off the courier documentation (removing header no. 3), then strips off the package and addressing, (the removal of headers no. 2 and no. 1), and now has the documents at hand.

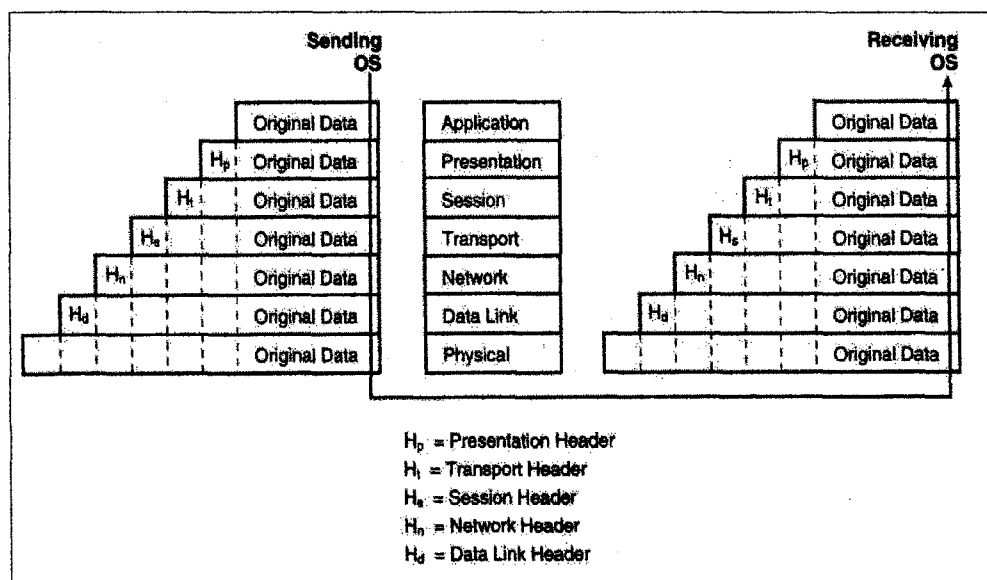


Figure 3.2 Each layer, except the Physical layer, adds a header to the frame as it travels down the OSI layers, and removes it as it travels up the OSI layers

3.2.2 Protocol Stacks

The OSI model (and other non-OSI protocol standards) breaks the complex process of network communication into layers. Each layer represents a category of related tasks. A protocol stack is an implementation of this layered protocol architecture. The protocols and services associated with the protocol stack interact to prepare, transmit, and receive network data (Glen Berg, 1998).

It is important to understand just what is meant by the terms "protocol" and "protocol stack." Often when people talk about protocol, they mention terms such as TCP/IP or IPX. This terminology can be misleading, for although these terms refer to protocols, they are a specific type of protocol: transport protocols. These transport protocols often do not encompass the entire mechanism for transferring communications. Two computers must run compatible protocol stacks before they can communicate, because each layer in one computer's protocol stack must interact with a corresponding layer in the other computer's protocol stack. To place this concept into perspective, imagine two people wishing to communicate. If one is blind and the other is deaf, there will be a communication problem. Both people need

to convey the thought through some form of media. However, the blind person uses voice to transmit, which requires the receiving person to use hearing, while the deaf person uses sign language to transmit, which requires the receiving person to use sight.

3.3 Conceptualising the Layers of the OSI Model

OSI model has 7 layers from the lowest layer (the physical connections) to the highest (user's applications). Each layer is able to communicate with the layer immediately above it or the layer immediately below it. The following sections provide a more detailed exposition of each of the seven layers of the OSI model.

3.3.1 OSI Physical Layer Concepts

Layer 1, the bottommost layer of the OSI model, is the Physical layer. This layer transmits the unstructured raw bit stream over a physical medium (such as the network cable). Although the OSI Physical layer does not define the media used, this layer is concerned with all aspects of transmitting and receiving data on the network media. By not defining the media, this layer is not responsible for saying whether a cable should be made of silver, copper, or gold. Specifically, the Physical layer is concerned with transmitting and receiving bits. This layer defines several key characteristics of the Physical network, including the following:

- ◆ Physical structure of the network (physical topology)
- ◆ Mechanical and electrical specifications for using the medium
- ◆ Bit transmission, encoding, and timing

Although the Physical layer does not define the physical medium, it defines clear requirements that the medium must meet. These specifications differ depending on the physical medium. Ethernet for UTP, for example, has different specifications from coaxial ethernet. This chapter is intended to give you an overview of the OSI model and which components work at each layer. The following sections examine in

detail the components that operate at each layer, presenting this detailed information from the bottom of the OSI model upwards.

The Physical layer is responsible for transmitting bits (zeros and ones) from one computer to another. The bits themselves have no defined meaning at this level. This layer defines data encoding and bit synchronisation, ensuring that when a transmitting host sends a 1 bit, it is received as a 1, not a 0 bit. This layer also defines how long each bit lasts and how each bit is translated into the appropriate electrical or optical impulse for the network cable.

3.3.2 OSI Data Link Layer Concepts

Layer 2, the Data Link layer, sends data frames from the Network layer to the Physical layer. On the receiving end, it packages raw bits from the Physical layer into data frames. A data frame is an organised, logical structure in which data can be placed. A primary function of the Data Link layer is to disassemble these frames into bits for transmission and then to reconstruct the frames from the bits received. The Data Link layer has other functions as well, such as addressing, error control, and flow control for a single link between network devices. The IEEE 802 standard divides the Data Link layer into two sub layers:

- ◆ **Media Access Control (MAC):** The MAC sub layer controls the means by which multiple devices share the same media channel for the transmission of information. This includes contention methods, or how data is transferred from a device, such as the network card, to the transmission medium. The MAC layer can also provide addressing information for communication between network devices
- ◆ **Logical Link Control (LLC):** The LLC sub layer establishes and maintains links between communicating devices.

3.3.2.1 Hardware Access at the Data Link Layer

As the preceding section mentions, the Data Link layer's MAC sub layer provides an interface to the network adapter card. The details necessary to facilitate access to

the network through the adapter card are thus assigned to the Data Link layer. Some of these details include the access control method and the network topology. The Data Link layer also controls the transmission method (for example, synchronous or asynchronous) used to access the transmission medium.

3.3.2.2 Addressing at the Data Link Layer

The Data Link layer maintains device addresses that enable messages to be sent to a particular device. The addresses are called physical device addresses. Physical device addresses are unique addresses associated with the networking hardware in the computer. In most cases (for example, Ethernet and Token Ring), the physical device address is burned into the NIC (network interface card) at the time the card is manufactured. Other devices, such as ARCNet, require the changing of DIP switches on the card to set a hardware address. The standards that apply to a particular network determine the format of the address. Because the address format is associated with the media access control method used, physical device addresses are frequently referred to as MAC addresses.

Packets on LANs are typically transmitted so that they are available to all devices on the network segment. Each device reads each frame far enough to determine the device address to which the frame is addressed. If the frame's destination address matches the device's own physical address, the rest of the frame is received. If the addresses do not match, the remainder of the packet is ignored. This is the case for all transmissions except for those sent as broadcasts. All devices on the network receive these broadcasts.

Bridges can be used to divide large networks into several smaller ones. Bridges use physical device addresses to determine which frames to leave on the current network segment and which to forward to devices on other network segments. Because they use physical device addresses to manage frame routing, bridges function at the level of the Data Link layer and are Data Link layer connectivity devices.

3.3.2.3 Error and Flow Control at the Data Link Layer

Several of the protocol layers in the OSI model play a role in the overall system of flow control and error control for the network. Flow control and error control are defined as follows:

- ◆ **Flow control:** Flow control determines the amount of data that can be transmitted in a given time period. Flow control prevents the transmitting device from overwhelming the receiver.
- ◆ **Error control:** Error control detects errors in received frames and requests retransmission of frames.

Error control of network communications often occurs at several different layers in the OSI model. At the Data Link layer, however, error control consists simply of confirmation that the receiving computer got all the packets the sending computer transmitted. Compare this to the transmission of physically shipped goods. When a company receives a shipment of goods one of the first things it does is see whether the correct number of boxes arrived and whether these boxes are damaged. This is essentially the type of error control that happens at the Data Link layer of the OSI model. But this error control in itself does not guarantee that the information being received by one computer is all there. Consider the model of the shipped boxes again: Just because all boxes arrived does not mean that the contents of all the boxes were correctly packed or that the merchandise in the boxes will work.

The Data Link layer's LLC sublayer provides error control and flow control for single links between communicating devices. The Network layer expands the system of error control and flow control to encompass complex connections that include routers, gateways, and internetworks.

3.3.3 OSI Network Layer Concepts

As you learned in the preceding section, the Data Link layer deals with communication between devices on the same network. Physical device addresses are

used to address data frames, and each device is responsible for monitoring the network and receiving frames addressed to that device.

Layer 3, the Network layer, is responsible for addressing messages and translating logical addresses and names into physical addresses. This layer also determines the route from the source to the destination computer. It determines which path the data should take based on network conditions, priority of service and other factors. It also manages traffic problems on the network, such as packet switching, routing and controlling the congestion of data. Within the Network layer, each network in the internetwork is assigned a network address that is used to route packets. The Network layer manages the process of addressing and delivering packets on internetworks.

3.3.3.1 Network Layer Addressing

You have already encountered the Data Link layer's physical device addresses that uniquely identify each device on a network. On larger networks, it is impractical to deliver network data solely by means of physical addresses. (Imagine if your network adapter had to check every packet sent from anywhere on the Internet to look for a matching physical address.) Larger networks require a means of routing and filtering packets to reduce network traffic and minimise transmission time. The Network layer uses logical network addresses to route packets to specific networks on an internetwork. Logical network addresses are assigned during configuration of the networks. A network installer must make sure that each network address is unique on a given internetwork.

The Network layer also supports service addresses. A service address specifies a channel to a specific process on the destination PC. The operating systems on most computers can run several processes at once. When a packet arrives, you must determine which process on the computer should receive the data in the packet. You do so by assigning service addresses, which identify upper-layer processes and

protocols. These service addresses are included with the physical and logical network addresses in the data frame.

To understand the many types of addresses used in networking, take a step back and analyse our information so far. The analogy to be used here is that of a house on a street in a residential neighbourhood. Imagine the address of the house is 1263 Main Street, Seattle, and Washington. As far as the postal system is concerned, all this information is the "address." In networking, the different components that really make up the address have names. The MAC address is similar to the house number-1263. The network address is similar to the street name-Main Street. Further information regarding the address-Seattle, Washington, in this case-is analogous to the logical network address.

A service address is similar to a room in a building. If you are delivering a packet to a company, often this package needs to go one step beyond just the front door. You can think of a service address representing a room or a department within a building, such as Apartment 404, 1263 Main St., Seattle, Washington.

Some service addresses, called well-known addresses, are universally defined for a given type of network. These well-known addresses are often used for services that are shared between many different vendors. An example of this would be a web service address. Many different vendors develop web servers and web browsers. For these components to operate with one another, a well-known address is needed.

3.3.3.2 Delivering Packets

Many internetworks often include redundant data paths that you can use to route messages. Typically, a packet passes from the local LAN segment of the source PC through a series of other LAN segments, until it reaches the LAN segment of the destination PC. The OSI Network layer oversees the process of determining paths and delivering packets across the internetwork.

This is similar to when you drive from your house to work. You can probably take a variety of routes, depending upon the events on the roadways, such as road work or traffic jams. Based on these conditions, you choose the route to take. This type of decision-making is what is done at the network level.

3.3.3.3 Connection-Oriented and Connectionless Modes

The OSI Network layer determines the route a packet will take as it passes through a series of different LANs from the source PC to the destination PC. The complexity and versatility of Network layer addressing gives rise to two different communication modes for passing messages across the network, both of which are recognised under OSI:

- ◆ **Connection-oriented mode:** Error correction and flow controls are provided at internal nodes along the message path.
- ◆ **Connectionless mode:** Internal nodes along the message path do not participate in error correction and flow control.

To understand the distinction between connection-oriented and connectionless communications, you must consider an important distinction between the OSI model's Data Link and Network layers. In theory, the Data Link layer facilitates the transmission of data across a single link between two nodes. The Network layer describes the process of routing a packet through a series of nodes to a destination on another link on the network. An example of this latter scenario is a message passing from a PC on one LAN segment through a series of routers to a PC on a distant part of the network. The internal nodes forwarding the packet also forward other packets between other end nodes.

In connection-oriented mode, the chain of links between the source and destination nodes forms a kind of logical pathway connection. The nodes forwarding the data packet can track which packet is part of which connection. This enables the internal nodes to provide flow control as the data moves along the path. For example, if an internal node determines that a link is malfunctioning, the node can send a

notification message backward, through the path to the source computer. Furthermore, because the internal node distinguishes among individual, concurrent connections in which it participates, this node can transmit (or forward) a "stop sending" message for one of its connections without stopping all communications through the node. Another feature of connection-oriented communication is that internal nodes provide error correction at each link in the chain. Therefore, if a node detects an error, it asks the preceding node to retransmit.

Connectionless mode does not provide these elaborate internal control mechanisms; instead, connectionless mode relegates all error-correcting and retransmitting processes to the source and destination nodes. The end nodes acknowledge the receipt of packets and retransmit if necessary, but internal nodes do not participate in flow control and error correction (other than simply forwarding messages between the end nodes). The advantage of connectionless mode is that connectionless communications can be processed more quickly and more simply because the internal nodes only forward data and thus don't have to track connections or provide retransmission or flow control.

The differences between connection-oriented and connectionless modes of communication may be easier to understand by analogy. Imagine talking to someone and then having her reaffirm that she understood what you have told her after each sentence. Connectionless mode is like having a conversation with someone, but the speaker just carries on and assumes that the listener understands. Connection-oriented is slower, yet more reliable. Connectionless is faster, but has less capability to correct errors (misunderstandings in the conversation example) as they occur. Connectionless mode does have its share of disadvantages, however, including the following:

- ◆ Messages sometimes get lost due to an overflowing buffer or a failed link along the pathway.
- ◆ If a message gets lost, the sender doesn't receive notification.
- ◆ Retransmission for error correction takes longer because a faulty transmission can't be corrected across an internal link.

It is important to remember that the OSI model is not a set of rules for communication; the OSI model is a framework in which models of communication are explained. As such, individual implementations of connectionless protocols can attenuate some of the preceding disadvantages. It is also important to remember that connection-oriented mode, although it places much more emphasis on monitoring errors and controlling traffic, doesn't always work either. Ultimately, the choice of connection-oriented or connectionless communications mode depends on interoperability with other systems, the premium for speed, and the cost of components.

3.3.3.4 Gateway Services

Routers can handle interconnection of networks whose protocols function in similar ways. When the rules differ sufficiently on the two networks, however, a more powerful device is required. A gateway is a device that can translate the different protocols used by different networks. Gateways can be implemented starting at the Network layer or at higher layers in the OSI model, depending on where the protocol translation is required.

3.3.4 OSI Transport Layer Concepts

Layer 4, the Transport layer, provides an additional connection level beneath the Session layer. The Transport layer ensures that packets are delivered error free, in sequence and with no losses or duplications. This layer repackages messages, dividing long messages into several packets and collecting small packets together in one package. This allows the packets to be transmitted efficiently over the network. At the receiving end, the Transport layer unpacks the messages, reassembles the original messages and typically sends an acknowledgement of receipt. The Transport layer provides flow control, error handling and is involved in solving problems concerned with the transmission and reception of packets.

3.3.4.1 Transport Layer Connection Services

Some services can be performed at more than one layer of the OSI model. In addition to the Data Link and Network layers, the Transport layer can take on some responsibility for connection services. The Transport layer interacts with the Network layer's connection-oriented and connectionless services and provides some of the essential quality control features. Some of the Transport layer's activities include the following:

- ◆ **Repackaging:** When large messages are divided into segments for transport, the Transport layer must repackage the segments when they are received before reassembling the original message.
- ◆ **Error control:** When segments are lost during transmission or when segments have duplicate segment IDs, the Transport layer must initiate error recovery. The Transport layer also detects corrupted segments by managing end-to-end error control using techniques such as checksums.
- ◆ **End-to-end flow control:** The Transport layer uses acknowledgements to manage end-to-end flow control between two connected devices. Besides negative acknowledgements, some Transport layer protocols can request the retransmission of the most recent segments.

3.3.5 OSI Session Layer Concepts

Layer 5, the Session layer, allows two applications on different computers to establish, use and end a connection called a session. This layer performs name recognition and the functions, such as security, needed to allow two applications to communicate over the network. The Session layer provides synchronisation between user tasks by placing checkpoints in the data stream. This way, if the network fails, only the data after the last checkpoint has to be retransmitted. This layer also implements dialog control between communicating processes, regulating which side transmits, when, for how long and so on. The Session layer also marks the data stream with checkpoints and monitors the receipt of those checkpoints. In the event

of a failure, the sending PC can retransmit, starting with the data sent after the last checkpoint, rather than resends the whole message.

3.3.6 OSI Presentation Layer Concepts

Layer 6, the Presentation layer, determines the format used to exchange data among networked computers. It can be called the network's translator. At the sending computer, this layer translates data from a format sent down from the Application layer into a commonly recognised, intermediary format. At the receiving computer, this layer translates the intermediary format into a format useful to that computer's Application layer. The Presentation layer is responsible for protocol conversion, translating the data, encrypting the data, changing or converting the character set, and expanding graphics commands. The Presentation layer also manages data compression to reduce the number of bits that need to be transmitted. The Presentation layer converts system-specific data from the Application layer into a common, machine-independent format that supports a more standardised design for lower protocol layers. The Presentation layer also attends to other details of data formatting, such as data encryption and data compression.

On the receiving end, the Presentation layer converts the machine-independent data from the network into the format required for the local system. This conversion could include the following:

- ◆ **Data formatting:** This is the organisation of the data. This topic is actually broken down into four subtopics:
 - **Bit-order translation:** When binary numbers are transmitted through a network, they are sent one bit at a time. The transmitting computer can start at either end of the number. Some computers start at the most significant digit (MSD); others start at the least significant digit (LSD). Essentially this has to do with whether information is read from right to left or from left to right.
 - **Byte-order translation:** Complex values generally must be represented with more than one byte, but different computers use different conventions to determine which byte should be transmitted first. Intel microprocessors, for

example, start with the least significant byte and are called little endian. Motorola microprocessors, on the other hand, start with the most significant byte and are called big endian. Byte-order translation might be needed to reconcile these differences when transferring data between a computer with an Intel processor and a Motorola processor.

- **Character code translation:** Different computers use different binary schemes for representing character sets. For instance: ASCII, the American Standard Code for Information Interchange, is used to represent English characters on all microcomputers and most minicomputers; EBCDIC, the Extended Binary Coded Decimal Interchange Code, is used to represent English characters on IBM mainframes and Shift JIS is used to represent Japanese characters.
- **File syntax translation:** File formats differ between computers. For instance, Macintosh files actually consist of two related files called a data fork and a resource fork. PC files, on the other hand, consist of a single file.
- ♦ **Encryption:** Encryption puts data into a form unreadable by unauthorised users. Encryption takes on two main forms:
 - **Public key:** This uses a rule of encryption (the key) and a known value. The manipulation of the key with a known value produces a mechanism for decrypting data.
 - **Private key:** This encryption uses one key. All components that have the key can decrypt the data.

3.3.7 OSI Application Layer Concepts

Layer 7, the topmost layer of the OSI model, is the Application layer. It serves as the window for application processes to access network services. This layer represents the services that directly support user applications, such as software for file transfers, for databases access, and for e-mail. The lower levels support these tasks performed at the application level. The application layer handles general network access, flow control and error recovery. The main purpose of this layer is

defining the protocols to be used between the application programs. Therefore, the applications such as SMTP, FTP and rlogin also operate at the application layer.

The Application layer, however, does provide an interface where by applications can communicate with the network. It is this interface that is often referred to as the Application Programming Interface (API). Some examples of APIs include MAPI (Messaging Programming Interface) and TAPI (Telephony Application Programming Interface). The Application layer also advertises the available services that your computer has to the network. An example of this is when you double-click on the Network Neighbourhood Icon in Windows 95 or Windows NT. The resulting picture shows a list of computers that have services available to network users.

3.4 Comparing TCP/IP to the OSI Reference Model

Although every network must use all seven layers of the OSI Reference Model in some form or another, not every network design provides distinct protocols or services that match all seven layers precisely. TCP/IP is one such networking design, with many layers that do not match up to each of the layers used by the OSI Reference Model (Eric A.Hall, 2000).

TCP/IP does not strictly conform to the OSI Reference Model. Some portions of the OSI Reference Model map directly to some of the protocols and services provided by TCP/IP, while many of the layers do not map to each other directly at all. For example, the actual delivery of data over the network is handled at the physical layer, and in this case, the wire is the physical layer. There are no services in TCP/IP that correspond with the physical or data-link layers. Rather, IP passes data to a network adapter's device driver, which provides an interface to the data-link layer in use with the physical layer. Figure 3.3 shows how TCP/IP matches up with the OSI Reference Model. Notice that TCP/IP does not provide any physical or data-link layer services directly, but instead relies on the local operating system for those services (Eric A.Hall, 2000).

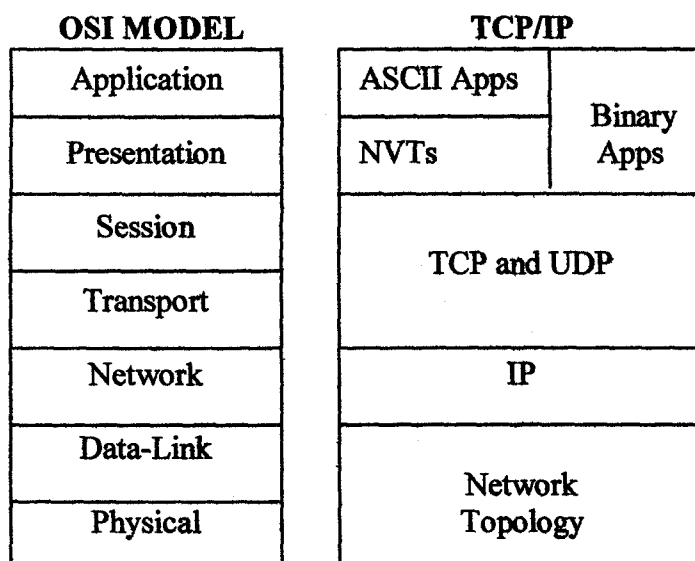


Figure 3.3 TCP/IP in comparison to the OSI Reference Model

The specific layers offered by TCP/IP include:

◆ **The Internet Protocol:** IP itself works at the network layer of OSI reference model. It is responsible for tracking the addresses of devices on the network, determining how IP datagrams are to be delivered, and sending IP packets from one host to another across a specific segment. In essence, IP provides a virtual representation of the network that is independent of any of the individual network segments, acting more like a national delivery service than a local courier service.

◆ **The Transport Protocols (TCP and UDP):** TCP/IP provides two protocols that work at the transport layer: TCP and UDP. TCP provides a highly monitored and reliable transport service, while UDP provides a simple transport with no error-correcting or flow-control services. It is also interesting to note that TCP and UDP also provide session layer services, managing all of the connections between the different hosts. When an application protocol such as HTTP is used to exchange data between a web client and a web server, the actual session-management for this exchange is handled by TCP.

◆ **Presentation Services:** TCP/IP does not provide a presentation layer service directly. However, some applications use a character-based presentation service called the Network Virtual Terminal (NVTs are a subset of the Telnet specification), while others might use IBM's NetBIOS or Sun's External Data Representation

(XDR) programming libraries for this service. In this regard, TCP/IP has many presentation layer services that it can use, but it does not have a formal service that every application protocol must use.

◆ **Application Protocols (HTTP, SMTP, etc):** TCP/IP provides an assortment of application protocols, providing the end-user applications with access to the data being passed across the transport protocols. These protocols include the Simple Message Transfer Protocol (SMTP), which is used by electronic mail systems to move mail messages around the Internet, and the Hyper-Text Transfer Protocol (HTTP), which is used by web browsers to access data stored on web servers, among many others.

All of these services get called upon whenever an application wants to exchange data with another application across the Internet. For example, a mail client will use the SMTP application protocol whenever a user wants to send a mail message to a remote mail server, and the SMTP protocol uses rules defined by the NVT specification whenever it exchanges data with TCP. In turn, TCP provides error-correction and flow-control services back to SMTP. IP is used to move the TCP segments between the source and destination networks, while hardware-specific protocols (like Ethernet-specific framing) will be used to move the IP packets between the various systems on the network itself (Eric A.Hall, 2000).

The OSI Reference Model does not contain a layer for internet protocols. Furthermore, the 7 layer reference model devotes an entire layer to session protocols, which have become much less important as computer systems have changed from large timesharing systems to private workstations. As a result, researchers who developed TCP/IP invented a new layering model. This section describes the new layering model briefly. The TCP/IP layering model, which is also called the Internet Layering Model or the Internet Reference Model, contains five layers as Figure 3.4 illustrates (Douglas E.Comer, 2001).

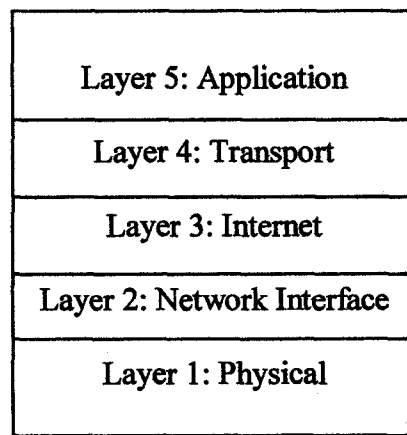


Figure 3.4 The five layers of the TCP/IP Reference Model

Four of the layers in the TCP/IP reference model correspond to one or more layers in the ISO reference model. However, the ISO model has no Internet Layer. This section summarizes the purpose of each layer.

- ◆ **Layer 1: Physical:** Layer 1 corresponds to basic network hardware just as Layer 1 in the ISO 7 layer reference model.
- ◆ **Layer 2: Network Interface:** Layer 2 protocols specify how to organize data into frames and how a computer transmits frames over a network, similar to Layer 2 protocols in the ISO reference model.
- ◆ **Layer 3: Internet:** Layer 3 protocols specify the format of packets sent across an internet as well as the mechanisms used to forward packets from a computer through one or more routers to a final destination.
- ◆ **Layer 4: Transport:** Layer 4 protocols, like layer 4 in the ISO model, specify how to ensure reliable transfer.
- ◆ **Layer 5: Application:** Layer 5 corresponds to layers 6 and 7 in the ISO model. Each layer 5 protocol specifies how one application uses an internet.

3.5 Standards that Utilise Multiple Levels of the OSI Model

The discussion in most of this chapter has focused on the explanation of the OSI model and its seven levels. This chapter has discussed what occurs at each level, and in some cases, has given examples of components that operate at these different levels. The remainder of this chapter looks at some other standards or protocols that

are common features of networks. These standards often encompass several layers of the OSI model at once. The three broad standards that will be examined are the following:

- ◆ SLIP and PPP
- ◆ The IEEE 802 suite of standards
- ◆ NDIS and ODI

3.5.1 Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP)

Two other standards vital to network communication are Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP). SLIP and PPP were designed to support dial-up access to networks based on the Internet transport protocols. SLIP is a simple protocol that functions at the Physical layer, whereas PPP is a considerably enhanced protocol that provides Physical layer and Data Link layer functionality. The relationship of both to the OSI model is shown in Figure 3.5.

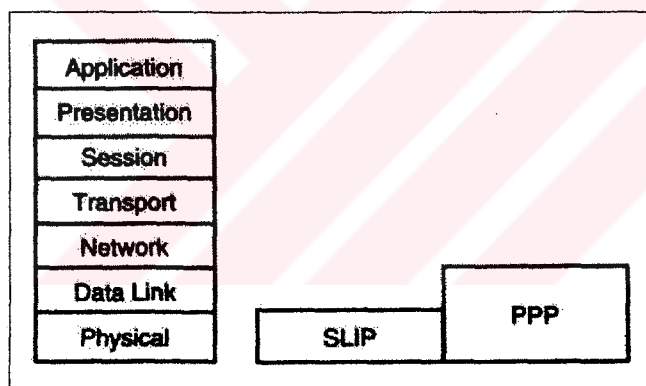


Figure 3.5 The relationship between SLIP, PPP and the OSI model

SLIP works on the Physical Layer of the OSI model while PPP works on both the Physical and Data Link layer. Although SLIP only works on the physical layer, sometimes we still call it a data link protocol. PPP and SLIP are both data link protocols that can be used for remote accessing the network.

SLIP (Serial Line IP) is a remote access protocol provides dial-up access to TCP/IP network. It transmits IP packets over serial connections. You can implement

a SLIP server or a SLIP client in the network. However, none of Microsoft's operating system such as Windows 95 or Windows NT supports SLIP server solution. SLIP is implemented as a client solution in Windows 95 and Windows NT for two purposes:

- ◆ Connecting other SLIP servers such as Unix SLIP servers.
- ◆ Configuring some network devices that are SLIP enabled.

Because the only network protocol supported by SLIP is TCP/IP, it requires fewer overheads than PPP. However, because SLIP lacks some features such as compression, dynamic IP address assignment as well as encryption, it is gradually being replaced by PPP. CSLIP (Compressed SLIP) provides the compression for the communication. However it is different from the SLIP

PPP, Point-to-Point Protocol, is a remote access protocol that provides dial-up access over serial lines. PPP supports several network protocols include NetBEUI, TCP/IP and IPX/SPX. PPP not only supports data compression but also provides password protection using PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) (Glen Berg, 1998).

Developed to provide dial-up TCP/IP connections, SLIP is an extremely rudimentary protocol that suffers from a lack of rigid standardisation in the industry, which sometimes hinders different vendor implementations of SLIP from operating with each other. Windows NT supports both SLIP and PPP from the client end using the Dial-Up Networking application. On the server end, Windows NT RAS (Remote Access Service) supports PPP but doesn't support SLIP. In other words, Windows NT can act as a PPP server but not as a SLIP server (Glen Berg, 1998).

SLIP is most commonly used on older systems or for dial-up connections to the Internet via SLIP-server Internet hosts.

PPP was defined by the Internet Engineering Task Force (IETF) to improve on SLIP by providing the following features:

- ◆ Security using password logon
- ◆ Simultaneous support for multiple protocols on the same link
- ◆ Dynamic IP addressing
- ◆ Improved error control

Different PPP implementations might offer different levels of service and negotiate service levels when connections are made. Due to its versatility, interoperability, and additional features, PPP is presently surpassing SLIP as the most popular serial-line protocol.

Certain dial-up configurations cannot use SLIP for the following reasons:

- ◆ SLIP supports the TCP/IP transport protocol only. PPP, however, supports TCP/IP, as well as a number of other transport protocols, such as NetBEUI, IPX, AppleTalk, and DECnet. In addition, PPP can support multiple protocols over the same link.

- ◆ SLIP requires static IP addresses. Because SLIP requires static or preconfigured IP addresses, SLIP servers do not support Dynamic Host Configuration Protocol (DHCP), which assigns IP addresses dynamically or when requested. (DHCP enables clients to share IP addresses so that a relatively small number of IP addresses can serve a larger user base.) If the dial-up server uses DHCP to assign an IP address to the client, the dial-up connection won't use SLIP

- ◆ SLIP does not support dynamic addressing through DHCP SLIP connections, therefore, cannot dynamically assign a WINS or DNS server.

Windows NT RAS (using PPP) offers a number of other interesting features, including the following:

- ◆ **PPP Multilink Protocol:** Multilink enables a single connection to use several physical pathways of the same type (such as modems, ISDN lines, and X.25 cards). Utilising multiple pathways for a single connection increases bandwidth and, therefore, performance.
- ◆ **NetBIOS Gateway:** A RAS server can connect a client running the NetBEUI protocol with a TCP/IP or IPX network by serving as a NetBIOS gateway.

- ♦ **IPX or IP Router:** A RAS server can act as a router for IPX/SPX and TCP/IP networks.

3.6 The IEEE 802 Family

The Institute of Electrical and Electronic Engineers (IEEE) is one of the largest professional organisations in the world, and is extremely influential with regard to setting standards. In February of 1980, the IEEE implemented a task force to develop a set of standards for connectivity between Network Interface Cards (NICs) and transmission media. This task force was known as the 802 committee. This 802 committee was broken down into several different subcommittees that were each responsible for some different implementation of data transfer that occurs at the Data Link level of the OSI model. These IEEE standards have also been adopted by ISO, and they are referred to as ISO 8802. The IEEE 802 series of standards, as well as all the other IEEE standards and research, can be found at <http://standards.ieee.org/802/index.html>. Figure 3.6 illustrates the position each standard occupies in the OSI reference model (Glen Berg, 1998).

