

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/283676932>

Computer networks and Communications

Book · October 2010

CITATIONS

0

READS

582

2 authors, including:



Abdelfatah A Tamimi
Al-Zaytoonah University of Jordan

49 PUBLICATIONS 228 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Class room face recognitjon system [View project](#)



A System for the Detection and Identification of Objects and Their Distances to Aid Blind People [View project](#)

COMPUTER NETWORKS

&

COMMUNICATIONS

COMPUTER NETWORKS

and

COMMUNICATIONS

THIRD EDITION

**Abdelfatah Aref Tamimi, Ph.D
Eng. Jamal M. Khalifeh, Ph.D**

PREFACE

This book is now in its third edition. The networking picture has changed radically since the second edition. The most important is the huge increase in wireless networks, including 802.11, cellular networks, Bluetooth, WAP, infrared, and others. Much has changed in the fields of computer networks and communications. The third edition has been updated to incorporate new advances in communication and networking technology that have emerged since the second edition.

The book covers all the main topics and problems of computer networks and communications: network standards, architecture, classification and topology, network access means, which protocol to use, routing policies and algorithms, distributed computer and network applications and services, etc. The book is liberally illustrated and written in simple language. It starts by explaining the basic principles of data networking and of layered protocols upon which all modern data communications are based. It then goes on to explain the transmission medium and transmission technologies, going through many detailed terms relevant to local area network technologies including Ethernet, wireless LAN, extended LANs and data link services. This book also covers modern IP networks including wireless MAN, mobile based computer networks and the Internet. Finally this book covers the transport layer and application layer services and protocols. Our goal is that readers who only want to ‘dip in’ to have a single topic explained should go away satisfied—able to build on any previous knowledge of a given subject.

The book is organized to serve as a reference as well as a source of learning. Therefore each chapter is self-contained in many respects.

Chapter 1: Introduction. The introductory chapter provides a presentation of the various classes of interconnection networks and a brief description of Computer Networking benefits, network building blocks, types of networks, and the network operating system (NOS).

Chapter 2: Network Standards. This chapter defines more carefully what we mean by network architecture by introducing the central ideas that are common to all network layering and architectures including OSI architecture, the Internet TCP/IP architecture and a brief description of ATM architecture.

Chapter 3: Network classification. In this chapter you will learn how to classify networks according to their size, topology, and applications. We will provide you a detailed description of switching technologies including circuit, packet, cell, and frame switching technologies. This chapter will be wrapped up with a general description of the Internet, Intranet and Extranet stating the differences and similarities between them.

Chapter 4: Data transmission. This chapter examines a number of concepts and defines a fundamental set of elements that apply universally to data transmission networks. The concept of signal is explored in both analog and digital terms, with the advantages and disadvantages of each being explained. The concept of encoding is discussed in detail, with variations on the theme detailed and illustrated. Finally, this chapter explores the various types of modulation techniques used to transmit analog and digital signals through digital and analog circuitry.

Chapter 5: Transmission medium. This chapter addresses all transmission medium commonly used in traditional voice, data, video, and image networks, whether analog or digital in nature. It focuses on twisted-pair, coaxial cable, optical fibers, as guided media and microwave satellite broadcasting radio, cellular communication infrared and Bluetooth as unguided medium.

Chapter 6: Data link services and LAN protocols. In this chapter we introduced the possible services that can be offered by a link-layer protocol including framing, medium access control, reliable delivery, flow control, error detection, and error correction.

Chapter 7: LAN technologies. This chapter focuses on the most popular LAN technologies, Ethernet, IEEE 802.12, Token Ring, Fiber Distributed Data Interface (FDDI), Wireless LANs and ATM LAN. Ethernet easily has the largest installation base, which continues to expand into the foreseeable future; it takes the largest part of this chapter.

Chapter 8: Extended LAN. This chapter explains how to expand the size and range of a computer network, and how to add devices that amplify, connect, and segment the transmission medium. These hardware devices are called repeaters, hubs, bridges, and routers. We will define VLAN's and examine the difference between a LAN and a VLAN. This is followed by a discussion on the advantages VLAN's introduce to a network. Finally we will focus in this chapter on how to wirelessly extend networks using wireless devices.

Chapter 9: WAN internetworking technologies. The vast majority of existing WAN connections work like what is described in this chapter. Here we will introduce the various transmission technologies used in wide-area network (WAN) environments. These include Frequency and Time Division Multiplexing techniques, Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN), Fiber Distributed Data Interface (FDDI), and Synchronous Optical Network (SONET), in addition to Broadband Wireless Access technology (BWA).

Chapter 10: IP protocols. This chapter describes how wide area networks can use the Internet Protocol. We will discuss in detail the two most important variations of the Internet Protocol—version 4 (IPv4) and version 6 (IPv6)—and we shall cover the functions and describe the structure of an IP packet and the basic IP processing including input, forwarding, and output. We discuss option processing and fragmentation and reassembly. In this chapter we will also cover the basics of ICMP, IGMP, ARP, and RARP protocols, their fundamental operations and functions, their characteristics, and how their data units are built and transferred.

Chapter 11: Network layer addressing. This chapter will help you become familiar with the old IPv4 addresses and addressing scheme and will also explain how IPv4 and IPv6 addressing work and why they have been designed the way they are. We will also cover the necessity, the principles and the methods of subnetting. Then we will explain the concepts of Network Address Translation (NAT).

Chapter 12: Routing. This chapter on routing and routing protocols covers a large amount of material, from the basics of routing and the techniques used to distribute routing

information, to the protocols that realize these techniques. This chapter briefly covers two classes of routing protocols: intradomain routing protocol or intranetwork routing protocol or intranet, and interdomain routing protocol or internetwork routing protocol or extranet. The chapter then outlines some of the issues of routing for mobile IP traffic. Combining the best of both wireless and IP technologies has brought us into the era of wireless IP.

Chapter 13: The transport layer protocols. We will begin this chapter by studying the services that a transport layer protocol can provide to network applications, including multiplexing/demultiplexing function for communicating processes. We then go on to describe in detail the UDP for connectionless service and TCP for connection-oriented service. Flow control and congestion control algorithms will be examined. We will cover reliable data transfer in this chapter while taking a close look at TCP. We will learn that TCP is complex, involving connection management, flow control, roundtrip time estimation, as well as reliable data transfer. We included a short description of mobile transport layer protocols and how TCP and UDP are modified to accommodate the requirement of mobility. In the final section of this chapter we will briefly cover the principles of communication between processes using client and server sockets.

Chapter 14: The application protocols. This chapter is intended to give the background to the standardized application protocols and to illustrate how they function and how they make use of IP and IP transport services by examining a few of the very common and most important protocols.

Glossary: The glossary of terms is intended to provide a single reference point for information.

The book is intended to provide a complete foundation textbook and reference of modern data networking which we hope will find a valued position in your bookcase.

Although special attention is given to wireless and mobile technology, new chapters are added to cover more aspects of communication and networking. The new chapters are:

Chapter 6: Data Link services and LAN Protocols

Chapter 12: Routing

Chapter 13: The Transport Layer Protocols

Chapter 14: The Application Protocols

This book may be used as a text book or as a reference for students in information technology, communication engineering or computer engineering disciplines. The level and details of the book may be suited for an introductory graduate course or for two undergraduate courses. In the latter case, the first course may include **chapters 1, 2, 3, 5, 7, 8, 11 and 14**, where the remaining Chapters are to be included in the second course.

Acknowledgments

Trying to selectively integrate as much material as we have attempted to do, it would not have been feasible without the generous support of many of our colleagues. We would like to thank all those people who contributed to this effort.

Writing a text is rarely an individual effort. Many experts from companies and academic staff graciously provided help. We would like to thank them all very warmly for

their support. Many of them have given us invaluable ideas and support during this project. We should acknowledge all those who helped us in this project.

We are grateful to all reviewers of this book for making constructive suggestions that helped us reshape the book to its present form. We would especially like to recognize the following people, who provided invaluable feedback during the writing phase of the manuscript. We took all their comments seriously and incorporated them into the manuscript. We would like to thank **Mrs. Dima Qutob** for taking the time and effort to edit this book.

We are truly indebted to our graduate students, who helped us throughout the long phase of preparing the manuscript of this textbook. Over the years, they read various portions of this book and made constructive comments. We wish them the best for their honest support and verbal comments on early versions of this book used in our class lectures.

This book would not have been possible without the indulgence and infinite patience of our families during what often appeared to be an overwhelming task. They graciously accommodated the lost time during evenings, weekends, and vacations. As a small measure of our appreciation, we dedicate this book to them.

Finally, we would like to thank every one who used the previous versions of this book, especially those who made comments and suggestions that helped improve the second and third editions.

How to Contact the Authors

Please feel free to send us any feedback at the Department of Computer Science, Al-Zaytoonah University, Amman, Jordan, or via e-mail at

drtamimi@alzaytoonah.edu.jo

drjamalkhalifeh@alzaytoonah.edu.jo

Your suggestions and comments will be highly valued and will be taken into consideration for future modifications. We hope the book will be enjoyable to you and will grant you some of our enthusiasm for computer communication.

CONTENTS

PREFACE	IX
CONTENTS	XIII
CHAPTER 1.....	1
INTRODUCTION	1
1.1 About This Chapter	1
1.2 Learning Outcome	1
1.3 What is a Network?.....	1
1.4 Benefits of Computer Networking	2
1.4.1 Powerful, Flexible Collaboration	3
1.4.2 Freedom to Choose the Right Tool	3
1.4.3 Cost-effective Resource Sharing	3
1.4.4 Worldwide, Instantaneous Access to Information.....	4
1.4.5 Secure Management of Sensitive Information	4
1.4.6 Effective Worldwide Communications	4
1.4.7 Easy, Immediate Information Dissemination	4
1.5 Network Building Blocks	4
1.5.1 End Systems, Clients and Servers	5
1.5.2 Network interface cards (NICs) or	5
1.5.3 Physical connecting medium.....	5
1.5.4 Intermediate switching devices	5
1.5.5 Network software	6
1.6 Types of Networks.....	6
1.6.1 Peer-to-Peer Network.....	6
1.6.1.1 Peer-to-Peer Advantages	6
1.6.1.2 Peer-to-Peer Disadvantages.....	7
1.6.2 Client-Server Network	7
1.6.2.1 Client-server Advantages	9
1.6.2.2 Client-server Disadvantages.....	9
1.6.2.3 Comparison between Peer-To-Peer and Client Server Types.....	10
1.6.3 Hybrid Networks	10
1.7 The Network Operating System (NOS)	10
1.7.1 Network Operating System Definition and Services.....	10
1.7.2 Peer-to-Peer Network Operating Systems	11
1.7.3 Client Server Network Operating System	11
1.7.3.1 Client Software	12
1.7.3.2 Server Software.....	14
1.7.4 Hybrid Network Operating System	16
1.8 Quick Review	16
1.9 Self Test Questions	17
CHAPTER 2.....	21
NETWORK STANDARDS.....	21
2.1 About This Chapter.....	21
2.2 Learning Outcome	21
2.3 What Dose Standard Mean?.....	21
2.4 Layered Network Architecture	23

2.4.1 Benefits of Using Layered Architecture	23
2.4.2 Communication Protocols	24
2.4.3 Communication between Systems	25
2.4.4 Information Exchange and Data Encapsulation	26
2.5 Reference Models	28
2.5.1 Benefits of Modularity	28
2.5.2 Open Systems Interconnection (OSI)	29
2.5.2.1 OSI Layers	29
2.5.2.1.1 Layer 1: Physical Layer	29
2.5.2.1.2 Layer 2: Data-Link Layer	30
2.5.2.1.3 Layer 3: Network Layer	31
2.5.2.1.4 Layer 4: Transport Layer	31
2.5.2.1.5 Layer 5: Session Layer	31
2.5.2.1.6 Layer 6: Presentation Layer	32
2.5.2.1.7 Layer 7: Application Layer	32
2.5.2.2 IEEE Specifications	33
2.5.3 The TCP/IP Model	35
2.5.3.1 TCP/IP Layers	35
2.5.3.1.1 Layer 1: Network Access Layer	35
2.5.3.1.2 Layer 2: Internet Layer	35
2.5.3.1.3 Layer 3: Transport Layer	35
2.5.3.1.4 Layer 4: Application Layer	36
2.5.4 Comparison of OSI and TCP/IP Models	36
2.5.4.1 Similarities	37
2.5.4.1 Differences	37
2.5.5 Equal-Size Packet Protocol Model	37
2.5.5.1 Physical Layer	37
2.5.5.2 ATM Layer	38
2.5.5.3 ATM Adaptation Layer (AAL)	38
2.5.5.4 Higher Layers	38
2.5.5.5 User Plane	38
2.5.5.6 Management Plane	38
2.6 Different Forms of Data Units	39
2.7 Quick Review	40
2.8 Self Test Questions	41
CHAPTER 3	47
NETWORK CLASSIFICATION	47
3.1 About This Chapter	47
3.2 Learning Outcome	47
3.3 General Network Classification Methods	47
3.4 Networks Classification by Geographical Coverage	48
3.5 Local Area Network (LAN)	49
3.5.1 LAN Topologies	49
3.5.1.1 Bus Topology	50
3.5.1.2 Star Topologies	51
3.5.1.3 Ring Topologies	52
3.5.1.4 Tree Topology	52
3.5.1.5 Mesh Topologies	53
3.6 Metropolitan Area Networks (MAN's)	53
3.7 Wide Area Network (WAN)	54
3.7.1 Private and Public WAN	55
3.7.2 Switched and Dedicated WAN	56

3.7.2.1 Circuit switching (CS).....	58
3.7.2.2 Packet switching (PS)	58
3.7.2.2.1 Types of Packet-Switched Networks	59
3.7.2.3 Frame Switching (Frame Relay)	61
3.7.2.4 Cell Switching.....	62
3.8 Internetworking (Internet).....	63
3.8.1 Connecting to the Internet Backbone	65
3.8.1.1 Internet Services Provider (ISP) and Network Access Points (Naps).....	65
3.8.1.2 Common Internet Accessing Methods	65
3.8.1.2.1 Residential Access Networks	65
3.8.1.2.2 Institutional Access Networks, (Enterprise Access Networks)	67
3.8.1.2.3 Mobile Access Networks	67
3.8.2 Intranet	68
3.8.3 Extranet	68
3.9 Quick Review	69
3.10 Self Test Questions	70
CHAPTER 4.....	75
DATA TRANSMISSION	75
4.1 About This Chapter	75
4.2 Learning outcome	75
4.3 Transmission Signals	76
4.3.1 Signal Parameters.....	76
4.3.1.1 Amplitude	76
4.3.1.2 Frequency.....	76
4.3.1.3 Phase	77
4.3.2 Signal Types.....	79
4.3.2.1 Analog Signals	79
4.3.2.1.1 Advantages of Analog Signals	79
4.3.2.1.2 Disadvantages of Analog Signals.....	79
4.3.2.2 Digital Signals.....	80
4.4 Data Transmission	81
4.4.1 Transmission Modes	81
4.4.1.1 Transmission Modes According to Data flow	81
4.4.1.1.1 Simplex Transmission.....	81
4.4.1.1.2 Half-duplex Transmission.....	81
4.4.1.1.3 Full-duplex Transmission	81
4.4.1.2 Transmission Modes According to Type of physical connection	82
4.4.1.2.1 Parallel Mode.....	82
4.4.1.2.2 Serial Mode.....	82
4.4.1.3 Transmission Modes According to the Bandwidth Requirements.....	84
4.4.1.3.1 Baseband Transmission	84
4.4.1.3.1 Broadband Transmission	84
4.5 Transmission Impairments	85
4.5.1 Attenuation.....	85
4.5.2 Dispersion	85
4.5.3 Distortion	85
4.5.4 Noise	86
4.5.4.1 Thermal Noise.....	86
4.5.4.2 Intermodulation Noise.....	87
4.5.4.3 Crosstalk	87
4.5.4.4 Impulse Noise	88
4.6 Data Channel Characteristics	88

4.6.1 Channel Capacity	88
4.6.2 Efficiency.....	90
4.6.3 Transmission Rate	90
4.6.3.1 Baud Rate (Modulation rate).....	90
4.6.3.2 Circuit Speed (Data signaling rate).....	90
4.6.4 Bit Error Rate.....	91
4.6.5 Data Transmission Channels	91
4.7 Digital Transmission of Digital Data.....	92
4.7.1 Purposes of Line Coding	92
4.7.2 General Classification of Line Coding	92
4.7.2.1 Non-Return-To-Zero (NRZ)	92
4.7.2.2 Return-To-Zero (RZ)	93
4.7.2.3 Bi-phase Encoding.....	93
4.7.3 Signaling Techniques.....	93
4.7.3.1 Polar Signaling.....	93
4.7.3.2 Unipolar Signaling.....	94
4.7.3.3 Bipolar	94
4.7.3.4 Multi-Level Signaling.....	94
4.7.4 Types of Line Codes	94
4.7.4.1 Nonreturn-to-Zero-Level (NRZ) Signal Encoding.....	94
4.7.4.1.1 Nonreturn-to-Zero-Level (NRZ-L).....	95
4.7.4.1.1 Nonreturn-to-Zero-Inverted (NRZ-I).....	95
4.7.4.2 Bipolar AMI Signal Encoding	95
4.7.4.3 Manchester Signal Encoding	95
4.7.4.4 Differential Manchester	96
4.7.5 Some IntermeDiate Encoding Techniques.....	97
4.7.5.1 4B/5B Encoding.....	97
4.7.5.2 5B/6B Encoding.....	97
4.7.5.3 8B10B Encoding.....	97
4.7.5.4 8B/6T Encoding	98
4.8 Analog Transmission of Digital Signal	98
4.8.1 Amplitude-Shift Keying (ASK).....	100
4.8.2 Frequency-Shift Keying (FSK).....	100
4.8.3 Phase-Shift Keying (PSK)	101
4.8.4 Multi level Sift Keying	101
4.8.5 Quadrature Amplitude Modulation (QAM)	102
4.9 Digital Transmission of Analog Data	103
4.9.1 Sampling	103
4.9.2 Encoding	103
4.10 Analog Transmission of Analog Data	105
4.10.1 Amplitude Modulation (AM).....	105
4.10.2 Single Sideband (SSB)	107
4.10.3 Frequency Modulation (FM)	108
4.10.4 Phase Modulation	109
4.11 Quick Review	109
4.12 Self Test Questions.....	110
CHAPTER 5	117
TRANSMISSION MEDIUM	117
5.1 About This Chapter	117
5.2 Learning Outcome	117
5.3 Fundamentals of Transmission Systems.....	118