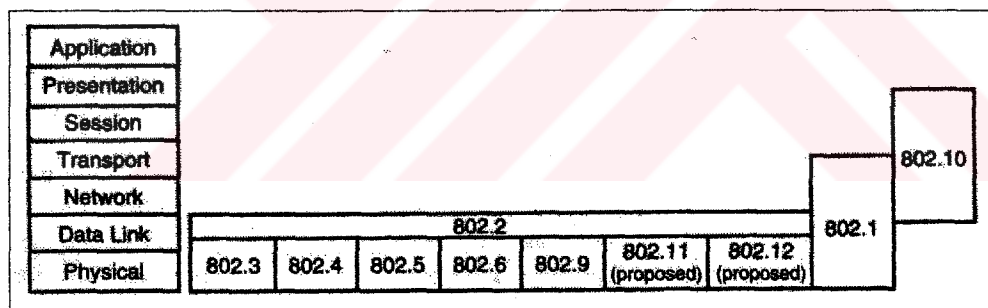


Figure 3.6 The relationship between the IEEE 802 standards and the OSI model

- ♦ **IEEE 802.1:** This standard is actually one that goes beyond the Data Link layer of the OSI model. This is a general standard for network management, and provides network management standards to the other 802 standards in the OSI model. This standard actually covers all layers from the Physical to the Transport layer.

◆ **IEEE 802.2:** The IEEE 802.2 standard defines an LLC sublayer that is used by other lower-layer protocols. Because these lower-layer protocols can use a single LLC protocol layer, Network layer protocols can be designed independently of both the network's Physical layer and MAC sublayer implementations.

◆ **IEEE 802.3:** The IEEE 802.3 standard defines a network derived from the ethernet network originally developed by Digital, Intel, and Xerox. This standard defines characteristics related to the MAC sublayer of the Data Link layer and the OSI Physical layer. With one minor distinction-frame type-IEEE 802.3 Ethernet functions identically to DIX Ethernet v.2. These two standards can even coexist on the same cabling system, although devices using one standard cannot communicate directly with devices using the other.

◆ **IEEE 802.4:** The 802.4 standard describes a network with a bus physical topology that controls media access with a token mechanism. This standard was designed to meet the needs of industrial automation systems but has gained little popularity. Both baseband and broadband (using 75-ohm coaxial cable) configurations are available.

◆ **IEEE 802.5:** The IEEE 802.5 standard was derived from IBM's Token Ring network, which employs a ring logical topology and token-based media access control. Data rates of 1, 4, and 16Mbps have been defined for this standard.

◆ **IEEE 802.6:** The IEEE 802.6 standard describes a MAN standard called Distributed Queue Dual Bus (DQDB). Much more than a data network technology, DQDB is suited to data, voice, and video transmissions. The network is based on fiber-optic cable in a dual-bus topology, and traffic on each bus is unidirectional. When operated in pairs, the two buses provide a fault-tolerant configuration. Bandwidth is allocated by using time slots, and both synchronous and asynchronous modes are supported.

◆ **IEEE 802.7:** This standard deals with integrating broadband solutions into a network environment. This standard is currently under development. The workgroup for this set of standards is currently inactive.

◆ **IEEE 802.8:** This standard deals with methods of implementing fiber optic technology into networking environments. This standard is currently under development.

♦ **IEEE 802.9:** The IEEE 802.9 standard supports a 10Mbps asynchronous channel, along with 96 64Kbps (6Mbps total bandwidth) channels that can be dedicated to specific data streams. The total bandwidth is 16Mbps. This standard is called Isochronous Ethernet (IsoEnet) and is designed for settings with a mix of bursty and time-critical traffic.

♦ **IEEE 802.10:** This standard deals with security and encryption standards. This standard is currently under development.

♦ **IEEE 802.11:** IEEE 802.11 is a standard for wireless LANs and is currently under development. A CSMA/CD method has been approved, but the final standard is pending.

♦ **IEEE 802.12:** The IEEE 802.12 standard is based on a 100Mbps proposal promoted by AT&T, IBM, and Hewlett-Packard. Called 100VG-AnyLAN, the network is based on a star wiring topology and a contention-based access method whereby devices signal the wiring hub when they need to transmit data. Devices can transmit only when granted permission by the hub.

♦ **IEEE 802.14:** The 802.13 designations are not used; hence the last standard is known as 802.14. This standard is for transmitting data over cable TV lines. The committee is currently looking at a hybrid fiber/coax media. This is one of the up and coming areas for fast Internet access from a person's home.

♦ **IEEE 802.3 and IEEE 802.5 Media:** IEEE 802.2 (topology independent), IEEE 802.3 (based on Ethernet), and IEEE 802.5 (based on token ring) are the most commonly used IEEE 802 standards. The IEEE 802.3 Physical layer definition describes signalling methods (both baseband and broadband) data rates media, and topologies. Several Physical layer variants also have been defined. Each variant is named following a convention that states the signalling rate (1 or 10) in Mbps, baseband (BASE) or broadband (BROAD) mode, and a designation of the media characteristics.

The following list details the IEEE 802.3 variants of transmission media:

♦ **1BASE5:** This 1Mbps network utilises UTP cable with a signal range up to 500 meters (250 meters per segment). A star physical topology is used.

- ◆ **10BASE5:** Typically called Thick Ethernet, or Thicknet, this variant uses a large diameter (10mm) "thick" coaxial cable with a 50-ohm impedance. A data rate of 10Mbps is supported with a signalling range of 500 meters per cable segment on a physical bus topology.
- ◆ **10BASE2:** Similar to Thicknet, this variant uses a thinner coaxial cable that can support cable runs of 185 meters. (In this case, the " 2" indicates only an approximate cable range.) The transmission rate remains at 10Mbps, and the physical topology is a bus. This variant typically is called Thin Ethernet, or Thinnet.
- ◆ **10BASE-F:** This variant uses fiber-optic cables to support 10Mbps signalling with a range of 4 kilometres. Three subcategories include 10BASE-FL (fiber link), 10BASE-FB (fiber backbone), and 10BASE-FP (fiber passive).
- ◆ **10BROAD36:** This broadband standard supports channel signal rates of 10Mbps. A 75-ohm coaxial cable supports cable runs of 1,800 meters (up to 3,600 meters in a dual-cable configuration) using a physical bus topology.
- ◆ **10BASE-T:** This variant uses UTP cable in a star physical topology. The signalling rate remains at 10Mbps, and devices can be up to 100 meters from a wiring hub.
- ◆ **100BASE-X:** This proposed standard is similar to 10BASE-T but supports 100Mbps data rates.

3.7 NDIS and ODI

The Network Driver Interface Specification (NDIS), a standard developed by Microsoft and 3Com Corp., 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 a NDIS-compliant protocol stack can operate with a 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 you 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. Originally, ODI was written for NetWare and Macintosh environments. Like NDIS, ODI provides rules that establish a vendor-neutral interface between the protocol stack and the adapter driver. This interface also enables one or more network drivers to support one or more protocol stacks. Essentially NDIS and ODI are standards to which a person wishing to develop a driver for a network card or a protocol will adhere. Standards are similar to how cars are manufactured. Cars destined for England are designed with the steering wheel on the right-hand side of the car. Cars for North America are designed with the steering wheel on the left-hand side of the car. This standard does not change the function of the car or the steering wheel; conforming to it simply ensures that the car will function properly for each country's driving environment. NDIS and ODI are similar. Neither standard changes the function of the network card or the network card's driver; they simply are standards enabling the network card to function in each operating system's environment (Glen Berg, 1998).

CHAPTER FOUR

NETWORK TRANSMISSION MEDIA

4.1 Introduction

On any network, the various entities must communicate through some form of media. Human communication requires some sort of media, whether it is technologically based (as are telephone wires) or whether it simply involves the use of our senses to detect sound waves propagating through the air. Likewise, computers can communicate through cables, light, and radio waves. Transmission media enable computers to send and receive messages but, as in human communication, do not guarantee that the messages will be understood.

This chapter discusses some of the most common network transmission media. One broad classification of this transmission media is known as guided transmission media. This includes cable types such as coaxial cable, shielded twisted-pair cable, unshielded twisted-pair cable, and fiber-optic cable. Another type of transmission is known as wireless; this transmission includes all forms of wireless communications. To lay the groundwork for these issues, the chapter begins with an introduction to the frequencies in the electromagnetic spectrum and a look at some important characteristics of the transmission media that utilize these different frequencies to transmit the data.

4.2 Transmission Frequencies

Transmission media make possible the transmission of the electronic signals from one computer to another. These electronic signals express data values in the form of binary (on/off) impulses, which are the basis for all computer information (represented as 1s and 0s). These signals are transmitted between the devices on the

network, using some form of transmission media (such as cables or radio) until they reach the desired destination computer(Glen Berg, 1998).

All signals transmitted between computers consist of some form of electromagnetic (EM) waveform, ranging from radio frequencies through microwaves and infrared light. Different media are used to transmit the signals, depending on the frequency of the EM waveform.

The electromagnetic spectrum consists of several categories of waveforms, including radio frequency waves, microwave transmissions, and infrared light. The frequency of a wave is dependent upon the number of waves or oscillations that occur during a period of time(Glen Berg, 1998).

Radio frequency waves are often used for LAN signaling. Radio frequencies can be transmitted across electrical cables (twisted-pair or coaxial) or by radio broadcast.

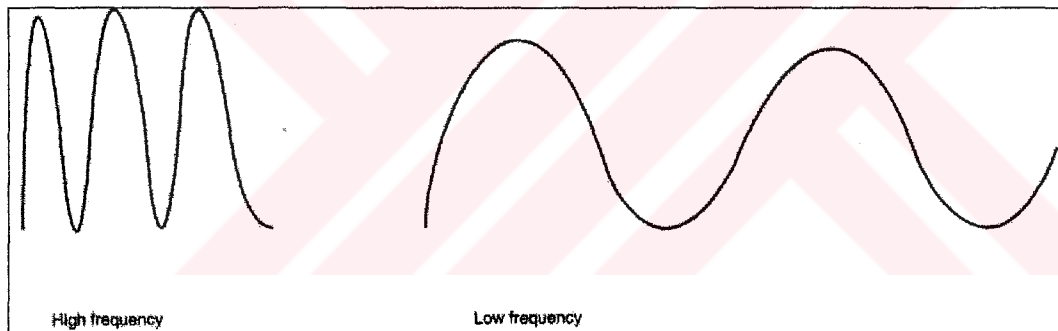


Figure 4.1 High frequency and low frequency waves

Microwave transmissions can be used for tightly focused transmissions between two points. Microwaves are used to communicate between earth stations and satellites, for example, and they are also used for line-of-sight transmissions on the earth's surface. In addition, microwaves can be used in low-power forms to broadcast signals from a transmitter to many receivers. Cellular phone networks are examples of systems that use low-power microwave signals to broadcast signals.

Infrared light is ideal for many types of network communications. Infrared light can be transmitted across relatively short distances and can be either beamed between two points or broadcast from one point to many receivers. Infrared and higher frequencies of light also can be transmitted through fiber-optic cables. A typical television remote control uses infrared transmission.

4.3 Transmission Media Characteristics

Each type of transmission media has special characteristics that make it suitable for a specific type of service. You should be familiar with these characteristics for each type of media:

- ◆ Cost
- ◆ Installation requirements
- ◆ Bandwidth
- ◆ Band usage (baseband or broadband)
- ◆ Attenuation
- ◆ Immunity from electromagnetic interference

4.3.1 Cost

One main factor in the purchase decision of any networking component is the cost. Often the fastest and most robust transmission media is desired, but a network designer must often settle for something that is slower and less robust, because it more than suffices for the business solution at hand. The major deciding factor is almost always price. It is a rare occasion in the field that the sky is the limit for installing a network. As with nearly everything else in the computer field, the fastest technology is the newest, and the newest is the most expensive. Over time, economies of scale bring the price down, but by then, a newer technology comes along.

4.3.2 Installation Requirements

Installation requirements typically involve two factors. One is that some transmission media require skilled labor to install. Bringing in a skilled outside technician to make changes to or replace resources on the network can bring about undue delays and costs. The second has to do with the actual physical layout of the network. Some types of transmission media install more easily over areas where people are spread out, whereas other transmission media are easier to bring to clusters of people or a roaming user.

4.3.3 Bandwidth

In computer networking, the term bandwidth refers to the measure of the capacity of a medium to transmit data. A medium that has a high capacity, for example, has a high bandwidth, whereas a medium that has limited capacity has a low bandwidth. Data transmission rates are frequently stated in terms of the bits that can be transmitted per second. An Ethernet LAN theoretically can transmit 10 million bits per second and has a bandwidth of 10 megabits per second (Mbps).

The bandwidth that a cable can accommodate is determined in part by the cable's length. A short cable generally can accommodate greater bandwidth than a long cable, which is one reason all cable designs specify maximum lengths for cable runs.

4.3.4 Band Usage (Baseband or Broadband)

The two ways to allocate the capacity of transmission media are with baseband and broadband transmissions. Baseband devotes the entire capacity of the medium to one communication channel. Broadband enables two or more communication channels to share the bandwidth of the communications medium.

Baseband is the most common mode of operation. Most LANs function in baseband mode, for example. Baseband signaling can be accomplished with both analog and digital signals.

Although you might not realize it, you have a great deal of experience with broadband transmissions. Consider, for example, that the TV cable coming into your house from an antenna or a cable provider is a broadband medium. Many television signals can share the bandwidth of the cable because each signal is modulated using a separately assigned frequency. You can use the television tuner to select the frequency of the channel you want to watch.

This technique of dividing bandwidth into frequency bands is called frequency-division multiplexing (FDM) and works only with analog signals. Another technique, called time-division multiplexing (TDM), supports digital signals. Figure 4.2 contrasts the difference between baseband and broadband modes of operation.

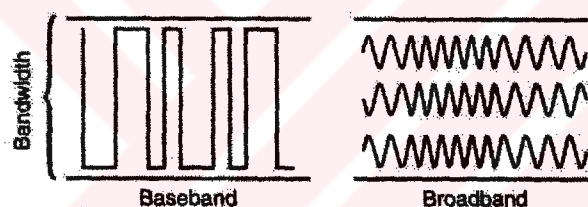


Figure 4.2 Baseband and Broadband Transmission Modes

4.3.4.1 Frequency-Division Multiplexing

Figure 4.3 illustrates frequency-division multiplexing (FDM). This technique works by converting all data channels to analog form. Each analog signal can be modulated by a separate frequency (called a "carrier frequency") that makes it possible to recover that signal during the demultiplexing process. At the receiving end, the demultiplexer can select the desired carrier signal and use it to extract the data signal for that channel.

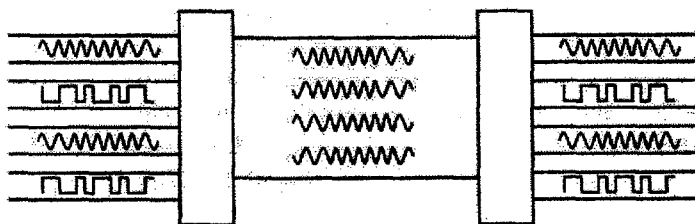


Figure 4.3 Frequency-division multiplexing

FDM can be used in broadband LANs. (A standard for Ethernet also exists.) One advantage of FDM is that it supports bi-directional signaling on the same cable. That is, a frequency can originate from both ends of the transmission media at once.

4.3.4.2 Time-Division Multiplexing

Time-division multiplexing (TDM) divides a channel into time slots that are allocated to the data streams to be transmitted, as illustrated in Figure 4.4. If the sender and receiver agree on the time-slot assignments, the receiver can easily recover and reconstruct the original data streams.

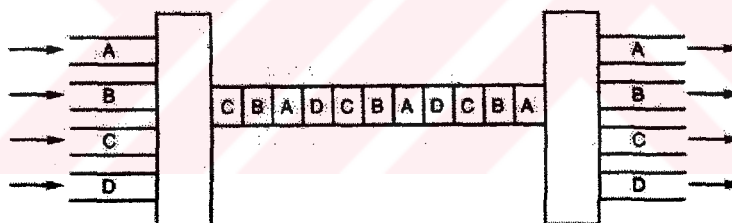


Figure 4.4 Time division multiplexing steams data depending on the data's allocated time slots

TDM transmits the multiplexed signal in baseband mode. Interestingly, this process makes it possible to multiplex a TDM signal as one of the data channels on an FDM system.

4.3.5 Attenuation

Attenuation is a contributing factor to why cable designs must specify limits in the lengths of cable runs. When signal strength falls below certain limits, the electronic equipment that receives the signal can experience difficulty isolating the original signal from the noise present in all electronic transmissions. The effect is exactly like trying to tune in distant radio signals. Even if you can lock on to the signal on your radio, the sound generally still contains more noise than the sound for a local radio station. As mentioned in the previous chapters, repeaters are used to regenerate signals; hence one solution to deal with attenuation is to add a repeater.

4.3.6 Electromagnetic Interference

Electromagnetic interference (EMI) consists of outside electromagnetic noise that distorts the signal in a medium. When you listen to an AM radio, for example, you often hear EMI in the form of noise caused by nearby motors or lightning. Some network media are more susceptible to EMI than others.

Crosstalk is a special kind of interference caused by adjacent wires. Crosstalk occurs when the signal from one wire is picked up by another wire. You may have experienced this when talking on a telephone and hearing another conversation going on in the background. Crosstalk is a particularly significant problem with computer networks because large numbers of cables often are located close together, with minimal attention to exact placement.

4.4 Guided Transmission Media

The following sections discuss three types of guided transmission media, as follows:

- ◆ Coaxial cable
- ◆ Twisted-pair cable
- ◆ Fiber-optic cable

4.4.1 Coaxial Cable

Coaxial cables were the first cable types used in LANs. As shown in Figure 4.5, coaxial cable gets its name because two conductors share a common axis; the cable is most frequently referred to as a "coax." A type of coaxial cable that you may be familiar with is your television cable.

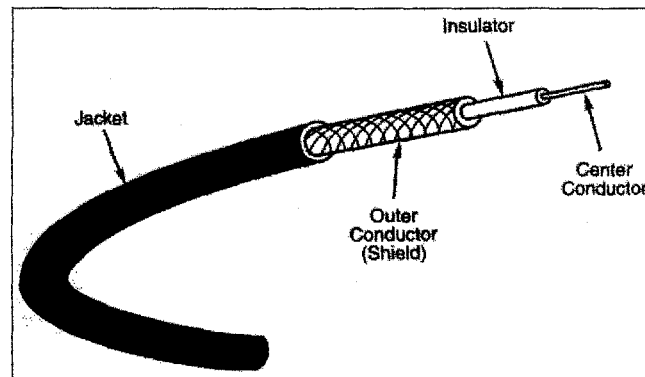


Figure 4.5 The structure of coaxial cable consists of four major components

The components of a coaxial cable are as follows:

- ◆ A center conductor, although usually solid copper wire, is sometimes made of stranded wire.
- ◆ An outer conductor forms a tube surrounding the center conductor. This conductor can consist of braided wires, metallic foil, or both. The outer conductor frequently called the shield serves as a ground and also protects the inner conductor from EMI.
- ◆ An insulation layer keeps the outer conductor spaced evenly from the inner conductor.
- ◆ A plastic encasement (jacket) protects the cable from damage.

4.4.1.1 Types of Coaxial Cable

The two basic classifications for coaxial cable are as follows:

- ◆ Thinnet
- ◆ Thicknet

4.4.1.1.1 Thinnet

Thinnet is a light and flexible cabling medium that is inexpensive and easy to install. Thinnet is approximately .25 inches (6 mm) in thickness. Thinnet cable can reliably transmit a signal for 185 meters (about 610 feet). Table 4.1 illustrates some Thinnet classifications.

Table 4.1 Thinnet Cable Classifications

Cable	Description	Impedance
RG-58/U	Solid copper center	50-ohm
RG-58 A/U	Wire strand center	50-ohm
RG-58 C/U	Military version of RG-58 A/U	50-ohm
RG-59	Cable TV wire	75-ohm
RG-62	ARCnet specification	93-ohm

4.4.1.1.2 Thicknet

Thicknet is thicker than Thinnet. Thicknet coaxial cable is approximately 0.5 inches (13 mm) in diameter. Because it is thicker and does not bend as readily as Thinnet, Thicknet cable is harder to work with. A thicker center core, however, means that Thicknet can carry more signals a longer distance than Thinnet. Thicknet can transmit a signal approximately 500 meters (1,650 feet). Thicknet can be used to connect two or more small Thinnet LANs into a larger network. Because of its greater size, Thicknet is also more expensive than Thinnet. However, Thicknet can be installed relatively safely outside, running from building to building.

4.4.1.2 Coaxial Characteristics

You should be familiar with the installation, cost, bandwidth, and EMI resistance characteristics of coaxial cable. The following sections discuss some of the characteristics of coaxial cable.

4.4.1.2.1 Installation

Coaxial cable is typically installed in two configurations: daisy chain (from device to device-Ethernet) and star (ARCnet). The daisy chain is shown in Figure 4.6.

The Ethernet cabling shown in the figure is an example of Thinnet, which uses RG-58 type cable. Devices connect to the cable by means of T connectors. Cables are used to provide connections between T connectors. One characteristic of this type of cabling is that the ends of the cable run must be terminated by a special connector, called a terminator. The terminator contains a resistor that is matched to the characteristics of the cable. The resistor prevents signals that reach the end of the cable from bouncing back and causing interference.

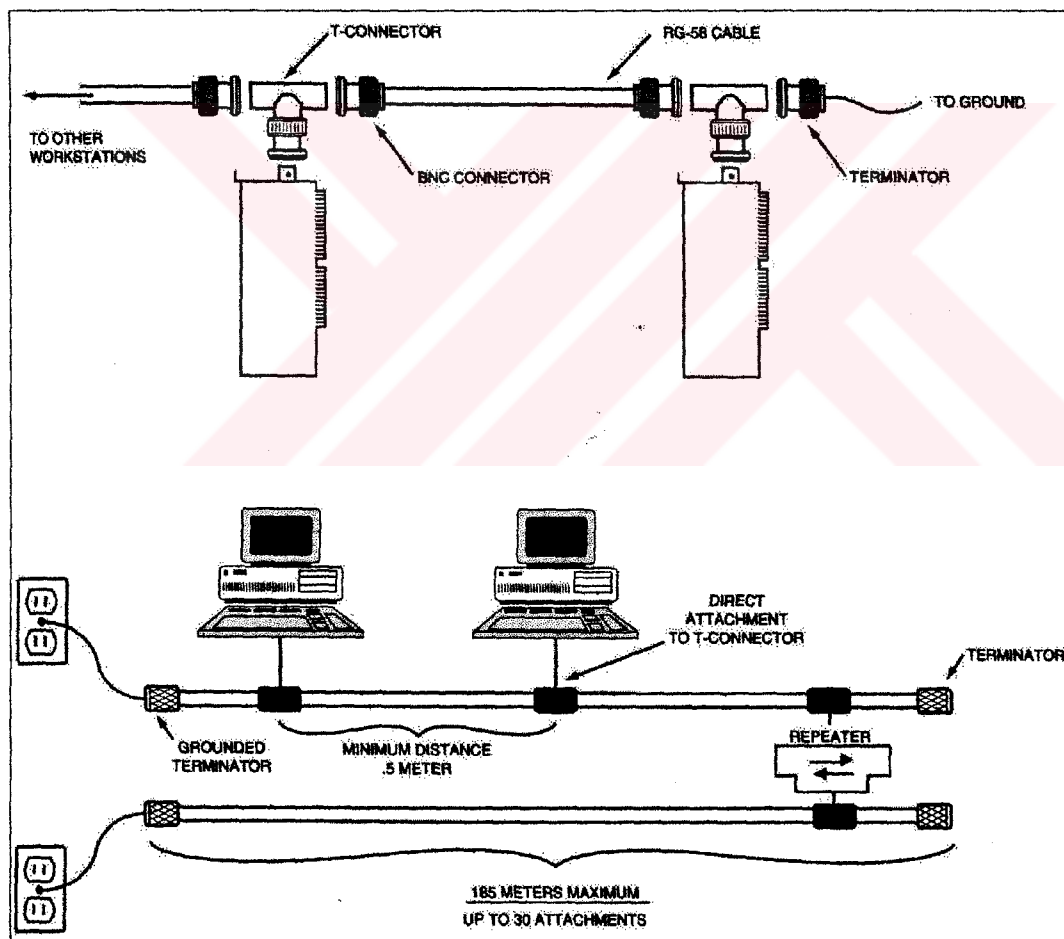


Figure 4.6 Coaxial cable wiring configuration

Coaxial cable is reasonably easy to install because the cable is robust and difficult to damage. In addition, connectors can be installed with inexpensive tools and a bit of practice. The device-to-device cabling approach can be difficult to reconfigure, however, when new devices cannot be installed near an existing cabling path.

4.4.1.2.2 Cost

The coaxial cable used for Thinnet falls at the low end of the cost spectrum, whereas Thicknet is among the more costly options.

4.4.1.2.3 Capacity

LANs that employ coaxial cable typically have a bandwidth between 2.5 Mbps (ARCNet) and 10Mbps (Ethernet). Thicker coaxial cables offer higher bandwidth, and the potential bandwidth of coaxial is much higher than 10Mbps.

4.4.1.2.4 EMI Characteristics

All copper media are sensitive to EMI, although the shield in coax makes the cable fairly resistant. Coaxial cables, however, do radiate a portion of their signal, and electronic eavesdropping equipment can detect this radiated signal.

4.4.1.3 Connectors for Coaxial Cable

Two types of connectors are commonly used with coaxial cable. The most common is the British Naval Connector (BNC). Figure 4.8 depicts the characteristics of BNC connectors and Thinnet cabling.

Key issues involving Thinnet cabling are

- ◆ A BNC T connector connects the network board in the PC to the network. The T connector attaches directly to the network board.
- ◆ BNC cable connectors attach cable segments to the T connectors.

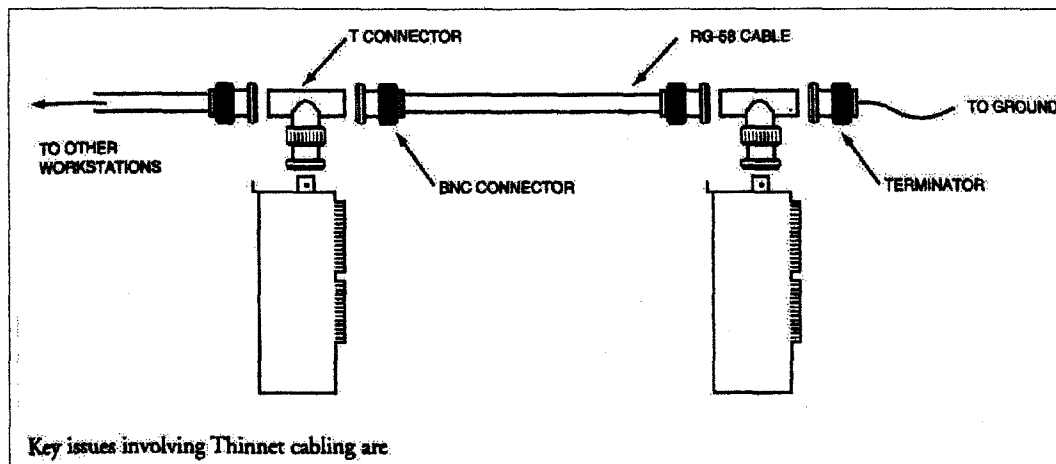


Figure 4.7 Thinnet is connected using BNC T-connectors

- ◆ A BNC barrel connector connects to Thinnet cables.
- ◆ Both ends of the cable must be terminated. A BNC terminator is a special connector that includes a resistor that is carefully matched to the characteristics of the cable system.
- ◆ One of the terminators must be grounded. A wire from the connector is attached to a grounded point, such as the center screw of a grounded electrical outlet.

In contrast, Thicknet uses N-connectors, which screw on rather than use a twist lock. As with Thinnet, both ends of the cable must be terminated, and one end must be grounded. Workstations don't connect directly to the cable with Thicknet. Instead, a connecting device called a transceiver is attached to the Thicknet cable. This transceiver has a port for an AUI connector (which looks deceptively like a joystick connector), and an AUI cable (also called a transceiver cable or a drop cable) connects the workstation to the Thicknet medium. Transceivers can connect to Thicknet cables in the following two ways:

- ◆ Transceivers can be connected by cutting the cable and splicing N-connectors and a T connector on the transceiver. Because it is so labor-intensive, this original method of connecting is used rather infrequently.
- ◆ The more common approach is to use a clamp-on transceiver, which has pins that penetrate the cable without the need for cutting it.

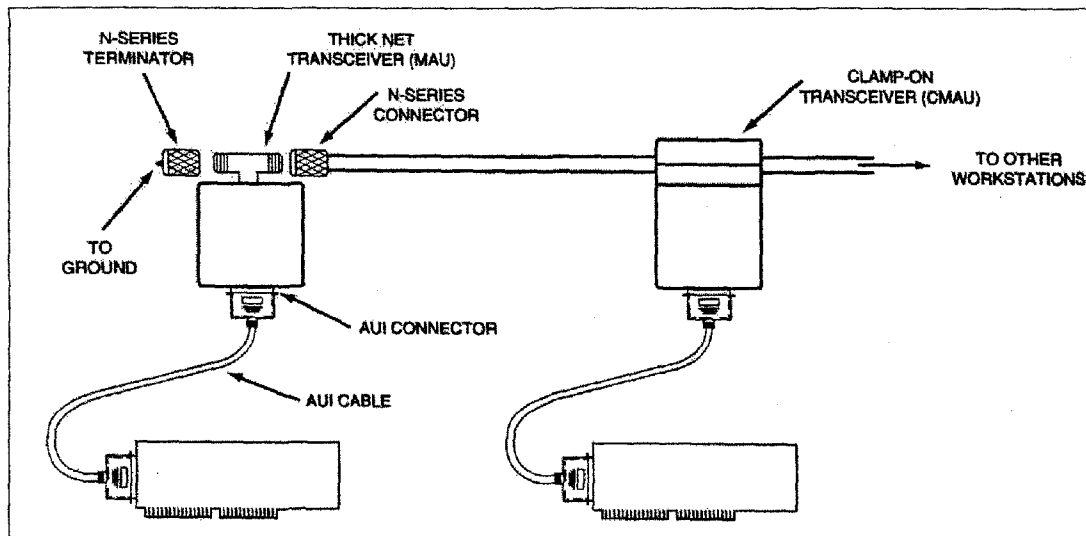


Figure 4.8 Connectors and cabling for Thicknet

4.4.2 Twisted-Pair Cable

Twisted-pair cable has become the dominant cable type for all new network designs that employ copper cable. Among the several reasons for the popularity of twisted-pair cable, the most significant is its low cost. Twisted-pair cable is inexpensive to install and offers the lowest cost per foot of any cable type. Your telephone cable is an example of a twisted-pair type cable.

A basic twisted-pair cable consists of two strands of copper wire twisted together. The twisting reduces the sensitivity of the cable to EMI and also reduces the tendency of the cable to radiate radio frequency noise that interferes with nearby cables and electronic components.

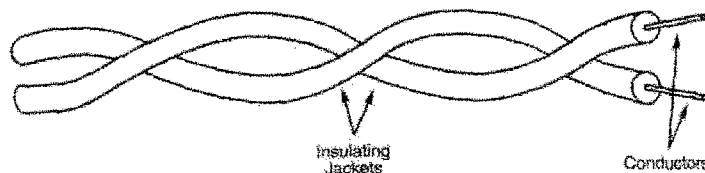


Figure 4.9 Twisted-pair cabling

Twisting of the wires also controls the tendency of the wires in the pair to cause EMI in each other. As noted previously, whenever two wires are in close proximity, the signals in each wire tend to produce crosstalk in the other. Twisting the wires in the pair reduces crosstalk in much the same way that twisting reduces the tendency of the wires to radiate EMI.

A twisted-pair cable is used in most cases to connect a PC to either a HUB or a MAU. Two types of twisted-pair cable are used in LANs: shielded and unshielded, as explained in the following section.

4.4.2.1 Shielded Twisted-Pair (STP) Cable

Shielded twisted-pair cabling consists of one or more twisted pairs of cables enclosed in a foil wrap and woven copper shielding. Figure 4.11 shows IBM Type 1 cabling, the first cable type used with IBM Token Ring. Early LAN designers used shielded twisted-pair cable because the shield performed double duty, reducing the tendency of the cable to radiate EMI and reducing the cable's sensitivity to outside interference.

Coaxial and STP cables use shields for the same purpose. The shield is connected to the ground portion of the electronic device to which the cable is connected. A ground is a portion of the device that serves as an electrical reference point, and usually it is literally connected to a metal stake driven into the ground. A properly grounded shield prevents signals from getting into or out of the cable.

The picture in Figure 4.10 is an example of IBM Type 1 cable, an STP cable, and includes two twisted pairs of wire within a single shield. Various types of STP cable exist, some that shield each pair individually and others that shield several pairs. The engineers who design a network's cabling system choose the exact configuration. IBM designates several twisted-pair cable types to use with their Token Ring network design, and each cable type is appropriate for a given kind of installation. A

completely different type of STP is the standard cable for Apple's AppleTalk network.