5.3.1 Data Terminal Equipments (DTE)	118
5.3.2 Physical Interface	119
5.3.3 Data Communication Equipments (DCE)	119
5.3.4 Transmission Medium	120
5.4 Transmission Medium General Classification and Characteristics	120
5.4.1 General classification of Transmission Medium	120
5.4.2 Frequency Considerations	121
5.5 Guided Transmission Medium	122
5.5.1 Twisted Pair	122
5.5.1.1 Twisted Pair Physical Description	122
5.5.1.2 Categories of Twisted-Pair	125
5.5.1.3 Twisted Pair Application	126
5.5.1.4 Twisted Pair Transmission Characteristics	126
5.5.2 Coaxial Cable	127
5.5.2.1 Coaxial Cable Physical Description	127
5.5.2.2 Coaxial Cable Application	128
5.5.2.3 Coaxial Cable Transmission Characteristics	129
5.5.3 Optical Fiber	129
5.5.3.1 Optical Fiber Physical Description	130
5.5.3.2 Types of Optical Fiber Cable	131
5.5.3.3 Optical Fiber Application	132
5.5.3.4 Optical fiber Transmission Characteristics	134
5.6 Unguided Transmission Medium	134
5.6.1 Terrestrial Microwave	134
5.6.1.1 Terrestrial Microwave Physical Description	135
5.6.1.2 Terrestrial Microwave Application	136
5.6.1.3 Terrestrial Microwave Transmission Characteristics	136
5.6.2 Satellite Microwave	138
5.6.2.1 Satellite Microwave Physical Description	138
5.6.2.2 Satellite Microwave Application	139
5.6.3 Broadcasting Radio	141
5.6.4 Infrared	142
5.6.5 Bluetooth	144
5.6.6 Cellular Mobile Systems	145
5.7 Summary	148
5.8 Self Test Questions	149
CHAPTER 6.....	155
DATA LINK SERVICES AND LAN PROTOCOLS.....	155
6.1 About This Chapter	155
6.2 Learning outcome	155
6.3 The Services Provided by the Data Link Layer	155
6.4 Framing	157
6.4.1 Frame Structure	157
6.4.2 MAC Addressing	159
6.5 Shared medium and multiple access problem	160
6.5.1 Channel Partitioning Protocols	160
6.5.2 Random Access Protocols	161
6.5.2.1 ALOHA, Slotted ALOHA	161
6.5.2.2 CSMA - Carrier Sense Multiple Access	161
6.5.2.3 Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)	162
6.5.3 Taking-Turns Protocols	163

6.5.3.1 Polling Protocol	163
6.5.3.2 Token-passing Protocol	163
6.5.3.3 Demand Priority (Round-Robin) Access Method	163
6.6 Reliable Transmission and Flow Control	164
6.6.1 Stop-and-Wait Flow Control	165
6.6.2 The Sliding Window Flow Control	166
6.7 Error detection	168
6.7.1 Parity Check	170
6.7.2 Two-Dimensional Parity	171
6.7.3 Internet Checksum Algorithm	171
6.7.4 Cyclic Redundancy Check (CRC)	173
6.7.5 Error Correction.....	176
6.8 Quick Review	176
6.9 Self Test Questions.....	177

CHAPTER 7	183
------------------------	------------

LAN TECHNOLOGY	183
-----------------------------	------------

7.1 About This Chapter	183
7.2 Learning Outcome	183
7.3 Ethernet LAN Architecture	183
7.3.1 Ethernet Frame Format	184
7.3.2 Ethernet Networks (IEEE 802.3 Standards)	185
7.3.2.1 10Base5 - "Thick Ethernet"	185
7.3.2.2 10Base2 - "Thin Ethernet"	187
7.3.2.3 10BaseT - "Standard Ethernet.....	187
7.3.2.4 10BaseF - "Fiber Ethernet"	188
7.3.2.5 10Broad36	189
7.3.2.6 Traditional Ethernet Summary.....	190
7.3.3 Fast Ethernet	191
7.3.3.1 100Base-T4.....	191
7.3.3.2 100Base-TX.....	192
7.3.3.3 100Base-T2.....	192
7.3.3.4 100Base-FX	192
7.3.3.5 Fast Ethernet Summary.....	193
7.3.4 Gigabit Ethernet.....	193
7.3.4.1 1000Base-LX	195
7.3.4.2 1000Base-SX	195
7.3.4.3 1000Base-CX.....	195
7.3.4.4 1000Base-T	195
7.3.4.5 The Gigabit Ethernet Extension Field.....	196
7.3.4.6 Gigabit Ethernet Summary	196
7.3.5 10 Gigabit Ethernet.....	196
7.3.5.1 10 Gigabit Ethernet Types	196
7.3.5.2 10 Gigabit Ethernet Frame Format	199
7.3.5.3 10 Gigabit Ethernet Applications.....	199
7.3.5.3.1 LAN Applications.....	199
7.3.5.3.2 MAN Applications	199
7.3.5.3.3 WAN Applications	199
7.3.6 Ethernet Auto-Negotiation.....	200
7.4 100VG-AnyLAN IEEE 802.12	201
7.4.1 Hub Priority	202
7.4.2 Hub Layers	202
7.4.3 100VG-AnyLAN Advantages and Disadvantages.....	203

7.4.3.1 Advantages.....	203
7.4.3.2 Disadvantages	203
7.5 Token Rings.....	203
7.5.1 Token Ring Topology and specifications.....	204
7.5.2 Token Ring and IEEE 802.5 Frame Format	206
7.5.3 Token Ring Operation.....	207
7.5.4 IBM Token ring and IEEE 805.5 differences.....	208
7.6 FDDI - Fiber Distributed Data Interface	209
7.6.1 FDDI Operation and Specifications	210
7.6.2 FDDI Frame Format.....	212
7.7 Wireless LAN (IEEE 802.11)	213
7.7.1 Wireless LANs General Characteristics.....	213
7.7.2 WLAN Architecture.....	214
7.7.3 WLAN IEEE 802.11Standard	216
7.7.3.1 802.11 Standard	216
7.7.3.2 802.11a Standard.....	216
7.7.3.3 802.11b Standard (Wi-Fi)	217
7.7.3.4 802.11g Standard	217
7.7.4 WLAN IEEE 802.11Frame Format.....	217
7.7.5 WLAN IEEE 802.11MAC Method.....	219
7.8 ATM LAN	222
7.9 Quick Review	223
7.10 Self Test Questions	224
CHAPTER 8.....	231
EXTENDED LAN.....	231
8.1 About This Chapter.....	231
8.2 Learning Outcome	232
8.3 Extending LAN Using Physical Layer Devices.....	232
8.3.1 Repeaters.....	232
8.3.1.1 General Description	232
8.3.1.2 Characteristics of Repeaters:.....	233
8.3.1.3 Drawbacks of Repeaters.....	233
8.3.2 Amplifiers	234
8.3.3 Hubs	234
8.3.3.1 General Description	234
8.3.3.2 Types of Hubs	235
8.4 Extending LAN Using Data Link Layer Devices	237
8.4.1 Bridges	237
8.4.1.1 General Description	237
8.4.1.2 Types of Bridges	237
8.4.1.3 Characteristics of Bridges	239
8.4.2 LAN Switches	241
8.4.2.1 General Description	241
8.4.2.2 Switching Technologies	243
8.4.2.3 LAN Switch Physical Structure	244
8.4.2.4 Switches Features.....	247
8.5 Extending LAN Using Network Layer Devices	247
8.5.1 Routers	247
8.5.1.1 General Description	247
8.5.1.2 Router Physical Structure.....	248
8.5.1.3 Router Characteristics and Functions.....	250

8.5.1.4 Routing Compared to LAN Switching.....	252
8.5.2 Brouters	252
8.6 Extending LAN Using Gateways	253
8.7 Other Techniques to Extend LANs	254
8.7.1Virtual LAN (VLAN)	254
8.7.1.1 General Description	254
VLAN Frame Format	255
8.7.1.3 VLAN Advantages	257
8.7.1.4 VLAN Trunking	258
8.7.2 Extending LAN Wirelessly.....	259
8.7.2.1 Wireless Access Points	259
8.7.2.2 Wireless Bridge:	261
8.7.2.3 Wireless Switches	263
8.7.2.4 Wireless Router	263
8.7.3 Extending LANs over longer distances (Optical fiber Converter).....	264
8.9 Quick Review	264
8.10 Self Test Questions.....	265

CHAPTER 9	273
------------------------	------------

WAN INTERNETWORKING TECHNOLOGY	273
---	------------

9.1 About This Chapter	273
9.2 Learning Outcome	273
9.3 Multiplexing	274
9.3.1 Frequency-Division Multiplexing (FDM)	275
9.3.2 Time-Division Multiplexing (TDM).....	276
9.3.2.1 TDM Link Control.....	278
9.3.2.2 Framing.....	278
9.3.2.3 Pulse Stuffing.....	279
9.3.3 Statistical TDM (STDM)	279
9.3.3.1 STDM Performance	280
9.4 Carrier Systems	281
9.4.1 Analog Carrier Systems	281
9.4.2 Digital Carrier System	282
9.4.2.1 Digital Carrier System Standards.....	283
9.4.2.2 Channel Banks	284
9.5 Synchronous Optical WAN Technology	286
9.5.1 Synchronous Optical Network (SONET)	286
9.5.1.1 SONET Hierarchy and Multiplexing	286
9.5.1.2 SONET Framing.....	287
9.5.2 Synchronous Digital Hierarchy (SDH)	289
9.5.2.1 SDH Hierarchy and Multiplexing	289
9.5.2.2 SDH Framing.....	290
9.6 Integrated Services Digital Network	291
9.6.1 ISDN Services	291
9.6.1.1 Basic Rate Interface (BRI).....	291
9.6.1.2 Primary Rate Interface (PRI)	292
9.6.2 ISDN Equipment Configurations.....	293
9.6.3 ISDN Applications.....	295
9.7 Digital Subscriber Line (DSL)	295
9.7.1 DSL General Description	295
9.7.2 DSL Advantages and Disadvantages	296
9.7.3 DSL Equipment	296

9.7.3.1 DSL Transceiver	297
9.7.3.2 DSLAM	297
9.7.4 DSL variations	298
9.8 Asynchronous Transfer Mode (ATM)	299
9.8.1 ATM General Description.....	299
9.8.2 ATM Cell Format.....	300
9.8.3 ATM Switches	301
9.8.4 ATM Cell Routing	302
9.8.5 Cell Switching versus Packet Switching	303
9.9 Broadband Wireless Access Technology (BWA)	304
9.9.1 BWA Introduction.....	304
9.9.2 Wireless MAN (WMANs)	305
9.9.3 Mobile Broadband Wireless Access (MBWA)	308
9.10 Quick Review	309
9.11 Self Test Questions	310
CHAPTER 10.....	319
IP PROTOCOLS	319
10.1 About This Chapter.....	319
10.2 Learning Outcome	320
10.3 TCP/IP Suite Protocol.....	320
10.4 The Network layer Protocols	322
10.5 Internet Protocol (IP)	322
10.5.1 IP v4 Data Unit	324
10.5.2 IP v6 Data Unit	326
10.5.3 IP v 6 Extension Header Types	327
10.5.4 Fragmentation of Datagrams	329
10.5.5 Mobile IP.....	329
10.6 Internet Control Message Protocol	330
10.6.1 ICMP Data Unit	330
10.6.2 ICMP Version 6 Protocol	332
10.7 Internet Group Management Protocol (IGMP).....	333
10.7.1 Multicasting and Multicast Group.....	334
10.7.2 IGMP Function	336
10.7.3 IGMP Message.....	336
10.7.4 IGMP Reports and Queries	338
10.8 Address Resolution Protocol.....	338
10.8.1 ARP Packet Format	341
10.9 Reverse Address Resolution Protocol (RARP).....	342
10.10 Quick Review	342
10.11 Self Test Questions	343
CHAPTER 11.....	349
NETWORK LAYER ADDRESSING	349
11.1 About This Chapter.....	349
11.2 Learning Outcome	349
11.3 IP Addressing.....	350
11.3.1 Types of Addresses	350
11.3.1 IPv4 Addressing Scheme	352
11.3.2 IP Classes	352

11.3.3.1 Class A Networks	352
11.3.3.2 Class B Networks.....	353
11.3.3.3 Class C Networks.....	353
11.3.3.4 Class D.....	354
11.3.3.5 Class E.....	354
11.3.4 Dotted-Decimal Notation.....	354
11.4 Subnet and Subnet Mask	355
11.4.1 Subnet Masks.....	357
11.4.2 Determining the network ID	358
11.4.3 Subnetting	359
11.4.3.1 Determining the Number of Host Bits	359
11.4.3.2 Enumerating Subnetted Network IDs	360
11.4.3.2 IP Addresses for Each Subnetted Network ID	361
11.5 Public and Private Addresses	365
11.5.1 Public Addresses.....	365
11.5.2 Private Addresses.....	365
11.6 Network Address Translation (NAT)	366
11.6.1 Automatic IP Address Allocation	368
11.6.1.1 Dynamic Host Configuration Protocol (DHCP)	368
11.6.1.2 Bootstrap Protocol (BOOTP).....	370
11.6.2 Prioritization of Automatic IP Addresses	371
11.7 IP v6 Addresses	371
11.7.1 Types of Address Inscription.....	371
11.7.2 IPv6 Address Formats.....	373
11.8 Managing the Address Space	376
11.9 Quick Review	377
11.10 Self Test Questions.....	378
CHAPTER 12	385
ROUTING.....	385
12.1 About This Chapter	385
12.2 Learning Outcome	385
12.3 Routing Principles	386
12.3.1 Building and Using a Routing Table	386
12.3.2 Static Routing versus Dynamic Routing.....	389
12.4 Routing Algorithms and Routing Protocols	390
12.4.1 Choosing the Least Cost Path	392
12.4.2 Classification of Routing Algorithms	394
12.4.2.1 Distance Vector Algorithm (DVA)	394
12.4.2.2 Link-State Routing Algorithm	397
12.4.2.3 Distance Vector versus Link State	399
12.5 Routing protocols	399
12.5.1 Intradomain and Interdomain Routing	400
12.5.2 Intradomain Routing Protocols	401
12.5.2.1 Routing Information Protocol (RIP)	401
12.5.2.1.1 RIP Data Unit Format.....	401
12.5.2.2 Open Shortest Path First	403
12.5.2.2.1 OSPF Packet Format	403
12.5.3 Interdomain Routing Protocols	404
12.5.3.1 Border Gateway Protocol.....	405
12.5.3.1.1 BGP Data Unit.....	406
12.6 Mobile Routing.....	408

12.6.1 Addresses and Agents	408
12.6.2 IP Routing in Mobile Network	409
12.6.3 Mobile Routing with IPv6.....	412
12.6.3.1 Mobile IPv6 Routing Steps	412
12.7 Quick Review	413
12.8 Self Test Questions	414
CHAPTER 13.....	419
THE TRANSPORT LAYER PROTOCOLS	419
13.1 About This Chapter.....	419
13.2 Learning Outcome	420
13.3 The Transport Layer services.....	420
13.4 Application multiplexing and demultiplexing	421
13.5 The Transport Control Protocol (TCP)	422
13.5.1 TCP Segment	423
13.5.2 TCP Connection Setup	425
13.5.3 TCP Flow Control	426
13.5.3.1 Sliding Window TCP Flow Control	427
13.5.3.2 Round Trip Time and Timeout.....	428
13.5.4 TCP Congestion Control	428
13.5.4.1 Slow Start Congestion Control Algorithm:	429
13.5.4.2 Internet Congestion Control Algorithm.....	430
13.6 User Datagram Protocol.....	431
13.6.1 UDP Segment.....	432
13.7 Choosing Between UDP and TCP	432
13.8 Transport Protocols for Mobility	433
13.8.1 TCP for Mobility	434
13.8.1.1 Indirect TCP	434
13.8.1.2 Fast Retransmit Mobile TCP.....	435
13.8.2 UDP for Mobility	435
13.9 Communicating Processes Using Sockets	435
13.10 Quick Review	437
13.11 Self Test Questions	438
CHAPTER 14.....	445
THE APPLICATION PROTOCOLS	445
14.1 About This Chapter.....	445
14.2 Learning Outcome	445
14.3 The Application Protocols	446
14.3.1 Application Layer Protocols Services	446
14.3.2 Client and Server Model	447
14.4 HyperText Transfer Protocol (HTTP).....	448
14.4.1 HTTP Message Formats.....	449
14.4.2 HTTP Requests and Responses	451
14.4.3 HTTP Protocol Coding	452
14.4.4 Uniform Resource Locators	453
14.4.5 Web Caching (Proxy Server)	453
14.5 TELNET Protocol.....	454
14.6 DNS Domain Name System	456
14.6.1 DNS Messages	458

14.6.2 DNS Directory Look-up Service	460
14.7 File Transfer Protocol (FTP)	461
14.8 Electronic Mail (email) Protocols.....	463
14.8.1 Internet Mail Transfer System	464
14.8.2 The Internet Mail Message Format.....	465
14.9 Network Management Protocols	466
14.9.1 Management Information Base (MIB).....	467
14.9.2 Simple Network Management Protocol (SNMP)	468
14.10 Quick Review	471
14.11 Self Test Questions.....	472
APPENDEX	ERROR! BOOKMARK NOT DEFINED.
ANSWER TO SELF TEST QUESTIONS	477
GLOSSARY	483
REFERENCES	511
INDEX.....	517
ACRONYMS	529

CHAPTER 1

INTRODUCTION

1.1 About This Chapter

As you begin your study, it is important that you understand some of the fundamental concepts upon which computer networks are built. This chapter introduces some basic principles of computer-based networking, discusses advantages of networking, presents the idea of connecting computers together and how the computers in the network are configured and how they share information determine whether the network is peer-to-peer or server based—another important network classification.

Without a network operating system of some kind, individual computers cannot share resources, and other users cannot make use of those resources.

This chapter provides a general introduction to network operating systems (NOSs). It describes the basic features and functions of NOS and contrasts these with each other.

1.2 Learning Outcome

At the end of this chapter, you should be able to:

1. Define a computer network.
2. Discuss advantages of using a network.
3. Identify network services.
4. Identify the network main blocks.
5. Identify a peer-to-peer network and a server-based network.
6. Identify the main functions of network operating systems
7. Identify essential NOS components.
8. Describe the elements and services of client software.
9. Describe the elements and services of server software.
10. Distinguish between network operating types.

1.3 What is a Network?

The information technology has been the driving force in most of the advances witnessed this century. There has been a revolution in the way information is gathered, processed and distributed. This revolution can't be done without the convergence of computing and communications. Telephones, radio, television, and computers nowadays are the tools for this information revolution. Geographically distributed computers can be hooked up together to permit the exchange of data and information. **Computer network** can be defined as a collection of devices that can store and manipulate electronic data, interconnected in such a way that network users can store, retrieve, and share information.