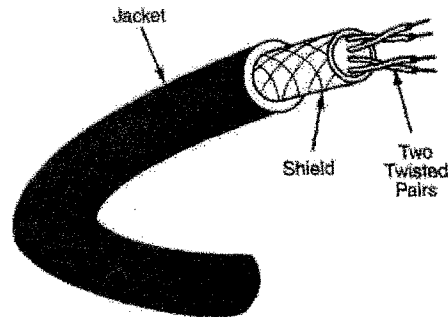


Figure 4.10 A shielded twisted-pair cable

4.4.2.1.1 Cost

STP cable costs more than thin coaxial or unshielded twisted-pair cable. STP is less costly, however, than thick coax or fiber-optic cable.

4.4.2.1.2 Installation

Different network types have different installation requirements. One major difference is the connector used. In many cases, installation can be greatly simplified with prewired cables—cables precut to length and installed with the appropriate connectors. You must learn to install the required connectors, however, when your installation requires the use of bulk cable. The installation of cables has been regulated or made part of building codes in some areas, to be performed only by a certified cable installer.

4.4.2.1.3 Capacity

STP cable has a theoretical capacity of 500Mbps, although few implementations exceed 155Mbps with 100-meter cable runs. The most common data rate for STP cable is 16Mbps, which is the top data rate for Token Ring networks.

4.4.2.1.4 Attenuation

All varieties of twisted-pair cable have attenuation characteristics that limit the length of cable runs to a few hundred meters, although a 100-meter limit is most common.

4.4.2.1.5 EMI Characteristics

The shield in STP cable results in good EMI characteristics for copper cable, comparable to the EMI characteristics of coaxial cable. This is one reason STP might be preferred to unshielded twisted-pair cable in some situations. As with all copper cables, STP is still sensitive to interference and vulnerable to electronic eavesdropping.

4.4.2.2 Unshielded Twisted-Pair (UTP) Cable

Unshielded twisted-pair cable doesn't incorporate a braided shield into its structure. However, the characteristics of UTP are similar in many ways to STP, differing primarily in attenuation and EMI. As shown in Figure 4.12, several twisted pairs can be bundled together in a single cable. These pairs are typically color-coded to distinguish them.

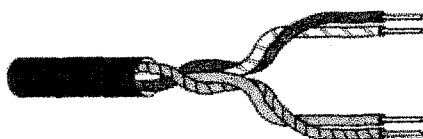


Figure 4.11 A multipair UTP cable

Telephone systems commonly use UTP cabling. UTP cable is available in the following five grades or categories:

- ◆ **Categories 1 and 2:** These voice-grade cables are suitable only for voice and for low data rates (below 4Mbps). Category 1 was once the standard voice-grade cable for telephone systems. The growing need for data-ready cabling systems,

however, has caused Categories 1 and 2 cable to be supplanted by Category 3 for new installations.

- ◆ **Category 3:** As the lowest data-grade cable, this type of cable generally is suited for data rates up to 10Mbps. Some innovative schemes utilizing new standards and technologies, however, enable the cable to support data rates up to 100Mbps. Category 3, which uses four twisted pairs with three twists per foot, is now the standard cable used for most telephone installations.

- ◆ **Category 4:** This data-grade cable, which consists of four twisted-pairs, is suitable for data rates up to 16Mbps.

- ◆ **Category 5:** This data-grade cable, which also consists of four twisted-pairs, is suitable for data rates up to 100Mbps. Most new cabling systems for 100Mbps data rates are designed around Category 5 cable.

4.4.2.2.1 Cost

The price of the grades of cable increase as you move from Category 1 to Category 5. UTP cable is the least costly of any cable type, although properly installed Category 5 tends to be fairly expensive. In some cases, existing cable in buildings can be used for LANs, although you should verify the category of the cable and know the length of the cable in the walls. Distance limits for voice cabling are much less stringent than for data-grade cabling.

4.4.2.2.2 Installation

UTP cable is easy to install. Some specialized equipment might be required, but the equipment is low in cost and its use can be mastered with a bit of practice. Properly designed UTP cabling systems easily can be reconfigured to meet changing requirements.

4.4.2.2.3 Capacity

The data rates possible with UTP have pushed up from 1Mbps, past 4 and 16Mbps, to the point where 100Mbps data rates are now common.

4.4.2.2.4 Attenuation

UTP cable shares similar attenuation characteristics with other copper cables. UTP cable runs are limited to a few hundred meters, with 100 meters (a little more than 300 feet) as the most frequent limit.

4.4.2.2.5 EMI Characteristics

Because UTP cable lacks a shield, it is more sensitive to EMI than coaxial or STP cables. The latest technologies make it possible to use UTP in the vast majority of situations, provided that reasonable care is taken to avoid electrically noisy devices such as motors and fluorescent lights. Nevertheless, UTP might not be suitable for noisy environments such as factories. Crosstalk between nearby unshielded pairs limits the maximum length of cable runs.

4.4.3 Fiber-Optic Cable

Fiber-optic cable is the ideal cable for data transmission. Not only does this type of cable accommodate extremely high bandwidths, but it also presents no problems with EMI and supports durable cables and cable runs as long as several kilometers. The two disadvantages of fiber-optic cable, however, are cost and installation difficulty. Despite these disadvantages, fiber-optic cable is now often installed into buildings by telephone companies as the cable of choice.

The center conductor of a fiber-optic cable is a fiber that consists of highly refined glass or plastic designed to transmit light signals with little loss. A glass core supports a longer cabling distance, but a plastic core is typically easier to work with.

The fiber is coated with a cladding or a gel that reflects signals back into the fiber to reduce signal loss. A plastic sheath protects the fiber.

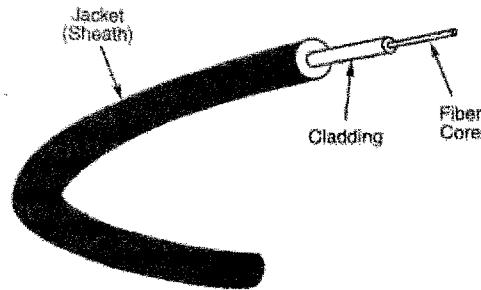


Figure 4.12 A fiber-optic cable

A fiber-optic network cable consists of two strands separately enclosed in plastic sheaths. One strand sends and the other receives. Two types of cable configurations are available: loose and tight configurations. Loose configurations incorporate a space between the fiber sheath and the outer plastic encasement; this space is filled with a gel or other material. Tight configurations contain strength wires between the conductor and the outer plastic encasement. In both cases, the plastic encasement must supply the strength of the cable, while the gel layer or strength wires protect the delicate fiber from mechanical damage.

Optical fiber cables don't transmit electrical signals. Instead, the data signals must be converted into light signals. Light sources include lasers and light-emitting diodes (LEDs). LEDs are inexpensive but produce a fairly poor quality of light suitable for only less-stringent applications.

The end of the cable that receives the light signal must convert the signal back to an electrical form. Several types of solid-state components can perform this service.

4.4.3.1 Fiber-Optic Characteristics

As with all cable types, fiber-optic cables have their share of advantages and disadvantages.

4.4.3.1.1 Cost

Fiber-optic cable is also the most expensive cable type to install.

4.4.3.1.2 Installation

Greater skill is required to install fiber-optic cable than to install most copper cables. Improved tools and techniques, however, have reduced the training required. Still, fiber-optic cable requires greater care because the cables must be treated fairly gently during installation. Every cable has a minimum bend radius, for example, and fibers are damaged if the cables are bent too sharply. It also is important to not stretch the cable during installation.

4.4.3.1.3 Capacity

Fiber-optic cable can support high data rates (as high as 200,000Mbps) even with long cable runs. Although UTP cable runs are limited to less than 100 meters with 100Mbps data rates, fiber-optic cables can transmit 100Mbps signals for several kilometers.

4.4.3.1.4 Attenuation

Attenuation in fiber-optic cables is much lower than in copper cables. Fiber-optic cables are capable of carrying signals for several kilometers.

4.4.3.1.5 EMI Characteristics

Because fiber-optic cables don't use electrical signals to transmit data, they are totally immune to electromagnetic interference. The cables are also immune to a variety of electrical effects that must be taken into account when designing copper cabling systems.

When electrical cables are connected between two buildings, the ground potentials (voltages) between the two buildings can differ. When a difference exists (as it frequently does), the current flows through the grounding conductor of the cable, even though the ground is supposed to be electrically neutral and no current should flow. When current flows through the ground conductor of a cable, the condition is called a ground loop. Ground loops can result in electrical instability and various other types of anomalies

4.4.4 Summary of Cable Characteristics

The table below summarizes the characteristics of the four cable types discussed in this section.

Table 4.2 Comparisons of Guided Transmission Media

Cable Type	Cost	Installation	Capacity	Range	EMI
Coaxial Thinnet	Less than STP	Inexpensive/easy	10Mbps typical	185 m	Less sensitive than UTP
Coaxial Thicknet	Greater than STP, less than fiber	Easy	10Mbps typical	500 m	Less sensitive than UTP
Shielded twisted-pair (STP)	Greater than UTP, less than Thicknet	Fairly easy	16Mbps typical up to 500 Mbps	100m typical	Less sensitive than UTP
Unshielded twisted-pair (UTP)	Lowest	Inexpensive/easy	10Mbps typical up to 100 Mbps	100m typical	Most sensitive
Fiber-optic	Highest	Expensive/difficult	100Mbps typical	10s of kilometers	Insensitive

4.5 Wireless Transmission

The extraordinary convenience of wireless communications has placed an increased emphasis on wireless networks in recent years. Technology is expanding rapidly and will continue to expand into the near future, offering more and better options for wireless networks.

Presently, you can subdivide wireless networking technology into three basic types corresponding to three basic networking scenarios:

- ◆ Local area networks (LANs). Occasionally you will see a fully wireless LAN, but more typically one or more wireless machines function as members of a cable-based LAN.
- ◆ Extended local networks. A wireless connection serves as a backbone between two LANs. For instance, a company with office networks in two nearby but separate buildings could connect those networks using a wireless bridge.
- ◆ Mobile computing. A mobile machine connects to the home network using cellular or satellite technology.

4.5.1 Reasons for Wireless Networks

Wireless networks are especially useful for the following situations:

- ◆ Spaces where cabling would be impossible or inconvenient. These include open lobbies, inaccessible parts of buildings, older buildings and historical buildings where renovation is prohibited, and outdoor installations.
- ◆ People who move around a lot within their work environment. Network administrators, for instance, must troubleshoot a large office network. Nurses and doctors need to make rounds at a hospital.
- ◆ Temporary installations. These situations include any temporary department set up for a specific purpose that soon will be torn down or relocated.
- ◆ People who travel outside of the work environment and need instantaneous access to network resources.

- ◆ Satellite offices or branches, ships in the ocean, or teams in remote field locations that need to be connected to a main office or location.

4.5.2 Wireless Communications with LANs

You can classify wireless LAN communications according to transmission method. The four most common LAN wireless transmission methods are as follows:

- ◆ Infrared
- ◆ Laser
- ◆ Narrow-band radio
- ◆ Spread-spectrum radio
- ◆ Microwave

4.5.2.1 Infrared Transmission

You use an infrared communication system every time you control your television with a remote control. The remote control transmits pulses of infrared light that carry coded instructions to a receiver on the TV. This technology also is used for network communication. Four varieties of infrared communications are as follows:

- ◆ Broadband optical telepoint. This method uses broadband technology. Data transfer rates in this high-end option are competitive with those for a cable-based network.
- ◆ Line-of-sight infrared. Transmissions must occur over a clear line-of-sight path between transmitter and receiver.
- ◆ Reflective infrared. Wireless PCs transmit toward a common, central unit, which then directs communication to each of the nodes.
- ◆ Scatter infrared. Transmissions reflect off floors, walls, and ceilings until (theoretically) they finally reach the receiver. Because of the imprecise trajectory, data transfer rates are slow. The maximum reliable distance is around 100 feet.

Infrared transmissions are typically limited to within 100 feet. Within this range, however, infrared is relatively fast. Infrared's high bandwidth supports transmission speeds of up to 10Mbps.

Infrared devices are insensitive to radio-frequency interference, but reception can be degraded by bright light. Because transmissions are tightly focused, they are fairly immune to electronic eavesdropping. Infrared transmissions are commonly used for LAN transmissions, yet can also be employed for WAN transmissions as well.

4.5.2.2 Laser Transmission

High-powered laser transmitters can transmit data for several thousand yards when line-of-sight communication is possible. Lasers can be used in many of the same situations as microwave links (described later in this chapter), but do not require a FCC license. On a LAN scale, laser light technology is similar to infrared technology. Laser light technology is employed in both LAN and WAN transmissions, though it is more commonly used in WAN transmissions.

4.5.2.3 Narrow-Band Radio Transmission

In narrow-band radio communications (also called single-frequency radio), transmissions occur at a single radio frequency. The range of narrow-band radio is greater than that of infrared, effectively enabling mobile computing over a limited area. Neither the receiver nor the transmitter must be placed along a direct line of sight; the signal can bounce off walls, buildings, and even the atmosphere, but heavy walls, such as steel or concrete enclosures, can block the signal.

4.5.2.4 Spread-Spectrum Radio Transmission

Spread-spectrum radio transmission is a technique originally developed by the military to solve several communication problems. Spread-spectrum improves reliability, reduces sensitivity to interference and jamming, and is less vulnerable to

eavesdropping than single-Frequency radio. Spread-spectrum radio transmissions are commonly used for WAN transmissions that connect multiple LANs or network segments together. Two techniques employed are frequency hopping and direct sequence modulation.

Frequency hopping switches among several available frequencies, staying on each frequency for a specified interval of time. The transmitter and receiver must remain synchronized during a process called a "hopping sequence" for this technique to work. Range for this type of transmission is up to two miles outdoors and 400 feet indoors. Frequency hopping typically transmits at up to 250Kbps, although some versions can reach as high as 2Mbps.

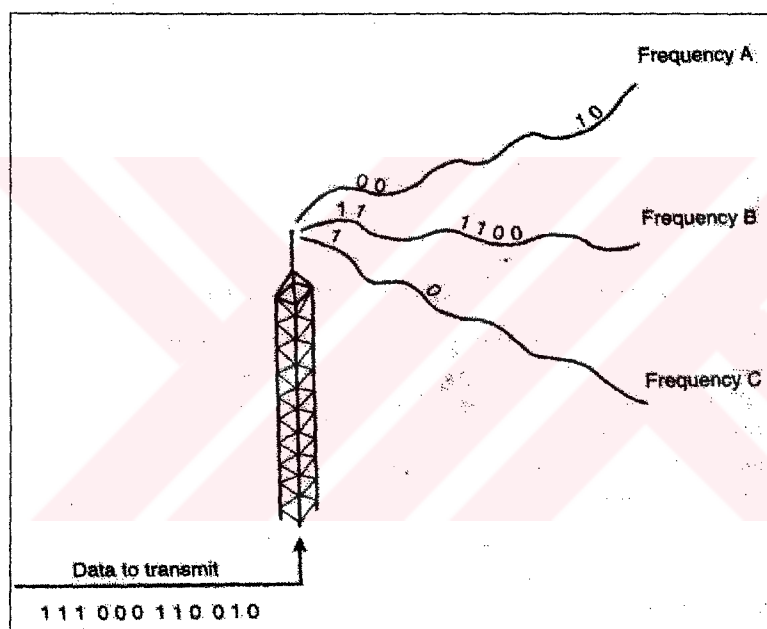


Figure 4.13 Frequency hopping transmits data over various frequencies for specific periods of time

Direct sequence modulation breaks original messages into parts called chips, which are transmitted on separate frequencies. To confuse eavesdroppers, decoy data also can be transmitted on other frequencies. The intended receiver knows which frequencies are valid and can isolate the chips and reassemble the message. Eavesdropping is difficult because the correct frequencies are not known, and the eavesdropper cannot isolate the frequencies carrying true data. Because different sets

of frequencies can be selected, this technique can operate in environments that support other transmission activity. Direct sequence modulation systems operating at 900MHz support bandwidths of 2-6Mbps.

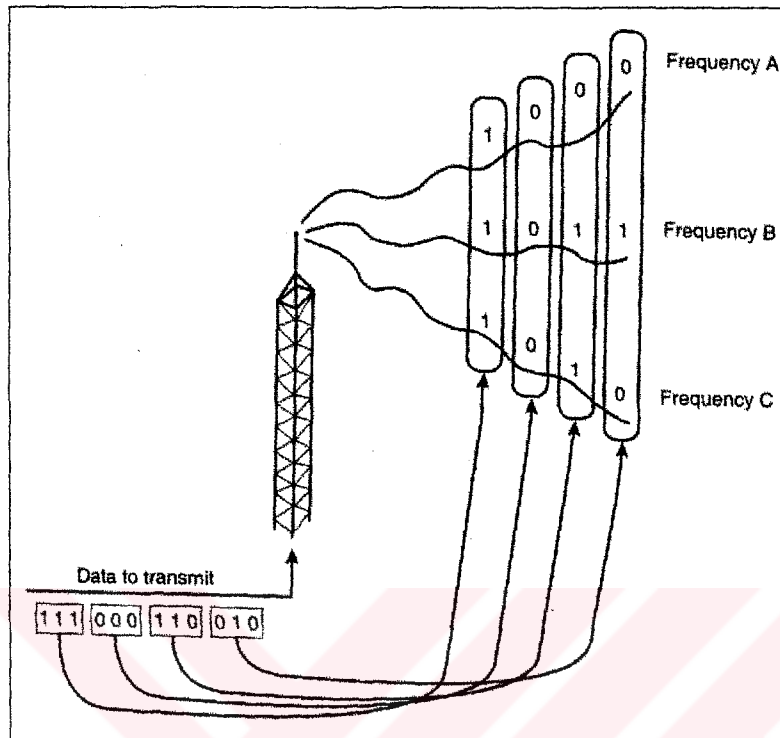


Figure 4.14 Direct sequence modulation

4.5.2.5 Microwave

Microwave technology has applications in all three of the wireless networking scenarios: LAN, extended LAN, and mobile networking. As shown in Figure 4.16, microwave communication can take two forms: terrestrial (ground) links and satellite links. The frequencies and technologies employed by these two forms are similar, but distinct differences exist between them.

Mobile computing is a growing technology that provides almost unlimited range for traveling computers by using satellite and cellular phone networks to relay the signal to a home network. Mobile computing typically is used with portable PCs or personal digital assistant (PDA) devices.

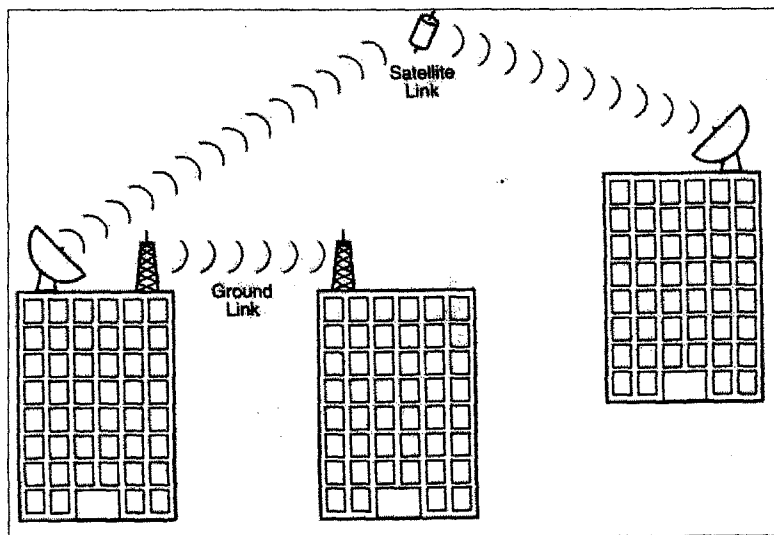


Figure 4.15 Terrestrial and satellite microwave links

Three forms of mobile computing are as follows:

- ◆ **Packet-radio networking:** The mobile device sends and receives network-style packets via satellite. Packets contain a source and destination address, and only the destination device can receive and read the packet.
- ◆ **Cellular networking:** The mobile device sends and receives cellular digital packet data (CDPD) using cellular phone technology and the cellular phone network. Cellular networking provides very fast communications.
- ◆ **Satellite station networking:** Satellite mobile networking stations use satellite microwave technology.

4.5.2.5.1 Terrestrial Microwave

Terrestrial microwave communication employs earth-based transmitters and receivers. The frequencies used are in the low giga hertz range, which limits all communications to line-of-sight. You probably have seen terrestrial microwave equipment in the form of telephone relay towers, which are placed every few miles to relay telephone signals across a country.

Microwave transmissions typically use a parabolic antenna that produces a narrow, highly directional signal. A similar antenna at the receiving site is sensitive to signals only within a narrow focus. Because the transmitter and receiver are highly focused, they must be adjusted carefully so that the transmitted signal is aligned with the receiver.

A microwave link is used frequently to transmit signals in instances in which it would be impractical to run cables. If you need to connect two networks separated by a public road, for example, you might find that regulations restrict you from running cables above or below the road. In such a case, a microwave link is an ideal solution.

Some LANs operate at microwave frequencies at low power and use nondirectional transmitters and receivers. Network hubs can be placed strategically throughout an organization, and workstations can be mobile or fixed. This approach is one way to enable mobile workstations in an office setting.

In many cases, terrestrial microwave uses licensed frequencies. A license must be obtained from the FCC, and equipment must be installed and maintained by licensed technicians. Terrestrial microwave systems operate in the low giga hertz range, typically at 4-6GHz and 21-23GHz, and costs are highly variable depending on requirements. Long-distance microwave systems can be quite expensive but might be less costly than alternatives. (A leased telephone circuit, for example, represents a costly monthly expense.) When line-of-sight transmission is possible, a microwave link is a one-time expense that can offer greater bandwidth than a leased circuit.

Costs are on the way down for low-power microwave systems for the office. Although these systems don't compete directly in cost with cabled networks, microwave can be a cost-effective technology when equipment must be moved frequently. Capacity can be extremely high, but most data communication systems operate at data rates between 1 and 10Mbps. Attenuation characteristics are determined by transmitter power, frequency, and antenna size. Properly designed

systems are not affected by attenuation under normal operational conditions; rain and fog, however, can cause attenuation of higher frequencies.

Microwave systems are highly susceptible to atmospheric interference and also can be vulnerable to electronic eavesdropping. For this reason, signals transmitted through microwave are frequently encrypted.

4.5.2.5.2 Satellite Microwave

Satellite microwave systems relay transmissions through communication satellites that operate in geosynchronous orbits 22,300 miles above the earth. Satellites orbiting at this distance remain located above a fixed point on earth.

Earth stations use parabolic antennas (satellite dishes) to communicate with satellites. These satellites then can retransmit signals in broad or narrow beams, depending on the locations set to receive the signals. When the destination is on the opposite side of the earth, for example, the first satellite cannot transmit directly to the receiver and thus must relay the signal through another satellite.

Because no cables are required, satellite microwave communication is possible with most remote sites and with mobile devices, which enables communication with ships at sea and motor vehicles.

The distances involved in satellite communication result in an interesting phenomenon: Because all signals must travel 22,300 miles to the satellite and 22,300 miles when returning to a receiver, the time required to transmit a signal is independent of distance on the ground. It takes as long to transmit a signal to a receiver in the same state as it does to a receiver a third of the way around the world. The time required for a signal to arrive at its destination is called propagation delay. The delays encountered with satellite transmissions range from 0.5 to 5 seconds. Satellite communication is extremely expensive. Building and launching a satellite can cost easily in excess of a billion dollars.

4.5.3 Comparisons of Different Wireless Transmission

The summary table below compares the different types of Wireless communication media .

Table 4.3 Comparisons of Wireless Transmission

Cable Type	Cost	Installation	Distance	Other Issues
Infrared	Cheapest of all the wireless	Fairly easy, may require line-of-sight	Under a kilometer	Can attenuate due to fog and rain
Laser	Similar to infrared	Requires line-of-sight	Can span several kilometers	Can attenuate due to fog and rain
Narrow-band radio	More expensive than infrared and laser; may need FCC license	Requires trained technicians and can involve tall radio towers	Can span hundreds of kilometers	Low-power devices can attenuate; can be eavesdropped upon; can also attenuate due to fog, rain, and solar flares
Spread-spectrum radio	More advanced technology than narrow band radio, thus more expensive	Requires trained technicians and can involve tall radio towers	Can span hundreds of kilometers	Low-power devices can attenuate; can also attenuate due to fog, rain and solar flares
Microwave	Very expensive, as requires link up to satellites often	Requires trained technicians and can involve satellite dishes	Can span thousands of kilometers	Can be eavesdropped upon; can also attenuate due to fog, rain and solar flares

CHAPTER FIVE

NETWORK TOPOLOGIES AND ARCHITECTURES

5.1 Network Topologies

A topology is a map of the network. It is a plan for how the cabling will interconnect the nodes, or devices, and how the nodes will function in relation to one another. A topology defines the arrangement of nodes, cables, and connectivity devices that make up the network.

Generally, there are four network topologies: star, bus, ring and mesh.

- ◆ **Bus:** A single cable (trunk) that connects all computers in a single line.
- ◆ **Star:** Computers connect to a centralized hub via cable segments.
- ◆ **Ring:** Connects all computers on a single cable. Ends are not terminated, but form a full loop connecting the last computer to the first computer.
- ◆ **Mesh:** Commonly used in WAN configurations. Routers are connected to multiple links for redundancy and to give the ability to determine the quickest route to a destination.

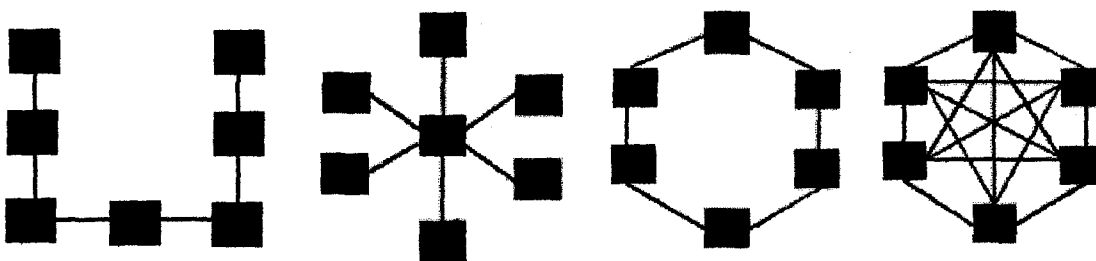


Figure 5.1 Bus, Star, Ring and Mesh Network Topologies

5.1.1 Bus Topologies

A bus physical topology is one in which all devices connect to a common, shared cable. A bus topology is shown in Figure 5.2.

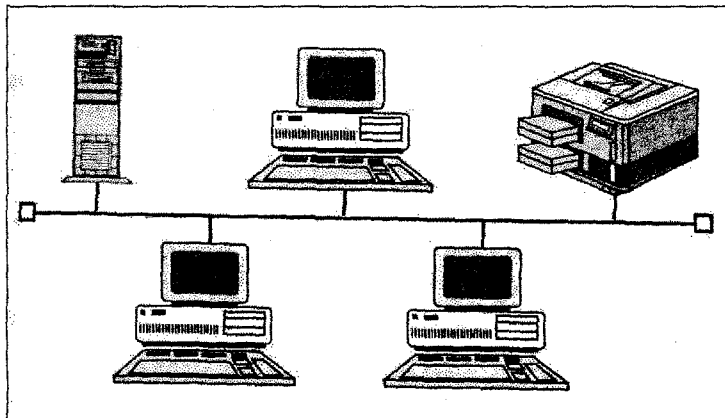


Figure 5.2 A bus topology

Most bus networks broadcast signals in both directions on the backbone cable, enabling all devices to directly receive the signal. Some buses, however, are unidirectional: Signals travel in only one direction and can reach only downstream devices. In the case of a unidirectional bus, the cable must be terminated in such a way that signals can go down the cable but do not reflect back up the cable and reach other devices, causing disruption (Glen Berg, 1998).

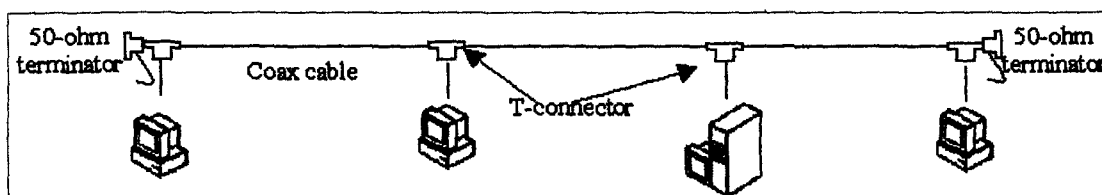


Figure 5.3 Bus topology

ThinNet and thicknet are typical bus topology networks. Imagine in a ThinNet with bus topology, if one of the T connector is broken, it may affect the whole network. Please make sure that this does not mean when one machine shutdown, the whole network doesn't work. Look at the following figure of T-connector:

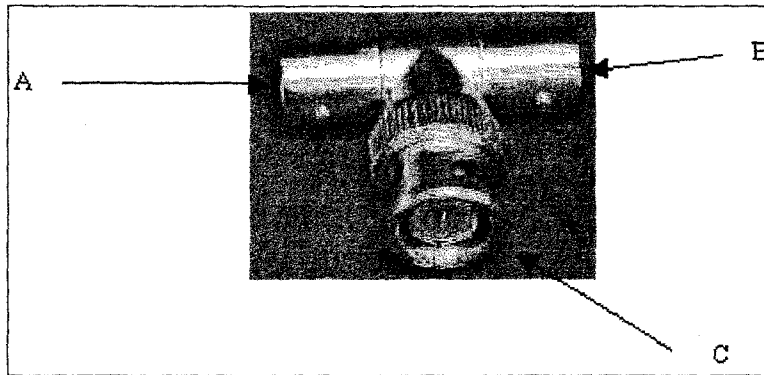


Figure 5.4 BNC T Connector

You connect the networking cable to port A and B, port C is connected to the NIC on the NIC on the PC directly. Therefore, if you shutdown the PC, you can still pass the signals from A to B, it will not affect the other machines on the network. However, if there are some broken in between A and B, the whole network will be down. To test the cable connectivity, you can use the cable tester.

5.1.2 Ring Topologies

Ring topologies are wired in a circle. Each node is connected to its neighbours on either side, and data passes around the ring in one direction only. Each device incorporates a receiver and a transmitter and serves as a repeater that passes the signal on to the next device in the ring. Because the signal is regenerated at each device, signal degeneration is low (Glen Berg, 1998).

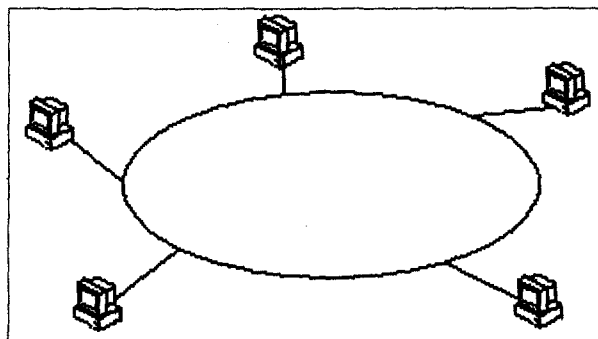


Figure 5.5 A ring topology

5.1.3 Star Topologies

Star topologies require that all devices connect to a central hub. The hub receives signals from other network devices and routes the signals to the proper destinations. Star hubs can be interconnected to form tree, or hierarchical, network topologies.

A star topology means that the nodes are all connected to a central hub. The path the data takes among the nodes and through that hub depends on the design of the hub, the design of the cabling, and the hardware and software configuration of the nodes (Glen Berg, 1998).

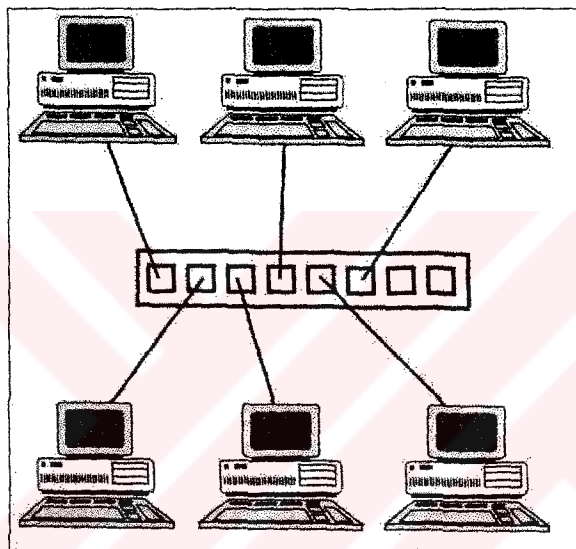


Figure 5.6 A star topology

5.1.4 Mesh Topology

A mesh topology is really a hybrid model representing an all-channel sort of topology. It is a hybrid because a mesh topology can incorporate all the topologies covered to this point. It is an all-channel topology in that every device is directly connected to every other device on the network. When a new device is added, a connection to all existing devices must be made. This provides for a great deal of fault tolerance, but it involves extra work on the part of the network administrator.

That is, if any transmission media breaks, the data transfer can take alternative routes. However, cabling becomes much more extensive and complicated.

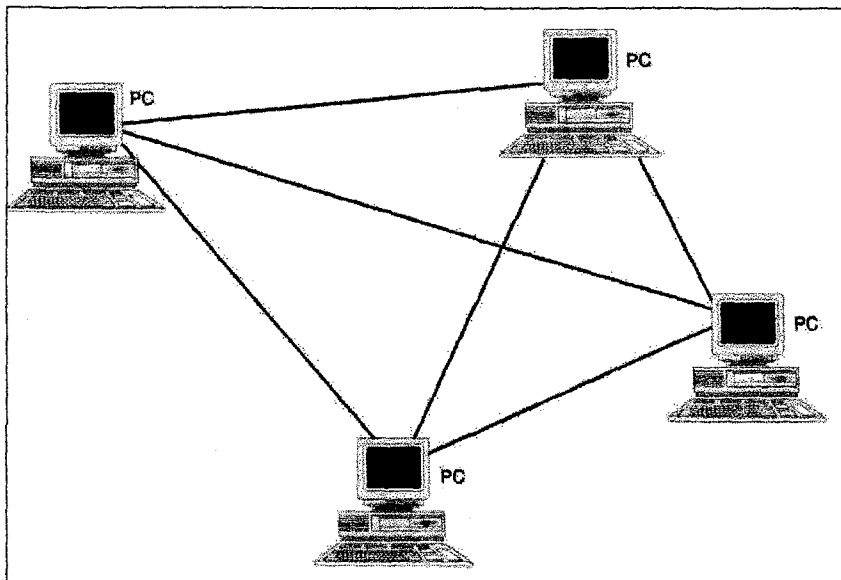


Figure 5.7 A mesh topology

5.2 Network Architectures

A network architecture is the design specification of the physical layout of connected devices. This includes the cable being used, the types of network cards being deployed, and the mechanism through which data is sent on to the network and passed to each device. Network architecture, in short, encompasses the total design and layout of the network.

5.2.1 Ethernet

Ethernet is a very popular local area network architecture. The original ethernet specification was the basis for the IEEE 802.3 specification. In present usage, the term "ethernet" refers to original ethernet (or Ethernet II, the latest version) as well as the IEEE 802.3 standards. The different varieties of ethernet networks are commonly referred to as ethernet topologies. Typically, ethernet networks can use a bus topology (Glen Berg, 1998).

Ethernet networks, depending on the specification, operate at 10 or 100Mbps using baseband transmission. Each IEEE 802.3 specification prescribes its own cable types. Ethernet topologies:

- ◆ 10BASE2
- ◆ 10BASE5
- ◆ 10BASE-T
- ◆ 10BASE-FL
- ◆ 100VG-AnyLAN
- ◆ 100BASE-X

Note that the name of each ethernet topology begins with a number (10 or 100). That number specifies the transmission speed for the network. For instance, 10BASE5 is designed to operate at 10Mbps, and 100BASE-X operates at 100Mbps. "BASE" specifies that baseband transmissions are being used. The "T" is for unshielded twisted-pair wiring, "FL" is for fiber optic cable, "VG-AnyLAN" implies Voice Grade, and "X" implies multiple media types.

Ethernet networks transmit data in small units called frames. The size of an ethernet frame can be anywhere between 64 and 1,518 bytes. Eighteen bytes of the total frame size are taken up by frame overhead, such as the source and destination addresses, protocol information, and error-checking information. There are many different types of ethernet frames, such as the Ethernet II, 802.2, and 802.3 frames to name a few. It is important to remember that 802.2 and 802.3 are IEEE specifications on how information is transferred onto the transmission media (Data Link layer) as well as the specification on how the data should be packaged.

A typical Ethernet II frame has the following sections:

- ◆ **Preamble:** A field that signifies the beginning of the frame.
- ◆ **Addresses:** A field that identifies the source and destination addresses for the frame.
- ◆ **Type:** A field that designates the Network layer protocol.
- ◆ **Data:** The data being transmitted.

- ◆ **CRC:** Cyclical Redundancy Check for error checking.

These parts of the frame are illustrated in Figure 5.8



Figure 5.8 A sample of part of an Ethernet II frame

The term "ethernet" commonly refers to original ethernet (which has been updated to Ethernet II) as well as the IEEE 802.3 standards. Ethernet and the 802.3 standards differ in ways significant enough to make standards incompatible in terms of packet formats, however. At the Physical layer, ethernet and 802.3 are generally compatible in terms of cables, connectors, and electronic devices.

Ethernet generally is used on light-to-medium traffic networks and performs best when a network's data traffic transmits in short bursts. Ethernet is the most commonly used network standard.

5.2.1.1 Ethernet Cabling

You can use a variety of cables to implement ethernet networks. Many of these cable types, such as Thinnet, Thicknet, UTP, and STP, are described in Chapter 4. Ethernet networks traditionally have used coaxial cables of several different types. Fiber-optic cables now are frequently employed to extend the geographic range of ethernet networks.

The contemporary interest in using twisted-pair wiring has resulted in a scheme for cabling that uses unshielded twisted-pair (UTP). The 10BASE-T cabling standard uses UTP in a star topology.

Ethernet remains closely associated with coaxial cable. Two types of coaxial cable still used in small and large environments are Thinnet (10BASE2) and Thicknet (10BASE5). Thinnet and Thicknet ethernet networks have different limitations that are based on the Thinnet and Thicknet cable specifications.

5.2.1.2 10BASE2

The 10BASE2 cabling topology (Thinnet) generally uses the onboard transceiver of the network interface card to translate the signals to and from the rest of the network. Thinnet cabling described in Chapter 4 uses BNC T connectors that attach directly to the network adapter. Each end of the cable should have a terminator, and you must use a grounded terminator on one end.

The main advantage of using 10BASE2 in your network is cost. When any given cable segment on the network doesn't have to be run farther than 185 meters, 10BASE2 is often the cheapest network cabling option.

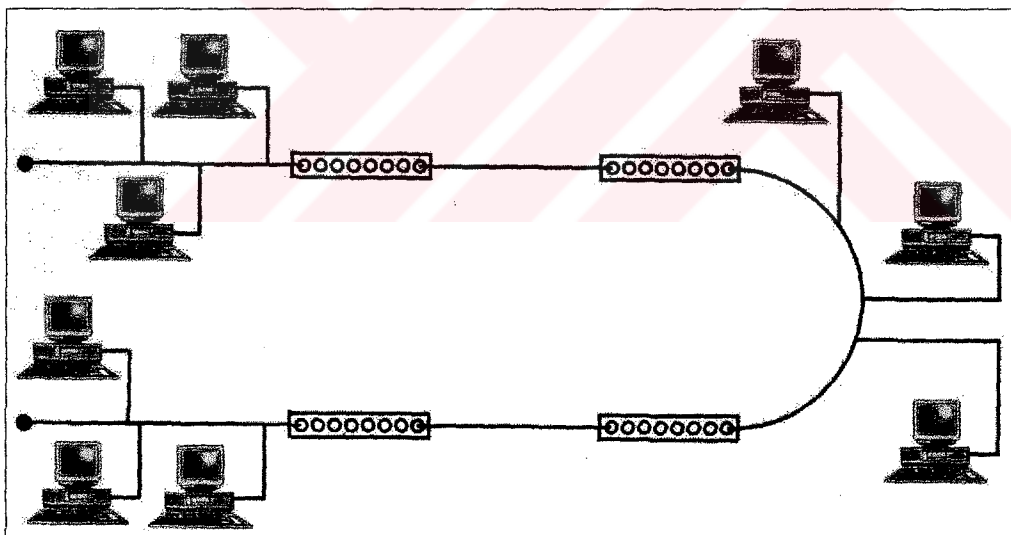


Figure 5.9 The 10BASE2 Cabling

10BASE2 is also relatively simple to connect. Each network node connects directly to the network cable with a T connector attached to the network adapter. For

a successful installation, you must adhere to several rules in 10BASE2 ethernet environments, including the following:

- ◆ The minimum cable distance between clients must be 0.5 meters.
- ◆ Pigtails, also known as drop cables, from T connectors shouldn't be used to connect to the BNC connector on the network adapter. The T connector must be connected directly to the network adapter.
- ◆ You may not exceed the maximum network segment limitation of 185 meters.
- ◆ The entire network-cabling scheme cannot exceed 925 meters.
- ◆ The maximum number of nodes per network segment is 30 (this includes clients and repeaters).
- ◆ A 50-ohm terminator must be used on each end of the bus with only one of the terminators having either a grounding scrap or a grounding wire that attaches it to the screw holding an electrical outlet cover in place.
- ◆ You may not have more than five segments on a network. These segments may be connected with a maximum of four repeaters, and only three of the five segments may have network nodes.

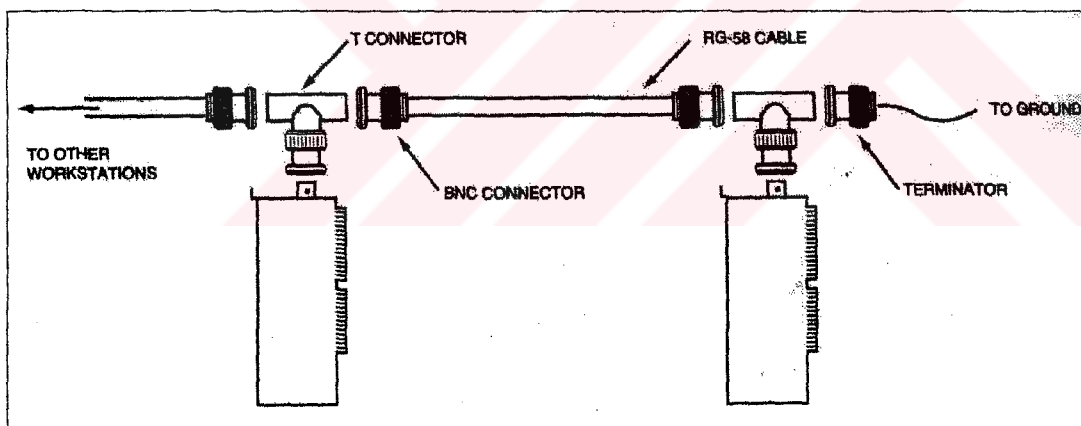


Figure 5.10 T connector and a BNC connector

Figure 5.11 shows two network segments using 10BASE2 cabling.

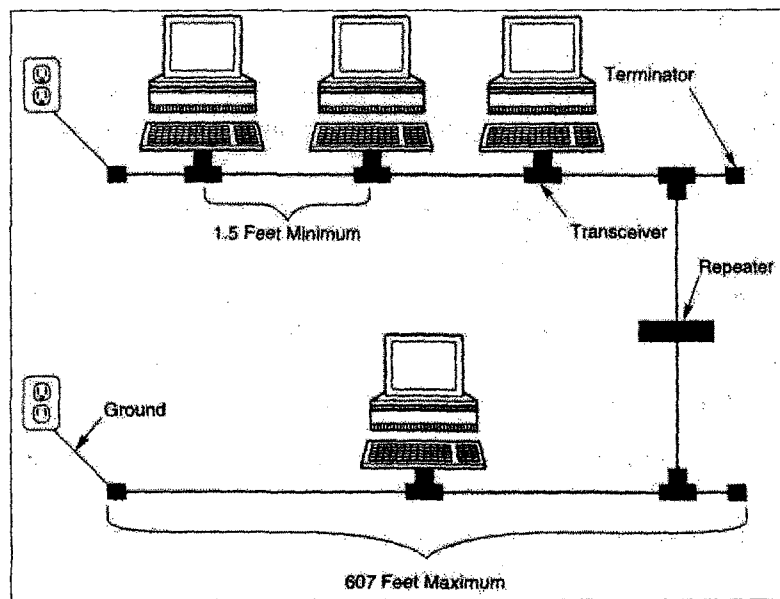


Figure 5.11 Two segments using 10BASE2 cabling

5.2.1.3 10BASE5

The 10BASE5 cabling topology (Thicknet) uses an external transceiver to attach to the network adapter card. The external transceiver clamps to the Thicknet cable. An Attachment Universal Interface (AUI) cable runs from the transceiver to a DIX connector on the back of the network adapter card. As with Thinnet, each network segment must be terminated at both ends, with one end using a grounded terminator.

The primary advantage of 10BASE5 is its capability to exceed the cable restrictions that apply to 10BASE2. 10BASE5 does pose restrictions of its own, however, which you should consider when installing or troubleshooting a 10BASE5 network. As with 10BASE2 networks, the first consideration when you troubleshoot a 10BASE5 network should be the established cabling rules and guidelines. You must follow several additional guidelines, when configuring Thicknet networks, such as the following:

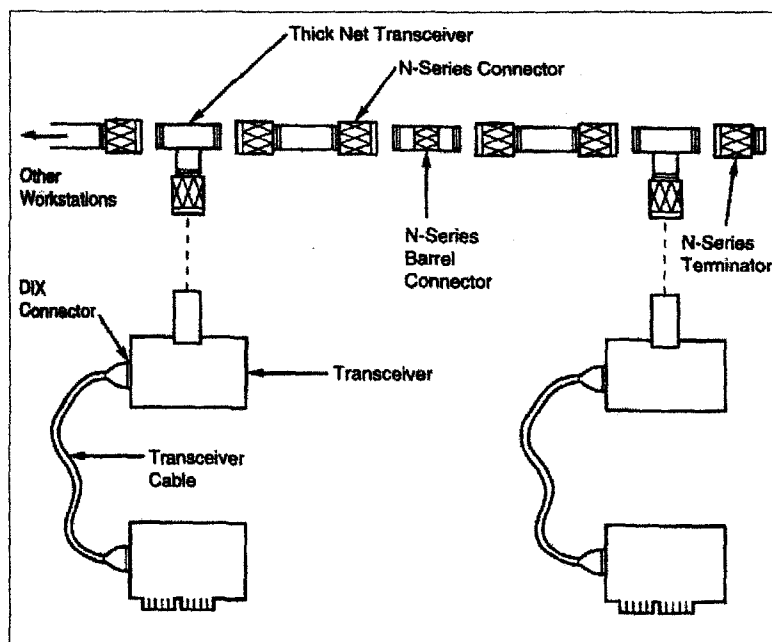


Figure 5.12 Components of a Thicknet network

- ◆ The minimum cable distance between transceivers is 2.5 meters.
- ◆ You may not go beyond the maximum network segment length of 500 meters.
- ◆ The entire network-cabling scheme cannot exceed 2.500 meters.
- ◆ One end of the terminated network segment must be grounded.
- ◆ Drop cables (transceiver cables) can be as short as required but cannot be longer than 50 meters from transceiver to computer.
- ◆ The maximum number of nodes per network segment is 100.

5.2.1.4 10BASE-T

The trend in wiring ethernet networks is to use unshielded twisted-pair (UTP) cable. 10BASE-T, which uses UTP cable, is also one of the more popular implementations for ethernet. It is based on the IEEE 802.3 standard. 10BASE-T supports a data rate of 10Mbps using baseband.

10BASE-T cabling is wired in a star topology. The nodes are wired to a central hub, which serves as a multiport repeater. A 10BASE-T network functions logically

as a linear bus. The hub repeats the signal to all nodes, and the nodes contend for access to the transmission medium as if they were connected along a linear bus. The cable uses RJ-45 connectors, and the network adapter card can have RJ-45 jacks built into the back of the card (An RJ-45 connector looks very similar to a telephone plug.)

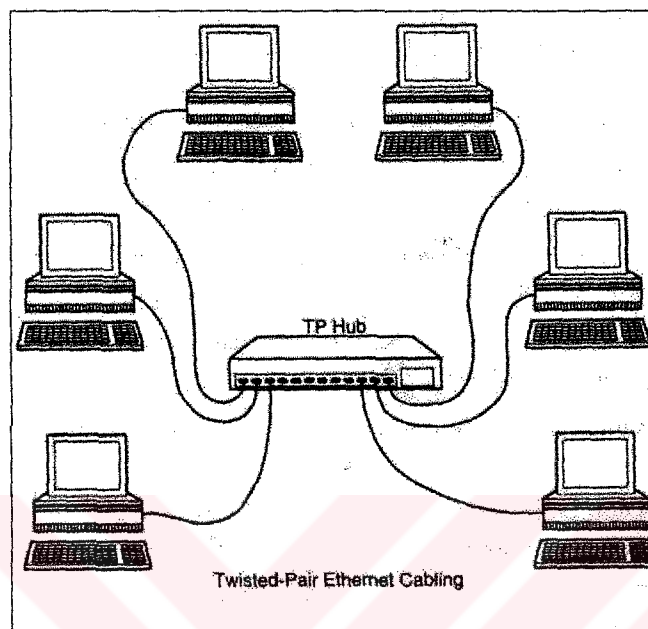


Figure 5.13 A 10BASE-T network wired in a star topology

10BASE-T segments can be connected using coaxial or fiber-optic backbone segments. Some hubs provide connectors for Thinnet and Thicknet cables (in addition to 10BASE-T UTP-type connectors). By attaching a 10BASE-T transceiver to the AUI port of the network adapter, you can use a computer set up for Thicknet on a 10BASE-T network.

The star wiring of 10BASE-T provides several advantages, particularly in larger networks. First, the network is more reliable and easier to manage because 10BASE-T networks use a concentrator (a centralised wiring hub). These hubs are "intelligent" in that they can detect defective cable segments and route network traffic around them. This capability makes locating and repairing bad cable segments easier.

Networks with star wiring topologies can be significantly easier to troubleshoot and repair than bus-wired networks. With a star network, you can isolate a problem node from the rest of the network by disconnecting the cable and directly connecting it to the cable hub. If the hub is considered intelligent, management software developed for that hub type, as well as the hub itself, can disconnect the suspect port. Another benefit to this is that one bad cable segment does not affect the entire network, only the machine connected to that bad cable.

10BASE-T enables you to design and build your LAN one segment at a time; growing as your network needs to grow. This capability makes 10BASE-T more flexible than other LAN cabling options. 10BASE-T is also relatively inexpensive to use compared to other cabling options. In some cases in which a data-grade phone system has already been used in an existing building, the data-grade phone cable can be used for the LAN.

The rules for a 10BASE-T network are as follows:

- ◆ The maximum number of computers on a LAN is 1,024.
- ◆ The cabling should be UTP Category 3, 4, or 5.
- ◆ The maximum unshielded cable segment length is 100 meters.
- ◆ The cable minimum distance between computers is 2.5 meters.
- ◆ The minimum distance between a hub and a computer, or between two hubs, is 0.5 meters.

5.2.1.5 10BASE-FL

10BASE-FL is a specification for ethernet over fiber-optic cables. The 10BASE-FL specification calls for a 10Mbps data rate using baseband. The most important advantages are long cabling runs (10BASE-FL supports a maximum cabling distance of about 2,000 meters) and the elimination of any potential electrical complications. Another advantage is that the number of nodes a segment can handle with 10BASE-FL is far greater than the maximum supported by 10BASE-T, 10BASE2, and 10BASE5.

5.2.1.6 100VG-AnyLAN

100VG-AnyLAN is defined in the IEEE 802.12 standard. IEEE 802.12 is a standard for transmitting ethernet and token-ring packets (IEEE 802.3 and 802.5) at 100Mbps. 100VG-AnyLAN is sometimes called 100BASE-VG. The "VG" in the name stands for "voice grade." 100VG-AnyLAN cabling uses four twisted-pairs in a scheme called quartet signaling.

100VG-AnyLAN uses a cascaded star topology, which calls for a hierarchy of hubs. Computers are attached to child hubs, and the child hubs are connected to higher-level hubs called parent hubs.

The maximum length for the two longest cables attached to a 100VG-AnyLAN hub is 250 meters. The specified cabling is Category 3, 4, or 5 twisted-pair or fiber-optic. 100VG-AnyLAN is compatible with 10BASE-T cabling.

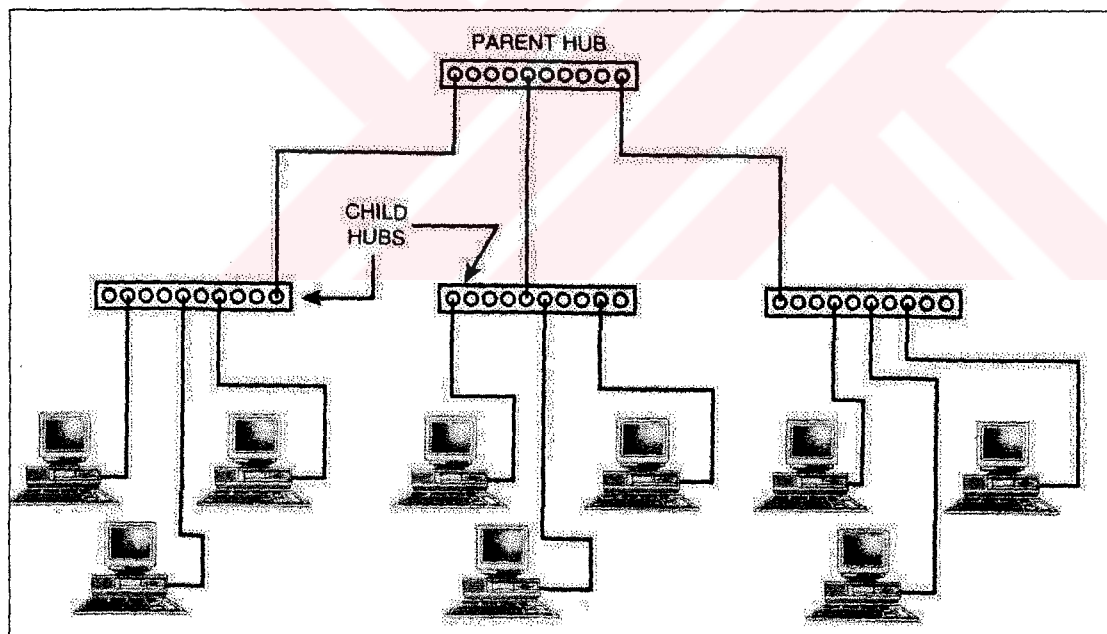


Figure 5.14 Cascaded star topology

5.2.1.7 100BASE-X

100BASE-X uses a star bus topology similar to 10BASE-T's. 100BASE-X provides a data transmission speed of 100Mbps using baseband.

The 100BASE-X standard provides the Following cabling specifications:

- ◆ **100BASE-TX:** Two twisted pairs of Category 5 UTP or STP
- ◆ **100BASE-FX:** Fiber-optic cabling using 2-strand cable.
- ◆ **100BASE-T4:** Four twisted-pairs of Category 3, 4, or 5 UTP

100BASE-X is sometimes referred to as Fast Ethernet. Like 100VGAnyLAN, 100BASE-X provides compatibility with existing 10BASE-T systems and thus enables plug-and-play upgrades from 10BASE-T.

5.2.2 Token Ring

The topology is physically a star, but token ring uses a logical ring to pass the token from station to station. Each node must be attached to a concentrator called a multistation access unit (MSAU or MAU) (Glen Berg, 1998).

Token-ring network interface cards can run at 4Mbps or 16Mbps. Although 4Mbps cards can run at that data rate only, 16Mbps cards can be configured to run at 4 or 16Mbps. All cards on a given network ring must run at the same rate.

As shown in Figure 5.15, each node acts as a repeater that receives tokens and data frames from its nearest active upstream neighbour (NAUN). After the node processes a frame, the frame transmits downstream to the next attached node. Each token makes at least one trip around the entire ring and then returns to the originating node. Workstations that indicate problems send a beacon to identify an address of the potential failure.

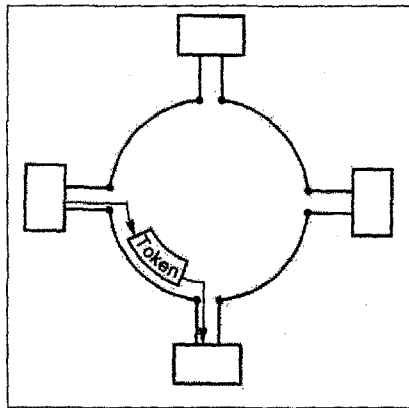


Figure 5.15 Operation of a token ring

5.2.2.1 Token Ring Cabling

Traditional token-ring networks use twisted-pair cable. The following are standard IBM cable types for token ring:

- ◆ **Type 1:** A braided shield surrounds two twisted pairs of solid copper wire. Type 1 is used to connect terminals and distribution panels or to connect between different wiring closets that are located in the same building. Type 1 uses two STPs of solid-core 22 AWG wire for long, high-data-grade transmissions within the building's walls. The maximum cabling distance is 101 meters.

- ◆ **Type 2:** Type 2 uses a total of six twisted pairs: two are STPs (for networking) and four are UTPs (for telephone systems). This cable is used for the same purposes as Type 1, but enables both voice and data cables to be included in a single cable run. The maximum cabling distance is 100 meters.

- ◆ **Type 3:** Used as an alternative to Type 1 and Type 2 cable due to its reduced cost, Type 3 has unshielded twisted-pair copper with a minimum of two twists per inch. Type 3 has four UTPs of 22 or 24 AWG solid-core wire for networks or telephone systems. Type 3 cannot be used for 16Mbps token-ring networks. It is used primarily for long, low-data-grade transmissions within walls. Signals don't travel as fast as with Type 1 cable because Type 3 doesn't have the shielding that Type 1 uses. The maximum cabling distance (according to IBM) is 45 meters. Some vendors specify cabling distances of up to 150 meters.

Type 3 cabling (UTP) is the most popular transmission medium for token ring. A token-ring network using Type 3 (UTP) cabling can support up to 72 computers. A token-ring network using STP cabling can support up to 260 computers.

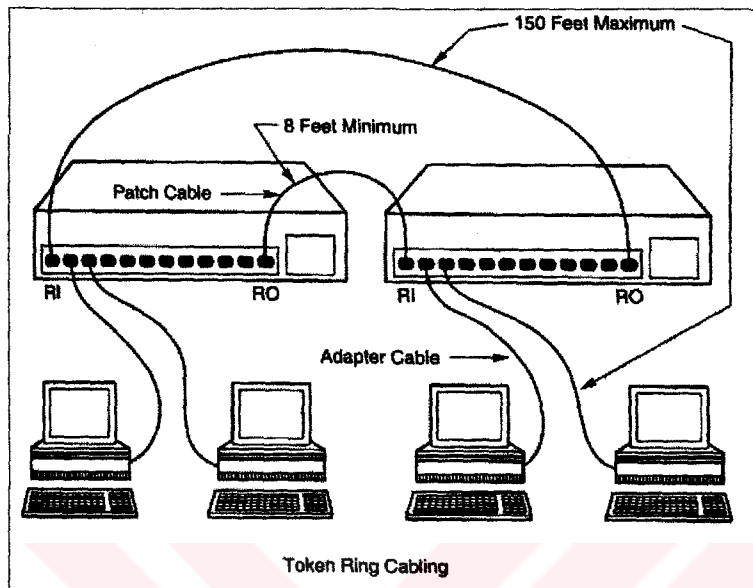


Figure 5.16 An example of token-ring cabling

5.2.3 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a high-bandwidth switching technology developed by the ITU Telecommunications Standards Sector (ITU-TSS). An organisation called the ATM Forum is responsible for defining ATM implementation characteristics. ATM can be layered on other Physical layer technologies, such as Fiber Distributed Data Interface (FDDI) and SONET. The relationships of these protocols to the OSI model are shown in Figure 5.17.

Several characteristics distinguish ATM from other switching technologies. ATM is based on fixed-length, 53-byte cells, whereas other technologies employ frames that vary in length to accommodate different amounts of data. Because ATM cells are uniform in length, switching mechanisms can operate with a high level of efficiency. This high efficiency results in high data transfer rates. Some ATM

systems can operate at an incredible rate of 622Mbps; a typical working speed for an ATM is around 155Mbps (Glen Berg, 1998).

The unit of transmission for ATM is called a cell. All cells are 53 bytes long and consist of a 5-byte header and 48 bytes of data. The 48-byte data size was selected by the standards committee as a compromise to suit both audio- and data-transmission needs. Audio information, for instance, must be delivered with little latency (delay) to maintain a smooth flow of sound. Audio engineers therefore preferred a small cell so that cells would be more readily available when needed. For data, however, large cells reduce the overhead required to deliver a byte of information.

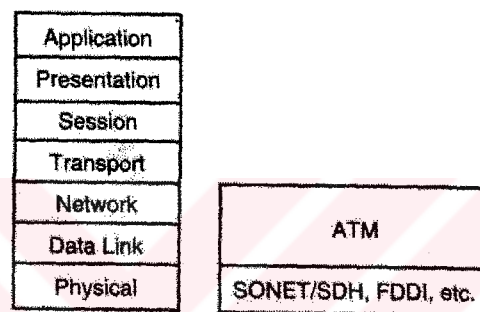


Figure 5.17 The relationship of ATM to the OSI reference model

Asynchronous delivery is another distinguishing feature of ATM. Asynchronous refers to the characteristic of ATM in which transmission time slots don't occur periodically but are granted at irregular intervals. ATM uses a technique called label multiplexing, which allocates time slots on demand. Traffic that is time-critical, such as voice or video, can be given priority over data traffic that can be delayed slightly with no ill effect. Channels are identified by cell labels, not by specific time slots. A high-priority transmission need not be held until its next time slot allocation. Instead, it might be required to wait only until the current 53-byte cell has been transmitted.

Devices communicate on ATM networks by establishing a virtual path, which is identified by a virtual path identifier (VPI). Within this virtual path, virtual circuits can be established, which are in turn associated with virtual circuit identifiers

(VCIs). The VPI and VCI together make up a 3-byte field included in the cell header.

ATM is relatively new technology, and only a few suppliers provide the equipment necessary to support it. (ATM networks must use ATM-compatible switches, routers, and other connectivity devices.) Other networks, such as a routed ethernet, require a 6-byte physical address as well as a network address to uniquely identify each device on an internetwork. An ATM can switch cells with 3-byte identifiers because VPIs and VCIs apply to only a given device-to-device link. Each ATM switch can assign different VPIs and VCIs for each link, and up to 16 million circuits can be configured for any given device to-device link.

Although ATM was developed primarily as a WAN technology, it has many characteristics of value for high-performance LANs. An interesting advantage of ATM is that ATM makes it possible to use the same technology for both LANs and WANs. Some disadvantages, however, include the cost, the limited availability of the equipment, and the present lack of expertise regarding ATM due to its relatively recent arrival.

5.2.4 ARCNet

ARCNet is an older architecture that is not found too often in the business world, but does have a presence in many older networks and school systems who often receive hand-me-downs from the business sector.

ARCNet utilises a token-passing protocol that can have a star or bus physical topology. These segments can be connected with either active or passive hubs. ARCNet, when connected in a star topology, can use either twisted pair or coaxial cable (RG-62). If coaxial cable is used to create a star topology, the ends of the cable can be attached directly to a BNC connector, without a terminator. When in a bus topology, ARCNet uses a 93-ohm terminator, which is attached to each end of the bus in a similar fashion to an ethernet bus.

Some important facts about ARCNet are as follows:

- ◆ ARCNet uses a 93-ohm terminator. (Ethernet uses a 50-ohm terminator.)
- ◆ ARCNet uses a token-like passing architecture, but does not require a MAU.
- ◆ The maximum length between a node and an active hub is 610 meters. The maximum length between a node and a passive hub is 30.5 meters.
- ◆ The maximum network segment cable distance ARCNet supports is 6100 meters.
- ◆ ARCNet can have a total of only 255 stations per network segment.

5.2.5 FDDI

FDDI is very similar to token ring in that it relies on a node to have the token before it can use the network. It differs from token ring in that it utilises fiber-optic cable as its transmission media, allowing for transmissions of up to 100Km. This standard permits up to 100 devices on the network with a maximum distance between stations of up to 2 kilometres (Glen Berg, 1998).

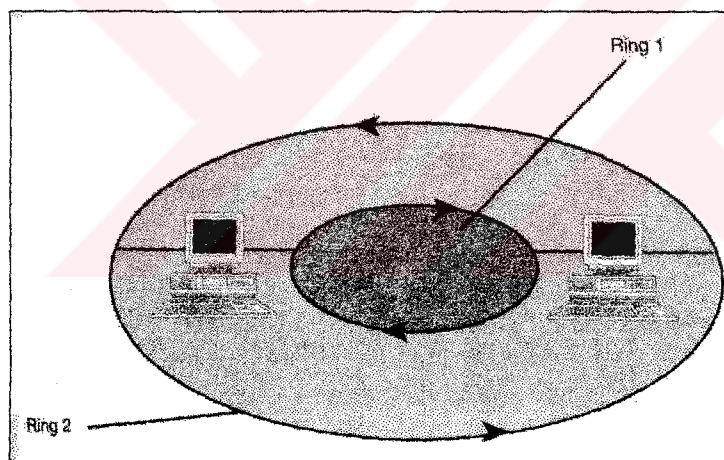


Figure 5.18 A FDDI Network

CHAPTER SIX

NETWORK ADAPTER CARDS

6.1 Network Adapter Cards

When devices are attached to a network, some mechanism must exist for transferring the information from one device to a transmission medium so that the other device or devices on the network can receive the information. Likewise, the receiving device must also have some mechanism to receive this information from the transmission medium, so that it can process the information. This chapter examines the role of the network adapter card also known as a network interface card (NIC). Because a network adapter card is the most common mechanism for attaching PCs to a network, it is deserving of an entire chapter.