Commonly connected devices include microcomputers, minicomputers, mainframe computers, terminals, printers, fax machines, pagers, mobiles and various data storage devices as shown in Figure 1.1.

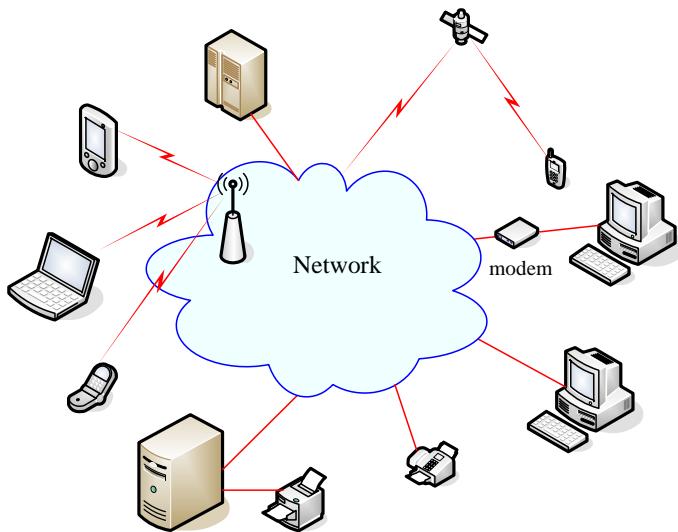


Figure 1.1: Computer Networking

 A network can be anything from a simple combination of hardware, software, and particular connectivity medium, which together allow multiple computing devices to communicate with each other.

In today's business world, a computer network is much more than a collection of interconnected devices. For many businesses, the computer network is the resource that enables them to gather, analyze, organize, and disseminate the information that is essential to their profitability. The rise of Intranets and Extranets is the latest indication of the crucial importance of computer networking to businesses. Intranets and Extranets are private business networks that are based on Internet technology. Intranets, Extranets, and the Internet will be treated in more details later. For now, it is enough to understand that businesses are currently implementing Intranets at a breakneck pace and for one reason only, an Intranet enables a business to collect, manage, and disseminate information more quickly and easily than ever before. Many businesses are implementing Intranets simply to remain competitive; businesses that delay are likely to see their competition outdistance them.

1.4 Benefits of Computer Networking

The most obvious benefit of computer networking is that you can store and retrieve virtually any kind of information on a computer network, including textual information such as letters and contracts, audio information such as voice messages, and visual images such as facsimiles, photographs, medical x-rays, and even videos. In addition to information storage and retrieval, there is a host of other important benefits of networking computers. Having a computer network enables us to combine the skills of

different people and the power of different equipment, regardless of the physical locations of the people or the equipment. Computer networking enables people to easily share information and hardware, allowing them to take advantage of communication medium such as electronic mail, newsgroups, and video conferencing. It also allows them to work more securely, efficiently, and productively. Never theless the major benefits of computer networking are:

1.4.1 Powerful, Flexible Collaboration

To be able to collaborate electronically from widely separate physical locations has significant advantages. It enables people to avoid the considerable time investments and costs connected with traveling. It enables people to communicate instantaneously, regardless of the distance, and to act before their competitors do. It frees people from having to reconcile the differences in multiple information files. Electronic collaboration enables people to minimize the amount of work required to complete projects, it frees them from redoing work they would do correctly in the first place if they had instantaneous access to up-to-date information and instructions. For example, users can engage in real time teleconferencing, talking face to face, while simultaneously viewing and editing the same document, adding and deleting notes and comments, and instantaneously viewing each other's changes as they are made. They can do this without having to worry about accidentally changing the work of others.

1.4.2 Freedom to Choose the Right Tool

Open networking products enable users to work on the type of computer best suited to the job they must do, without placing restrictions on their file-sharing capabilities. The design of any particular computer can make it well suited for some tasks and not suited for others. In an open environment, you can combine many kinds of computers to take advantage of the special strengths of each type of machine. For example, Novel network users can use IBM PCs running any version of Windows or DOS, Macintosh computers running a version of the Macintosh operating system, Sun workstations running the UNIX operating system, and many other types of computers, all on the same network. Scientists, secretaries, doctors, lawyers, writers, editors, artists, engineers, everyone can use the type of computer equipment best suited to the type of work he or she does, yet each can still easily share information with others.

1.4.3 Cost-effective Resource Sharing

A network enables users to share any networkable equipment or software and realize the benefits that you would enjoy from resource sharing. On a network, users can share printers, modems; data storage devices, such as hard disks and CD-ROM drives; data backup devices, such as tape drives; E-mail systems; facsimile machines; and all networkable software. When you compare sharing these resources to purchasing them for each computer, the cost savings can be enormous.

When we implement an Intranet, we can share network resources with suppliers, consultants, and other outside partners. We will be able to rent applications over the Internet. Businesses have capability to explore Intranet resource sharing.

1.4.4 Worldwide, Instantaneous Access to Information

With access to our business's Intranet and Web server, we will be able to easily and inexpensively access any new or updated information, from anywhere in the world, within a few seconds after it is published. The Internet provides the low-cost backbone for global access to your Intranet, and existing Web browsers and other Intranet tools make it easy for even the most novice computer user to access the information and Intranet resources they need.

The best networks have extremely powerful security features that enable us to exercise flexible control of who will have access to sensitive data, equipment, and other resources.

1.4.5 Secure Management of Sensitive Information

There is another advantage to computer networking that may be even more important than instantaneous, coordinated information and resource sharing. The best networks have extremely powerful security features that enable you to exercise flexible control of who will have access to sensitive data, equipment, and other resources.

1.4.6 Effective Worldwide Communications

If you choose a networking company that offers a full suite of products—including robust directory services—and that supports open standards, you will be able to connect heterogeneous computing equipment at distant geographic locations into one cohesive network. As a result, you will be able to disseminate critical information to multiple locations anywhere in the world, almost instantaneously.

1.4.7 Easy, Immediate Information Dissemination

When we implement a business Intranet, we can create or update information that will be easily and immediately make it accessible to all company employees. With a World Wide Web server running on our Intranet and with today's powerful Web publishing tools, we can create or change any information using a favorite, familiar application, and we can have that information automatically and instantaneously published on our Web server. This information will then be available to anyone who has the rights to access it, anywhere in the world.

1.5 Network Building Blocks

All networks, large or small, require specialized network hardware to make them work. Small or large, all networks are built from the following basic building blocks:

1.5.1 End Systems, Clients and Servers

In computer networking jargon, we often referre to the computers that we use on a daily basis as "hosts" because they host (run) application-level programs such as a Web browser or server program, or an e-mail program. They are also referred to as "end systems" because they sit at the "edge" of the networks, as shown in Figure 1.2.

The computers that end users use to access the resources of the network are Client computers. They are typically located on the users' desks, while computers that provide shared resources, such as disk storage and printers, as well as network services, such as e-mail and Internet access are known as Server computers.

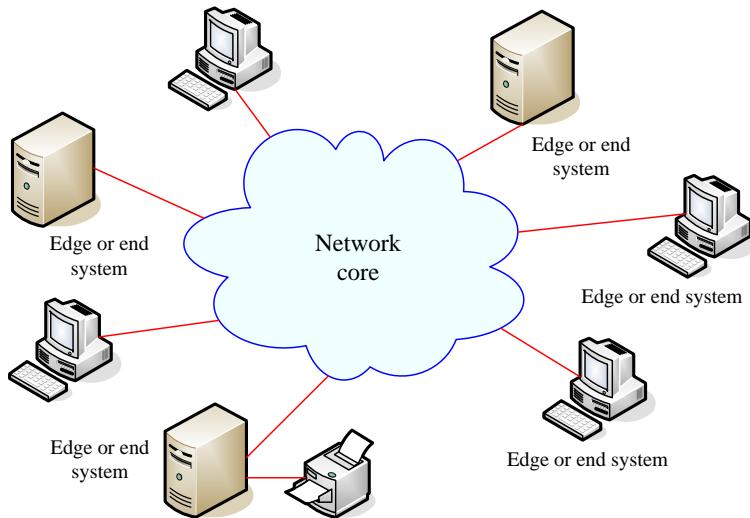


Figure 1.2: Network building blocks

1.5.2 Network interface cards (NICs) or network adapters

NIC enables the computer to communicate over a network. Every end system must have a network interface card (or a built-in network port) in order to be a part of a network.

1.5.3 Physical connecting medium

The physical medium can take many shapes and forms, and does not have to be of the same type for each transmitter-receiver pair along the path. Examples of physical medium include twisted-pair copper wire, coaxial cable, multimode Optical fiber cable, terrestrial radio spectrum and satellite radio spectrum.

1.5.4 Intermediate switching devices

Physical medium usually doesn't connect computers directly to each other. Instead, each end system is connected to a device that in turn, connects it to the rest of the network. Router, switches, hubs, bridges, and gateways, are examples of connecting and switching devices, we refer to the combination of these devices as a **network core**.

1.5.5 Network software

Although network hardware is essential, what really makes a network work is software. A whole bunch of software has to be set up just right in order to get a network working. Server computers typically use a special *network operating system* (also known as NOS) in order to function efficiently and client computers need to have their network settings configured properly in order to access the network.

1.6 Types of Networks

Not all computers are equal in a network - their status depends on the role they perform. There are three kinds of computers in a network:

1. Client computers: Use network resources.
2. Peer computers: Use and provide network resources.
3. Servers: Only provide network resources.

We cannot assume that the role of a computer in a network is tied to the operating system it runs. A Macintosh is not a peer unless it is sharing network resources. And do not be surprised if somebody decides to run Windows NT as merely a client, it would be a tragic waste of resources. The operating system merely determines the networking potential of a computer.

Depending on how we assign roles to individual computers in our network, we can classify all networks into three broad categories.

1.6.1 Peer-to-Peer Network

Peer-to-peer is a style of networking in which a group of computers communicate directly with each other, rather than through a central server. Every computer in this network functions as both clients and servers to the other computer on the network. Peer nodes may differ in local configuration, processing speed, and network bandwidth and storage quantity. Popular examples of peer-to-peer are file-sharing networks.

Peer to peer networks have no role for servers and are thus marked by the total absence of central control. All you have to do is an individual log into workgroups and start working. Everybody shares disk resources and devices like printers in the manner they deem fit. You also need to use a network operating system to recognize the other workstations in the network. In this configuration, each user in the network determines which data Base or resources they wish to share. Figure 1.3 illustrates a peer-to-peer.

1.6.1.1 Peer-to-Peer Advantages

1. A peer-to-peer network is a simple solution for interconnecting computers. Just add a network interface card (NIC) to each system, connect the systems with cabling and begin sharing information.
2. Peer to peer networks allow economical communication with other users when there is a limited amount of data to exchange. Sharing expensive peripherals becomes easy. Moreover, your productivity will increase with the ability to send files and messages without having to leave your workstation.

3. These networks are relatively inexpensive (no server hardware, no administrator) and work quite well for very small operations.

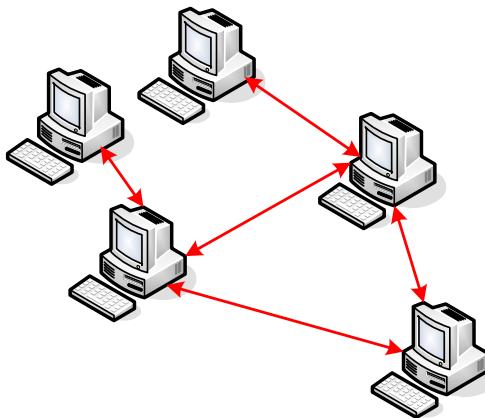


Figure 1.3: Peer-to-peer network

1.6.1.2 Peer-to-Peer Disadvantages

1. In peer-to-peer networks, all users must be located in the same general area. If you exceed 5-10 users with this type of network, the network management may become very difficult.
2. Because there is no dedicated server to handle the file and print sharing administration, peer to peer networking may not be practical for intensive file transfer/storage or heavy printer sharing applications.
3. Security in these networks is lax, work can be cumbersome if every peer decides to put up a password on his/her machine, and system performance suffers dramatically if there is too much traffic on a particular machine.
4. Plus, the absence of central control means that data is disorganized and very tough to locate over the network.
5. When the numbers of workstations in the network increase, problems will arise due to the cost of administration and security.



Peer-to-peer networking is ideal for small workgroups, but offers limited security and is easily disrupted by computer shutdowns.

Peer-to-peer networking sharing resources among networked client systems which can also act as servers, so no dedicated server is needed.

1.6.2 Client-Server Network

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a

single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program on your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program that sends a request to a data base server at another bank computer to retrieve your account balance. The balance is returned back to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you.

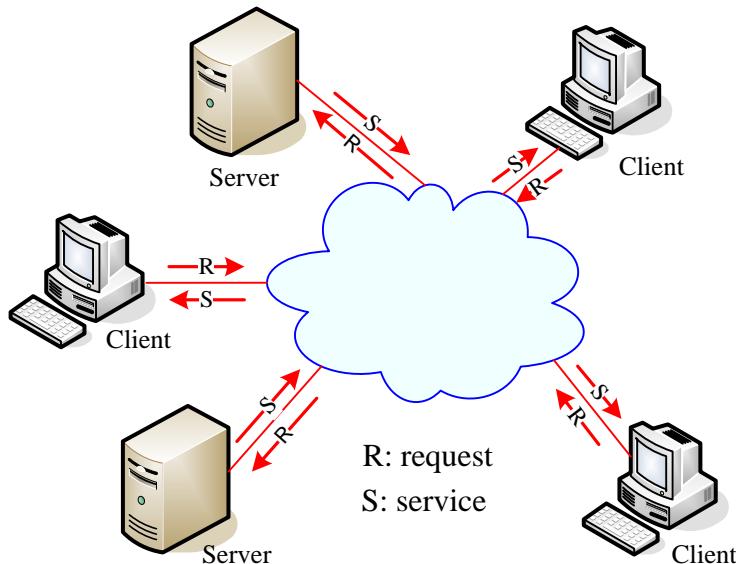


Figure 1.4: Client-Server network

Servers and clients are usually connected with network interface cards using a cabling system and hub to work with the chosen protocol. Figure 1.4 illustrates a small client/ server network. A dedicated server provides responsive, highly available file storage and backup for all the users; expedited printing capabilities, as well as e-mail or Internet access for the group. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. In the usual client/server model, one server is activated and awaits client requests. Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, the Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which technically is called a Hypertext Transport Protocol or HTTP server) in another computer somewhere on the Internet.

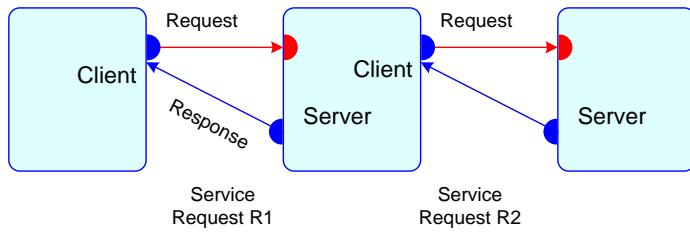


Figure 1.5: Conceptual Client/Server Model

In the old days, the clients were simply dumb tubes. They had a monitor and a keyboard. This type of system is still common in banks and hotels where storage of data locally at the client is undesired or unnecessary. The trend has been to use smart clients in most new client/server networks. Smart clients will have their own local storage of data and programs that offer far more flexibility.

1.6.2.1 Client-server Advantages

1. A client-server networking strategy provides powerful and secure communication services for workgroups from 3-4 users up to hundreds of users.
2. The server provides high levels of control over resources shared on the network and makes administrating the network much easier than in a peer-to-peer environment. The Client / Server networking is cost efficient since you can use basic workstations and a fast server.
3. Workstations may be equipped with less memory and smaller hard drives, thus saving on total setup costs. Users will have access to all the power of the server and all the resources on the network with excellent response time, even though hundreds of other users may also be connected.
4. Client-Server networks revolve around powerful machines that take care of the security and administration on the network.
5. Servers normally have very specific roles in the network, therefore they split the support objectives of the network.

1.6.2.2 Client-server Disadvantages

Even though the Client-Server type of network has many advantages, there are some disadvantages:

1. The cost of this type of network is relatively high up front. Not only must you purchase the server hardware, but most server software is very expensive, especially for larger networks. This is due to the fact that some software companies charge more for each client computer that requires connection to the main server.
2. Another downside to be considered is the possibility of the main server having problems. How fast must you have the network working again? If you need all time operability, you should allow in your budget a second "redundant" server. Hence if the main server goes down, the redundant server will step in and provide services until the primary server is back up again. An experienced administrator should be able to setup redundant servers that will assume control of failing servers without user intervention.

1.6.2.3 Comparison between Peer-To-Peer and Client Server Types

Consideration	Peer-to-Peer Network	Server-Based Network
Size	Good for 10 or fewer computers	Limited only by server and network hardware
Security	Security established by the user of each computer	Extensive and consistent resource and user security
Administration	Individual users responsible for their own administration; no full-time administrator necessary	Centrally located for network control; requires at least one knowledgeable administrator

1.6.3 Hybrid Networks

Most networks in the world are hybrid networks that run clients, peers and servers together. Users get the best of all worlds - shared resources are located on servers but the users can still directly touch their peers (bypassing the PDC) for shared resources. This has an important implication on security - users can be assigned variable levels of access to the server and peer machines depending on the importance of the data.

1.7 The Network Operating System (NOS)

1.7.1 Network Operating System Definition and Services

A network operating system acts as the command center, enabling all of the network hardware and all other network software to function together as one cohesive, organized system. It is the heart of the network. The term *network operating system*, however, is generally reserved for software that enhances a basic operating system by adding networking features.



NOS are an application, which allows two or more computers to communicate transparently and to share data, peripherals and processing power.

NOS, includes special functions for connecting computers and devices into a local-area network (LAN). It is installed onto each PC that requires network access. It is like a traffic warden that monitors the exchange and flow of files, electronic mail, and other network information.

NOS is a specialized system software designed to provide networking functionality. It has all the features of a stand alone operating system but offers many more facilities in a complex environment. In addition to the usual lower level computing functions, a network operating system is responsible for other functions such as:

1. Directing data traffic through the network
2. Security functions such as authentication, authorization, logon restrictions and access control so it can allow and prevent access to data.
3. Protection and synchronization functions that enable it to prevent access to data files while they are being processed

4. Managing the flow of information between a variety of workstations
5. Internetworking functions to support data traffic using internetworking device such as switches, routers and other devices.
6. Functions to manage requests for file, print, web services, back-up and replication.
7. Functions to manage connections between the network and remote sites.
8. Functions that provide name and directory services
9. User management and support functions for logon and logoff, remote access; system management, administration and auditing tools with graphic interfaces

Network Operating System (NOS) is an operating system that includes special functions for connecting computers and devices into a local-area network (LAN) or Internetworking. You can use NOS to create local area networks (LANs) that function as either peer-to-peer networks or server-based networks, depending on the needs and budget.

1.7.2 Peer-to-Peer Network Operating Systems

Peer-to-peer network operating systems enable networked computers to function as both a server and a workstation. In a peer-to-peer network, the operating system is installed on every networked computer; this enables any networked computer to provide resources and services to all other networked computers. For example, each networked computer can allow other computers to access its files and use connected printers while it is in use as a workstation. Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers.

Peer-to-peer operating systems have advantages and disadvantages when compared to client-server operating systems. They provide many of the same resources and services as do client-server operating systems, and, under the right circumstances, can provide good performance. They are also easy to install and usually inexpensive.

However, peer-to-peer networks provide fewer services than client-server operating systems. The services they provide are less robust than those provided by mature, full-featured client-server operating systems. The performance of peer-to-peer networks commonly decreases significantly under a heavy load. Furthermore, maintenance is often more difficult: Because there is no method of centralized management, there are often many servers to manage (rather than one centralized server), and many people may have access to and the ability to change the configuration of different server computers.

Windows XP, Windows Me, Windows 2000 Professional, Windows 98, Windows 95, and Windows for Workgroups offer peer-to-peer networking features.

1.7.3 Client Server Network Operating System

The components of the client server network operating system include:

1. Client Software which is the network software installed on the client's machines. They provide the capabilities required for clients to access and use the network resources.
2. Server Software which is the network software that is installed on the servers. They provide the capabilities required for network operation.

1.7.3.1 Client Software

The network client software actually performs an operation that makes the computer think the network resource is just a local resource.

In a network environment when a user initiates a request to use a resource that exists on a server in another part of the network, the request has to be forwarded or redirected to the server that is managing the requested resource. The two component of the client software that does this task are:

Redirector may also be referred to as a requester. When a standalone computer accesses a file on the local hard drive or prints to a directly connected local printer, this request for service goes to the computer's processor. The processor then makes this request a reality and either opens the specified file or sends a print job to the printer. All this activity is managed locally. This process is handled by the redirector.



The redirector is a small section of code in the client NOS that:

- ▶ Intercepts requests in the computer.
- ▶ Determines if the requests should continue in the local computer's bus or be redirected over the network to another server.

If the redirector finds that the user wants to access a remote file on a server or print to a network printer, the request is forwarded to the network server. If the request is for the access of a local file (on the computer's hard drive), the redirector allows the request to proceed to the computer's processor so that the request can be processed locally. Figure 1.6 shows a diagram of how the redirector directs requests to either the local processor or the network server. The client computer is fooled by the redirector into thinking that all the resources it accesses (whether local or remote) are local.

Drive Designators may be associated with the shared network resources. They are used by the redirector to locate the network resource. For instance, if you want to access a particular shared directory on a remote computer you can assign a letter of the alphabet say E to it. You can then refer to the shared directory on the remote computer as E and the redirector will locate it. Designators make it unnecessary for users to worry about the actual location of data or peripherals. They can send requests to computers or peripherals.

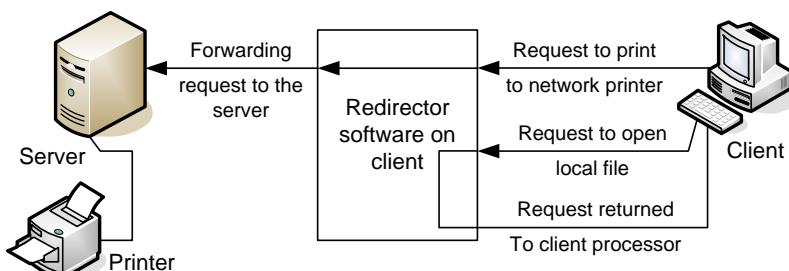


Figure 1.6: redirector directs requests to either the local processor or the network server



Client/server networking focuses primarily on the applications rather than the hardware. The same device may function as both client and server; for example, Web server hardware functions as both client and server when local browser sessions are run there. Likewise, a device that is a server at one moment can reverse roles and become a client to a different server (either for the same application or for a different application).

Client workstations can provide business functions using a mixture of personal productivity products in conjunction with a custom application. For example, a document created by a word processor can include input from a spreadsheet program and the invoice data created by the client/server application. The capability to cut and paste input from several different sources is one of the most powerful aspects of a client workstation. It provides the end user with tools to create new applications—without the need to go to professional programmers for assistance.

The client almost always provides presentation services. User input and final output, if any, are presented at the client workstation.

- **Request for Service:** Client workstations request services from the attached server. NOS software translates or adds the specifics required by the targeted requester to the application request. The most basic service provided by the NOS is *redirection*.
- **Remote Procedure Call (RPC):** Remote procedure calls (RPCs) standardize the way programmers must write calls, so that remote procedures can recognize and respond correctly.
- **Fax/Print Services:** The NOS enables the client to generate print requests even when the printer is busy. The client workstation can view the status of the print queues at any time.
- **Window Services:** The capabilities to activate, view, move, size, or hide a particular window is provided by the window services of the client operating system. These services interact with message services provided to notify the user of events that occur on a server.
- **Remote Boot Services:** Some applications operate well on workstations without any local disk storage; The client workstation must provide sufficient software burned into erasable programmable read-only memory (E-PROM) to start the initial program load (IPL)—that is, boot—process. E-PROM is included in all workstations to hold the Basic Input/Output System (BIOS) services.
- **Other Remote Services:** Software is provided by the NOS to run on the client workstation to initiate some remote applications like Backup services, Business functions such as downloading data from a host or checking a list of stock.
- **Utility Services:** Local functions such as copy, move, edit, compare, and help that execute on the client workstation.

- **Message Services:** Provide the buffering, scheduling, and arbitration services to support this function.
- **Network Services:** Set of services and APIs that create, send, receive, and format network messages. These services provide support for communications protocols, such as NetBIOS, IPX, TCP/IP, APPC, Ethernet, Token Ring, FDDI, and X.25.
- **Application Services:** Custom applications use APIs embedded in an RPC to invoke specialized services from a remote server.
- **Data base Services:** Data base requests are made using the SQL syntax. SQL is an industry standard language supported by many vendors.
- **Network Management Services-Alerts:** Most network interface cards (NICs) can alerts to signify detected errors and perhaps to signify messages sent and received. These alerts are generated by (NICs) and are valuable in remote LAN management to enable early detection of failures.
- **Dynamic Data Exchange (DDE):** DDE is a feature that enables users to pass data between applications from different vendors through support for common APIs.
- **Object Linking and Embedding (OLE):** This is an extension to DDE that enables objects to be created with the object components software *aware*, which automatically launches the appropriate software to manipulate the data. OLE focuses on data sharing between applications on a single desktop.
- **Common Object Request Broker Architecture (CORBA):** CORBA addresses cross-platform data transfer and the process of moving objects over networks. CORBA support enables Windows and UNIX clients to share objects.



The client is a computer system that makes use of shared network resources.

1.7.3.2 Server Software

The server software makes it possible for users on machines to share the server's data and peripherals including shared directories, printers, plotters and disks.

The server software not only allows the sharing of resources but also determines the degree of sharing. The degree of sharing includes:

1. Allowing different users different levels of access to the resources. For example a file server could give Read, Write or Read and Write permissions to different users.
2. Coordinating access to the resources to make sure that two users do not use the same resource at the same time.

The sever software is used to:

1. Create user privileges which indicates who will be using the various resources on the network
2. Validate user names and passwords at the time of logging on
3. Grant or deny user privileges on the network
4. Add and remove users.

Servers are designed for nearly every purpose imaginable, from simple email servers to more complicated application servers. Every application will have specific server requirements, and is typically designed to run on Windows NT/2000/2003, Novell Netware, or Linux. Many servers can run multiple applications to serve a variety of needs. The following is just a brief of the most common types of server applications . . .

➤ **File and Print Servers**

○ *File servers* store files created by application programs. In some configurations, the file servers might also hold the application programs themselves. A file server is a computer that has a hard disk drive large enough to share. File servers provide the ability to simultaneously access the same file.

○ *Print servers* accept print jobs sent by anyone across the network. The print-server software also reports the status of jobs waiting for printing and recognizes the priorities assigned to specific users.

➤ **Mail Servers:** Mail servers manage local (within your network) and global (Internet-wide) electronic messaging. The mail server you choose should support the Internet standards such as POP3, and SMTP.

➤ **Fax Servers:** Fax servers manage fax traffic in and out of the network, allowing multiple users to send and receive faxes without a fax machine.

➤ **Web Servers:** Web servers allow Internet users to attach to your server to view and maintain web pages. The two most popular web servers are Apache **and** Microsoft Internet Information Services (IIS).

➤ **Data base Servers or Data base Management Systems (DBMS):** Though not exactly a server, DBMS systems allow multiple users to access the same data base at the same time. While this functionality is typically built into data base software (ex. Microsoft Access allows concurrent connections to its dataBases), a larger data base or a data base with many users may need a dedicated DBMS to serve all the requests.

➤ **Application Servers:** Application servers have undergone many changes and have grown in both quantity and variety with the growth of the Internet. An application server acts as an intermediary to information. In many usages, the application server works with a Web server and is called a Web application server. The web application server receives requests from a web page then returns the information in a new web page based on the results and uniquely created.

➤ **Terminal Servers or Communication Server:** Generally, a terminal server refers to a piece of hardware that allows devices to be attached to the network without a need for network cards. PCs, "dumb" terminals supporting just a mouse and

monitor, or printers can all be attached via standard ports, and can then be managed by the network administrator.

- **Proxy Servers:** Proxy servers act as interne diaries between your network users and the wide world of the Internet. Proxy servers perform a number of functions:

1. Masks network users IP addresses
2. Strengthens security by only allowing certain requests to come through and by providing virus protection
3. Caches web page data for a given period to allow for more rapid access



The Server is a computer system that provides and manages shared network resources.

Windows NT Server, Windows 2002 Server, Windows 2003 Server, Linux and the Macintosh OS/X Server are good examples of Server NOS.

1.7.4 Hybrid Network Operating System

Some NOS producers build peer-to-peer networking into their operating systems from the ground up. The two systems essentially run on top of each other. Users can share files on their workstations in addition to the resources available to them on the network. The focus of the network however, remains on the fileserver and users are normally discouraged from using the peer-to-peer functionality available to them.

Windows NT networks are a perfect example of a hybrid network operating system.

1.8 Quick Review

- ❖ A network can be anything from a simple collection of computers at one location that have been tied together using a particular connectivity medium to a giant global network, such as the Internet, that uses a number of different connectivity medium, including microwave and satellite technology.
- ❖ The network is used to transmit data, voice, and even video between users on the network.
- ❖ Computer networks have experienced enormous growth over the past decade and are now positioned to provide a wide range of services—remote file access, digital libraries, videoconferencing—to hundreds of millions of users.
- ❖ The primary reasons for networking computers are to share information, to share hardware and software, and to centralize administration and support.
- ❖ Networks are classified into two principal groups based on how they share information: peer-to-peer networks and server-based networks.
- ❖ In a peer-to-peer network, all computers are equal. They can either share their resources or use resources on other computers.
- ❖ In a server-based network, one or more computers act as servers and provide the resources to the network. The other computers are the clients and use the resources provided by the server.

- ❖ Most networks in the world are hybrid networks that run clients, peers and servers together.
- ❖ Without a network operating system (NOS) of some kind, individual computers cannot share resources, and other users cannot make use of those resources.
- ❖ NOS can be part of a computer operating system or a separate application that runs on top of the computer operating system.
- ❖ Server software is the means by which NOS provides services to other computers on a network.
- ❖ Redirector is used to forward client requests to the network. Using redirectors, users can access peripheral devices as if the devices were attached directly to the client computer.
- ❖ Designators may be associated with the shared network resources. They are used by the redirector to locate the network resource.
- ❖ The first step in choosing a network operating system is to decide which network architecture—client/server or peer-to-peer—best meets your needs; this can often be accomplished by determining what level of security your network requires.

1.9 Self Test Questions

A- Answer the following questions

1. What is computer network?
2. What are the services provided by networks?
3. What are the advantages of using a computer network?
4. What is Network Operating System?
5. List types of networks.
6. Compare between peer-to-peer and server based networks.
7. What are the services provided by NOS?
8. What is client software?
9. What is server software?
10. What is redirector?
11. What is client/server system's primary function?
12. List the most common server types you know.
13. List the most common presentation services provided by client software.

B- Identify the choice that best completes the statement or answers the question.

1. Which of the following is a workstation that accesses software and data through the network on another computer?

a. client	c. server
b. host	d. mainframe
2. Which of the following has connections for one or more printers and a network interface card?

a. host	c. server
b. client	d. interface

3. Which of the following is a single computer that offers multiuser access?
 - a. workstation
 - b. client
 - c. server
 - d. peer
4. In which networking environments, certain computers take specialized roles and function mainly as servers, and ordinary users' machines tend to function mainly as clients?
 - a. LAN
 - b. internetwork
 - c. peer-to-peer
 - d. client/server
5. Computers that participate on a network run a ____ that determines what services that computer can offer or request.
 - a. NOS
 - b. WPAN
 - c. domain
 - d. controller
6. Client/server also called ____.
 - a. domain controlled
 - b. server-based
 - c. workgroup model
 - d. Web enabled
7. In which type of networks every user must also act as a network administrator, controlling access to the resources on their machines?
 - a. LAN
 - b. internetwork
 - c. peer-to-peer network
 - d. client/server network
8. Most ____ consist of collections of typical end-user PCs linked by a common network medium.
 - a. LANs
 - b. internetworks
 - c. peer-to-peer networks
 - d. client/server networks
9. Which type of servers supplies the server side of client/server applications, and often the data that goes along with them, to network clients?
 - a. Application
 - b. File
 - c. Web
 - d. Directory
10. Which type of servers manages fax traffic for a network?
 - a. RRAS
 - b. Fax
 - c. Communication
 - d. Domain
11. Which type of servers handles e-mail messages for network users; this function might involve simply acting as a clearinghouse for local exchange of messages.
 - a. Mail
 - b. Communication
 - c. RRAS
 - d. File
12. What is the most widely used Web server in the world?
 - a. Active Directory
 - b. eDirectory
 - c. Apache
 - d. IIS
13. Which Microsoft redirector is included in all Windows OSs, starting with Windows for Workgroups?
 - a. Network Neighborhood
 - b. Client for Microsoft Networks

- c. CIFS
 - d. File and Printer Sharing for Microsoft Networks
14. Which protocol is used by E-mail clients to download incoming messages from an e-mail server to their local desktops?
- a. SMTP
 - b. POP3
 - c. IMAP
 - d. X.400
15. What is the current standard protocol for sending Internet and other TCP/IP-based e-mail?
- a. SMTP
 - b. POP3
 - c. IMAP
 - d. X.400
16. What is the server that masks your network users IP addresses and caches web page data for a given period to allow for more rapid access?
- a. Web
 - b. Communication
 - c. Proxy
 - d. File
17. What is the server that allows devices to be attached to the network without a need for network cards?
- a. Mail
 - b. Communication
 - c. Proxy
 - d. Application
18. What is the set of services and APIs that create, send, receive, and format network messages, and provide support for communications protocols?
- a. Application Services
 - b. Message Services
 - c. Utility Services
 - d. Network Services
19. What is the server that provides the ability to simultaneously access the same file?
- a. Web
 - b. Communication
 - c. File
 - d. Application
20. Which of the following support enables Windows and UNIX clients to share objects?
- a. OLE
 - b. DDE
 - c. FDDI
 - d. CORBA
21. ____ is the Windows network component that is not required for client functionality.
- a. A redirector
 - b. A service
 - c. A protocol
 - d. A network interface adapter driver
22. ____ is the Windows component that enables an application to access a network resource in the same way as a local one.
- a. A redirector
 - b. A protocol
 - c. A client
 - d. A service
23. ____ is the name that given to a computer that can act as both a client and a server?
- a. A multitasking computer
 - b. A mainframe computer
 - c. A peer-to-peer computer
 - d. Apache
24. Which of the following statements is true?

- a. A peer-to-peer server is the best choice for a large corporate network.
 - b. Client/server networks are more robust than peer-to-peer networks.
 - c. Novell NetWare is an example of a peer-to-peer NOS.
 - d. Windows 98 SE does not support peer-to-peer networking
25. Choose an example of a client operating system
- a. Microsoft Windows XP®
 - b. Microsoft Windows NT
 - c. UNIX
 - d. A LAN computer

CHAPTER 2

NETWORK STANDARDS

2.1 About This Chapter

Networks wouldn't work today unless all the networking vendors followed the same set of plans, or standards. Networking standards define a set of rules that must be followed by anyone who creates networking products, including cables, hardware, and software. When you follow these standards, the products should work together. This chapter describes several of the most popular standards and explains some of the benefits of using standards for networking.

Designing a network to meet its requirements is no small task. To help deal with the complexity of networks, a general blueprints-usually called a *network architecture*-that guides the design and implementation of networks has developed. This chapter defines more carefully what we mean by network architecture by introducing the central ideas that are common to all network Layering and architectures.

This chapter also introduces two of the most widely referenced architectures-the OSI architecture and the Internet TCP/IP architecture. ATM is often used as a link-layer technology in the backbone of the Internet. This chapter includes a brief description of ATM architecture.

2.2 Learning Outcome

After reading this chapter, you should be able to

1. Explain the benefits of using standards
2. Explain the Layered structure of networking
3. Summarize the purpose of protocols and interfaces in networking
4. Explain the encapsulation process
5. Summarize the purpose of a networking model
6. Understand the most well-known networking models
7. List and correlate the layers of the TCP/IP Internet and OSI networking models.
8. Describe the 802 enhancements to the OSI reference model and the sublayers to the data-link layer of the OSI reference model.
9. Describe the primary function of each layer of the OSI and TCP/IP reference model.
10. Understand the similarities and differences between the OSI and TCP/IP reference model.
11. Understand the general structure of ATM model.

2.3 What Does Standard Mean?

Standards play an important role in networking. Without standards, manufacturers of networking products have no common ground on which to build their systems. Interconnecting products from various vendors would be difficult, if not impossible.

These days many vendors are hesitant to support new technology unless there is standardization base from which to work. Vendors want to know there will be some measure of interoperability for their hardware and software. Otherwise, releasing a product could be a marketing nightmare if it is not compatible with standards that are later embraced by the marketplace.