A network adapter card is a hardware device that installs in a PC and provides an interface from a PC to the transmission medium. Most PC networks, including ethernet, token-ring and ARCNet, use network adapter cards.

6.2 Defining The Workings of a Network Adapter Card

Network adapter cards act as the physical interface or connection between the computer and the network cable. The cards are installed in an expansion slot in each computer and server on the network. After the card has been installed, the network cable is attached to the card's port to make the actual physical connection between the computer and the rest of the network.

Network adapter cards play an important role on the network. They are responsible for translating data from a device on the network mostly computers and converting this data into some form of signal that can be transmitted across the

must convert these signals coming to it in parallel form, into a serial signal that can travel across the transmission medium.

When data is received, this serial form of data that is in the signal must be converted into a parallel form matching the bus type (8, 16, or 32 bit) being used by the receiving device.

The mechanism of this data conversion is handled in two ways. First, when data is coming from the computer, to be prepared to be sent out on the network, the network adapter card's driver, or software interface, is responsible for converting this data into a format that can be understood by the network adapter card.

The second part of the data conversion is performed by the physical network card itself. It is here that the actual data that has been passed along from the computer is converted into a serial format using either a digital, analog, or light signal. The network card not only converts the data into this signal, but it also is responsible for accessing the transmission medium and forming a channel to conduct the signals onto the network. In essence, a network card is like the doorway to the network for the PC or other device.

6.4 How a Network Card Works

A physical address is used to distinguish machine A from machine B in a way the network cards can understand. This physical address, a unique identifier assigned to a network card, is often referred to as the Media Access Control (MAC) address, the hardware address, or the ethernet address. All these terms represent the same thing.

A MAC address is a 48-bit address represented by six pairs of hexadecimal values (for example, 00-C0-DF-48-6F-13). The MAC address, which is assigned by the manufacturer of the network card before it is shipped to be sold, is designed to be unique and is used to help identify a single machine on a network. At this level of the networking model, the Physical Layer, data being passed over the network appears to

be nothing more than the transmission and error-checking of negative and positive voltages, represented as 1s and 0s, on the wire. These 1s and 0s are transmitted in a group called a frame. The network card is responsible for determining whether the data is intended for it or another network card. Each network card is given a set of rules. First, there is a preamble used to synchronise the card so it can determine where the data within the frame begins.

After the network card determines where the data begins, it discards the preamble before continuing to the next process. Next, the network card deciphers the data to determine the physical address for which the frame is destined. If the destination address matches the physical address of the network card, or if it is a broadcast, it continues to process the information and pass the remaining data to the protocol. If the destination address specifies some other machine's physical address, the network card silently discards the data within the frame and starts listening for other messages.

To enable you to fully appreciate how a network card functions, two important concepts must be explained. These are signals and clocking.

6.4.1 Signals

Two basic types of signals are used with transmission media:

- ◆ Analog signal.
- ◆ Digital signal.

6.4.1.1 Analog Signals

Analog signals constantly vary in one or more values, and these changes in values can be used to represent data. Analog waveforms frequently take the form of sine waves.

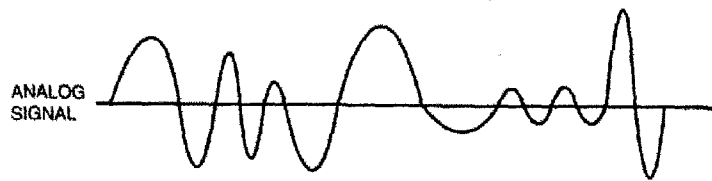


Figure 6.2 An example of an analog signal

The two characteristics that define an analog waveform are as follows:

♦ **Frequency:** Indicates the rate at which the waveform changes. Frequency is associated with the wavelength of the waveform, which is a measure of the distance between two similar peaks on adjacent waves. Frequency generally is measured in Hertz (Hz), which indicates the frequency in cycles per second. Frequency is illustrated in Figure 6.3.

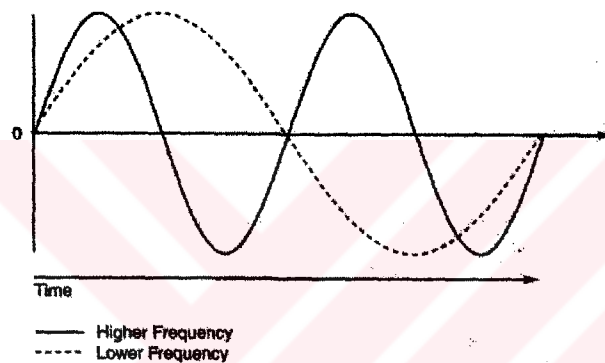


Figure 6.3 These two analog waveforms differ in frequency

♦ **Amplitude:** Measures the strength of the waveform. Amplitude is illustrated in Figure 6.4.

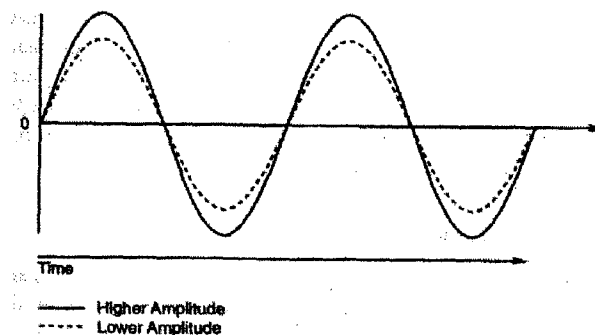


Figure 6.4 These two waveforms differ in amplitude

6.4.1.2 Digital Signals

Digital signals are different than analog signals in that digital signals have two discrete states. These states are either "off" or "on." An example of how a digital signal is represented is seen in Figure 6.5.

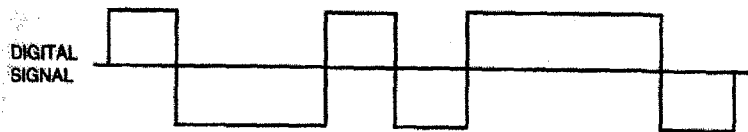


Figure 6.5 An example of a digital signal

6.4.2 Clocking

Clocking is the mechanism used to count and pace the number of signals being sent and received. Signals are expected to be sent in a continuous flow, representing the start and ending of the data. Clocking is the mechanism used by the network adapter card to determine how much data has been sent. For example, if a network card is designed to transmit data at 20,000 Megahertz a second, other cards receiving this data will also read the data at 20,000MHz a second. Clocking is a mechanism used by all network adapter cards to measure how much data has been sent or received.

CHAPTER SEVEN

CONNECTIVITY DEVICES

7.1 Introduction

This chapter examines some important connectivity devices. Connectivity devices include: Modems, repeaters, routers, brouters and gateways. In the following sections, you learn about modems, repeaters, bridges, routers, brouters, and gateways.

7.2 Modems

Standard telephone lines can transmit only analog signals. Computers store and transmit data digitally. Modems can transmit digital computer signals over telephone lines by converting them to analog form.

Converting one signal form to another (digital to analog in this case) is called modulation: Recovering the original signal is called demodulation. Modems can be used to connect computer devices or entire networks that are at distant locations. Some modems operate constantly over dedicated phone lines. Others use standard public switched-telephone network (PSTN) dial-up lines and make a connection only when one is required (Glen Berg, 1998).

Modems enable networks to exchange email and to perform limited data transfers, but the connectivity made possible is extremely limited due to the limited bandwidth most modems offer. Modems don't enable networks to connect to remote networks, like a muter, to directly exchange data. Instead modems act like network cards in that they provide an access point onto the transmission medium in this case the telephone

lines, in order to send analog signals to another device, most likely another modem, on the network.

Until recently, modem manufacturers used a parameter called baud rate to gauge modem performance. The baud rate is the oscillation speed of the sound wave transmitted or received by the modem. Although baud rate is still an important parameter, recent advances in compression technology have made it less meaningful. Some modems now provide a data transfer rate (in bits per second-a more meaningful measure of network performance) that exceeds the baud rate. In other words, you can no longer assume the baud rate and the data transfer rate are equal.

7.3 Repeaters

The most basic LAN connection device, repeaters strengthen the physical transmission signal. A repeater simply takes the electrical signals that reach it and then regenerates them to full strength before passing them on. Repeaters generally extend a single network (rather than link two networks).

The purpose of a repeater is to extend the maximum range for the network cabling. A repeater is a network device that repeats a signal from one port onto the other ports to which it is connected. Repeaters operate at the OSI Physical layer. A repeater does not filter or interpret-it merely repeats (regenerates) a signal, passing all network traffic in all directions.

A repeater doesn't require any addressing information from the data frame because a repeater merely repeats bits of data. This means that if data is corrupt, a repeater will regenerate the signal anyway.

The advantages of repeaters are that they are inexpensive and simple. Also, although they cannot connect networks with dissimilar data frames (such as a token-ring network and an Ethernet network), some repeaters can connect segments with similar frame types but dissimilar-cabling.

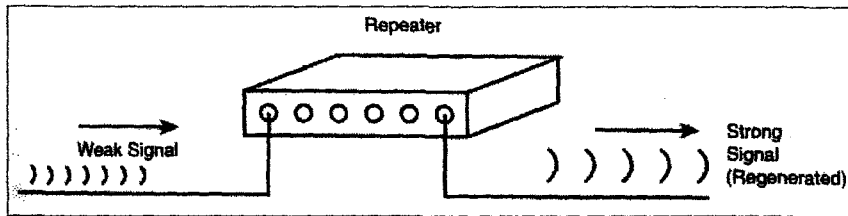


Figure 7.1 A repeater regenerates a weak signal

Figure 7.1 shows the use of a repeater to connect two Ethernet cable segments. The result of adding the repeater is that the potential length of the overall network is doubled.

Some repeaters simply amplify signals. Although this increases the strength of the data signal, it also amplifies any noise on the network. In addition, if the original signal has been distorted in any way, an amplifying repeater cannot clean up the distortion.

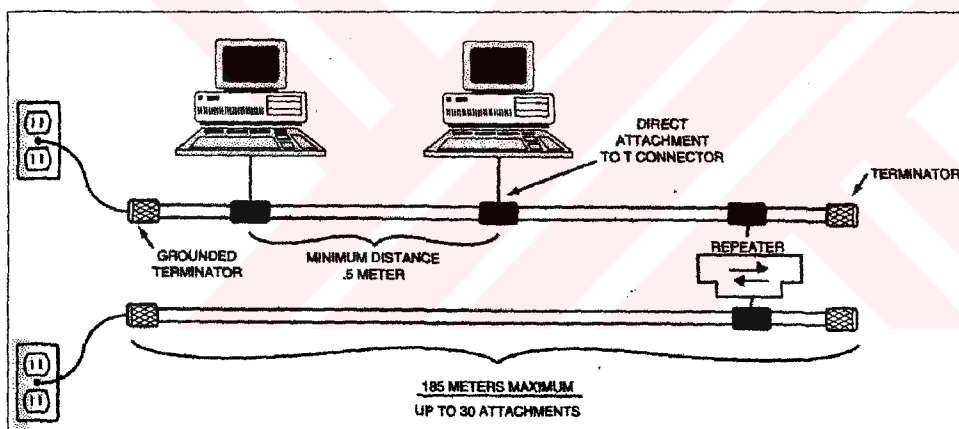


Figure 7.2 Using a repeater to extend an Ethernet LAN

7.4 Hubs

Hubs, also called wiring concentrators, provide a central attachment point for network cabling. Hubs come in two types: Passive and active.

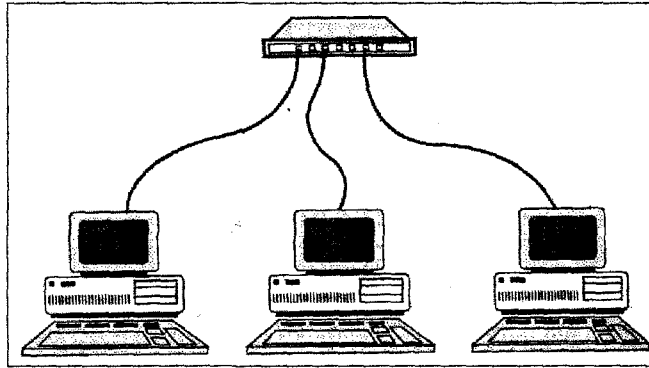


Figure 7.3 A network wired to a central hub

7.4.1 Passive Hubs

Passive hubs do not contain any electronic components and do not process the data signal in any way. The only purpose of a passive hub is to combine the signals from several network cable segments. All devices attached to a passive hub receive all the packets that pass through the hub.

Because the hub doesn't clean up or amplify the signals (in fact, the hub absorbs a small part of the signal), the distance between a computer and the hub can be no more than half the maximum permissible distance between two computers on the network. For example, if the network design limits the distance between two computers to 200 meters, the maximum distance between a computer and the hub is 100 meters.

As you might guess, the limited functionality of passive hubs makes them inexpensive and easy to configure. That limited functionality, however, is also the biggest disadvantage of passive hubs. Often small networks use passive hubs, due to the fact that there are few machines on the LAN and small distances between them.

7.4.2 Active Hubs

Active hubs incorporate electronic components that can amplify and clean up the electronic signals that flow between devices on the network. This process of cleaning

up the signals is called signal regeneration. Signal regeneration has the following benefits:

- ◆ The network is more robust (less sensitive to errors).
- ◆ Distances between devices can be increased.

These advantages generally outweigh the fact that active hubs cost considerably more than passive hubs. Earlier in this chapter, you learned about repeaters, devices that amplify and regenerate network signals. Because active hubs function in part as repeaters, they occasionally are called multiport repeaters.

7.5 Switches

Switches are enhanced active hubs. Several functions can add intelligence to a hub:

- ◆ **Hub management:** Hubs now support network management protocols that enable the hub to send packets to a central network console. These protocols also enable the console to control the hub; for example, a network administrator can order the hub to shut down a connection that is generating network errors.

- ◆ **Switching:** The latest development in hubs is the switching hub, which includes circuitry that very quickly routes signals between ports on the hub. Instead of repeating a packet to all ports on the hub, a switching hub repeats a packet only to the port that connects to the destination computer for the packet. Many switching hubs have the capability of switching packets to the fastest of several alternative paths. Switching hubs are replacing bridges and routers on many networks.

7.6 Bridges

Bridges are used to connect multiple networks, subnets, or rings into one large logical network. A bridge maintains a table of node addresses. Based on this table, it forwards packets to a specific subnet, reducing traffic on other subnets.

Bridges can extend the maximum size of a network. Although the bridged network in Figure 7.4 looks much like the earlier example of a network with a repeater, the bridge is a much more flexible device. Bridges operate at the MAC sublayer of the OSI Data Link layer.

A repeater passes on all signals that it receives. A bridge, on the other hand, is more selective and passes only those signals targeted for a computer on the other side. A bridge can make this determination because each device on the network is identified by a unique physical address.

Each packet that is transmitted bears the address of the device to which it should be delivered. The process works as follows:

1. The bridge receives every packet from either side of it on LAN A.
2. The bridge references an internal table of addresses. This table is either learned by the bridge, from previous packet deliveries on the network, or manually programmed into the bridge.

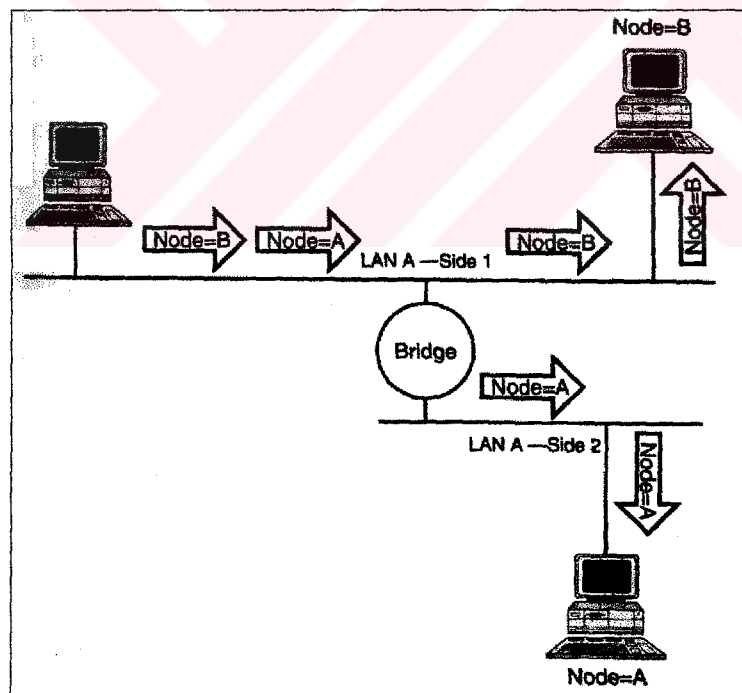


Figure 7.4 Separating signals on a LAN segment with a bridge

3. Packets on LAN A -Side 1 that are addressed to devices on LAN A - Side 1 and packets on LAN A -Side 2 that are addressed to devices on LAN A - Side 2, are not passed along to the other side by the bridge. These packets can be delivered without the help of the bridge.

4. Packets on LAN A - Side 1 addressed to devices on LAN A Side 2 are retransmitted, by the bridge to LAN A -Side 2 for delivery. Similarly, the appropriate packets on LAN A - Side 2 are retransmitted to LAN A - Side 1.

Bridges come in two main forms. One type of bridge is what is known as a transparent or learning bridge. This type of bridge is transparent to the device sending the packet. At the same time this bridge will learn over time what devices exist on each side of it. This is done by the bridge's ability to read the Data-Link information on each packet going across the network. By analysing these packets, and seeing the source MAC address of each device, the bridge is able to build a table of which devices exist on what side of it. There usually is a mechanism for a person to go in and also program the bridge with address information as well. Learning bridges function as described in step 2, automatically updating their address tables as devices are added to or removed from the network. Ethernet networks almost always use a transparent bridge.

Another type of bridge is a source routing bridge. This type of bridge is employed on a token-ring network. A source routing bridge is a bridge that reads information appended to the packet by the sending device. This additional information in the packet will state the route to the destination segment on the network. A source routing bridge will analyse this information to determine whether or not this stream of data should or should not be passed along.

Bridges accomplish several things. First, they divide busy networks into smaller segments. If the network is designed so that most packets can be delivered without crossing a bridge, traffic on the individual network segments can be reduced. If the Accounting and Sales departments are overloading the LAN, for example, you might divide the network so that Accounting is on one segment and Sales on another. Only

when Accounting and Sales must exchange packets does a packet need to cross the bridge between the segments.

Bridges also can extend the physical size of a network. Although the individual segments still are restricted by the maximum size imposed by the network design limits, bridges enable network designers to stretch the distances between segments and extend the overall size of the network. A general rule of thumb for deciding which side of a bridge a device should be placed on is that 80% of the device's traffic should be destined to devices on the same side of the bridge that the device in question resides on.

Bridges cannot join LANs that are utilising different network addresses. This is because bridges operate at the Data Link layer of the OSI model and depends on the physical addresses of devices and not at the Network Layer, which relies on logical network addresses.

7.7 Routing

An internetwork consists of two or more physically connected independent networks that are able to communicate. The networks that make up an internetwork can be of very different types. For example, an internetwork can include Ethernet and token-ring networks.

Because each network in an internetwork is assigned an address, each network can be considered logically separate; that is, each network functions independently of other networks on the internetwork. Internetwork connectivity devices, such as routers, can use network address information to assist in the efficient delivery of messages. Delivering packets according to logical network address information is called routing. The common feature that unites internetwork connectivity devices (routers and brouters) is that these devices can perform routing. The following list details some common internetwork connectivity devices: Routers and Brouters.

7.7.1 Routers

Bridges are suitable for relatively simple networks, but bridges have certain limitations that become more significant in complex network situations. One limitation of bridges is that packets intended for all people on a subnet, also known as a broadcast, are received by every single device on the network. By being able to section off a LAN segment into different network segments, routers allow you to control and group devices that work together to be on the same network segment.

Consider the network in Figure 7.5. Both bridges are aware of the existence of Node B, and both can pick up the packet from Net A and forward it. At the very least, the same packet can arrive twice at Node B.

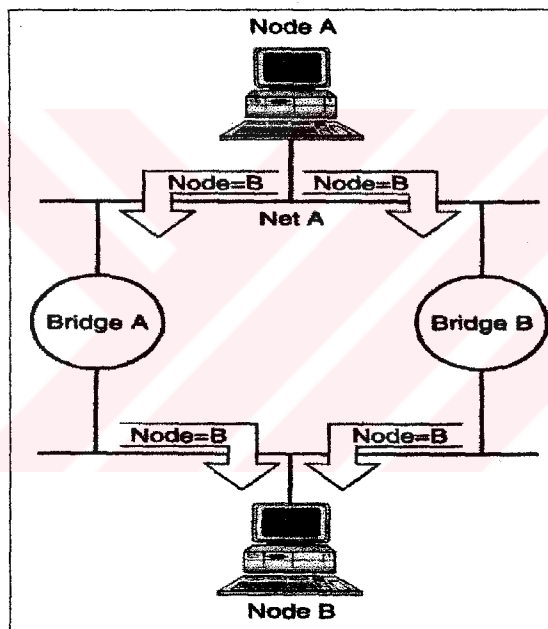


Figure 7.5 A complex network with bridges

A worse case, however, is that these relatively unintelligent bridges can start passing packets around in loops, which results in an ever increasing number of packets that circulate on the network and never reach their destinations. Ultimately, such activity can (and will) saturate the network.

Another problem is that the bridges cannot analyze the network to determine the fastest route over which to forward a packet. When multiple routes exist, this is a desirable capability, particularly in wide area networks (WANs), where some routes are often considerably- slower than others.

Routers organise the large network in terms of logical network segments. Each network segment is assigned an address so that every packet has both a destination network address and a destination device address. Routers are more "intelligent" than bridges. Not only do routers build tables of network locations, but they also use algorithms to determine the most efficient path for sending a packet to any given network. Even if a particular network segment isn't directly attached to the router, the router knows the best way to send a packet to a device on that network. In Figure 7.6, for example, Router A knows that the most efficient step is to send the packet to Router C, not Router B.

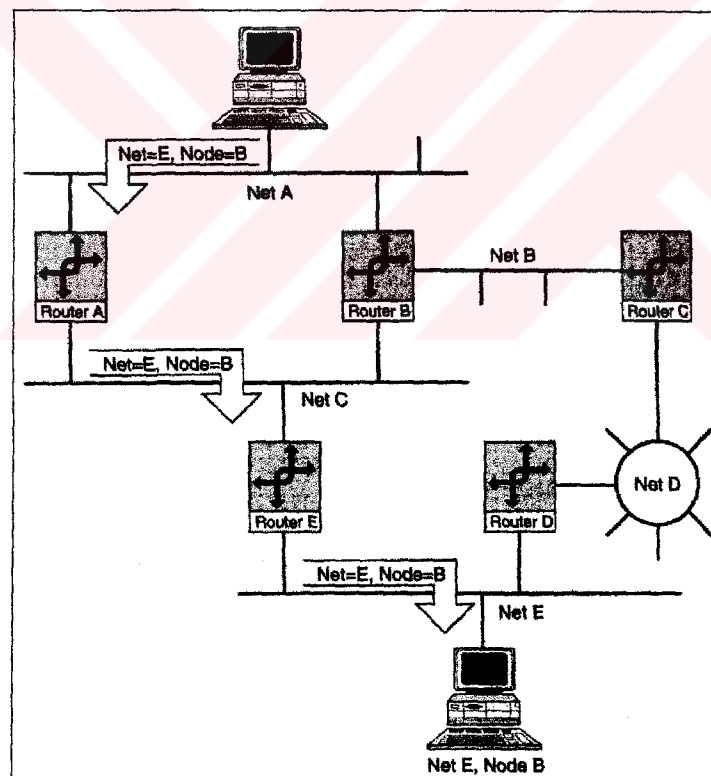


Figure 7.6 An internetwork: A series of networks separated by routers

Notice that Router B presents a redundant path to the path Router A provides. Routers can cope with this situation because they exchange routing information to ensure that packet loops don't occur. In Figure 7.6, if Router A fails, Router B provides a backup message path, thus making this network more robust.

One consequence of all the processing a router performs on a packet is that routers generally are slower than bridges. You can use routers to divide large, busy LANs into smaller segments, much as you can use bridges. But that's not the only reason to select a router. Routers also can connect different network types. An example of this would be a router that connected a token-ring segment with the Ethernet segments. On such networks, a router is the device of choice, as a bridge cannot perform this function.

The protocols used to send data through a router must be specifically designed to support routing functions. IP, IPX, and DDP (the AppleTalk Network-layer protocol) are routable transport protocols. NetBEUI is a non-routable transport protocol.

The Network layer functions independently of the physical cabling system and the cabling system protocols-independently, that is, of the Physical and Data Link layers. This is the reason that routers easily can translate packets between different cabling systems. Bridges, on the other hand, cannot translate packets in this way because they function at the Data Link layer, which is closely tied to physical specifications.

Routers come in two general types:

- ◆ **Static Routers:** These routers do not determine paths. Instead, you must configure the routing table, specifying potential routes for packets.
- ◆ **Dynamic Routers:** These routers have the capability to determine routes (and to find the optimum path among redundant routes) based on packet information and information obtained from other routers.

7.7.2 Routers

A router is a router that also can act as a bridge. A router attempts to deliver packets based on network protocol information, but if a particular Network layer protocol isn't supported, the router bridges the packet using device addresses.

7.8 Gateways

The term "gateway" more commonly refers to a system functioning at the top levels of the OSI model that enables communication between dissimilar protocol systems. A gateway generally is dedicated to a specific conversion, and the exact functioning of the gateway depends on the protocol translations it must perform. Gateways commonly function at the OSI Application layer, but actually can operate at any level of the OSI model. Gateways connect dissimilar environments by removing the layered protocol information of incoming packets and replacing it with the packet information necessary for the dissimilar environment.

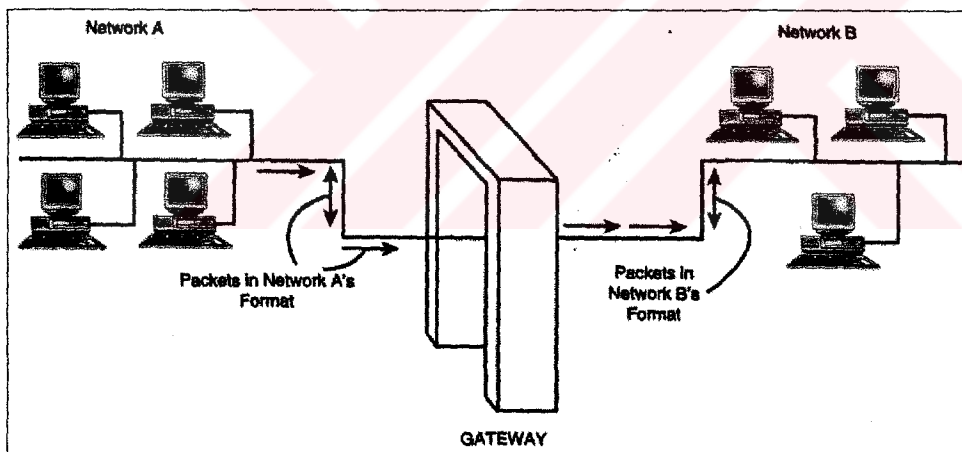


Figure 7.7 Gateways convert protocol information to dissimilar environments

Gateways can be implemented as software, hardware, or a combination of both. An example of a gateway is often seen in email systems. When you send email, say from Microsoft Exchange to someone on the Internet, a gateway is responsible for converting the Microsoft Exchange message contents and addressing, to one that is compatible with the SMTP (Internet) message format and addressing.

CHAPTER EIGHT

TRANSPORT PROTOCOLS

8.1 Introduction

This chapter begins by reviewing and placing into context the information learned from the previous chapters. The analysis begins with an examination of packets and protocols, as well as protocols and their reference back to the OSI model. From that point, the transport protocols of TCP/IP, IPX/SPX, NetBEUI, AppleTalk, and DLC are examined. When analysing these transport protocols, issues such as addressing, routing mechanisms, and services are addressed. The chapter continues by examining NetBIOS naming schemes that are used in Microsoft networks.

8.2 Packets and Protocols

The purpose of a network is to exchange information among computers, and protocols are the rules by which computers communicate. Computers, like humans, can adopt any number of systems for passing messages, as long as the sending and receiving computers are using the same (or compatible) rules. Computers, therefore, must agree on common protocols before they can communicate (Glen Berg, 1998).

Protocols describe the way in which network data is encapsulated in packets on the source end, sent via the network to a destination, and then reconstructed at the destination into the appropriate file, instruction, or request. Breaking network data into packet-sized chunks provides smoother throughput because the small packets don't tie up the transmission medium as a larger unit of data might. Also, packets simplify the task of error detection and correction. Each file is checked separately for errors, and if an error is discovered, only that packet must be retransmitted.

The exact composition of a network packet depends on the protocols you're using. In general, network packets contain the following:

- ◆ **Header:** The header signifies the start of the packet and contains a bundle of important parameters, such as the source and destination address and time/synchronisation information.
- ◆ **Data:** This portion of the packet contains the original data being transmitted.
- ◆ **Trailer:** The trailer marks the end of the packet and typically contains error-checking (Cyclical Redundancy Check, or CRC) information.

As the data passes down through the protocol layers, each layer performs its prescribed function, such as interfacing with an application, converting the data format, or adding addressing and error checking parameters.

When the packet reaches the transmission medium, the network adapter cards of other computers on the network segment examine the packet, checking the packet's destination address. If the destination address matches the PC's address, the network adapter interrupts the processor, and the protocol layers of the destination PC process the incoming packet.

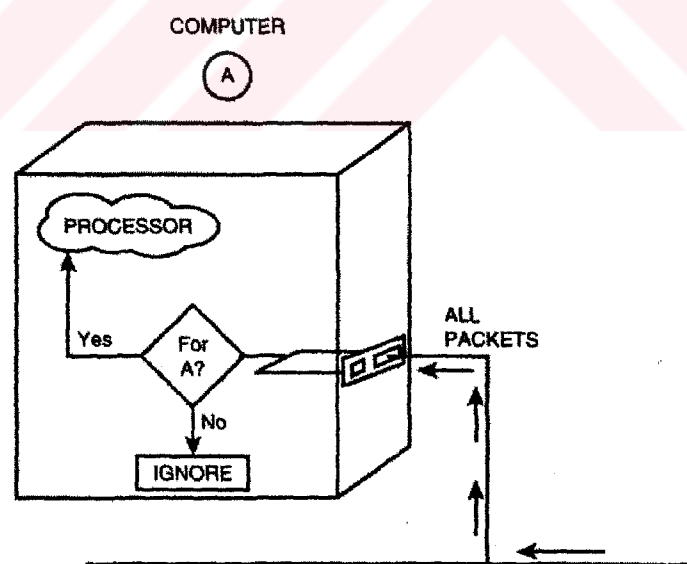


Figure 8.1 The network adapter card checks whether the destination address matches the PC's address

8.3 Protocols and Protocol Layers

Many of the addressing, error-checking, retransmission, and acknowledgement services most commonly associated with networking take place at the Network and Transport OSI layers. Protocol suites are often referred to by the suite's main Transport and Network protocols. In TCP/IP, for instance, TCP is a Transport layer protocol and IP is a Network layer protocol. IPX/SPX is another protocol suite known by its Transport and Network layer protocols, but the order of the protocols is backward from the way the protocols are listed in TCP/IP IPX is the Network and Transport layer protocol; SPX is the Transport layer protocol (Glen Berg, 1998).

The lower Data Link and Physical layers of the OSI model provide a hardware-specific foundation, addressing items such as the network adapter driver, the media access method, and the transmission medium. Transport and Network layer protocols such as TCP/IP and IPX/SPX rest on that Physical and Data Link layer foundation, and, with the help of the NDIS and ODI standards, multiple protocol stacks can operate simultaneously through a single network adapter.

This chapter describes the common protocol suites and many of the important protocols associated with them. In addition to TCP/IP and IPX/SPX, some of the common Transport and Network layer protocols are the following:

- ◆ **NWLink:** Microsoft's version of the IPX/SPX protocol essentially spans the Transport and Network layers.
- ◆ **NetBEUI:** Designed for Microsoft networks, NetBEUI includes functions at the Network and Transport layers. NetBEUI isn't routable and therefore doesn't make full use of Network layer capabilities.
- ◆ **AppleTalk:** Transaction Protocol (ATP) and Name Binding Protocol (NBP). ATP and NBP are AppleTalk Transport layer protocols.
- ◆ **Data Link Control (DLC).** This is used to connect to IBM Mainframes and Hewlett-Packard JetDirect printers.