To guarantee reliable transmission of data, there must be an agreed method that governs how data is sent and received. For example, how does a sending computer indicate which computer it is sending data to? And, if the data will be passed through intervening devices, how are these devices understand how to handle the data so that it will get to the intended destination? And, what if the sending and receiving computers use different data formats and data exchange conventions—how will the data be translated to allow its exchange? These are only a few of the questions that must be answered before data can be reliably transmitted and received across a computer network.



The standards define physical and operational characteristics of personal computing equipment, networking and communication equipment, operating systems, and software.

A *standard* is an agreed-upon definition of a protocol. In the early days of computer networking, each computer manufacturer developed its own networking protocols. As a result, you weren't able to easily mix equipment from different manufacturers on a single network. Standards are industry-wide protocol definitions that are not tied to a particular manufacturer. With standard protocols, you can mix and match equipment from different vendors.

To address the issues surrounding standardization, several independent organizations have created standard design specifications for computer-networking products. When these standards are adhered to, communication is possible between hardware and software products produced by a variety of vendors.

There are several sources for standards. Vendors may provide standards and references. Also standards may be created by organizations devoted to setting them up. Among the most well known organizations involved in setting standards for networking are:

- **American National Standards Institute (ANSI):** ANSI is an organization of U.S. industry and business groups dedicated to the development of trade and communication standards.
- **Comité Consultatif Internationale de Télégraphie et Téléphonie (CCITT):** The CCITT, which is also known as the International Telegraph and Telephone Consultative Committee, was established as part of the United Nations International Telecommunications Union (ITU), and ITU remains its parent organization.

- **Electronics Industries Association (EIA)** It develops industry standards for the interface between data processing and communications equipment.**Institute of Electrical and Electronics Engineers (IEEE):** It is a U.S.-based society that publishes a variety of standards including those for data communications. A subgroup of the IEEE, the 802 committees began developing network specifications in 1980 to ensure low-cost interfaces.
- **International Organization for Standardization (ISO):** It is a Paris-based organization of member countries, each of which is represented by its leading standard-setting organization.
- **Internet Engineering Task Force (IETF):** The organization responsible for the protocols that drive the Internet.
- **World Wide Web Consortium (W3C):** An international organization that handles the development of standards for the World Wide Web.

2.4 Layered Network Architecture

2.4.1 Benefits of Using Layered Architecture

To reduce networks design complexity, most networks are organized as a series of layers or levels, each one built upon one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network and from one standard to another. However, in all networks, the purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

Layer N on one-machine carries on a conversation with layer N on another machine (see Figure 2.1). The rules and conventions used in this conversation are collectively known as the layer N protocol. Basically, a protocol is an agreement between the communicating parties on how communication is to proceed.



The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.

Between each pair of adjacent layers there is an interface. The interface defines which primitive operations and services the lower layer offers to the upper one. When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers. Doing so, in turn, requires that each layer perform a specific collection of well-understood functions.

A set of layers and protocols is called network architecture. A well-designed layered system must use the following principles.

- Layers should be created for every level of abstraction needed.
- Every layer should perform a very well defined function.

- There should be a minimum of information flow between the layers.

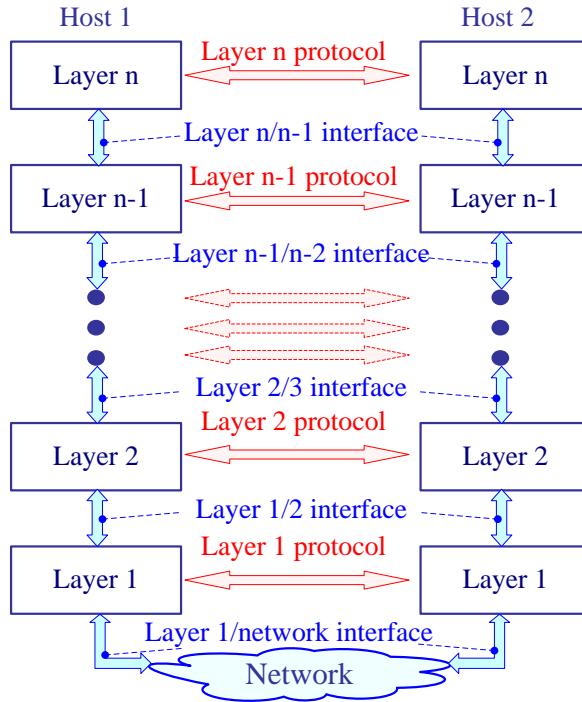


Figure 2.1: Layered model

2.4.2 Communication Protocols

The specification of architecture must contain enough information to allow implementers to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol. Neither the details of the implementation nor the specification of the interfaces are part of the architecture because these are hidden away inside the machines and not visible from the outside. It is not even necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols.

The reference model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols. In the context of data networking, a protocol is a formal set of rules and conventions that governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the reference model layers. A wide variety of communication protocols exist, but all tend to fall into one of the following groups: LAN protocols, WAN protocols, network protocols, and routing protocols. For Example LAN protocols operate at the physical and data-link layers of the OSI model and define communication over the various LAN medium. WAN protocols operate at the lowest three layers of the OSI model and define communication over the various wide-area medium. Routing protocols are network-layer protocols that are responsible for path determination and traffic switching.

 **Interfaces** describe how one layer communicates to another. **Protocols** refer to the communication between peer.

Finally, network protocols are the various upper-layer protocols that exist in a given protocol suite.

 A list of protocols used by a certain system, one protocol per layer, is called a **protocol stack**.

2.4.3 Communication between Systems

Information being transferred from a software application in one computer system to a software application in another must pass through each of the reference model layers. If, for example, a software application in System A has information to transmit to a software application in System B, the application program in System A will pass its information to the application layer (Layer n) of System A. The application layer then passes the information to the Layer n-1, which relays the data to the Layer n-2, and so on down to the physical layer (Layer 1). At the physical layer, the information is placed on the physical network medium and is sent across the medium to System B. The physical layer of System B removes the information from the physical medium, and then its physical layer passes the information up to the Layer 2, which passes it to the Layer 3, and so on until it reaches the application layer (Layer n) of System B. Finally, the application layer of System B passes the information to the recipient application program to complete the communication process.

A given layer in the architecture generally communicates with three other layers:

1. the layer directly above it
2. the layer directly below it
3. its peer layer in other networked computer systems.

The second layer in System A, for example, communicates with the third layer of System A, the first layer of System A, and the second link layer in System B.

One model layer communicates with another layer to make use of the services provided by this layer. The services provided by adjacent layers help a given layer communicate with its peer layer in other computer systems. Three basic elements are involved in layer services: the service user, the service provider, and the service access point (SAP)

 The service user is the layer that requests services from an adjacent layer. The service provider is the layer that provides services to service users. The SAP is a conceptual location at which one layer can request the services of another layer.

2.4.4 Information Exchange and Data Encapsulation

Layers in the model use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions that are exchanged between peer reference model layers.

Control information typically takes one of two forms: headers and trailers. As the name suggests, headers are usually attached to the front of a message. In some cases, however, this peer-to-peer control information is sent at the end of the message, in which case it is called a *trailer*.



Generally speaking, a header and trailer are small data structures—from a few bytes to a few dozen bytes—that are used among peers to communicate with each other.

The exact format for the header attached by layer (n) protocol is defined by its protocol specification. The rest of the message—that is, the data being transmitted on behalf of the application—is called the message’s *body* or *payload*. We say that the application’s data is *encapsulated* in the new message created by layer (n) protocol



Headers, trailers, and data are relative concepts, depending on the layer that analyzes the information unit. In other words, the data portion of an information unit at a given layer potentially can contain headers, trailers, and data from all the higher layers.

The information exchange process occurs between peer layers. Each layer in the source system adds control information to data and each layer in the destination system analyzes and removes the control information from that data.

Every machine that can be connected to a network goes through similar process in transferring that data out on the wire. The information must be placed in a format suitable for the application that will receive it on the other side. Once this is done, the machine goes through the process of encoding the data into a network-ready format. This is done by breaking the data up into small units called data units. The data units not only contain raw data (just a few bytes in each data units), but it contains other important information such as where the data will go, type of data unit and how to detect and correct errors.

When one of the application programs sends a message to its peer, it passes the message to layer (n) protocol. Layer (n) protocol does not care that these bytes represent an array of integers, an email message, a digital image, or whatever; it is simply charged with sending them to its peer. However, layer (n) protocol must communicate control information to its peer, instructing it how to handle the message when it is received. Layer (n) protocol does this by attaching a *header* to the message.

This process of encapsulation is then repeated at each level of the protocol graph; for example, layer (n-1) encapsulates layer (n)’s message by attaching a header of its own. If

we now assume that layer (n-1) sends the message to its peer over some network, then when the message arrives at the destination host, it is processed in the opposite order: layer (n-1) first strips its header off the front of the message, interprets it (i.e., takes whatever action is appropriate given the contents of the header), and passes the body of the message up to layer (n) protocol, which removes the header that its peer attached, takes whatever action is indicated by that header, and passes the body of the message up to the application program. The message passed up from layer (n) protocol to the application on host 2 is exactly the same message as the application passed down to layer (n) protocol on host 1; the application does not see any of the headers that have been attached to it to implement the lower-level communication services. This whole process is illustrated in Figure 2.2.

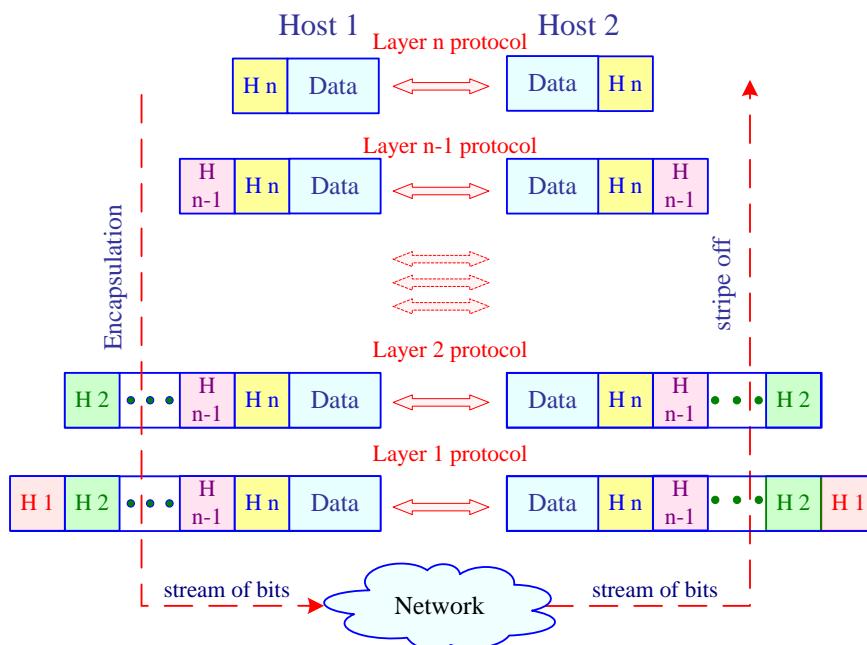


Figure 2.2: A packet moving from layer n down to layer 1



Encapsulation is the adding of layer specific header and sometimes trailer information to each data packet at the sending end. At the receiving end when data is coming in packets are "stripped off" and the data is passed up to the next layer.

The complex process of network activity involves sending data from one computer to another can be broken into discrete, sequential tasks. The sending computer must:

1. Recognize the data.
2. Divide the data into manageable chunks.
3. Add information to each chunk of data to determine the location of the data and to identify the receiver.

4. Add timing and error-checking information.
5. Put the data on the network and send it on its way.



Sometimes the low-level protocol applies some simple transformation to the data it is given, such as to compress or encrypt it. In this case, the protocol is transforming the entire.

2.5 Reference Models

2.5.1 Benefits of Modularity

Modularity brings many benefits, including the all-powerful benefit of not having to understand all parts of a problem at the same time in order to solve it. Modularity thus plays a role in presenting ideas in a book, as well as in writing code. If a book's material is organized effectively-modularly-the reader can start at the beginning and actually make it to the end.

A *network model* reflects a design or architecture to accomplish communication between different systems. Network models are also referred to as network *stacks* or *protocol suites*.

A network model usually consists of *layers*. Each layer of a model represents specific functionality. Within the layers of a model, there are usually *protocols* specified to implement specific tasks. You may think of a protocol as a set of rules or a language. Thus, a layer is normally a collection of protocols.

There are a number of different network models. Some of these models relate to a specific implementation, such as the TCP/IP network model. Others simply describe the process of networking, such as the International Organization for Standardization/Open System Interconnection Reference Model (ISO/ OSI, or more simply, OSI).

The models, discussed below reflect a layered approach to modularity, is almost universally used as a starting point for discussions of protocol organization, whether the design in question conforms to the model or deviates from it. We will introduce you to the most popular reference models, they are:

- Seven-layer OSI protocol model
- TCP/IP model
- Equal-size packet protocol model

2.5.2 Open Systems Interconnection (OSI)

Perhaps no other standard has affected networking more than the OSI model. Presented by the ISO in the late 1970s, this model was to serve as a framework for worldwide communications. It has been adhered to in one respect or another by all network vendors. However, few have based their own implementation completely on the model with its seven layers of functions. Most believe that having individual functions broken into so many layers is impractical for their protocols (packet types) because of the overhead each layer adds. This will become clearer to us as we examine the functions of each layer and what is involved in using those functions.

2.5.2.1 OSI Layers

As the data is being prepped for transfer, it is in effect, passing down through the layers of the OSI model. The highest layer is the application; the lowest is the cable or other physical medium. While passing through these layers, other information may be tacked on to the packet in order to ensure the data is delivered correctly. Once the recipient machine receives the information, the data passes up through the layers where information that has been tacked on at the sender is peeled off. Last on the layer list is the application running on the receiver device. It gets the raw data originally sent by the source machine. Figure 2.2 illustrates this concept.



The OSI reference model architecture divides network protocols into seven layers: the application, presentation, session, transport, network, data-link, and physical layers.

The lower layers 1, 2, and 3 are network dependent. These layers are highly involved with the exact network protocol with which the system is directly interfacing. Layers 5 through 7 are application oriented, while layer 4 is a transition layer between the network and the application.

Another important feature of the OSI reference model is the concept of layers that are **point-to-point** versus **peer-to-peer** as shown in Figure 2.3. Functions in point-to-point layers are performed at each and every location between the source and destination as well as being performed at the source and destination. Since there may be thousands of nodes between the source and destination, point-to-point functions may be performed thousands of times while a message is traveling from its source to its destination. All functions defined in layer 1 through 3 are point-to-point. Functions in peer –to-peer layers (layer 4 through 7) are only performed at the source and destination.

2.5.2.1.1 Layer 1: Physical Layer

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission

distances, and physical connectors. Physical-layer implementations can be categorized as either LAN or WAN specifications.



Physical Layer: Binary transmission signals and encoding. Layout of pins, voltages, cable specifications, modulation.

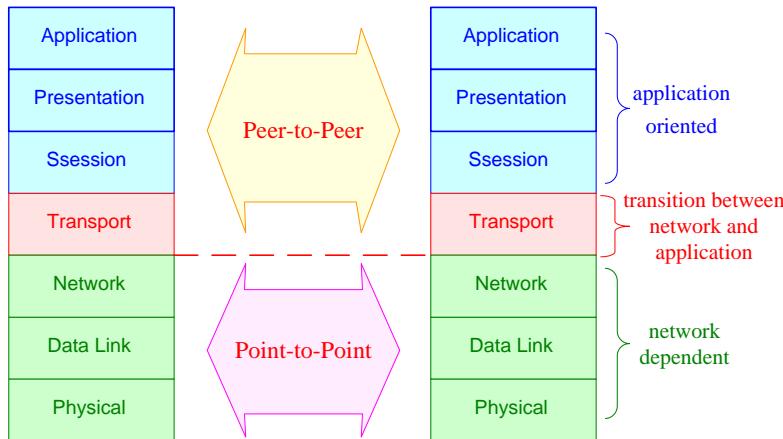


Figure 2.3: OSI Upper and Lower Layers

2.5.2.1.2 Layer 2: Data-Link Layer

The data link layer provides reliable transit of data across a physical network link. Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer. Network topology consists of the data-link layer specifications that often define how devices are to be physically connected, such as in a bus or a ring topology. Error notification alerts upper-layer protocols that a transmission error has occurred, and the sequencing of data frames reorders frames that are transmitted out of sequence. Finally, flow control moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the data-link layer into two sub-layers: Logical Link Control (LLC) and Medium Access Control (MAC).



Data Link Layer: Responsible for the framing of data packets and the movement of the data across the physical link.

2.5.2.1.3 Layer 3: Network Layer

The network layer provides routing and related functions that enable multiple data links to be combined into an internetwork. This is accomplished by the logical addressing (as opposed to the physical addressing) of devices. The network layer supports both connection-oriented and connectionless service from higher-layer protocols. Network-layer protocols typically are routing protocols, but other types of protocols are implemented at the network layer as well. Some common routing protocols include Border Gateway Protocol (BGP), an Internet interdomain routing protocol; Open Shortest Path First (OSPF), a link-state, interior gateway protocol developed for use in TCP/IP networks; and Routing Information Protocol (RIP), an Internet routing protocol that uses hop count as its metric.



Network Layer: Provides the logical addressing system used to route data on the network and reporting delivery errors.

2.5.2.1.4 Layer 4: Transport Layer

The transport layer implements reliable internetwork data transport services that are transparent to upper. Transport-layer functions typically include flow control, multiplexing, virtual circuit management, and error checking and recovery.

Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables data from several applications to be transmitted onto a single physical link. Virtual circuits are established, maintained, and terminated by the transport layer. Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves taking an action, such as requesting that data be retransmitted, to resolve any errors that occur.

Some transport-layer implementations include Transmission Control Protocol Name Binding Protocol, and OSI transport protocols. Transmission Control Protocol (TCP) is the protocol in the TCP/IP suite that provides reliable transmission of data. Name Binding Protocol (NBP) is the protocol that associates AppleTalk names with addresses. OSI transport protocols are a series of transport protocols in the OSI protocol suite.



Transport Layer: Responsible for segmentation/desegmentation of data, end-to-end data transmission, flow control, error checking, and recovery.

2.5.2.1.5 Layer 5: Session Layer

The session layer establishes, manages, and terminates communication sessions between presentation layer entities. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session

layer. Some examples of session-layer implementations include Zone Information Protocol (ZIP), the AppleTalk protocol that coordinates the name binding process; and Session Control Protocol (SCP), DECnet Phase IV session-layer protocol.



Session Layer: Establishes, manages and terminates connection between applications of sending and receiving nodes.

2.5.2.1.6 Layer 6: Presentation Layer

The presentation layer provides a variety of coding and conversion functions that are applied to application layer data. These functions ensure that information sent from the application layer of one system will be readable by the application layer of another system. Some examples of presentation-layer coding and conversion schemes include common data representation formats, conversion of character representation formats, common data compression schemes, and common data encryption schemes.

Common data representation formats, or the use of standard image, sound, and video formats, enable the interchange of application data between different types of computer systems. Conversion schemes are used to exchange information with systems by using different text and data representations, such as EBCDIC and ASCII. Standard data compression schemes enable data that is compressed at the source device to be properly decompressed at the destination. Standard data encryption schemes enable data encrypted at the source device to be properly deciphered at the destination.

Presentation-layer implementations are not typically associated with a particular protocol stack. Some well-known standards for video include QuickTime and Motion (MPEG). QuickTime is an Apple Computer specification for video and audio, and MPEG is a standard for video compression and coding.

Among the well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF). GIF is a standard for compressing and coding graphic images. JPEG is another compression and coding standard for graphic images, and TIFF is a standard coding format for graphic images.



Presentation Layer: Serves as the translator layer of the OSI model and is responsible for data conversion encryption, encoding, and formatting.

2.5.2.1.7 Layer 7: Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.

This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist.

In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer.

Two key types of application-layer implementations are TCP/IP applications and OSI applications. TCP/IP applications are protocols, such as Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP) that exist in the Internet Protocol suite. OSI applications are protocols, such as File Transfer, Access, and Management (FTAM), Virtual Terminal Protocol (VTP), and Common Management Information Protocol (CMIP) that exist in the OSI suite.



Application Layer: Provides the interface and services that support user applications such as file, print, messaging, and data base services and provides general access to the network.

2.5.2.2 IEEE Specifications

The Institute of Electrical and Electronic Engineers (IEEE) has done notable work in the standards area of networking. This organization is huge with over 300,000 members made up of engineers, technicians, scientists, and students in related areas. The Computer Society of IEEE alone has over 100,000 members. IEEE is credited with having provided definitive standards in local area networking. These standards fall under a group of standards known as the 802 Project executed by the Computer Society's 802 subcommittee.

The 802 standards were the culmination of work performed by the subcommittee starting in 1980. The first published work was 802.1, which specified a framework for LANs and internetworking. This was followed in 1985 with specific LAN-oriented standards titled 802.2- 802.5. Since that time there have been other references set up as well.

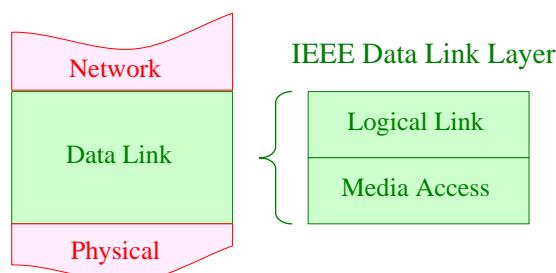


Figure 2.4: IEEE Data link Layer

Specification	Description
802.1	Sets Internetworking standards related to network management.
802.2	Defines the general standard for the data-link layer. The IEEE divides this layer into two sublayers: the LLC and MAC layers. The MAC layer varies with different network types and is defined by standard IEEE 802.3.
802.3	Defines the MAC layer for bus networks that use Carrier-Sense Multiple Access with Collision Detection (CSMA/CD). This is the Ethernet Standard.
802.4	Defines the MAC layer for bus networks that use a token-passing mechanism (Token Bus LAN).
802.5	Defines the MAC layer for token ring networks (Token Ring LAN).
802.6	Sets standards for metropolitan area networks (MANs), which are data networks designed for towns or cities. In terms of geographic breadth, MANs are larger than LANs, but smaller than WANs. MANs are usually characterized by very-high-speed connections using fiber-optic cables or other digital medium.
802.7	Used by the Broadband Technical Advisory Group.
802.8	Used by the Fiber-Optic Technical Advisory Group.
802.9	Defines integrated voice/data networks.
802.10	Defines network security.
802.11	Defines wireless network standards.
802.12	Defines Demand Priority Access LAN, 100BaseVG-AnyLAN.
802.13	Unused.
802.14	Defines cable modem standards.
802.15	Defines wireless personal area networks (WPAN).
802.16	Defines broadband wireless standards.

Table 2.1: 802 Specification Categories

Most of the work performed by the (802) Project committee revolves around the first two layers of the OSI model initiated by the ISO. These layers involve the physical medium on which we move data (cable type) and the way that we interact with it. It addresses such crucial issues of how data is placed on the network and how we insure its accuracy and flow. For a better definition of these functions, the IEEE split the Data Link layer of the OSI model up into two separate components as illustrated in Figure 2.4. The 802 Specification Categories are listed in the table 2.1.



- The 802 specifications set standards for:
 - ▶ Network interface cards (NICs).
 - ▶ Wide area network (WAN) components.
 - ▶ Components used to create twisted-pair and coaxial cable networks.

2.5.3 The TCP/IP Model

2.5.3.1 TCP/IP Layers

TCP/IP has become the standard protocol used for interoperability among many different types of computers. This interoperability is a primary advantage of TCP/IP. Most networks support TCP/IP as a protocol. TCP/IP also supports routing and is commonly used as an internetworking protocol, that's why TCP/IP reference model is the network model used in the current Internet architecture. It has its origins back in the 1960's with the grandfather of the Internet, the ARPANET. This was a research network sponsored by the Department of Defense in the United States.

The TCP/IP model does not exactly match the OSI model. There is no universal agreement regarding how to describe TCP/IP with a layered model but it is generally agreed that there are fewer levels than the seven layers of the OSI model. Most descriptions present from three to five layers. In this book we will consider TCP/IP protocols map to a four-layer conceptual model. Each layer in this model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) model as shown in Figure 2.5.

2.5.3.1.1 Layer 1: Network Access Layer

In TCP/IP the Data Link Layer and Physical Layer are normally grouped together to make the Network Access layer (also called the *Network Interface layer*). This layer is responsible for placing TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP was designed to be independent of the network access method, frame format, and medium. In this way, TCP/IP can be used to connect differing network types including LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay. Independence from any specific network technology gives TCP/IP the ability to be adapted to new technologies such as Asynchronous Transfer Mode (ATM).

2.5.3.1.2 Layer 2: Internet Layer

The *Internet layer* is responsible for addressing, packaging, and routing functions. The Internet Protocol (IP) is normally described as the TCP/IP Network Layer. Because of the Inter-Networking emphasis of TCP/IP this is commonly referred to as the Internet Layer. All upper and lower layer communications travel through IP as they are passed through the TCP/IP protocol stack.

The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- *Internet Protocol (IP)*
- *Address Resolution Protocol (ARP)*
- *Internet Control Message Protocol (ICMP)*
- *Internet Group Management Protocol (IGMP)*

2.5.3.1.3 Layer 3: Transport Layer

The *Transport layer* (also known as the Host-to-Host Transport layer) is responsible for providing the Application layer with session and datagram communication services. In TCP/IP there are two Transport Layer protocols. The Transmission Control Protocol (TCP) guarantees that information is received as it was sent. The User Datagram Protocol (UDP) performs no end-to-end reliability checks.

2.5.3.1.4 Layer 4: Application Layer

In TCP/IP the Application Layer also includes the OSI Presentation Layer and Session Layer. In this document an application is any process that occurs above the Transport Layer. This includes all of the processes that involve user interaction. The application determines the presentation of the data and controls the session. In TCP/IP the terms **socket** and **port** are used to describe the path over which applications communicate.

There are many Application layer protocols and new protocols are always being developed. The most widely-known Application layer protocols are those used for the exchange of user information:

- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Simple Mail Transfer Protocol (SMTP)
- Telnet, a terminal emulation protocol
- Additionally, the following Application layer protocols help facilitate the use and management of TCP/IP networks:
- Domain Name System (DNS)
- Simple Network Management Protocol (SNMP)

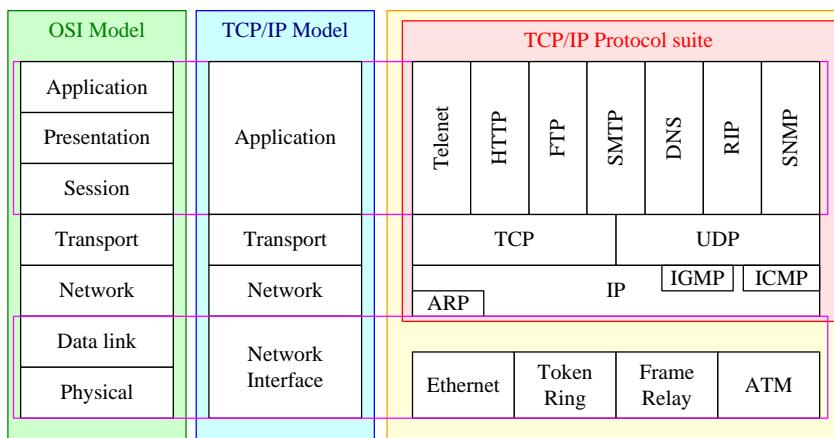


Figure 2.5: TCP/IP Protocol Architecture

2.5.4 Comparison of OSI and TCP/IP Models

As it can be seen from the previous pages there are a number of comparisons which can be drawn between the two models. This section will therefore be focusing on highlighting the similarities and differences between the OSI and TCP/IP models.

2.5.4.1 Similarities

The main similarities between the two models include:

- Both of the OSI & TCP/IP models share a similar architecture (They are both constructed with layers).
- Both models share a common "application layer". However in practice this layer includes different services depending on the model.
- Both models have comparable transport and network layers: whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.

2.5.4.1 Differences

The main differences between the two models are as follows:

- The OSI model consists of 7 architectural layers whereas the TCP/IP has only 4 layers.
- TCP/IP Protocols are considered to be standards around which the internet has developed. The OSI model however is a "**generic, protocol-independent standard.**" it is merely used as a guidance tool.
- TCP/IP combines the presentation and session layer issues into its application layer.
- TCP/IP combines the OSI data link and physical layers into the network access layer.
- TCP/IP appears to be a simpler model. This is mainly due to the fact that it has fewer layers.



- The network interface layer of TCP/IP maps to the physical and data-link layers of OSI.
- The Internet layer of TCP/IP maps to the network layer of OSI.
- The transport layer of TCP/IP maps to the transport layer of OSI.
- The application layer of TCP/IP maps to the session, presentation, and application layers of OSI.

2.5.5 Equal-Size Packet Protocol Model

The ATM protocol structure is shown in Figure 2.6. The three-dimensional model includes four layers in the vertical dimension.

2.5.5.1 Physical Layer

The physical layer includes two sublayers:

- physical medium sublayer defines the physical and electrical/optical interfaces with the transmission medium on both the transmitter and the receiver. This layer also provides timing information and line coding.
- transmission convergence sublayer provides frame adaptation and frame generation/recovery.

2.5.5.2 ATM Layer

ATM Layer is the core of the ATM standard. It defines the structure of the ATM cell and provides services which include:

- cell multiplexing and demultiplexing
- generic flow control
- header cell check generation and extraction
- remapping of virtual circuits and paths

2.5.5.3 ATM Adaptation Layer (AAL)

This layer is analogous to the transport layer in the Internet protocol stack.

- maps higher-layer service data units, which are fragmented into fixed-size cells to be delivered over the ATM interface
- collects and reassembles ATM cells into service data units for transporting to higher layers.

ATM includes many different types of AALs to support many different types of services.

2.5.5.4 Higher Layers

The higher layers incorporate some of the functionality of layers 3 through 5 of the TCP/IP model. The control plane at the top of the cube shown in involves all kinds of network signaling and control.

2.5.5.5 User Plane

The user plane involves the transfer of user information, such as the flow-control and error-control mechanisms.

2.5.5.6 Management Plane

The management plane provides management function and an information-exchange function between the user plane and the control plane. The management plane includes

1. plane management that performs management and coordination functions related to a system as a whole
2. the layer management that monitors bit error rates on a physical communications medium.

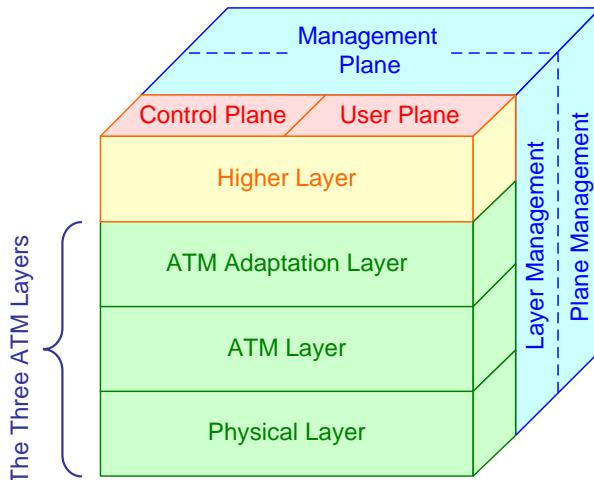


Figure 2.6: ATM protocol reference model

 ATM is often used as a link-layer technology in the backbone of the Internet as ATM switches can switch packets (cells) at very high rates, where the need to transport traffic at high rates is most acute.

2.6 Different Forms of Data Units

The data and control information that is transmitted through internetworks takes a wide variety of forms. The terms used to refer to these information formats are not used consistently in the internetworking industry but sometimes are used interchangeably.

Common information formats include frame, packet, datagram, segment, message, cell, and data unit. These terms are defined below:

- A **frame** is an information unit whose source and destination are data link layer entities. A frame is composed of the data-link layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the data-link layer entity in the destination system. Data from upper-layer entities is encapsulated in the data-link layer header and trailer.
- A **packet** is an information unit whose source and destination are network-layer entities. A packet is composed of the network-layer header (and possibly a trailer) and upper-layer data. The header and trailer contain control information intended for the network-layer entity in the destination system. Data from upper-layer entities is encapsulated in the network-layer header and trailer.
- The term **datagram** usually refers to an information unit whose source and destination are network-layer entities that use connectionless network service.
- **Segment** usually refers to an information unit whose source and destination are transport-layer entities.

- **Message** is an information unit whose source and destination entities exist above the network layer (often the application layer).
- A **cell** is an information unit of a fixed size whose source and destination are data-link layer entities. Cells are used in switched environments, such as Asynchronous Transfer Mode (ATM) and Switched Multimegabit Data Service (SMDS) networks. A cell is composed of the header and payload. The header contains control information intended for the destination data-link layer entity and is typically 5 bytes long. The payload contains upper-layer data that is encapsulated in the cell header and is typically 48 bytes long. The length of the header and the payload fields always are exactly the same for each cell.

Data unit is a generic term that refers to a variety of information units. Some common data units are service data units (SDUs), protocol data units, and bridge protocol data units (BPDUs). SDUs are information units from upper-layer protocols that define a service request to a lower-layer protocol. PDU is OSI terminology for a packet. BPDUs are used by the spanning-tree algorithm as hello messages.

2.7 Quick Review

- ❖ Standards play an important role for interconnecting products from various vendors. They may be created by organizations devoted to setting them up.
- ❖ Layering is used to reduce networks design complexity. The purpose of each layer is to offer certain services to the higher layers Layer N on one-machine carries on a conversation with layer N on another machine.
- ❖ The interface defines which primitive operations and services the lower layer offers to the upper one and describe how one layer communicates to another
- ❖ A set of layers, interfaces and protocols is called network architecture.
- ❖ Encapsulation is the adding of layer specific header and some times trailer information to each data packet at the sending end. At the receiving end when data is coming in packets are decapsulated and the data is passed up to the next layer.
- ❖ The reference model of network architecture provides a conceptual framework for communication between computers, but the model itself is not a method of communication.
- ❖ Actual communication is made possible by using communication protocols; which is a formal set of rules and conventions that governs how computers exchange information over a network medium.
- ❖ The OSI reference model architecture divides network protocols into seven layers: the application, presentation, session, transport, network, data-link, and physical layers.
- ❖ IEEE 802 standards define the specifications for NICs, networking components, and medium for the data-link and physical layers of the OSI reference model.
- ❖ The IEEE 802 standards divide the data-link layer into two subgroups: Logical Link Control (LLC) and Medium Access Control (MAC).
- ❖ Protocols in a networking environment define the rules and procedures for transmitting data.

- ❖ To send data over a network successfully requires a series of separate steps that must be carried out in a prescribed order.
- ❖ Internet network protocols TCP/IP layered architecture model provides a communication service for peers running on different machines and in a heterogeneous environment.
- ❖ The four layers of TCP/IP are the network-interface layer, Internet layer, transport layer, and application layer.
- ❖ The network interface layer of TCP/IP maps to the physical and data-link layers of OSI. The Internet layer of TCP/IP maps to the network layer of OSI. The transport layer of TCP/IP maps to the transport layer of OSI. The application layer of TCP/IP maps to the session, presentation, and application layers of OSI.
- ❖ The ATM equal-size packet protocol structure is a three-dimensional model includes four layers in the vertical dimension: physical, ATM, adaptation and higher layers
- ❖ The control plane at the top of the cube involves all kinds of network signaling and control.
- ❖ The user plane involves the transfer of user information.
- ❖ The management plane provides management function and an information-exchange function between the user plane and the control plane.
- ❖ Common information formats that the data and control information is transmitted through internetworks include: frame, packet, datagram, segment, message, cell, and data unit.

2.8 Self Test Questions

A- Answer the following questions

1. What is the role of standard?
2. What are the three general parts of data unit?
3. What is the purpose of the data field?
4. How is the header defined?
5. Is there always a data field in a message?
6. Are trailers common?
7. What are the devices that the physical link connects?
8. Which layers govern LAN transmission?
9. Which layers govern WAN transmission?
10. Distinguish between what the internet and transport layer standards govern.
11. What do application layer standards govern?
12. Why do standards architectures break down the standards development process into layers?
13. At what layer will you find HTTP, FTP, SMTP, and POP?
14. When a layer creates a message, what does it usually do immediately afterward?
15. What does the layer below it usually do after receiving the next-higher-layer message?
16. What is encapsulation?
17. What is a protocol?
18. Are all standards protocols? Explain.

19. What are the two dominant network standards architectures?
 20. Do LAN standards come from OSI or TCP/IP?
 21. Do WAN standards come from OSI or TCP/IP?
 22. What is the benefit of reliable protocols?
 23. Which layers govern transmission in LANs and WANs?
 24. Which layers govern internetworking?
 25. At Which layer are messages called frames?
 26. At Which layer are they called packets?
 27. If a source host and a destination host are separated by 23 networks, how many packets will there be?
 28. Which device encapsulates—the sending or the receiving device?
 29. How are OSI and TCP/IP complementary?
 30. Compare the dominance of OSI at the physical and data link layers with the dominance of TCP/IP at higher layers.
 31. What are the functions of each layer in ATM reference model?
 32. What are the functions of each plane in ATM reference model?