8.3.1 TCP/IP-Internet Protocols

Select the appropriate network and transport protocols for various token-ring and ethernet networks. Protocols include the following: DLC, AppleTalk, IPX, TCP/IP, NFS, and SMB.

One reason for the popularity of TCP/IP is that no one vendor owns it, unlike the IPX/SPX, DNA, SNA, or AppleTalk protocol suites, all of which are controlled by specific companies. TCP/IP evolved in response to input from a wide variety of industry sources. Consequently, TCP/IP is the most open of the protocol suites and is supported by the widest variety of vendors. Virtually every brand of computing equipment now supports TCP/IP. This has led to some problems, though. Because TCP/IP is an open standard, sometimes one vendor's implementation of TCP/IP does not work with another's implementation.

Figure 8.2 illustrates the relationship of the protocols in the Internet suite to the layers of the OSI reference model. Notice that the suite doesn't include protocols for the Data Link or Physical layers. TCP/IP was designed to be hardware-independent and thus is able to work over established standards such as ethernet, token-ring, and ARCnet, to name but a few lower OSI layer standards. Over time, TCP/IP has been interfaced to the majority of Data Link and Physical layer technologies.

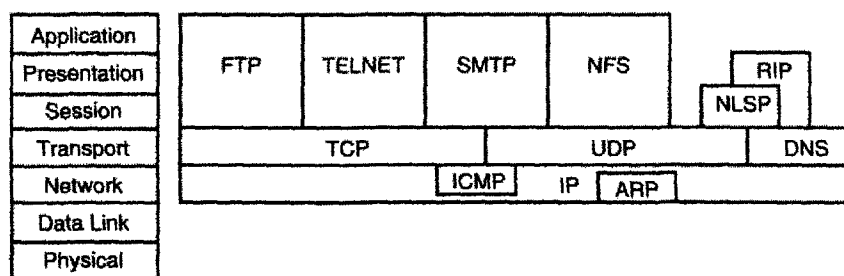


Figure 8.2 TCP/IP or the “Internet Protocol Suite”

One huge advantage of using TCP/IP is that TCP/IP is required for communication over the Internet; thus the Internet can be used as a communication backbone. One disadvantage is that the size of the protocol stack makes TCP/IP

difficult to implement on some older machines. TCP/IP has traditionally been considered slower than other protocol stacks, because data must be analysed up to the Network layer of the OSI model to be evaluated.

A large number of protocols are associated with TCP/IP. These different protocols are grouped into the following unofficial categories:

- ◆ General TCP/IP Transport Protocols
- ◆ TCP/IP Services
- ◆ TCP/IP Routing

8.3.1.1 General TCP/IP Transport Protocols

This subsection covers general protocols dealing with the addressing and transportation of packets across the LAN using TCP/IP. All services and routing issues that fall into the TCP/IP protocol stack use one or more of these Network or Transport layer protocols.

8.3.1.1.1 Addressing in TCP/IP

One of the first aspects of transport protocols that needs to be discussed is how the protocols address entities on the network. As discussed several times previously in this book, there are two main forms of addresses: a node address and a logical network address. A node address is the address of the entity or device on the network, whereas the logical network address is the segment on the network to which the node is attached.

TCP/IP uses a unique numbering scheme that encapsulates the network and node address into a set of numbers. This number is what is known as an IP address. All devices on a network that runs the TCP/IP protocol suite need a unique IP address.

An IP address is a set of four numbers, or octets, that can range in value between 0 and 255. Each octet is separated by a period. Some examples are shown here:

- ◆ 34.120.66.79
- ◆ 200.200.20.2
- ◆ 2.5.67.123
- ◆ 107.219.2.34

These addresses are actually broken down into three distinct classes. These are known as class A, class B, and class C addresses. Class A IP addresses contain a number between 1 and 127 before the first dot. Some examples are 3.3.6.8, 102.100.77.8, and 23.23.45.67. In a class A address, this first octet represents the network address, and the last three octets represent the node or host number. Hence an IP address of 69.23.104.200 would represent host number 23.104.200 on network 69.

Class B and C addresses follow a similar principal to that exemplified in the class A addresses. In the case of a class B address, the first octet can range in value from 128 to 191, but it is the first two octets that make up the network address, and the last two octets that make up the host ID. In the case of a class C address, the first octet can range in value from 192 to 223, and the first three octets make up the host ID. There are class D and E addresses as well. For these addresses, the first octet is a number greater than 223. These addresses are not currently available to be used and are reserved for other purposes (Glen Berg, 1998).

In summary, the differences in the classes of the IP addresses reside in which numbers are to be used in the first octet, which octets represent the Network ID, and which numbers represent the host ID. Table 8.1 shows three examples, one from each class of address.

Table 8.1 Classes and Addresses

Class	IPAddress	Network ID	Host ID
Class A	102.44.7.100	102.0.0.0	X.44.7.10
Class B	131.107.4.6	131.107.0.0	X.X.4.6
Class C	200.9.88.250	200.9.88.0	X.X.X.250

8.3.1.1.2 Internet Protocol (IP)

The Internet Protocol (IP) is a connectionless protocol that provides datagram service, and IP packets are most commonly referred to as IP datagrams. IP is a packet-switching protocol that performs the addressing and route selection. An IP header is appended to packets, which are transmitted as frames by lower-level protocols. IP routes packets through internetworks by utilising routing tables that are referenced at each hop. Routing determinations are made by consulting logical and physical network device information, as provided by the Address Resolution Protocol (ARP).

IP performs packet disassembly and reassembly as required by packet size limitations defined for the Data Link and Physical layers being implemented. IP also performs error checking on the header data using a checksum, although data from upper layers is not error checked.

8.3.1.1.3 Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is an internetwork connection-oriented protocol that corresponds to the OSI Transport layer. TCP provides full-duplex, end-to-end connections. When the overhead of end-to-end communication acknowledgement isn't required, the User Datagram Protocol (UDP) can be substituted for TCP at the Transport (host-to-host) level. TCP and UDP operate at the same layer.

TCP corresponds to SPX in the NetWare environment. TCP maintains a logical connection between the sending and receiving computer systems. In this way, the integrity of the transmission is maintained. TCP detects any problems in the transmission quickly and takes action to correct them. The trade-off is that TCP isn't as fast as UDP, due to the number of acknowledgements received by the sending host.

TCP also provides and assumes message fragmentation and reassembly and can accept messages of any length from upper-layer protocols. TCP fragments message streams into segments that can be handled by IP. This process enables the application being used to not break up the data into smaller blocks. IP still can perform fragmentation for UDP packets and further fragmentation for TCP packets. When used with IP, TCP adds connection-oriented service and performs segment synchronisation, adding sequence numbers at the byte level.

In addition to message fragmentation, TCP can multiplex conversations with upper-layer protocols and can improve use of network bandwidth by combining multiple messages into the same segment. Each virtual-circuit connection is assigned a connection identifier called a port, which identifies the datagrams associated with that connection.

8.3.1.1.4 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless Transport (host-to-host) layer protocol. UDP does not provide message acknowledgements; rather, it simply transports datagrams.

Like TCP, UDP utilises port addresses to deliver datagrams. These port addresses, however, aren't associated with virtual circuits and merely identify local host processes. UDP is preferred over TCP when high performance or low network overhead is more critical than reliable delivery. Because UDP doesn't need to establish, maintain, and close connections, or control data flow, it generally outperforms TCP. The downfall in UDP is that it does not perform as reliably as TCP when transmitting data; thus, UDP is often used when transmitting smaller amounts of data.

UDP is the Transport layer protocol used with the Simple Network Management Protocol (SNMP), the standard network management protocol used with TCP/IP.

networks. UDP enables SNMP to provide network management with a minimum of network overhead.

8.3.1.1.5 Address Resolution Protocol (ARP)

Three types of address information are used on TCP/IP internetworks:

- ◆ **Physical addresses:** Used by the Data Link and Physical layers.
- ◆ **IP addresses:** Provide logical network and host IDs. IP addresses consist of four numbers typically expressed in dotted-decimal form.
- ◆ **Logical node names:** Identify specific hosts with alphanumeric identifiers, which are easier for users to recall than the numeric IP addresses. An example of a logical node name is MYHOSTCOM.

Given an IP address, the Address Resolution Protocol (ARP) can determine the physical address used by the device containing the IP address. ARP maintains tables of address resolution data and can broadcast packets to discover addresses on the network segment or use previously cached entries. The physical addresses discovered by ARP can be provided to Data Link layer protocols. All addresses in the ARP table are only local addresses. Any non-local address contains the hardware address of the local port on the router that is used to access that non-local segment.

8.3.1.1.6 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) enhances the error control provided by IP Connectionless protocols, such as IP, cannot detect internetwork errors, such as congestion or path failures. ICMP can detect such errors and notify IP and upper-layer protocols. A network card that is generating an error often delivers a message to other network cards, via an ICMP packet.

8.3.1.2 TCP/IP Services

This section focuses on some of the TCP/IP services that exist within the TCP/IP protocol suite. These services are just some of the more common ones that you would deal with on a Microsoft network.

8.3.1.2.1 Dynamic Host Configuration Protocol (DHCP)

When dealing with IP addressing, it can be very management intensive to manually assign IP addresses and subnet masks to every computer on the network. The Dynamic Host Configuration Protocol enables automatic assignment of IP addresses. This is usually performed by one or more computers that assigns IP addresses and subnet masks, along with other configuration information, to a computer as it initialises on the network.

Most routers are configured not to forward broadcasts. DHCP, however, exchanges information by issuing broadcasts. A DHCP server, therefore, needs to be on each segment. An alternative to placing a DHCP server on each segment is to have a DHCP relay agent that forwards on the client's broadcast request for an IP address to a DHCP server on another segment.

8.3.1.2.2 Domain Name System (DNS)

The Domain Name System (DNS) protocol provides host name and IP address resolution as a service to client applications. DNS servers enable humans to use logical node names, utilising a fully qualified domain name structure, to access network resources. Host names can be up to 260 characters long.

8.3.1.2.3 Windows Internet Naming Services (WINS)

Windows Internet Naming Service (WINS) provides a function similar to that of DNS, with the exception that it provides NetBIOS names to IP address resolution.

This is important, because all of Microsoft's networking requires the ability to reference NetBIOS names. Normally NetBIOS names are obtained with the issuance of broadcasts, but because routers normally do not forward broadcasts, a WINS server is one alternative that can be used to issue IP addresses to NetBIOS name requests.

8.3.1.2.4 File Transfer Protocol (FTP)

The File Transfer Protocol (FTP) is a protocol for sharing files between networked hosts. FTP enables users to log on to remote hosts. Logged-on users can inspect directories, manipulate files, execute commands, and perform other commands on the host. FTP also has the capability of transferring files between dissimilar hosts by supporting a file request structure that is independent of specific operating systems.

8.3.1.2.5 Simple Mail Transfer Protocol (SMTP)

The Simple Mail Transfer Protocol (SMTP) is a protocol for routing mail through internetworks. SMTP uses the TCP and IP protocols. SNMP doesn't provide a mail interface for the user. Creation, management, and delivery of messages to end-users must be performed by an email application.

8.3.1.2.6 Remote Terminal Emulation (TELNET)

TELNET is a terminal emulation protocol. TELNET enables PCs and workstations to function as dumb terminals in sessions with hosts on internetworks. TELNET implementations are available for most end-user platforms, including UNIX (of course), DOS, Windows, and Macintosh OS.

8.3.1.2.7 Network File System (NFS)

Network File System (NFS), developed by Sun Microsystems, is a family of file-access protocols that are a considerable advancement over FTP and TELNET. Because Sun made the NFS specifications available for public use, NFS has achieved a high level of popularity. NFS consists of two protocols:

- ◆ **eXternal Data Representation (XDR):** Supports encoding of data in a machine-independent format. C programmers use XDR library routines to describe data structures that are portable between machine environments.
- ◆ **Remote Procedure Call (RPC):** Functions as a service request redirector that determines whether function calls can be satisfied locally or must be redirected to a remote host. Calls to remote hosts are packaged for network delivery and transmitted to RPC servers, which generally have the capability of servicing many remote service requests. RPC servers process the service requests and generate response packets that are returned to the service requester.

8.3.1.3 TCP/IP Routing Protocols

The following sections describe two of the most common routing protocols used by TCP/IP.

8.3.1.3.1 Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) in the TCP/IP suite is not the same protocol as RIP in the NetWare suite, although the two serve similar functions. Internet RIP performs route discovery by using a distance-vector method, calculating the number of hops that must be crossed to route a packet by a particular path.

Although it works well in localised networks, RIP presents many weaknesses that limit its utility on wide-area internetworks. RIP's distance vector route discovery method, for example, requires more broadcasts and thus causes more network traffic than some other methods. The entire route table is also sent out on the broadcast,

causing large amounts of traffic, as route tables become large. The Open Shortest Path First (OSPF) protocol, which uses the link-state route discovery method, is gradually replacing RIP.

8.3.1.3.2 Open Shortest Path First (OSPF)

The Open Shortest Path First (OSPF) protocol is a link-state route discovery protocol that is designed to overcome the limitations of RIP. On large internetworks, OSPF can identify the internetwork topology and improve performance by implementing load balancing and class-of-service routing.

8.3.2 NetWare IPX/SPX

The protocols utilised with NetWare are summarised in Figure 8.3. The NetWare protocols have been designed with a high degree of modularity. This modularity makes the NetWare protocols adaptable to different hardware and simplifies the task of incorporating other protocols into the suite. Windows NT doesn't use the IPX/SPX suite to communicate with NetWare resources. Microsoft instead developed a clone of IPX/SPX called NWLink-IPX/SPX Compatible Transport. IPX/SPX is generally smaller and faster than TCP/IP and, like TCP/IP, it is routable. However, it operates down to the Data Link layer of the OSI model so it is more dependent upon hardware devices than the TCP/IP protocol.

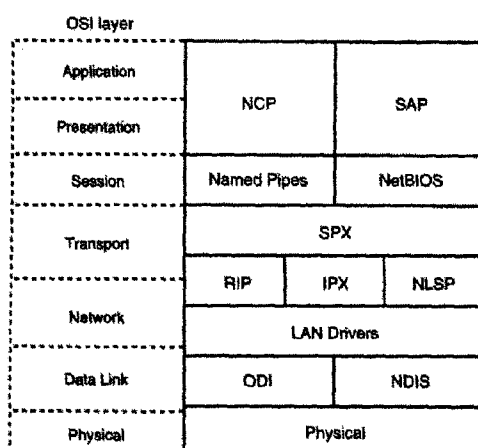


Figure 8.3 The NetWare protocol architecture

8.3.2.1 General IPX/SPX Transport Protocols

The following subsections deal with protocols in the IPX/SPX protocol suite that relate back to the Network and Transport layers of the OSI model.

8.3.2.1.1 Addressing in IPX

Addressing in IPX/SPX (NWLink) is much simpler than that in TCP/IP. IPX/SPX also has two distinct addresses: a host address and a network address. Unlike TCP/IP, the host address, or ID, is often something that is not configured by the administrator. The host address in IPX/SPX is based on the hardware address of the network adapter card used by the device attaching to the network. These addresses are hexadecimal in nature, and address ranges used by network adapter cards are assigned by the IEEE. Usually the first two to three sets of numbers indicate the manufacturer of the network adapter card.

Two examples of these addresses are:

44-45-53-54-00-00

07-00-4d-55-64-3e

As for the network address, this logical address is assigned by the administrator of the cable segment. Usually when a server or router is installed, the logical network address is assigned by the administrator. The logical network address is an eight-character hexadecimal address. Some possible examples include:

903E04G7, BEEF0000, E8012000

Again, any set of hexadecimal values is acceptable, but each network address must be unique on the internetwork. In general, addresses in an IPX/SPX network are often represented as Host address: Network Address, as seen below:

55-GG-00-e4-7a: E8022000

This address represents Host 55-GG-00-e4-7a on Network E8022000.

8.3.2.1.2 IPX

The Internetwork Packet Exchange Protocol (IPX) is a Network layer protocol that provides connectionless (datagram) service. (IPX was developed from the XNS protocol originated by Xerox.) As a Network layer protocol, IPX is responsible for internetwork routing and for maintaining network logical addresses. Routing uses the RIP protocol (described later in this section)-to make route selections. IPX provides similar functionality as UDP does in the TCP/IP protocol suite.

IPX relies on hardware physical addresses found at lower layers to provide network device addressing. IPX also uses sockets, or upper layer service addresses, to deliver packets to their ultimate destinations. On the client, IPX support is provided as a component of the older DOS shell and the current DOS NetWare requester. Windows 3.1 utilises the DOS shell client, whereas Windows 95 and Windows NT supports IPX if you install a Novell-supplied client. Microsoft-supplied clients use the NWLink transport protocol supplied by Microsoft.

8.3.2.1.3 SPX

Sequenced Packet Exchange (SPX) is a Transport layer protocol that extends IPX to provide connection-oriented service with reliable delivery. Reliable delivery is ensured by the retransmitted of packets in the event of an error. SPX is derived from a similar SPX protocol in the XNS network protocol suite.

SPX establishes virtual circuits called connections. The connection ID for each connection appears in the SPX header. A given upper-layer process can be associated with multiple-connection IDs. SPX is used in situations where reliable transmission of data is needed. SPX sequences the packets of data. Missing packets or packets that don't arrive in the order in which they were sent are detected immediately. In addition, SPX offers connection multiplexing, which is used in the printing environment. Many accounting programs, for example, call upon the services of SPX to ensure that data is sent accurately. On the client, SPX support is provided as a

component of the older DOS shell and of the current NetWare requester. SPX provides functionality similar to that of TCP in the TCP/IP protocol suite.

As a network administrator, you do not often get to pick whether you wish to use IPX or SPX. It is often the applications one uses that are preprogrammed to use one or the other. For example, in most Novell networks, all file transfers are done using IPX. In the case of printing, SPX is the protocol used.

8.3.2.1.4 Frame Type

When dealing with the IPX/SPX protocol suite, frame type is an important issue. Frame type deals with the issue of how the data is read by the adapter card. As you have seen in earlier chapters, data is transmitted in digital format within a computer, and the network card converts this digital information into a signal. This signal not only contains the data being transferred, but also headers of information being used by all the protocols in the OSI seven layers. When this data arrives at its destination, it gets converted from a signal back into a recognisable format understood by the computer. Frame type has to do with interpreting the bits of data as they come in. As you will see in the following five sections, each of the five frame types orders the information in the data differently than the other frame types. Two computers not running the same frame type cannot communicate.

When installing the IPX/SPX (or Microsoft's NWLink) protocol on a system, the frame type will either be automatically detected or must be manually assigned. Most modern computers can run multiple frame types at once. The frame types to be discussed below include:

- ◆ 802.2
- ◆ 802.3
- ◆ Ethernet II
- ◆ Ethernet SNAP
- ◆ Token-Ring
- ◆ Token-Ring SNAP

8.3.2.2 IPX/SPX Services

IPX/SPX services are similar to those used by TCPIIP in that they provide a service to the user rather than being solely concerned with transport issues. These services presented usually require the use of either IPX or SPX as their transport mechanism, although recently the capability to port these services over to TCP/IP has been included. Two services are briefly discussed in the following subsections. These are SAP and NCP.

8.3.2.2.1 Service Advertising Protocol (SAP)

With Service Advertising Protocol (SAP), a device provides location information by indicating what services it is offering. Devices can see each other on the network by listing the SAPS each server issues. In the case of NetWare, by default a SAP is issued every minute, telling other computers what service the server is offering, as well as on which node on what network this server is located.

8.3.2.2.2 NetWare Core Protocol (NCP)

The NetWare Core Protocol (NCP) provides numerous function calls that support network services, such as file service, printing, name management, file locking, and synchronisation. NetWare client software interfaces with NCP to access NetWare services. NCP is to NetWare networks as SMB is to Microsoft.

8.3.2.3 IPX/SPX Routing

This section looks at some of the more common routing protocols that can be used in a network running IPX/SPX.

8.3.2.3.1 Router Information Protocol (RIP)

The Router Information Protocol (RIP) uses the distance vector route discover method to determine hop counts to other devices. Like IPX, RIP was developed from

a similar protocol in the XNS protocol suite. RIP is implemented as an upper-layer service and is assigned a socket (service address). RIP is based directly on IPX and performs Network layer functions.

8.3.2.3.2 NetWare Link Services Protocol (NLSP)

NetWare Link Services Protocol (NLSP) is a link-state routing protocol used by routers (NetWare servers with two or more adapter cards can act as routers) to advertise networks when their address tables change.

8.3.3 NetBEUI

NetBEUI is a transport protocol that serves as an extension to Microsoft's Network Basic Input/Output System (NetBIOS). Because NetBEUI was developed for an earlier generation of DOS-based PCs, it is small, easy to implement, and fast. It is actually the fastest transport protocol available with Windows NT. Because it was built for small, isolated LANs, however, NetBEUI is non-routable, making it somewhat anachronistic in today's diverse and interconnected networking environment. NetBEUI is also a broadcast-based protocol and as such can cause congestion in larger networks. Fortunately, the NDIS standard enables NetBEUI to coexist with other routable protocols. For instance, you could use NetBEUI for fast, efficient communications on the LAN segment and use TCP/IP for transmissions that require routing.

8.3.4 AppleTalk

AppleTalk is the computing architecture developed by Apple Computer for the Macintosh family of personal computers. Although AppleTalk originally supported only Apple's proprietary Local Talk cabling system, the suite has been expanded to incorporate both ethernet and token-ring Physical layers. Within Microsoft operating systems, AppleTalk is only supported by Windows NT Server. Windows NT Workstation and Windows 95 do not support AppleTalk. AppleTalk cannot be used

for Microsoft-to-Microsoft operating system communication. It can be used only through Windows NT servers supporting Apple clients.

The Local Talk, Ether Talk, and Token Talk Link Access Protocols (LLAP, ELAP, and TLAP) integrate AppleTalk upper-layer protocols with the Local Talk, ethernet, and token-ring environments.

Apple's Datagram Deliver Protocol (DDP) is a Network layer protocol that provides connectionless service between two sockets. A socket is the AppleTalk term for a service address. A combination of a device address, network address, and socket uniquely identifies each process. DDP performs network routing and consults routing tables maintained by Routing Table Maintenance Protocol (RTMP) to determine routing. Packet delivery is performed by the data link protocol operating on a given destination network.

The AppleTalk Transaction Protocol (ATP) is a connectionless Transport layer protocol. Reliable service is provided through a system of acknowledgements and retransmissions. Retransmissions are initiated automatically if an acknowledgement is not received within a specified time interval. ATP reliability is based on transactions. A transaction consists of a request followed by a reply. ATP is responsible for segment development and performs fragmentation and reassembly of packets that exceed the specifications for lower-layer protocols. Packets include sequence numbers that enable message reassembly and retransmission of lost packets. Only damaged or lost packets are retransmitted.

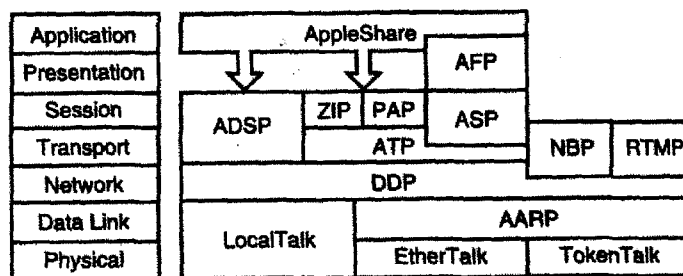


Figure 8.4 The AppleTalk protocol suite

The AppleTalk File Protocol (AFP) provides file services and is responsible for translating local file service requests into formats required for network file services. AFP directly translates command syntax and enables applications to perform file format translations. AFP is responsible for file system security, and verifies and encrypts logon names and passwords during connection setup.

8.3.5 Data Link Control (DLC)

The Data Link Control (DLC) protocol does not provide a fully functioning protocol stack. In Windows NT systems, DLC is used primarily to access Hewlett-Packard JetDirect network-interface printers. DLC also provides some connectivity with IBM mainframes and for the Windows NT remote boot service used by Diskless Windows 95 workstations. DLC is not a protocol that can be used to connect Windows NT or 95 computers together.

8.4 NetBIOS Names

NetBIOS is an interface that provides NetBIOS-based applications with access to network resources. Every computer on a Windows NT network must have a unique name for it to be accessible through the NetBIOS interface. This unique name is called a computer name or a NetBIOS name.

8.4.1 NetBIOS Background

NetBIOS (Network Basic Input/Output System) is an application interface that provides PC-based applications with uniform access to lower protocol layers. NetBIOS was once most closely associated with the NetBEUI protocol-NetBEUI, in fact, is an abbreviation for NetBIOS Extended User Interface. In recent years, however, other vendors have recognised the importance of providing compatibility with PC-based applications through NetBIOS, and NetBIOS is now available with

many protocol configurations. For instance, such terms as "NetBIOS over IPX" or "NetBIOS over TCP/IP" refer to the protocols used with NetBIOS.

8.4.2 Assigning NetBIOS Names

On a NetBIOS network, every computer must have a unique name. The computer name must be 15 characters long or fewer. A NetBIOS name can include alphanumeric characters and any of the following special characters:

!@#\$%^&()-_'.~

Note that you cannot use an asterisk or all periods in a NetBIOS name. It is also not recommended to use spaces in NetBIOS names as well, as some applications are not able to work with a space in a NetBIOS name. Also, NetBIOS names are not case-sensitive. Within these character limitations, you can choose any name for a PC. The rule of thumb is to choose a name that helps you to identify the computer. Names such as PC1, PC2, and PC3 are difficult to visualise and easy to confuse. Likewise, names such as MYPC or WORTHLESSPC could confuse you in the long run, especially if you have many computers on your network. For these reasons, names that include a hook relating the name of the owner or the location of the computer generally are more effective. Consider the following names, for example:

- ◆ BILLS_PC
- ◆ MARKETINGPC
- ◆ LUNCHROOM PC
- ◆ BILLS_LAPTOP

You must specify a computer name for a Windows NT or Windows 95 computer at installation. The computer name then becomes part of the network configuration. In either Windows NT or Windows 95, you can change the name of the computer through the Control Panel Network application.

CHAPTER NINE

DISASTER RECOVERY

9.1 Introduction

The administrator must handle two major issues to guard against the danger of a failed server: Protecting data and reducing downtime. This chapter discusses both issues and examines how the use of fault-tolerant disk configurations and a backup strategy can help reduce the danger of lost time and data.

9.2 Protecting Data

Natural disasters, equipment failures, power surges, and deliberate vandalism can cause the catastrophic loss of precious network data. Microsoft highlights these important strategies for preventing data loss:

- ◆ Backup
- ◆ Uninterruptible Power Supply (UPS)

9.2.1 Backup

A backup schedule is an essential part of any data-protection strategy. You should design a backup system that is right for your situation and the data on your network. A number of different strategies can be used in backing up files. One way is simply to copy a file to another drive. Operating systems, however, typically have special backup commands that help you with some of the bookkeeping required for maintaining a systematic backup schedule. Most backup commands mark the file with the date and time of the backup so that you can know when a copy of the file was last saved. This is the purpose of the FAT file system's Archive attribute. To

determine whether this attribute exists, check the properties of any file on a FAT partition. If the Archive attribute is enabled, the file has changed since the last time a backup was done. In this chapter, you will see that some backup techniques reset this attribute, whereas others do not.

Although backups can be accomplished by saving files to a different drive, they typically are performed with some form of tape drive. Commonly called DAT drives, these devices are capable of storing many gigabytes of information quickly and economically. Moreover, the tapes are small and portable and cheaper on a per-megabyte basis than a hard drive.

In addition to two types of copy commands, Microsoft identifies the following backup types:

- ◆ **Full backup:** Backs up all specified files.
- ◆ **Incremental backup:** Backs up only those files that have changed since the last full or incremental backup.
- ◆ **Differential backup:** Backs up the specified files if the files have changed since the last backup. This type doesn't mark the files as having been backed up, however.
- ◆ **Daily Copy:** This is a Microsoft Windows NT NTBACKUP utility specific command. This command backs up only those files that were changed the day that this option was selected when doing a Daily Copy backup and does not modify the archive bit of the files being backed up.
- ◆ **Copy:** This is the other Microsoft Windows NT NTBACKUP utility specific command. This command backs up all selected files, but does not modify the archive bit of those files being backed up.

A typical backup plan includes some combination of these backup types performed at regular intervals. One common practice is to perform an incremental or differential backup each day and a full backup every week. Full backups make the restoration process easier because there is theoretically only one set of tapes from which to restore.

Differential backups are similar to incremental backups except that they do not reset the Archive attribute, which means that each backup during the week backs up all files changed since the last full backup. A full backup once a week (generally Friday or Saturday) and differentials every other day means that theoretically only two tapes are needed in case of failure: the last full backup and the last differential.

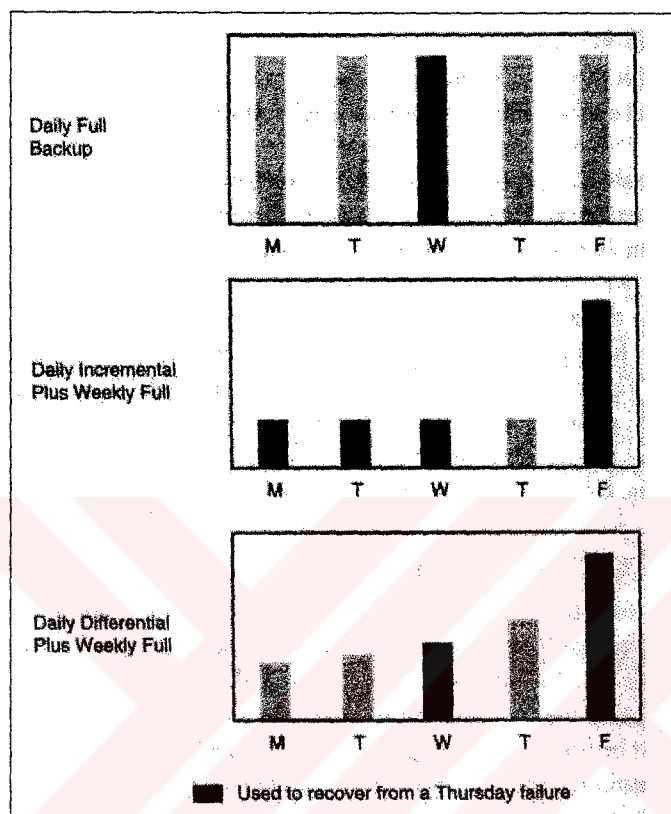


Figure 9.1 An ideal backup scheme implements a schedule of different backup types

Keeping a log of all backups is important. Most backup utilities can generate a backup log. Microsoft recommends that you make two copies of the backup log—store one with the backup tapes and keep one at the computer site. Always test your backup system before you trust it. Perform a sample backup, restore the data, and check the data to be sure it is identical to the original (Glen Berg, 1998).

You can attach a tape drive directly to a single server, or you can back up several servers across the network at once. Backups over the network are convenient for the

administrator, but they can produce considerable network traffic. You can reduce the effects of this extra traffic if you place the computer attached to the tape drive on an isolated network segment and connect it directly to secondary network interface cards on each of the servers.

9.2.2 Uninterruptible Power Supply

An Uninterruptible Power Supply (UPS) is a special battery (or sometimes a generator) that supplies power to an electronic device in the event of a power failure. UPSs are commonly used with network servers to prevent a disorderly shutdown by warning users to log out. After a predetermined waiting period, the UPS software performs an orderly shutdown of the server. Many UPS units also regulate power distribution and serve as protection against power surges. Remember that in most cases a UPS generally does not provide for continued network functionality for longer than a few minutes. A UPS is not intended to keep the server running through a long power outage, but rather is designed to give the server time to do what it needs to before shutting down. This can prevent the data loss and system corruption that sometimes results from sudden shutdown (Glen Berg, 1998).

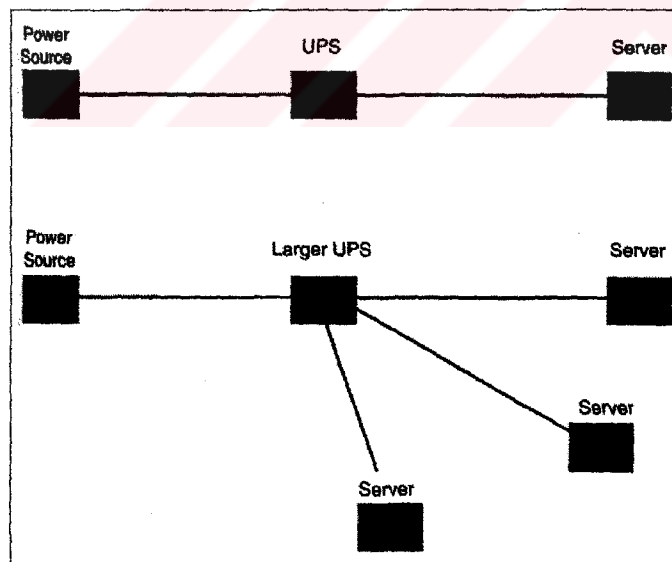


Figure 9.2 A large UPS can service numerous components at once

9.3 Recovering From System Failure

Next to data security, keeping the network up and running properly is the most crucial day-to-day task of an administrator. The loss of a hard drive, even if not disastrous, can be a major inconvenience to your network users and may cost your organisation in lost time and money. Procedures for lessening or preventing downtime from single hardware failures should be implemented. Disk configurations that enable this sort of protection are called fault-tolerant configurations. It should be noted that fault-tolerant configurations are not designed as a replacement for system tape backups.