B- Identify the choice that best completes the statement or answers the question.

8. Which layer tells the receiving computer where a transmission begins and ends?
a. Session
b. Data Link
c. Network
d. Transport

9. Which layer provides the encryption services when data encryption is used in network communications?
a. Presentation
b. Session
c. Network
d. Transport

10. How many layers is the OSI model comprised of?
a. 4
b. 3
c. 8
d. 7

11. Layer 3 of OSI model layer is commonly referred to as ____.
a. Data Link
b. Session
c. Internetwork
d. Network

12. Which of the following is a defined method for communicating between systems?
a. protocol data unit
b. datagram
c. protocol
d. language

13. TCP/IP protocols span the Network layer and the _____ layer of the OSI reference model.
a. Physical
b. Data Link
c. Network
d. Transport

14. Which TCP/IP layer defines the functionality of the upper layers, including support for data formatting, conversion, and encryption?
a. Internetwork
b. Transport
c. Application
d. Network Interface

15. The Network Interface layer of the TCP/IP model maps to both the _____ layers of the OSI reference model.
a. Data Link and Physical
b. Network and Data Link
c. Transport Network and
d. Session and Transport

16. Which layer in the TCP/IP model handles software, or logical, addressing?
a. Internetwork
b. Application
c. Transport
d. Network Interface

17. Which IEEE standard covers the Logical Link Control.
a. 802.2
b. 802.3
c. 802.4
d. 802.5

18. The OSI model consists of _____ distinct layers stacked on one another.
a. eight
b. three
c. five
d. seven

19. Which layer in a LAN that its task is to organize bits so that they are formatted into frames?
a. Network
b. Transport
c. Data Link
d. Physical

32. TCP is an example of ____.
- The data-link layer protocol
 - The presentation layer protocol
 - The Transport layer protocol
 - The Network layer protocol
33. ____ is the name of the process of building a frame around network layer information.
- Data buffering
 - Signal encoding
 - Data encapsulation
 - Data framing
34. ATM is ____.
- a cell-based data transmission protocol
 - an opto-electronic component
 - a circuit-switched access systems
 - non of them
35. ____ layer of the OSI model is divided into two sublayers.
- Session
 - Application
 - Data Link
 - Physical
36. Each layer communicates from one computer to another with ____ logically.
- the same layer
 - the layer below
 - the layer above
 - any higher layer
37. ____ layer of the OSI Model is responsible for accepting data from the Session layer and managing end-to-end delivery of data.
- Data Link
 - Session
 - Transport
 - Network
38. The Internet Protocol (IP) belongs to the ____ layer.
- Network
 - Transport
 - Data Link
 - Application
39. ____ are the PDU that are used at the physical layer.
- Packets
 - Bits
 - Frames
 - Segments
40. The ____ provides an information-exchange function between the user plane and the control plane.
- management plane
 - control plane
 - ATM layer
 - physical layer

CHAPTER 3

NETWORK CLASSIFICATION

3.1 About This Chapter

Computer networks can be classified based on several factors, for example bandwidth, common applications, common hardware. The most known classification is based on the physical size of the network.

In this chapter you will learn how to classify networks according to their size, topology, and applications in particular local area networks (LAN's), metropolitan area networks (MAN's), and wide area networks (WAN's). We will describe the standard topologies and their variations, advantages and disadvantages.

Internetworking is based on connecting and switching technologies. So we will provide you a detailed description of these technologies.

Finally this chapter provides a general description of the Internet, Intranet and Extranet and the differences and similarities between them.

3.2 Learning Outcome

At the end of this chapter, you should be able to:

1. Describe a local area network (LAN) metropolitan area network (MAN) a wide area network (WAN) and identify the primary difference between a LAN and a WAN.
2. Describe the standard topologies their variations and identify the advantages and disadvantages of each topology.
3. Determine an appropriate topology for a given network plan.
4. Classify the wide area network (WAN)
5. Describe how packet switching works.
6. Generally explain the concept of the internetworking
7. Generally explain the concept of switching technologies
8. Describe the Internet, Intranet an Extranet and identify the primary difference between them.

3.3 General Network Classification Methods

Computer networks have become an integral and indispensable part of scientific as well as public life today. Over the last couple of decades data networks have changed their character from a slow speed point to point connection to a high speed data communication backbone supporting full multimedia information transfer. The last few years have seen a phenomenal rise in the interest in the collection of computers and networks known as the **Internet, intranet and extranet**.

Networks span the entire globe and belong to many different nations and network operators. Such networks can be classified in many ways depending on the geographical

coverage, the network topology, the ownership, the switching mechanism, the transmission speed, etc.

The different types of computer networks are working with different speeds. In general, networks with smaller geographic expansion run at a faster speed: WANs often slower than 1 Mbps, LANs at about 10 Mbps, and High-speed LANs up to 100 Mbps. New technologies like ATM promise speeds up to two Gbps and more for all kinds of networks. Remember that not all of this performance can be used to transmit the true data, because considerable parts of the data are headers with control information.

Figure 3.1 displaying the speed-requirements of different applications shows, why permanently higher speeds are necessary.

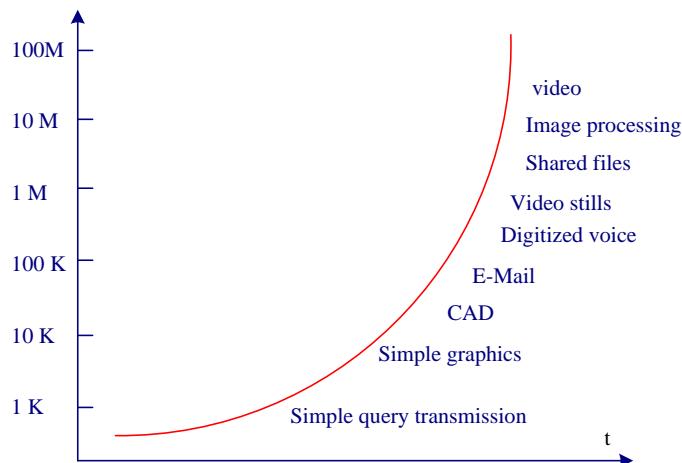


Figure 3.1: Speed-requirements of different applications

3.4 Networks Classification by Geographical Coverage

Networks can be classified into 3 categories depending on their geographical coverage (from the smallest to the largest) as follows:

1. Local Area Networks (LANs)
2. Metropolitan Area Networks (MANs)
3. Wide Area Networks (WANs).

Table 2.1 shows the distance between two communication points connected on the different types of networks.

Distance	Type
10 m - 2 km	Local Area network
2 km - 100 km	Metropolitan Area network
100 km - 1000 km	Wide Area Network
10000 km and up	Internet

Table 2.1: The distance between two communication points according to geographical coverage.

3.5 Local Area Network (LAN)

A LAN is a data communication network, which connects many computers or workstations (computers terminal, printer etc.) and permits exchange of data and information among them, within a localized area, typically confined to a building, or a cluster of buildings.

LAN applications include communications between the workstation and host computers, other workstations, and servers. The servers may serve to provide the workstation with access to text files, image files, applications, printers, or communications software for access to the WAN.

The shared medium for LANs includes most known transmission medium. Although coaxial cable was the original medium and still is used widely in various configurations, twisted-pair has recently become the medium of choice in many environments. Optical fiber cable is used widely as a backbone technology, although it seldom is deployed to the desktop. Wireless (microwave, Bluetooth and infrared) LANs generally are limited to special radio technologies. Satellite rarely is used in any way, as propagation delay renders it generally unsatisfactory for interactive communications.

LANs are not rigidly defined but tend to share most of all of the following characteristics:

- All the connected devices in the network share the transmission media.
- Each device connected in the network can either operate standalone or in the network.
- Area covered is small.
- Data transfer rates are high.
- Each device connected in the network can communicate with any other device in network.
- The setting up cost of the network is usually low.

Limitations:

1. Higher administrative costs
2. Higher installation costs
3. Difficult troubleshooting.
4. Higher security risks.

Advantages:

1. Sharing Resources
2. GroupWare and communication applications
3. Centralized administration
4. Centralized policy (support, licensing, etc.)

3.5.1 LAN Topologies

Networks extend over physical areas, just as rivers and mountains do. When data communication experts are designing new networks, they are concerned with how the networks traverse these physical areas. The spatial arrangement of communication nodes

in a distributed computing environment is called the network topology. Each topology is suited to specific tasks and has its own advantages and disadvantages. A communication node is any end-point or intersection point in the communication network. A node might be a computer or some other form of data terminal equipment (DTE) that is attached to the network and serve as the end receiver or originating sender of messages sent over the network. At intersection points within the network nodes involve data communication equipment (data circuit-terminating equipment) (DCE) such as bridges, switches, hubs, and routers, which tie individual segments of the network together. The choice of topology is dependent upon:

1. Type and number of equipment being used.
2. Planned applications and rate of data transfers
3. Required response times
4. Cost

3.5.1.1 Bus Topology

A bus topology was the first, and is still quite commonly used topology for simple networks. It connects end-nodes, which are strung out along a line, like pearls on a necklace. Bus topologies evolved very early in the history of communication networks, before the invention of the computer. Figure 3.2 shows a Bus topology.

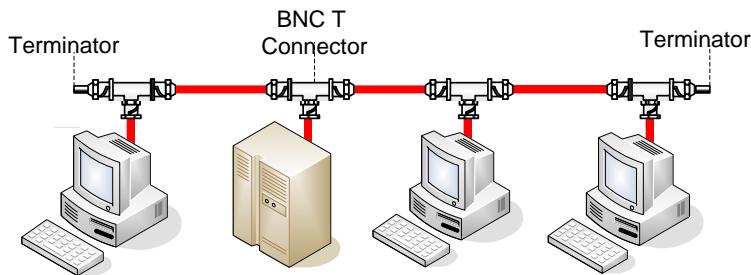


Figure 3.2: Bus Topology

Busses are still used extensively today in the topology of many local area networks that connect computers located within a short distance of one another.

Busses have some particular attributes that make them especially useful in the wiring of local area networks. The wires of the bus line can be run down hallways in wiring conduits or under floors or above ceiling panels. At each office where a network connection is required, which in the terminology of bus topology may be called a drop points, connections tap into the bus line. If needed, sidelines called spurs can be attached to the main bus; for example, these may provide connections to offices located down adjacent hallways.

Another frequent way to interconnect bus topologies in local area networks is by a wiring hub. These simple devices connect each node on the network into a central wiring box. However, the connections still operate logically as a bus; no switching or routing is performed in the wiring hub. These interconnection devices are frequently used in

situations where all of the computers on the network are grouped in a single location, such as in an office or in a computer lab.

Among the main advantages of bus topologies is that they are easy to design and install. Also, bus topologies tend to make efficient use of wiring; all end nodes tap into the same bus and use the same “bus route.” However, this can lead to a disadvantage when, as with the case of many local area networks, the individual nodes share the same physical wire, in such a case, many nodes that are all busy transmitting can reduce overall throughput. A main disadvantage of bus topology is that any break in the bus line will result in the split of the network into two non-communicating pieces. Usually, this disruption will result in the inability of one or more nodes to lose communication ability. In network slang, one would say, “the line break brought down the network.”

The bus cable carries the transmitted message along the cable. As the message arrives at each workstation, the workstation computer checks the destination address contained in the message to see if it matches its own. If the address does not match, the workstation does nothing more.

If the workstation’s address matches that contained in the message, the workstation processes the message. The message is transmitted along the cable and is visible to all computers connected to that cable.

3.5.1.2 Star Topologies

A major type of topographical configuration that evolved from early-centralized communication networks is called the star topology. It is frequently used in wide area networks to connect several nodes into a central computer. Early computer networks frequently consisted of dumb terminals connected to the centralized host using a network constructed in a star topology. Figure 3.3 shows a Star topology.

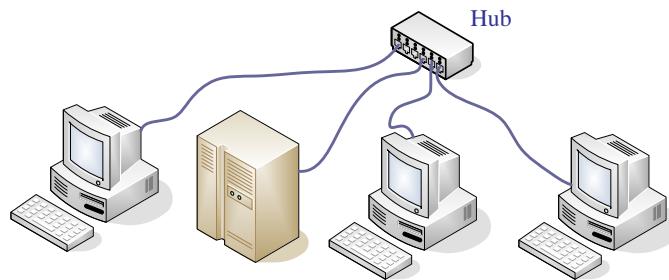


Figure 3.3: Star topology

Star networks have an advantage that if any of the lines running to a node is disrupted, the other nodes will normally not suffer any loss of communication and the network remains operative. However, it suffers from one very disturbing problem, which is generally considered a great flaw in network design; it involves a single point of failure. This is a condition where a failure in one single element in the equipment of a network results in the “outage” (meaning general failure) of the entire network. Under certain conditions, star networks can lead to excessive line installation and maintenance costs,

because a separate wiring path must be established between the central point and the end-nodes. Another problem may arise when the star's central point is a switching device designed simply to pass communications between attached nodes. In such cases, excessive communication traffic can lead to congestion and cause delays or delivery failures.

3.5.1.3 Ring Topologies

In Ring architecture, each workstation on the network is connected to two other workstations, forming a loop or ring as illustrated in the Figure 3.4. Data is sent around the loop in one direction (two-way rings also exist). Conflicts in the

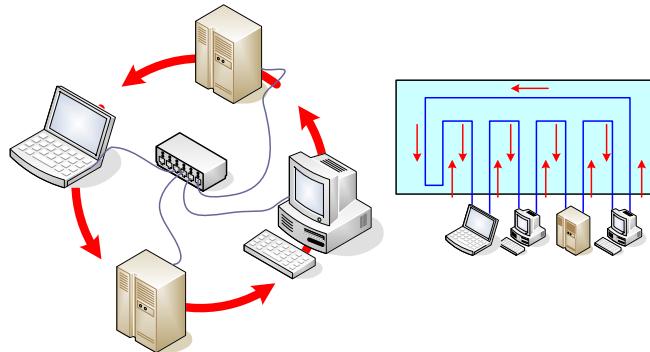


Figure 3.4: Ring topology

Transmission of data is avoided with token ring technology, which grants messages a “token” or permission to send. Each workstation receives regenerates and retransmits a token signal until it reaches its destination.

Ring topology provides stable networking for over 10 users. Like Bus topologies, rings are easy and relatively inexpensive to install. The number of workstations on the ring determines response time on a ring. Even if one connection fails, the rest of the network will function.

The ring topology is an older technology with a few limitations. The ring is difficult to troubleshoot, because when one connection fails, it is hard to determine where that problem is. Reconfiguring a ring will shut down the network.

3.5.1.4 Tree Topology

In Tree architecture, each device is connected to its own port on a hub, just like the star topology. A tree or "star of stars" topology interconnects hubs in a hierarchy; so one hub at the top of the hierarchy will connect to more hubs, which will break off to clients and even more hubs. Figure 3.5 shows a simple tree topology.

The highly flexible tree topology lets you add users by simply adding a hub. Centralized monitoring and administration makes it easier to control a large network or reconfigure it. Isolating problems is easy, and if one node goes down, the rest of the network stays online.

An extensive tree topology will be more expensive to administer than any of the previous topologies due to its size and complexity. If a hub cable or a hub fails, a portion of the network will go down.

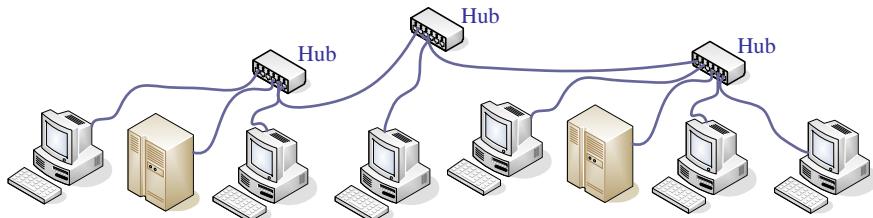


Figure 3.5: Tree Topology

3.5.1.5 Mesh Topologies

Large networks often use combinations of the above network topologies. Such complex network topologies go by several names, but we will simply refer to them collectively as mesh topology networks. They provide the network designer a great deal of flexibility in meeting the needs of a complex communications environment. Using communications equipment to connect buses, stars, rings and "stand-alone" computers forms mesh networks. The overall topologies of large modern businesses mostly are mesh topology. Such mesh networks can be quite difficult to manage and may often prove less reliable to operate due to their complexity. For the purpose of simplifying the tasks of network design or management, network analysts and administrators may "decompose" these complex networks into their elementary star, ring, or bus topological components.



The network may operate logically as though the physical layout were different. Bus LAN might be configured physically as a star. The bus still exists, but protected under the skin of the central hub to which all stations are connected via UTP. Similarly, a ring network might operate logically as a ring, but be supported physically by a collapsed backbone bus.

3.6 Metropolitan Area Networks (MAN's)

A MAN is a data communications network or interconnected groups of data networks that have geographic boundaries of a metropolitan area. MANs are used to connect networks that are totally or partially segregated from other networks. MAN's offer the ability to connect networks across a metropolitan area as if they were co-located in the same building or on the same campus. To create a MAN, businesses install communications links between the LANs. The backbone interconnection for a MAN is routinely high capacity fiber-based systems. This provides a fairly high data transfer rate and provides a high degree of fault tolerance. MAN's commonly use dual ring fiber systems that are self-healing (automatic connection rerouting) to allow uninterrupted

communication if fiber line is cut or damaged. MAN can mean several things in different contexts:

- Multiple local area networks (LANs) that are connected on a campus or industrial complex using a high-speed backbone.
- Multiple networks that are connected within the same city to form a citywide network for a specific government or industry.
- Any network bigger than a LAN but smaller than a wide area network (WAN).

Figure 3.6 shows a five node MAN to connect several LAN systems via a FDDI system. This diagram shows that each LAN may be connected within the MAN using different technology such as T1 copper access lines, digital subscriber line (DSL), coax, microwave, or fiber connections. In each case, a router provides a connection from each LAN to connect to the MAN.

By late years wireless standards are designed as a broadband data delivery system for Metropolitan Area Networks (MANs) to overcome many of the shortcomings of FDDI when used in a MAN environment, and can operate in licensed and unlicensed wide bands.