9.3.1 Implementing a Fault-Tolerant Design

Connecting network components into a fault-tolerant configuration ensures that one hardware failure doesn't halt the network. You can achieve network fault tolerance by providing redundant data paths, redundant hubs, and other such features. Generally, however, the data on the server itself is the most crucial.

9.3.2 Using RAID

A vital tool for protecting a network's data is the use of a Redundant Array of Inexpensive Disks (RAID). Using a RAID system enables you to set up the best disk array design to protect your system. A RAID system combines two or more disks to create a large virtual disk structure that enables you to store redundant copies of the data. In a disk array, the drives are co-ordinated into different levels of RAID, to which the controller card distributes the data (Glen Berg, 1998).

RAID uses a format of splitting data among drives at the bit, byte, or block level. The term data striping refers to the capability of arranging data in different sequences across drives. Demonstration of data striping are shown in Figure 9.3. Microsoft calls this disk striping.

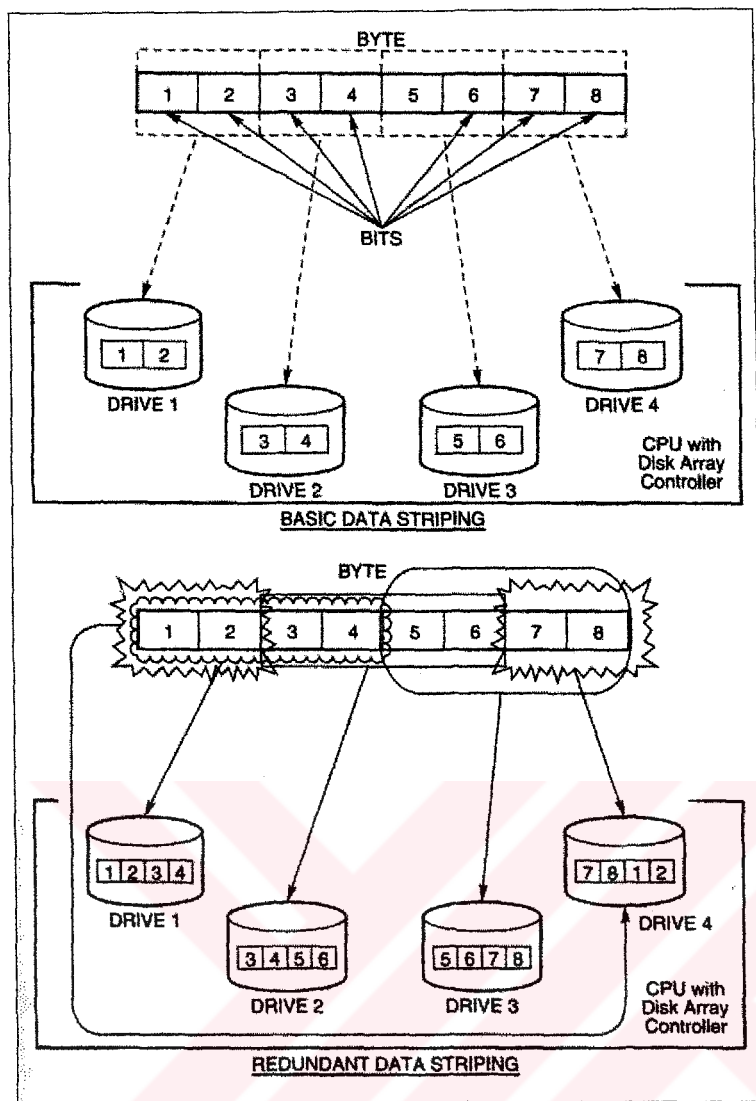


Figure 9.3 Data striping arranges data in different sequences across drives

Your input in designing the most reliable drive setup for your network is an important responsibility. You must choose the best RAID implementation level to meet your users' requirements in data integrity and cost. Seven levels of RAID are available on the market today: 0, 1, 2, 3, 4, 5, G, and 10. A higher number isn't necessarily indicative of a better choice, so you must select the best level for your environment. The following paragraphs present a brief discussion of some of these available levels, notably RAID 0, 1, and 5, which Windows NT Server supports. Windows NT Workstation supports only RAID 0, and Windows 95 is not able to use any RAID levels at all (Glen Berg, 1998).

9.3.2.1 RAID 0

RAID 0 uses data striping and block interleaving, a process that involves distributing the data block by block across the disk array in the same location across each disk. Data can be read or written to these same sectors from either disk, thus improving performance. RAID 0 requires at least two disks, and the striped partitions must be of the same size. Note that redundancy of data is not provided in RAID 0, which means that the failure of any single drive in the array can bring down the entire system and result in the loss of all data contained in the array

9.3.2.2 RAID 1

In RAID 1, drives are paired or mirrored: Each byte of information is written to two identical drives. Disk mirroring is defined as two hard drives—one primary, one secondary—that use the same disk channel (controller cards and cable), as shown in Figure 9.4. Disk mirroring is most commonly configured by using disk drives contained in the server.

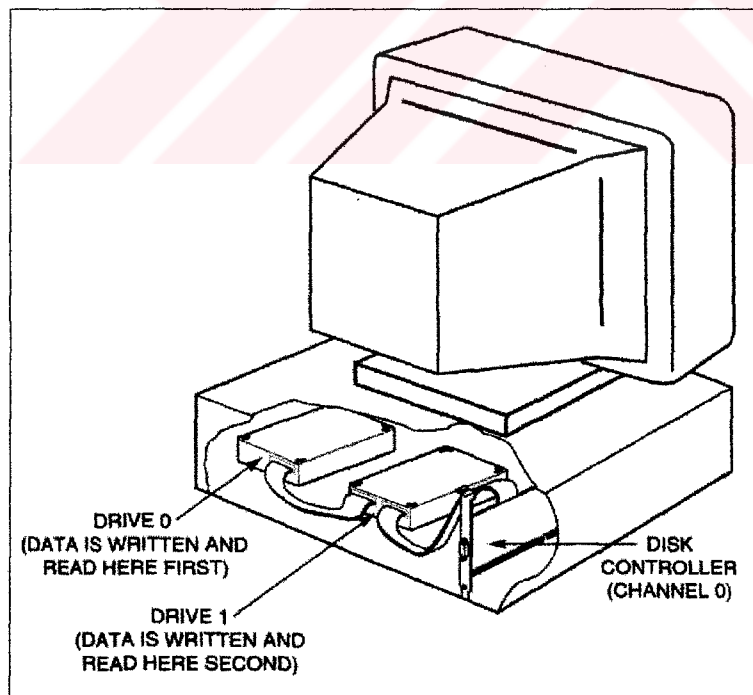


Figure 9.4 In disk mirroring, two hard drives use the same disk channel

Disk mirroring is called disk duplexing when a separate drive controller is added for each drive. Duplexing, which is covered later in this chapter, is a form of mirroring that enables you to configure a more robust hardware environment.

Mirroring does not provide a performance benefit such as RAID 0 provides. You can use mirroring, however, to create two copies of the server's data and operating system, which enables either disk to boot and run the server. If one drive in the pair fails, for instance, the other drive can continue to operate. Disk mirroring can be expensive, though, because it requires 2GB of disk space for every 1GB you want to mirror. You also must make sure that your power source has enough wattage to handle the additional devices. Mirroring requires two drives, and the mirrored partitions must be of the same size. Windows NT Server supports mirroring, but Windows NT Workstation and Windows 95 do not.

Remember that mirroring is done for fault-tolerant, not performance reasons. With this said, it should be noted that a Windows NT machine running a mirror set runs at about normal speed. It may exhibit a degradation if only one controller card is shared by the two hard drives. The controller must make each write twice, once for each drive. On the other hand, a mirrored hard drive set can produce marginal performance gains reading from the set because either drive can satisfy the read. For the best of both worlds, though, consider RAID 5.

9.3.2.3 RAID 5

RAID 5 uses striping with parity information written across multiple drives to enable fault tolerance with a minimum of wasted disk space. This level also offers the advantage of enabling relatively efficient performance on writes to the drives, as well as excellent read performance.

Striping with parity is based on the principle that all data is written to the hard drive in binary code (ones and zeros). RAID 5 requires at least three drives because this version writes data across two of them and then creates the parity block on the

third. This writing of data and the parity bit is spanned across all drives being used. If the first byte is 00111000 and the second is 10101001, then the system computes the third by adding the digits together using this system:

$$1+1=0, 0+0=0, 0+1=1, 1+0=1$$

The sum of 00111000 and 10101001 is 10010001, which is written to the third disk. This process would continue as the next parity bit is written to the first drive, and the data to the second and third. On the third round, the parity bit is written to the second drive and the data to the first and third drive. Then this cycle repeats itself.

If any of the disks fail, the process can be reversed and any disk can be reconstructed from the data and parity bits on the other two. See Figure 9.5 for an illustration of the process. Recovery includes replacing the bad disk and then regenerating its data through the Disk Administrator. A maximum of 32 disks can be connected in a RAID-5 array under Windows NT.

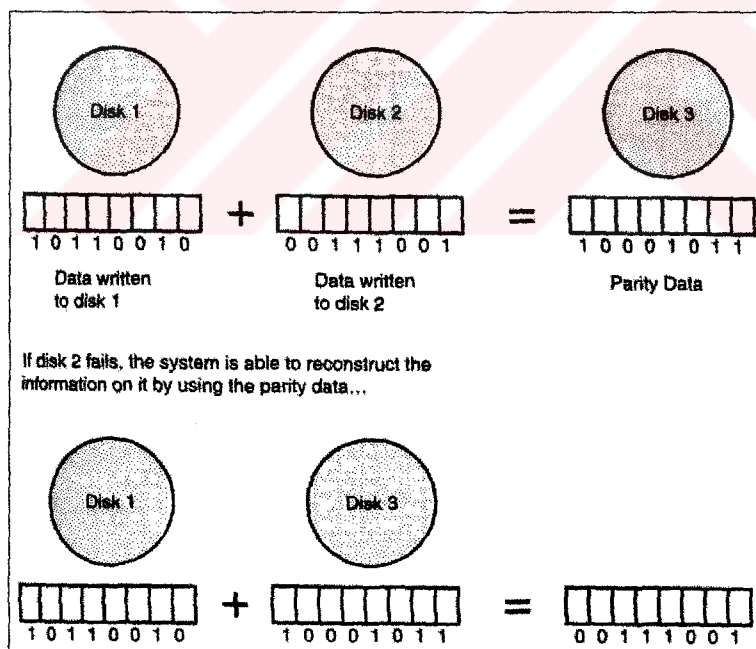


Figure 9.5 In this example, if Disk 2 fails, the system can reconstruct the information on it using the parity data

9.3.2.4 Choosing a RAID Level

Most network administrators prefer the RAID 5 solution, at least on larger servers with multiple drive bays. Because this level is a hybrid of striping and mirroring, it enables greater speed and more redundancy. Mirroring, however, offers the advantage of working well with non-SCSI hardware, because some older machines accommodate two IDE drives only, and is common as a fault-tolerant option on smaller, non-dedicated servers. Striping without parity should be reserved for workstations and servers on which speed considerations are paramount and possible downtime is an acceptable risk. See Figure 9.6 for a graphical comparison.

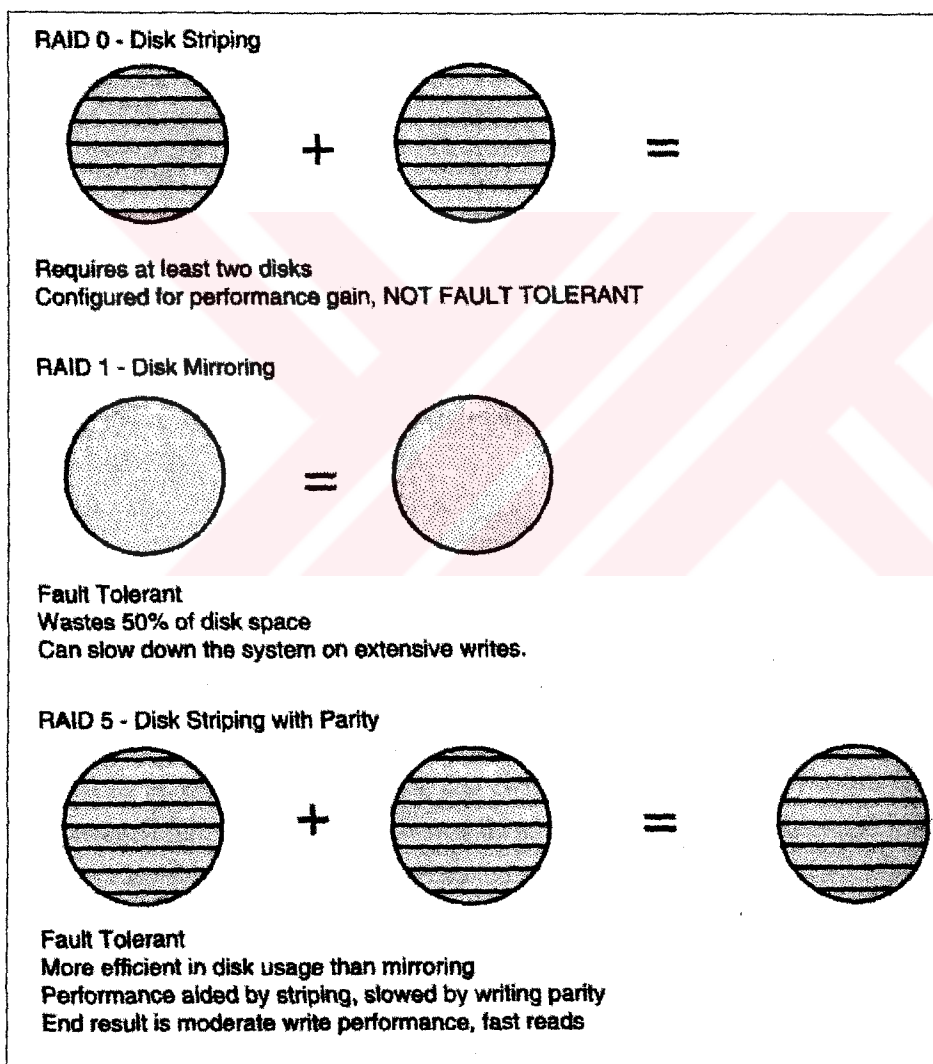


Figure 9.6 Different RAID levels offer their own unique capabilities

9.3.2.5 Disk Duplexing

In the event of disk channel failure (by a controller card or cable), access to all data on the channel stops and a message appears on the file server console screen (if your users don't let you know about it first). Even though drives can be mirrored, all disk activity on the mirrored pair ceases if the mirrored drives are connected to the same disk controller.

Disk duplexing performs the function of simultaneously writing data to disks located on different channels. As Figure 9.7 illustrates, each hard disk in a duplexed pair connects to a separate hard disk controller. This figure shows a configuration in which the drives are housed in separate disk subsystems. Each subsystem also has a separate power supply. Disk duplexing offers a more reliable setup than is possible with mirroring because a failure of one disk drive's power supply doesn't disable the server. Instead, the server continues to work with the system that remains under power.

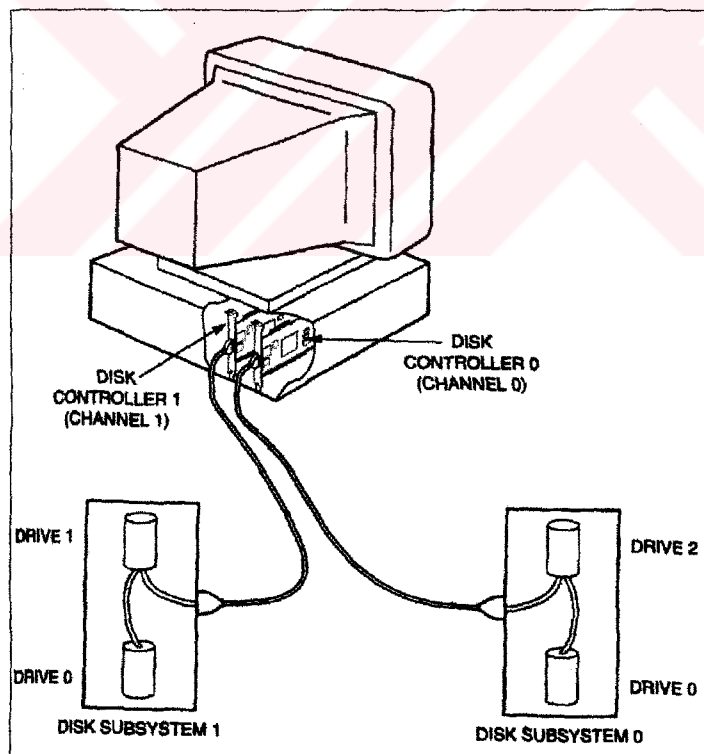


Figure 9.7 Disk duplexing simultaneously writes data to two disks located on different controller cards

Duplexing protects information at the hardware level with duplicate channels (controller cards and cables) and duplicate hard drives. Mirroring uses one controller card and two hard drives. The point of failure for this setup is primarily the controller card or the cable connecting the drives to the controller card. Disk duplexing uses two controller cards and a minimum of one drive per controller card. The point of failure is reduced with duplicate hardware.

9.4 Other Fault-Tolerance Mechanisms

Two other forms of fault tolerance exist on the market today. One of these is known as server mirroring while the other is a hardware solution known as a super server.

Server mirroring refers to having one server completely mirrored in all forms to another server. This means that if Server A goes down for any reason whatsoever, such as a failed hard drive, failed network card, or even a blown motherboard, the mirrored Server B takes over the duties of Server A.

A second option on fault tolerance is a super server. A super server is a hardware solution offered by several different hardware manufacturers. The idea behind a super server is that almost any piece of equipment can be changed on the super server without shutting down the server. This can mean that the super server can have hot swappable components such as hard drives; CPUs, and even RAM.

CHAPTER TEN

NETWORK MANAGEMENT

10.1 Introduction

Network management can be defined as OAM&P (operations, administration, maintenance and provisioning) of network and services. The operations group is concerned with daily operations in providing network services. Network administration is concerned with establishing and administering the overall goals, policies and procedures of network management. The installation and maintenance group handles functions that include both installation and repairs of facilities and equipment. Provisioning involves network planning and circuit provisioning, traditionally handled by the engineering or provisioning department (Mani Subramanian, 2000).

In the preceding chapters, the process of establishing a physical connection between the machines on your network and installing the drivers and services necessary to enable network communication was examined. With these initial considerations out of the way, the next step is to begin organising and controlling the manner and scope of network usage. This chapter deals with the process of implementing resource sharing, with the main focus being the administration of a Microsoft network.

The process of implementing resource sharing will be presented in the following order: First, a general overview of some key resource terms is presented. From this perspective, several different administrative models will be presented and contrasted. You should focus on the administrative models supported by Windows NT and Windows 95. After you have this background, file security and then print security

will be analysed from both Windows NT and Windows 95 perspectives. The final area of discussion will focus on some additional administrative tasks that should be performed on a network.

10.2 Resource Sharing Basics

Microsoft uses very specific terms to describe elements of its networking structure. The five most basic terms that you must understand are resources, sharing, users, groups, and security.

10.2.1 Resources

A resource is essentially any component that you would like to use on the network. This could be as simple as a file on another machine, to a printer located at the end of the hall, to even a certain task available by a specific program. The two key resources detailed in this chapter are data files and printers, but in theory, a resource can be any information or device relating to the network. Without networking, a resource can be accessed only by physically sitting at the machine on which the resource is installed. This would mean that you could only access a local file or a local printer. The creation of a networking structure grants you the capability to use a server computer to share resources with others at remote client machines.

10.2.2 Sharing

This brings us to the second important concept: sharing. Only by specifying that you want to grant others access to a resource—be it a directory, a CD-ROM drive, or a printer—do you make the resource available for use from remote computers and devices. A shared resource is simply a resource whose owner has leveraged networking to make it available for use by others. Some resources are not available until an administrator actually manually shares out the resource. Some examples of these resources are files and printers. Other resources are automatically shared out

when installed. An example of this is the ability to see a computer on the network when browsing the network.

10.2.3 Users

A user is anyone who requests network resources. In most cases, you assign a unique username and password to every individual on your network. Users can be created on a number of operating systems, including Windows NT, NetWare, and UNIX. Users cannot be created on Windows 95 or Windows for Workgroups because neither of these operating systems have the capability of establishing a user database. Both Windows 95 and Windows for Workgroups do enable the creation of individualised profiles, they must rely on another machine's database to provide true user authentication, such as an Windows NT domain controller.

10.2.4 Groups

A group is a collection of user accounts that you use to manage user access to shared resources, such as network shared folders, directories and printers. A group allows you to grant permissions for shared resource once to the group, instead of multiple times to individual users.

10.2.5 Security

The issue of security is one of the main focuses of this chapter. Security is the process of giving "Rights" or "Permissions" to groups or users, such that they can access resources on the network. Different Network operating systems use different terms to describe these types of security issues. Windows NT makes a distinction between "Rights" and "Permissions." The details of these differences between these "Rights" and "Permissions" will be addressed in greater detail later on in this chapter.

10.3 General Network Administrative Models

This section will discuss four commonly used network security models. These are:

- ◆ Workgroups
- ◆ Bindery-based
- ◆ Domains
- ◆ Directory services

10.3.1 Workgroup Model

One common security model used on small networks is the workgroup model. This administrative model is built into network operating systems such as Windows 95, Windows for Workgroups, and Windows NT. In a workgroup model, there is no centralised database or server that stores user account information. This type of security model is found on a peer-to-peer type network. In a workgroup model, there are one or more machines that have a resource to share. Assume this resource is a directory containing some files. In order to allow other computers to access these files, the computers containing these files in the directory must have a service running that allows them advertise this sharing of resources.

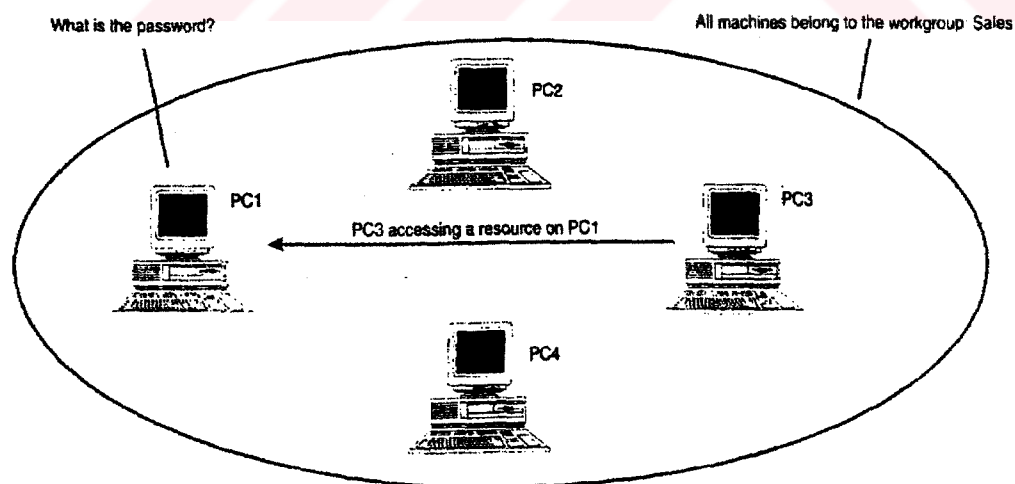


Figure 10.1 A workgroup does not rely on a centralised user account database

A workgroup is just a name associated with a group of computers. Any computer, when installed, can be part of any workgroup they wish. There are two variations found within the Workgroup model. One is a Windows 95 and Windows for Workgroups variation, while the other is a Windows NT variation.

10.3.1.1 Windows 95

In order for users on other computers to access files or printers on other computers, their computers must have a redirector installed that will allow them to connect to the advertising service. In Windows 95, the redirector is called "Client for Microsoft Networks," and the service allows shared files to be accessed over the network is called "File and printer sharing for Microsoft networks."

When a resource is shared out on the network, this provides the capability to allow users access to the resource, but there is no capability to give this access to the resource on a user-by-user or group by-group basis. This is because when sharing out a resource, you can only specify a password to protect the resource. When anyone tries to connect, to this shared resource, they will be prompted, for a password. If then type in the correct password, when prompted, they will get access to the resource. If they do not know the password, they will be denied access.

This security model works well in small networks. As a network grows, the use of passwords on every shared resource becomes cumbersome. There is also no method of controlling anyone from telling others the password to your shared resources.

10.3.1.2 Windows NT

Windows NT Workstation and Server both have the ability to be installed within a workgroup. This option is selected during the installation of the software. The Windows NT workgroup model works in a fashion similar to that used by Windows 95. Each Windows NT computer does contain a local database of user accounts. In order to access a local Windows NT computer, you would need to log on to the

computer using a name and password found in the local user account database. The contents of this local user account database are not used with any other computers.

Windows NT in a workgroup model has the capability to reference users on a user-by-user basis when assigning security to shared resources. The users a Windows NT computer can reference are only the ones found within its own user account database. To have a security model, you would need to create all of the users on your network in each of the Windows NT local databases. If your network had ten users and ten Windows NT computers, if you added one new computer, you would have to recreate all of your ten users within that new computer's local user account database. Likewise, if a new user is added to the network, their name would have to be added to all of the local databases on each of the existing Windows NT computers. The same would go if a user changed their password; each Windows NT computer would need to be updated with the new password of the user.

10.3.2 Bindery-Based Model

The bindery-based model is one that is used by Novell NetWare versions up to NetWare 3.2. Bindery-based networks follow the client/server model of networking. Novell bindery-based servers still have a large presence in many networks to this day.

In a bindery model, there is one server and many clients. The server contains a flat user account database. A flat user account database is one that contains the names of users, in one single list from A to Z, who are allowed to log onto the system. Also, this database of user accounts is used to assign who has rights or privileges to use different resources on the network. These rights are either assigned on a user-by-user basis or a group-by-group basis.

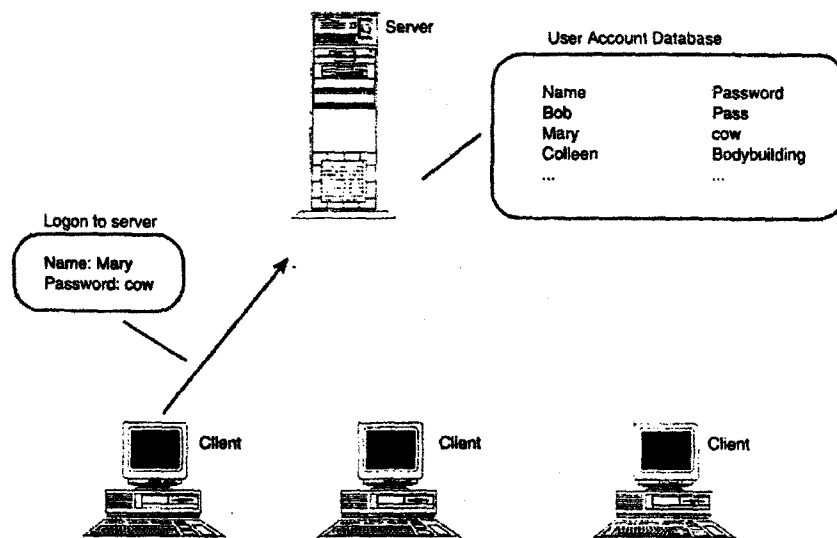


Figure 10.2 A Bindery-based network has a centralised user account database. Client machines run no services

The server is also responsible for containing all of the services on the network. The client machines are not designed to provide any services at all. This allows for a more centralised method of management of the network.

A client machine on this system is one that has a redirector installed on it, such that it will connect to a central server, and try to authenticate against that server's user account database. The user will supply a valid name that exists within the user account database (logon name) and an associated password.

If the name and password exist within the server's user account database, the user is granted permission to use the network, and in turn, the user's computer is given a "key" by the authenticating server.

10.3.3 Domain Model

The domain model is another client/server model that is used in Windows NT Server and OS/2 networks. It is similar to the bindery security model, in its

centralised administration of user accounts and flat list of user accounts, but scales better for larger networks.

The domain model is a security model that uses a flat user account database similar to the bindery model. The main difference is that this database is stored on one or more computers known as domain controllers. When a Windows NT server is installed, one of the parameters that must be configured is what role the server should assume. There are three possibilities:

- ◆ Primary domain controller (PDC)
- ◆ Backup domain controller (BDC)
- ◆ Member server

Primary and backup domain controllers perform essentially the same function. It is their role to store the user account database. The difference is that a PDC stores the master copy of this database. It is in this master copy that changes can occur. If a new user were added, the PDC's database would be affected. The backup domain controller's user account database is a replicated copy of that from the PDC. There can only exist one PDC in a domain, yet you can specify as many BDCs as you wish. At any time a BDC can be promoted to a PDC, and thus a PDC demoted to a BDC.

The role of a member server is that it contains resources such as files, printers, and applications that users may wish to access on the network. It in itself does not store a domain user account database, but instead gives access to resources to users based upon the users drawn from the list of user accounts on the domain controllers. The member servers are also not involved with processing logon request for client machines as this is a function that is only performed by domain controllers.

10.3.4 Directory Services Model

Directory Services, also known as the X.500 standard, is the latest in security management to be offered for networking security. It currently is used by Banyan

Vines, Novell] NetWare 4.x and higher, and is to be incorporated into the release of Windows NT 5.

Directory Services is a powerful security management system for a network, as it can accommodate a small to extremely large network. It solves many of the limitations found in the work group, bindery, and domain security models. Directory Services is based upon a hierarchical distributed database model. This model allows for the management of all resources through one utility, as well as providing a high level of fault tolerance within the system.

Management on a Directory Service security system is based on a hierarchical user account database. The idea behind this is similar to a file system database. No one stores all of their files in one directory on their hard drive. Files are grouped together into directories such that files that go together or are related to one another are placed together for management purposes and ease of reference. The same can be said for a Directory Service user account database. Instead of directories, containers store users together that work together or access the same resources together. In fact, many Directory Services databases are organised in a manner that is similar to their corporate organisational charts.

The management of resources is not limited to users and groups within a Directory Services database. Other resources on the network also have objects within the database. Thus when a printer is installed, its object is placed into the database as well. Management of this printer can also be done from the Directory Services database. So could the management of a fax server or any other device on the network.

The third main benefit of Directory Services is that it allows the partitioning of the database such that portions of it, partitioned around the containers, can be placed on different servers. This would mean that if a user is added in Los Angeles, the server in London, England does not need to be updated. This feature allows for the minimisation of network traffic over slow WAN links. In a domain model, all user accounts are copied to all BDCs whenever a user account is added.

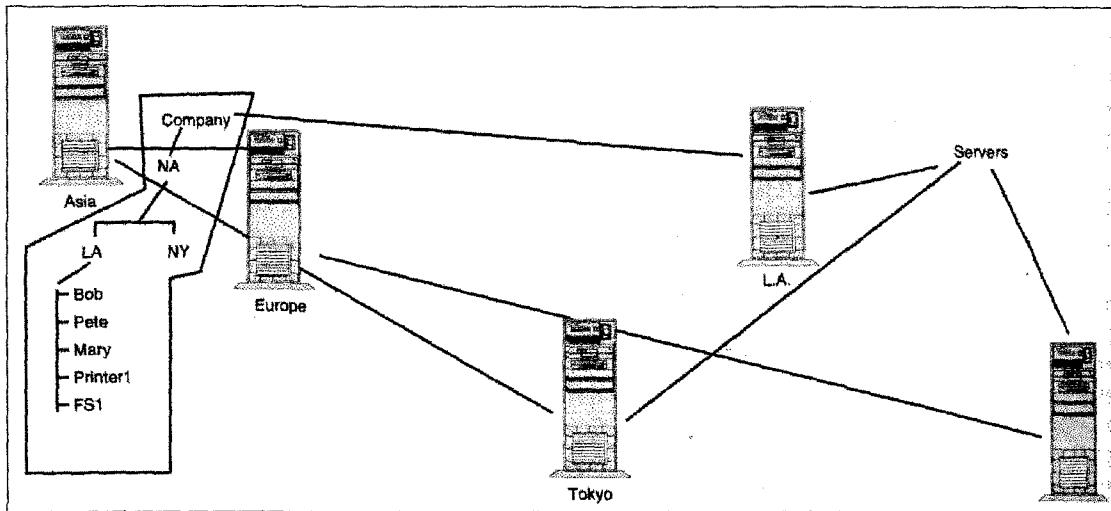


Figure 10.3 Directory Services has a distributed hierarchical database

In short, the Directory Services model is the standard that all operating systems are migrating toward, as this model has features that can ease administration of the network, as well as allow a network to scale to any size desired.

In summary, here are the following features of the four administrative models:

- ◆ There are two derivatives of workgroup models. One used by Windows 95, the other by Windows NT
- ◆ Windows 95 workgroup models have no user account databases; all security is done with the use of passwords.
- ◆ Windows NT workgroups have a decentralised user account database requiring administrators to perform repetitive administrative tasks such as creating users multiple times.
- ◆ Bindery-based systems use a flat user account database. This user account database is not shared with other servers. You must use different utilities to manage different resources.
- ◆ Domain-based systems are similar to bindery-based systems with the exception that more than one server shares the same user account database.
- ◆ Directory Services allows for a distributed hierarchical database shared by all servers, from which all resources can be managed.

10.4 Managing User Accounts and Groups Using Windows NT

This section will focus on the Windows NT domain administrative model in describing how a domain is managed and how security for files and printers is accomplished.

10.4.1 User Accounts

In most instances, a user account is created for each individual on the network and is meant for use only by that one person. This is done through the "User Manager for Domains". This account generally is a contracted form of the person's name or some other unique value, and no two users can have the same username in a single user account database. At their most basic level, a user account usually contains values for the following three properties:

- ◆ **An username:** This element distinguishes one account from another. This property requires a value.
- ◆ **A password:** This element confirms the user's identity. Individual passwords should be kept private to avoid unauthorised access. This property may be optional, depending upon security restrictions.
- ◆ **The groups of which the user is a member:** These groups determine the user's rights and permissions on the network. This is an optional property.

A number of other optional properties, such as a home directory (a place where a user can store personal files on the network) or specific information about the user such as their full name or description, also exist. None of these properties are crucial to the functioning of the account in the way that the elements enumerated above are.

In the creation of user accounts and their passwords, you must strike a balance between security and user friendliness. Passwords have settings such as expiration dates, uniqueness, and how often they must be changed. Setting these options such that a password must be changed on a basis that is too frequent or one that requires too many long, unique passwords is almost certain to result in a less, rather

than more, secure environment. If users are unable to remember such a password, they often simply will stick a note to their monitor with their password on it or come up with some other highly insecure way of jogging their memory. If this starts happening, you know that your policies are probably too stringent.

10.4.2 Groups

Now that a user has been established, the next step in granting that individual access to resources is to assign proper permissions. To ease the management of all users in the system, this should be done by creating a group or a set of groups, assigning permissions to the groups, and then placing the user inside the appropriate groups. As mentioned before, it is easier to manage five groups than five hundred users.

By default, Windows NT creates a number of built-in groups that are defined with the rights necessary to perform particular tasks. These groups are task-specific and are inherently different from the type of groups you normally create, which are resource-specific. Windows networks can include four types of the resource specific groups: global, local, security and distribution groups. Each of these has very specific functions.

10.4.2.1 Global Groups

Global groups, like user accounts, are created only on the primary domain controller of a Microsoft domain. Backup domain controllers receive a copy of this database; thus, they also contain global groups. These groups function primarily as containers for user accounts. Global groups are designed to contain general groupings of people such as Sales, Accounting, or the IS department. Global groups cannot contain other groups-only users from the domain in which the global group is created are permitted to be part of a global group.

10.4.2.2 Local Groups

Local groups, on the other hand, can be created on Windows NT Server or Workstation and can include both user accounts and global groups. Moreover, these groups are assigned permissions.

10.4.2.3 Security Groups

Security groups are used for security-related purposes, such as granting permissions to gain access to resources in Windows 2000 networks. You can also use them to send e-mail messages to multiple users. Sending an e-mail message to a group sends the message to all members of the group. Therefore, security groups share the capabilities of distribution groups.

10.4.2.4 Distribution Groups

Applications use distribution groups as lists for non-security related functions, such as sending e-mail messages to groups of users in Windows 2000 networks. You cannot grant permissions to security groups. Even though security groups have all of the capabilities of distribution groups, distribution groups are still required, because some applications can only read distribution groups.

10.4.2.5 Built-in Global and Local Groups in Windows NT

Windows NT also contains some built-in global and local groups. These groups are given permissions and rights to various components on the network in order to provide some general functionality on the system. Users can be added to or removed from these groups. These global groups only exist on domain controllers.

- ◆ **Domain Users:** All users created within a domain are placed into this group.
- ◆ **Domain Admins:** The Administrator account is placed within this group. All domain-wide administrators should also be placed in this group.

These local groups are found on domain controllers, member servers, and Windows NT workstations that are part of a domain.

- ◆ **Administrators:** Contains the Domain Admin global group. This group can manage all security and resources on the computer.

- ◆ **Users:** This group contains the global Users group.

- ◆ **Guest:** This group contains the guest account.

- ◆ **Account Operators:** Members of this group have the ability to create users and groups, both global and local. This group cannot manipulate the Administrator, the Administrators group, the Domain Admins group, or the Server operators group. This group is only found on domain controllers.

- ◆ **Backup Operators:** Members of this group have the rights needed to backup and restore files on the computer.

- ◆ **Print Operators:** Members of this group can manage all printers on the computer. This group is only found on domain controllers.

- ◆ **Server Operators:** Members of this group can share and stop-sharing resources on the server, backup and restore files on the server, and shut down the server. This group is only found on domain controllers.

- ◆ **Replicator:** This group is used with the Directory Replicator Service.

Usually, the default rights associated with these built-in groups will be fine to perform the functions for which they are intended. The Administrators, Server Operators, Backup Operators, Print Operators, and Account Operators groups all have the right to log on to Windows NT Server interactively

For managing resources, you create the group and add users to it, at which time the group is ready to be given permissions in the file system, such as Read permissions to a directory or Print permissions to a printer.

Creating groups and users provides the base upon which the rest of your security is built. You should now know what a user is, and how users and groups interact. Do not get overly caught up on the different groups and their abilities. That is the

purpose of the Windows NT Server exam. The next section explores using these groups and users to give or restrict access to network resources.

10.4.3 Permissions

Permissions refer specifically to the level of trust that the owner of a resource has in the people with which he or she shares the resource. Although very subtle permission structures can be constructed using Windows NT and Windows 95, a resource generally will either be shared as read-only or full-control. BY default, both Windows NT and Windows 95 share resources with full control, which means that others cannot only view your shared resources but also can append, modify, and even delete them. For the less-trusting owner, a good compromise is to grant read-only permissions, which enable others to view your files or print to your printer, but not to modify those files or change the printer's settings.

10.4.4 Rights

The difference between having rights and receiving permissions might seem like nothing more than a matter of semantics, but this is not the case. In Microsoft terminology, rights are general attributes that particular users or groups have. These rights include the Capability to log on locally or to load and unload device drivers. These particular user rights make administrators more powerful than users. Permissions refer to the level of control a particular user or group has over a specific resource. Examples of resource control would be the "Read" permission to a file or directory, or the ability to "Print" to a shared printer.

10.5 Additional Administrative Tasks

Besides setting up the network and making sure that your users have access to what they need (and can't get to things they don't), an administrator also has a number of other important day-to-day tasks to fulfill. The remainder of this chapter gives you a brief introduction to the following responsibilities:

- ◆ Auditing
- ◆ Handling data encryption
- ◆ Handling virus protection
- ◆ Securing equipment

10.5.1 Auditing

Another option you might need to consider is auditing, which is the process of creating a database that records particular events that occur on your network. You can decide what events to audit, from application information to security, options. Figure 10.4 shows one of many different auditing windows in Windows NT. The utilities to perform auditing come with Windows NT and Windows 95. These tools are known as Event Viewer and Performance Monitor in NT.

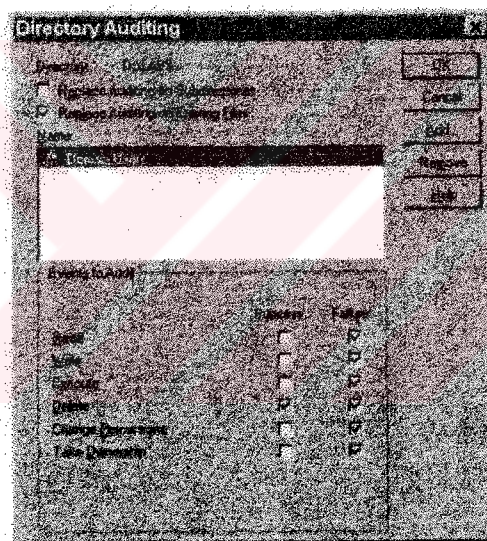


Figure 10.4 A directory auditing window in Windows NT

10.5.2 Handling Data Encryption

Usually, the file and share security discussed previously is more than adequate. However, if your network is used for especially sensitive data and you want to prevent anyone from stealing information, you can take an additional security

measure by forcing data encryption. Encryption codes the information sent on the network using a special algorithm and then decodes it on the other end.

10.5.3 Handling Virus Protection

Much like humans, computers are susceptible to certain types of viruses. Unlike those that strike us, though, computer viruses are created intentionally with the aim of injuring or altering your machines. Viruses can be spread through computer systems- in many ways, but the most common is through an executable file. Having a good virus scanning program-none come with any Microsoft program-is a necessity for an administrator. Numerous third-party companies make virus-scanning software, including Norton and MacAfee, to name just two.

10.5.4 Securing Equipment

You might think that if you have taken care of backup, RAID, shares, NTFS permissions, virus scanning, and encryption, your data is completely safe. There is, however, one more thing of which you should be sure. Any computer is far more insecure if people can get to its server so you always should lock your server in a room that only authorised personnel have access to. Having the server out in the open provides a security risk, such that it is open to anyone to tamper with it. Most companies have a "server room"-often a large wiring closet-where all server machines are stored. Make sure this location is neither too cold nor too hot, that it has adequate ventilation, and that only authorised individuals have access to it. Additionally, whenever you make a change to the network, be certain to document the changes you have made. This can make troubleshooting and maintenance far easier and can save you valuable time.

Anti-Virus Software Anti-virus software cannot simply detect any virus: rather, this software generally is designed to look for particular infections. Because of this, scanning software is updated regularly, often at no extra charge. Even if it does cost a bit, though always keep your virus-checking software as new as possible.

CHAPTER ELEVEN

MONITORING THE NETWORK

11.1 Introduction

An important part of network management involves monitoring trends on the network. By effectively monitoring network behaviour, you can anticipate problems and correct them before they disrupt the network. Monitoring the network also provides you with a baseline, a sampling of how the network functions in its equilibrium state. By establishing a baseline on your system, you can determine whether your network can handle the current resource usage or whether additional resources are needed (Glen Berg, 1998).

This chapter presents various programs or mechanisms that can be used to monitor and record information about the network. The explanation of what these different mechanisms are and when you would utilise them is addressed in this chapter.

11.2 Monitoring Network Trends

Monitoring the network is an ongoing task that requires data from several different areas. The following list details some tools you can use to document network activities:

- ◆ Written documentation
- ◆ A statistics-gathering or performance-monitoring tool, such as Windows NT's Performance Monitor
- ◆ A network-monitoring and protocol-analysis program-such as Windows NT's Network Monitor or the more powerful Network Monitor tool included with

Microsoft's BackOffice System Management Server (SMS) package-or a hardware - based protocol analyser

- ◆ A system event log, such as the Windows NT event log, which you can access through Windows NT's Event Viewer application

11.3 Keeping Records

A detailed history of changes to the network serves as a tremendous aid in troubleshooting. When a problem occurs, the first thing you want to know is what has changed and when it was changed. This information can be gathered from written documentation.

Your documentation of the network should begin from the day the network is installed. The layout, design, components, and software should all be recorded within your network documentation. Contact names, service contracts, as well as important support telephone numbers should also be part of your network's documentation.

The following list details some items your configuration records should include:

- ◆ Descriptions of all hardware, including installation dates, repair histories, configuration details (such as interrupts and addresses), and backup records for each server.
- ◆ A map of the network showing locations of hardware components and cabling details.
- ◆ Documentation describing why certain layouts or naming conventions were chosen, so that these conventions can be followed in the future.
- ◆ Current copies of workstation configuration files, such as CONFIG.SYS and AUTO EXEC. BAT files for DOS and Windows 3.1 machines, or backup copies of the registry files for Windows 95 and NT.
- ◆ Service agreements and important telephone numbers, such as the numbers of vendors, contractors, and software support lines.
- ◆ Software licenses to ensure that your network operates within the bounds of the license terms.

- ◆ A history of past problems and related solutions

Records of the network are used for more than just troubleshooting. They also supply a wealth of information for future planning. Records can help you maintain consistency within the hardware and software. Detailed records also save a lot of time when software and hardware audits are performed—a common event within medium and large-sized organisations.

11.4 Monitoring Performance

One of the most important tasks that should be performed on the network is some form of statistical collecting. These statistics can range from the performance of servers, workstations, and other devices on the network to the performance of individual components within a program or service itself. This section looks at three types of performance monitoring tools: Simple Network Management Protocol (SNMP), Windows NT Performance Monitor, and Windows 95's System Monitor.

11.4.1 Simple Network Management Protocol (SNMP)

One important protocol used within the TCP/IP protocol suite that assists in statistic collecting is the Simple Network Management Protocol (SNMP). SNMP is a protocol that is supported by most pieces of hardware and software that support the TCP/IP protocol stack. This protocol allows for the collection of statistics of various resources on the network. For this information to be collected about a resource, the resource must run an SNMP service, or have some other device run the SNMP service on its behalf.

The SNMP service collects predefined information. This information is stored in a Management Information Base (MIB). An MIB is a database of information that can be read by management software designed to work with SNMP.

Management software issues one of the following three main commands:

- ◆ The get command gathers information within an MIB.

- ◆ The get next command gets the next piece of information within the MIB.
- ◆ The set command places information within the MIB.

These devices that have an SNMP service monitoring them can also be configured to issue traps, or system messages, when certain parameters are reached or exceeded.

11.4.2 Windows NT Performance Monitor

Windows NT's Performance Monitor tool lets you monitor important system parameters for the computers on your network in real time. Performance Monitor can keep an eye on a large number of system parameters, providing a graphical or tabular profile of system and network trends. Performance Monitor also can save performance data in a log for later reference. You can use Performance Monitor to track statistical measurements (called counter) for any of several hardware or software components (called objects). An example of these counters for an object being displayed in a chart format can be seen in Figure 11.1.

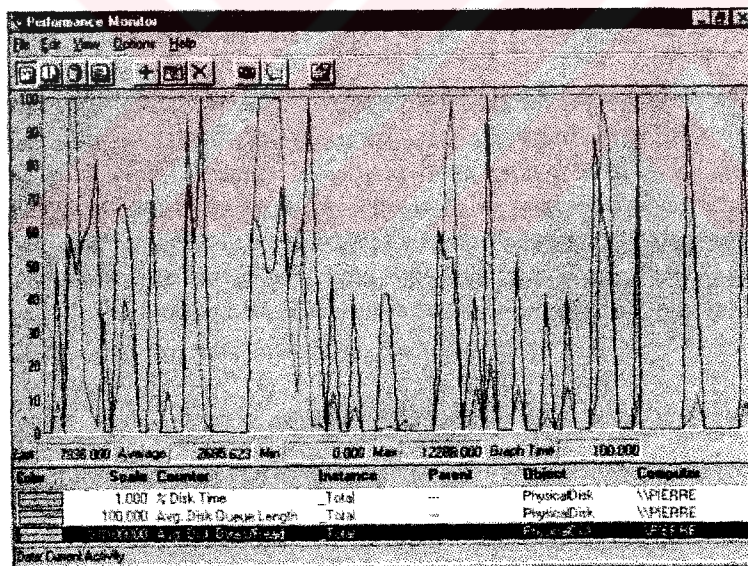


Figure 11.1 A Windows NT Performance Monitor chart

Some Performance Monitor objects that relate to network behaviour are as follows:

- ◆ Network segment.
- ◆ Server.
- ◆ Server work queues.
- ◆ Workstation or other Redirectors.
- ◆ Protocol-related objects, such as TCP, UDP IP, NetBEUI, NWLink and NetBIOS.
- ◆ Service-related objects, such as Browser and Gateway Services for NetWare.

Some Performance Monitor counters that relate to the performance of components or resources on a computer are as follows:

- ◆ Processor
- ◆ Memory
- ◆ Physical Disk

11.4.3 Windows 95 System Monitor

Windows 95 includes a program called System Monitor that also enables you to collect information on the Windows 95 machine in real time. System Manager collects information on different Categories of Items on the system.

The main categories within System Monitor are as follows:

- ◆ **File System:** Information written to or read from the hard drive
- ◆ **IPX/SPX compatible protocol:** Information on the number of IPX and SPX packets sent out from and received by the computer
- ◆ **Kernel:** Processor usage, number of threads being processed, and the number of virtual machines running on the computer
- ◆ **Memory Manager:** Various memory items that can be tracked on the computer
- ◆ **Microsoft Network Client:** The number of files, sessions, resources, and bytes sent or received by the network client.

11.5 Monitoring Network Traffic

Protocol analysis tools monitor network traffic by intercepting and decoding frames. Software-based tools, such as Windows NT Server's Network Monitor, analyse frames coming and going, in real time, from the computer on which they run. Network Monitor records a number of statistics, including the percent of network utilisation and the broadcasts per second. In addition, Network Monitor tabulates frame statistics (such as frames sent and received) for each network address.

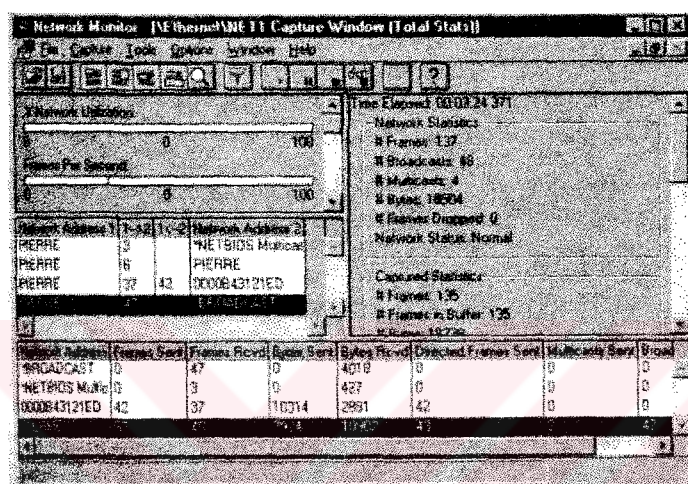


Figure 11.2 Windows NT Server's Network Monitor main screen

An enhanced version of Network Monitor, which is included with the Microsoft BackOffice System Management Server (SMS) package, monitors traffic on more than just the traffic between the local computer and other devices. It will also monitor traffic that is just between other devices, and also traffic on remote networks, provided a monitor agent is installed on the remote network segment.

For large networks, or for networks with complex traffic patterns, you might want to use a hardware-based protocol-analysis tool. A hardware-based protocol analyser is a portable device that can be as small as a palmtop PC or as large as a suitcase. The advantage of a hardware-based protocol analyser is that you can carry it to strategic places around the network (such as a network node or a busy cabling intersection) and monitor the traffic at that point.

Some protocol analysers are quite sophisticated. In addition to keeping network traffic statistics, they can capture bad frames and often isolate the source. They also can help determine the cause of bottlenecks, protocol problems, and connection errors. A hardware-based protocol analyser is often a good investment for a large network because it concentrates a considerable amount of monitoring and troubleshooting power into a single, portable unit. For a smaller network, however, a hardware-based analyser might not be worth the initial five-figure expense because less expensive software-based products perform many of the same functions.

11.6 Logging Events

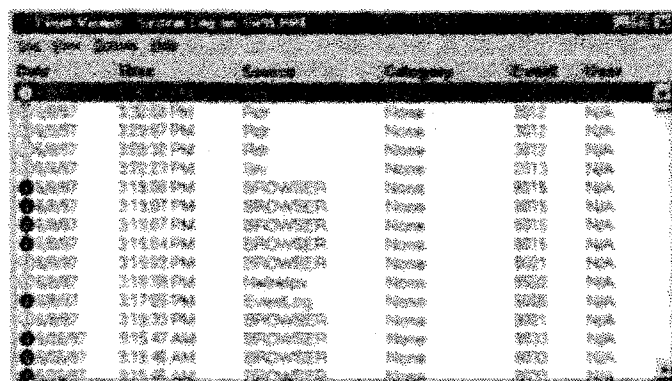
Some operating systems, such as Windows NT have the capability to keep a running log of system events. That log serves as a record of previous errors, warnings, and other messages from the system. Studying the event log can help you find recurring errors and discover when a problem first appeared. The event log should also be scanned on a regular basis to look for any indications of potential problems.

Windows NT's Event Viewer application provides you with access to the event log. You can use Event Viewer to monitor the following types of events:

- ◆ **System events:** Warnings, error messages, and other notices describing significant system events. Examples of system log entries include browser elections, service failures, and network connection failures.
- ◆ **Security events:** Events tracked through Windows NT's auditing features.
- ◆ **Application events:** Messages from Win32 applications. If you're having a problem with an application, you can check the application log for an application-related error or warning message, provided the application is programmed to write to the event log.

Event Viewer is part of the Windows NT Server Administrative Tools group. To start Event Viewer, click on the Start button and choose Programs, Administrative Tools, Event Viewer. Figure 11.3 shows the Event Viewer main screen. Click on the

Log menu to select the System, Security, or Application log. If you double-click on a log entry in Event Viewer, an Event Detail dialog box appears on your screen. An Event Detail provides a detailed description of the event.



Date	Time	Source	Category	Event	Type
10/27/97	1:23:21 PM	Winlogon	None	6002	Info
10/27/97	1:23:21 PM	Winlogon	None	6003	Info
10/27/97	1:23:21 PM	Winlogon	None	6004	Info
10/27/97	1:23:21 PM	Winlogon	None	6005	Info
10/27/97	1:23:21 PM	Winlogon	None	6006	Info
10/27/97	1:23:21 PM	Winlogon	None	6007	Info
10/27/97	1:23:21 PM	Winlogon	None	6008	Info
10/27/97	1:23:21 PM	Winlogon	None	6009	Info
10/27/97	1:23:21 PM	Winlogon	None	6010	Info
10/27/97	1:23:21 PM	Winlogon	None	6011	Info
10/27/97	1:23:21 PM	Winlogon	None	6012	Info
10/27/97	1:23:21 PM	Winlogon	None	6013	Info
10/27/97	1:23:21 PM	Winlogon	None	6014	Info
10/27/97	1:23:21 PM	Winlogon	None	6015	Info
10/27/97	1:23:21 PM	Winlogon	None	6016	Info
10/27/97	1:23:21 PM	Winlogon	None	6017	Info
10/27/97	1:23:21 PM	Winlogon	None	6018	Info
10/27/97	1:23:21 PM	Winlogon	None	6019	Info
10/27/97	1:23:21 PM	Winlogon	None	6020	Info
10/27/97	1:23:21 PM	Winlogon	None	6021	Info
10/27/97	1:23:21 PM	Winlogon	None	6022	Info
10/27/97	1:23:21 PM	Winlogon	None	6023	Info
10/27/97	1:23:21 PM	Winlogon	None	6024	Info
10/27/97	1:23:21 PM	Winlogon	None	6025	Info
10/27/97	1:23:21 PM	Winlogon	None	6026	Info
10/27/97	1:23:21 PM	Winlogon	None	6027	Info
10/27/97	1:23:21 PM	Winlogon	None	6028	Info
10/27/97	1:23:21 PM	Winlogon	None	6029	Info
10/27/97	1:23:21 PM	Winlogon	None	6030	Info
10/27/97	1:23:21 PM	Winlogon	None	6031	Info
10/27/97	1:23:21 PM	Winlogon	None	6032	Info
10/27/97	1:23:21 PM	Winlogon	None	6033	Info
10/27/97	1:23:21 PM	Winlogon	None	6034	Info
10/27/97	1:23:21 PM	Winlogon	None	6035	Info
10/27/97	1:23:21 PM	Winlogon	None	6036	Info
10/27/97	1:23:21 PM	Winlogon	None	6037	Info
10/27/97	1:23:21 PM	Winlogon	None	6038	Info
10/27/97	1:23:21 PM	Winlogon	None	6039	Info
10/27/97	1:23:21 PM	Winlogon	None	6040	Info
10/27/97	1:23:21 PM	Winlogon	None	6041	Info
10/27/97	1:23:21 PM	Winlogon	None	6042	Info
10/27/97	1:23:21 PM	Winlogon	None	6043	Info
10/27/97	1:23:21 PM	Winlogon	None	6044	Info
10/27/97	1:23:21 PM	Winlogon	None	6045	Info
10/27/97	1:23:21 PM	Winlogon	None	6046	Info
10/27/97	1:23:21 PM	Winlogon	None	6047	Info
10/27/97	1:23:21 PM	Winlogon	None	6048	Info
10/27/97	1:23:21 PM	Winlogon	None	6049	Info
10/27/97	1:23:21 PM	Winlogon	None	6050	Info
10/27/97	1:23:21 PM	Winlogon	None	6051	Info
10/27/97	1:23:21 PM	Winlogon	None	6052	Info
10/27/97	1:23:21 PM	Winlogon	None	6053	Info
10/27/97	1:23:21 PM	Winlogon	None	6054	Info
10/27/97	1:23:21 PM	Winlogon	None	6055	Info
10/27/97	1:23:21 PM	Winlogon	None	6056	Info
10/27/97	1:23:21 PM	Winlogon	None	6057	Info
10/27/97	1:23:21 PM	Winlogon	None	6058	Info
10/27/97	1:23:21 PM	Winlogon	None	6059	Info
10/27/97	1:23:21 PM	Winlogon	None	6060	Info
10/27/97	1:23:21 PM	Winlogon	None	6061	Info
10/27/97	1:23:21 PM	Winlogon	None	6062	Info
10/27/97	1:23:21 PM	Winlogon	None	6063	Info
10/27/97	1:23:21 PM	Winlogon	None	6064	Info
10/27/97	1:23:21 PM	Winlogon	None	6065	Info
10/27/97	1:23:21 PM	Winlogon	None	6066	Info
10/27/97	1:23:21 PM	Winlogon	None	6067	Info
10/27/97	1:23:21 PM	Winlogon	None	6068	Info
10/27/97	1:23:21 PM	Winlogon	None	6069	Info
10/27/97	1:23:21 PM	Winlogon	None	6070	Info
10/27/97	1:23:21 PM	Winlogon	None	6071	Info
10/27/97	1:23:21 PM	Winlogon	None	6072	Info
10/27/97	1:23:21 PM	Winlogon	None	6073	Info
10/27/97	1:23:21 PM	Winlogon	None	6074	Info
10/27/97	1:23:21 PM	Winlogon	None	6075	Info
10/27/97	1:23:21 PM	Winlogon	None	6076	Info
10/27/97	1:23:21 PM	Winlogon	None	6077	Info
10/27/97	1:23:21 PM	Winlogon	None	6078	Info
10/27/97	1:23:21 PM	Winlogon	None	6079	Info
10/27/97	1:23:21 PM	Winlogon	None	6080	Info
10/27/97	1:23:21 PM	Winlogon	None	6081	Info
10/27/97	1:23:21 PM	Winlogon	None	6082	Info
10/27/97	1:23:21 PM	Winlogon	None	6083	Info
10/27/97	1:23:21 PM	Winlogon	None	6084	Info
10/27/97	1:23:21 PM	Winlogon	None	6085	Info
10/27/97	1:23:21 PM	Winlogon	None	6086	Info
10/27/97	1:23:21 PM	Winlogon	None	6087	Info
10/27/97	1:23:21 PM	Winlogon	None	6088	Info
10/27/97	1:23:21 PM	Winlogon	None	6089	Info
10/27/97	1:23:21 PM	Winlogon	None	6090	Info
10/27/97	1:23:21 PM	Winlogon	None	6091	Info
10/27/97	1:23:21 PM	Winlogon	None	6092	Info
10/27/97	1:23:21 PM	Winlogon	None	6093	Info
10/27/97	1:23:21 PM	Winlogon	None	6094	Info
10/27/97	1:23:21 PM	Winlogon	None	6095	Info
10/27/97	1:23:21 PM	Winlogon	None	6096	Info
10/27/97	1:23:21 PM	Winlogon	None	6097	Info
10/27/97	1:23:21 PM	Winlogon	None	6098	Info
10/27/97	1:23:21 PM	Winlogon	None	6099	Info
10/27/97	1:23:21 PM	Winlogon	None	6100	Info

Figure 11.3 The Event Viewer main screen

The Windows NT Event Viewer utility contains the following five types of events:

- ◆ **Information:** These events simply state that something of importance has been done, such as the loading of a protocol. These events are recorded for a matter of information only.

- ◆ **Warning:** These events serve as a warning that some event that may be important has occurred. Often when services are stopped, a warning event is generated.

- ◆ **Stop:** These events occur when something of significance such as a detrimental event, has occurred. Often when services or hardware fail, a Stop event is generated.

- ◆ **Success:** This event is generated within the auditing log. Success events are generated when an object that was audited as successful has occurred. You might, for example, audit the successful logon of users.

- ◆ **Failure:** This event is generated within the auditing log. Failure events are generated when an object that was audited as a Failure has occurred, such as the failure of users to log on.

CHAPTER TWELVE

CONCLUSIONS

The project has introduced you to a number of terms commonly used in computer networking. It also has addressed many of the basic networking structures. Networks come in a few standard forms or architectures and each form is a complete system of compatible hardware, protocols, transmission media and topologies.

In the networking environment understanding of the standards is essential for understanding networking standards as follows: OSI model, SLIP, PPP, IEEE 802 standards, NDIS and ODI.

Each form of transmission media was analyzed and compared in terms of each evaluation criteria. Cable media are often cheaper than wireless media, yet cable media are also limited in the distances they can cover. Wireless media are often more susceptible to EMI than fiber-optic cable is, but wireless media are not subject to accessibility and other installation problems faced by cable. In conclusion, each transmission media should be evaluated in terms of the obstacles one will face in trying to relay a signal from one device on the network to another.

An essential component in ethernet and token-ring networks is network adapter card. The network adapter card performs several functions, including preparing, sending and controlling the flow of data to the network transmission medium.

Some of the connectivity devices can be use to expand, optimise and interconnect networks. These devices have some similarities, but each is designed for a spesific task, as described in the following list:

- ◆ Repeaters regenerate a signal and are used to expand LANs beyond cabling limits.

- ◆ Bridges know the side of the bridge on which a node is located. A bridge passes only packets addressed to computers across the bridge, so a bridge can thus filter traffic, reducing the load on the transmission medium.

- ◆ Routers forward packets based on a logical address. Some routers can determine the best path for a packet based on routing algorithms.

- ◆ Gateways function under a process similar to routers except that gateways can connect dissimilar network environments. A gateway replaces the necessary protocol layers of a packet so that the packet can circulate in the destination environment.

When devices communicate over the network, they must utilise some form of transport protocol or set of rules to move data from one device to another. This objective reflects the need for you to know the transport protocols. Some of the most common protocol suites, as follows:

- ◆ **TCP/IP:** The Internet protocol suite.
- ◆ **IPX/SPX:** A protocol suite used for Novell NetWare networks.
- ◆ **NetBEUI:** A non-routable protocol used on Microsoft networks.
- ◆ **Apple Talk:** The Apple Macintosh protocol system.
- ◆ **DLC:** A protocol that Windows NT networks use to connect with HP JetDirect printers and IBM mainframes.

All Microsoft machines on a network use NetBIOS names and that these names have some rules regarding their construction. Microsoft networking components rely on the capability to reference other machines on the network using NetBIOS names.

Through the use of a regular backup plan, the installation of a UPS, and the implementation of a fault-tolerant disk scheme, you can help to ensure that your network will run efficiently and safely as possible.

- ◆ Monitoring the network includes some of the tools and resources that can be used to monitor network trends and information.

REFERENCES

- Glen Berg, (1998). MCSE Training Guide: Networking Essentials, Second Edition, New Riders Publishing
- Eric A. Hall, (2000). Internet Core Protocols The Definitive Guide, First Edition
- Douglas E. Comer, (2001). Computer Networks and Internet with Internet Applications, Third Edition
- Mani Subramanian, (2000). Network Management Principles and Practice
- Microsoft Corporation, (1996). Networking Essentials: Hands-on Self-paced Training for Local and Wide Area Networks, Microsoft Press
- Microsoft Corporation, (1999). Supporting Microsoft Windows NT Server 4.0-Enterprise Technologies, Microsoft Press
- Microsoft Corporation, (1998). Internetworking with Microsoft TCP/IP on Microsoft Windows NT 4.0, Microsoft Press
- Microsoft Corporation, (1999). Supporting Microsoft Windows NT 4.0 Core Technologies, Microsoft Press
- Microsoft Corporation, (1999). Administering Microsoft Windows NT 4.0
Microsoft Press
- Rob Scrimger, Kelli Adam, (1999). MCSE Training Guide: TCP/IP, Second Edition, New Riders Publishing