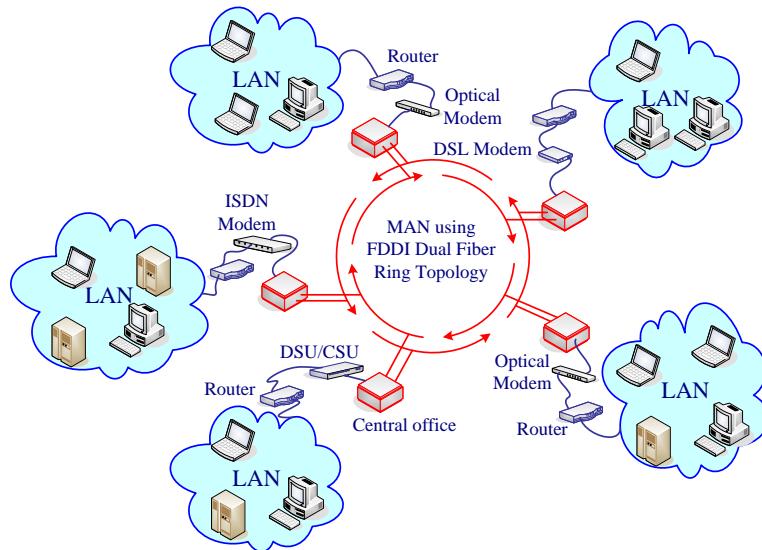


Figure 3.6: MAN connecting several LAN systems via a FDDI system.

3.7 Wide Area Network (WAN)

A Wide Area Network or WANs are communication networks that provide data transmission services through large geographically separate areas as shown in Figure 3.7. A WAN is usually composed of several different data networks such as PDNs, LANs, and MANs. Different types of communication lines such as leased lines (dedicated connections), packet data systems, or fiber transmission lines can interconnect these networks. WANs may be interconnected to and/or through the public switched telephone

network (PSTN) or public packet data networks (such as the Internet). WAN can be established by linking together two or more metropolitan area networks, which enables data terminals in one city to access data resources in another city or country using most other types of circuit including satellite networks, and integrated service digital network (ISDN). When wide area networks use wireless technologies, they are commonly called mobile data networks (MDNs).

WAN can be useful when companies have multiple locations that need to share network resources. For example, maybe the company's accounting system runs at the headquarters building where the accounting and MIS staff are located, but the warehouse across town still needs access to the accounting system for inventory picking tickets, data entry, and other order fulfillment and inventory tasks.

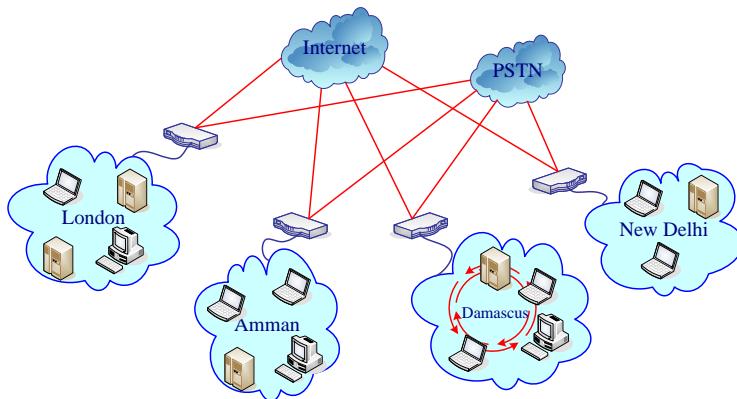


Figure 3.7: Wide Area Network

A particular WAN technology depends on many factors such as:

- the locations that will participate in the WAN
- the kind of WAN services available to them
- The data traffic and transmission rate from site to site
- The speed needed to transfer data
- Does the data transfer need to be synchronous or can it be asynchronous?
- The schedule of data transfers(all the time, occur once every 30 minutes, or follow some other)
- the budget constraints.

WAN can be classified by ownership as private networks and public networks, and can be classified by transmission and switching mechanism as switched and dedicated networks.

3.7.1 Private and Public WAN

A *private network* is exclusively owned by a particular company. All LANs are private networks, but WANs can be private or public.

Private WAN is a term used to describe a private network that crosses public areas. In Internet terminology, a **private network** is a network that uses private IP address space when it is necessary for computers to communicate with other on an internal (non-Internet) network, these addresses can't be used to access the Internet.

An alternative to the private network is the VPN (virtual private network). The carrier preprograms a path through the network, called a *virtual circuit*, and provides a contracted amount of bandwidth (called the *CIR* or *committed information rate*). The advantage of packet switching as compared to leased lines is that you only pay for the bandwidth you need.



Often the need for a WAN can be satisfied using a technology called Virtual Private Networks (VPNs). A VPN is a private network created through a public network, typically the Internet. A VPN is called “private” because all of the packets between two points are encrypted, so even though the packets are transmitted over a public network, their information remains secure. VPN is called “virtual” because they use the Internet, instead of dedicated WAN links, and often can make use of existing Internet connections.

A public WAN such as the Internet. The Internet is a network through which many companies data passes. Public networks are less secure than private networks, but the advantages are that public networks are less expensive to use and you don't have to maintain the external network yourself.

Public network are preferred to be used under these conditions:

- If the data does not need to be secure or you have the ability to make it secure over the public network.
- No matter if data occasionally takes longer to reach its destination or if the delay between sites is relatively unpredictable.
- If the high cost of the network relative to the benefits that network brings.
- If you want the lowest cost network connection possible.

Private network are preferred to be used under these conditions:

- If data security is important.
- If a large number experienced staff to set up and maintain the network exist.
- If the benefits the network brings are important in relevance to the cost.
- If there is a full, reliable control over the network's bandwidth.

3.7.2 Switched and Dedicated WAN

In most wide area networks, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines (also called circuits, channels, link or trunks) move bits between machines.

The switching elements are specialized computers used to connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line to forward them on. According to these components WANs is divided to switched and dedicated networks.

A *switched* WAN is one that uses a switched connection. Switched connection is not active all the time such as a dial-up modem connection or an ISDN connection from one location to another. These types of connections are formed only when you need them, and you usually pay for the time the connection is open, rather than the amount of data you're able to transmit over the connection. Figure 3.8 is an example of a switched WAN link.

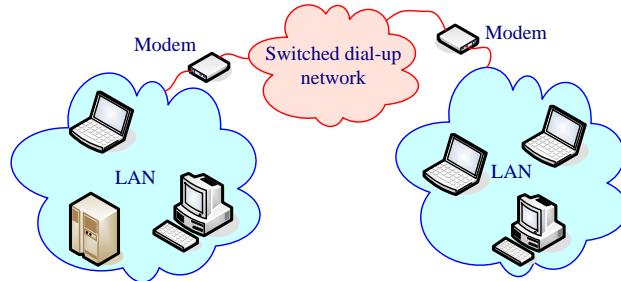


Figure 3.8: Switched WAN connection.

Switched links can be either circuit-based (circuit-switched) or packet-based (packet-switched). A circuit-switched *link* forms a connection as needed and makes a fixed amount of bandwidth available over that link. A packet-switched link sends data packets into a network cloud in which they can follow a number of paths to their destination and then emerge from the cloud.

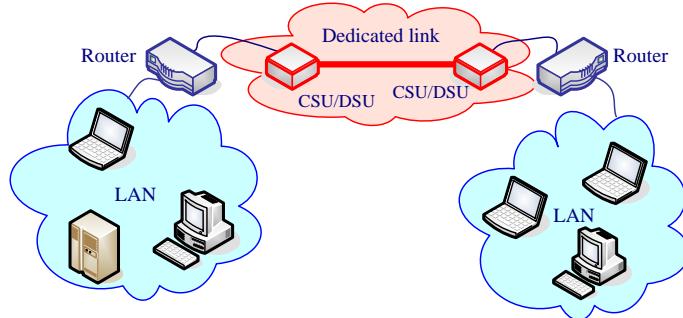


Figure 3.9: dedicated WAN connection.



Packet-switched networks can be more reliable because the data can take many different paths, but you are not guaranteed that each packet will arrive in a certain amount of time.



A circuit switched link just gives you one “pipe” from your source to your destination, but you can control what goes into the pipe and how long it will take to get to its destination.

A dedicated WAN connection is one that is always up and running such as DS1 (T-1) lines, xDSL lines, or leased telephone lines. You use a dedicated connection when you need the connection to be up all the time or when the overall economics show that such a connection is cheaper than a switched link. Figure 3.9 illustrates a dedicated WAN connection.

3.7.2.1 Circuit switching (CS)

Circuit-switched networks, as the basis of conventional telephone systems, were the only existing personal communication infrastructures prior to the invention of packet-switched networks. In conventional telephone networks, a circuit between two users must be established for a communication to occur. Circuit-switched networks require resources to be reserved for each pair of end users. This implies that no other users can use the already dedicated resources for the duration of network use. The reservation of network resources for each user results in an inefficient use of bandwidth for applications in which information transfer is bursty.

In circuit switching networks, when establishing a call a set of resources is allocated for this call. These resources are dedicated for this call, and can't be used by any of the other calls. Circuit Switching is ideal when data must be transmitted quickly, must arrive in sequencing order and at a constant arrival rate. So when transmitting real time data, such as audio and video, Circuit Switching networks will be used.

Each connection results in setup of a physical channel between the two parties, which is not terminated until the end of all communication telephone system is an example of circuit switched networks. CS provide a fixed, guaranteed data rate and allows rapid transmission of data that cannot be delayed, so both parties must operate at the same data rate. A limitation for this switching is that a long time may be needed to establish connection and time is wasted with no data being transmitted.

3.7.2.2 Packet switching (PS)

The major difference between Packet switching and Circuit Switching is that the communication lines are not dedicated to passing messages from the source to the destination. In Packet Switching, different messages can use the same network resources within the same time period. Since network resources are not dedicated to a certain session, the protocol avoids waste of resources when no data is transmitted in the session. Packet Switching is more efficient and robust for data that is bursty in its nature; it can withstand delays in transmission, such as e-mail messages, and Web pages.

Packet switching refers to protocols in which messages are broken up into small packets before they are sent. Each packet is transmitted individually across the net. The packets may even follow different routes to the destination, depending on the type of packet switching. Thus, each packet has header information which enables it to route the

packet to its destination. At the destination the packets are reassembled into the original message.

To prevent unpredictably long delays and ensure that the network has a reliably fast transit time, a maximum length is allowed for each packet. It is for this reason that the message submitted to the transport layer may first have to be divided by the transport protocol entity into a number of smaller packet units before transmission. In turn, they will be reassembled into a single message at the destination.

The goal of a broadband packet-switched network is to provide flexible communication in handling all kinds of connections for a wide range of applications, such as telephone calls, data transfer, teleconferencing, video broadcasting, and distributed data processing. One obvious example for the form of traffic is multirate connections, whereby traffic containing several different bit rates flow to a communication node.

3.7.2.2.1 Types of Packet-Switched Networks

Packet-switched networks are classified into datagram or connectionless networks and virtual-circuit or connection-oriented networks, depending on the technique used for transferring information.

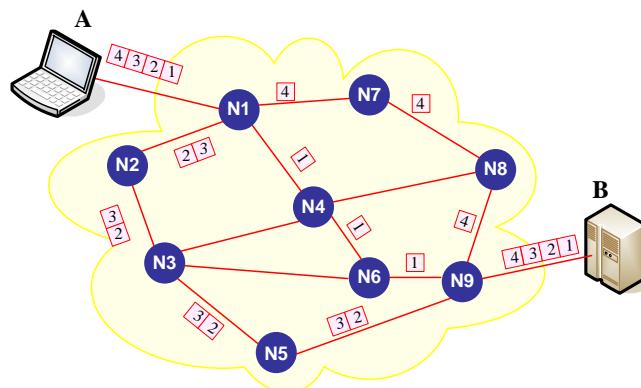


Figure 3.10: routing of four packets in a connectionless-oriented network from point A to point B

Datagram or Connection-less service: Datagram transmission is the simplest form of a network service based on the connectionless protocol. In this type of network, a user can transmit a packet anytime, without notifying the network layer. Packets are encapsulated into a certain "formatted" header, resulting in the basic Internet transmission unit of data, or datagram. A datagram is then sent over the network, with each router receiving the datagram forwarding it to the best router it knows, until the datagram reaches the destination. In this scheme, packets may be routed independently over different paths. However, the packets may arrive out of sequence. In this case, a certain network function takes care of the error control, flow control, and resequencing packets.

Figure 3.10 shows the routing of four packets in a connectionless network from point A to point B, the packets move on separate paths. The packets traverse the intermediate nodes in a store-and-forward fashion, whereby packets are received and

stored at a node on a route; when the desired output of the node is free for that packet, the output is forwarded to its next node. In other words, on receipt of a packet at a node, the packet must wait in a queue for its turn to be transmitted. Nevertheless, packet loss may still occur if a node's buffer becomes full. The node determines the next hop read from the packet header.

Virtual circuit or Connection-oriented service: A related, though more complex, service is the connection-oriented protocol. Packets are transferred through an established virtual circuit between a source and a destination. When a connection is initially set up, network resources are reserved for the call duration. After the communication is finished, the connection is terminated, using a connection-termination procedure. During the call setup, the network can offer a selection of options, such as best-effort service, reliable service, guaranteed delay service, and guaranteed bandwidth service.

Connection is requested. If a call accepted a link is established, same reference number is assigned to each packet so packets relating to different connections between the same machines can be distinguished. Once the path of the virtual circuit is established packets can be sent in order and arrive in the same order. This service provides more reliable service and in some cases faster service.

When a packet arrives at a node it is buffered in memory until it can be sent on the next node on the way to its destination. Since many packets can arrive at once it is necessary for some to be retained in node memory until forwarding.



The most important goal for a node is to get the packet to the final node, which then handles local sending of the packet to an attached computer.



Routing table used to store information about the addresses of all nodes, which interconnect with a given node and the interface is to be used to reach that packet.

The connection set-up procedure shown in Figure 3.11 requires packets to move along path from point A to point B with a prior connection establishment. During the connection setup process, a virtual path is dedicated, and the forwarding routing tables are updated at each node in the route.

Virtual-circuit packet switching typically reserves the network resources, such as the buffer capacity and the link bandwidth, to provide guaranteed quality of service and delay. The main disadvantage in connection-oriented packet-switched networks is that in case of a link or switch failure, the call set-up process has to be repeated for all the affected routes. Furthermore, each switch needs to store information about all the flows routed through the switch.

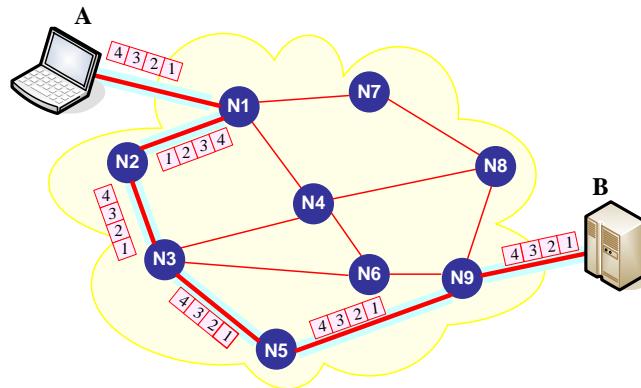


Figure 3.11: routing of four packets in a connection-oriented network from point A to point B

3.7.2.3 Frame Switching (Frame Relay)

A frame relay was first offered commercially in 1992. Much like packet switching, each frame is addressed individually. Frame relay also makes use of special switches and a shared network of very high speed. Unlike packet switching, frame relay supports the transmission of virtually any computer data stream in its native form—frames are variable in length (up to 4,096 bytes). Rapidly gaining in popularity, frame relay is widely available in many highly developed nations. International frame relay service is also becoming widely available. Disadvantages include the fact that frame relay, like packet switching, is oriented towards data transmission. Further, transmission delays are variable and uncertain in duration. While increasingly satisfactory technologies have been added for support of voice and video, frame relay is not designed with those applications in mind.

Prior to recognition of ATM as the preferred network platform for WAN application, Frame Relay gained significant market penetration for WAN application. Frame relay networks connect multiple client sites on what appears to be dedicated circuits using a high speed (reaching of 45 Mbps) variable-length packet switching technology. Frame Relay is well suited to high speed data applications, but not suited for delay sensitive applications such as voice and video because of the variable length of frames. Figure 3.12 shows a point-to-point system that uses a private virtual circuit (PVC) to transmit variable length frames at the data-link layer.

To connect a network to a frame relay service, a special bridge, router, or CSU/DSU (Channel Service Unit/Data Service Unit) device called a frame relay access device (FRAD) is used. The FRAD connects customer premises to an Edge Switch (ES) on provider's frame relay cloud (the collection of all frame relay circuits belonging to your provider) cloud.



Cloud is the collection of all frame relay circuits belonging to your provider.

 Frame relay is a WAN solution that provides bandwidth similar to that of a leased line, but with greater flexibility.

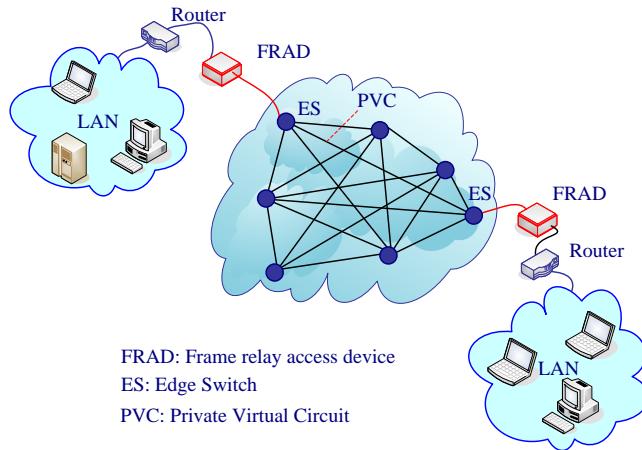


Figure 3.12: Frame relay uses a point-to-point system

3.7.2.4 Cell Switching

This service was invented to take advantage of the best of circuit switching (guaranteed bandwidth) and packet switching (no need for a permanent physical connection) by offering both as separate services. Cell switching is used in ATM switches (cellplexes) as illustrated in figure 3.12. Encompassing both Switched Multimegabit Data Service (SMDS) and Asynchronous Transfer Mode (ATM), data is organized into cells of fixed length (53 octets), shipped across very high speed facilities and switched through very high speed, specialized switches. This technology provides a connection-oriented, full-duplex, point-to-point service between devices.

 Network equipment can switch, route, and move uniform-sized frames much more quickly than it can move random-sized frames. The consistent, standard-sized cell uses buffers efficiently and reduces the work required to process incoming data. The uniform cell size also helps in planning application bandwidth.

Cell switching offers a high bandwidth service that is capable of carrying voice, Data, Fax, real-time video, CD-quality audio, imaging and multimegabit data transmission both on LANs and WANs over great distances. It can provide interfaces to transmission speeds ranging from 1Mbit/sec to 10Gbits/sec. It offers low latency, making it suitable for time-sensitive or isochronous services such as video and voice. Plus, it is protocol and distance-independent.

Today, this technology is sometimes used for network backbones, but it is more commonly found in WAN connections.

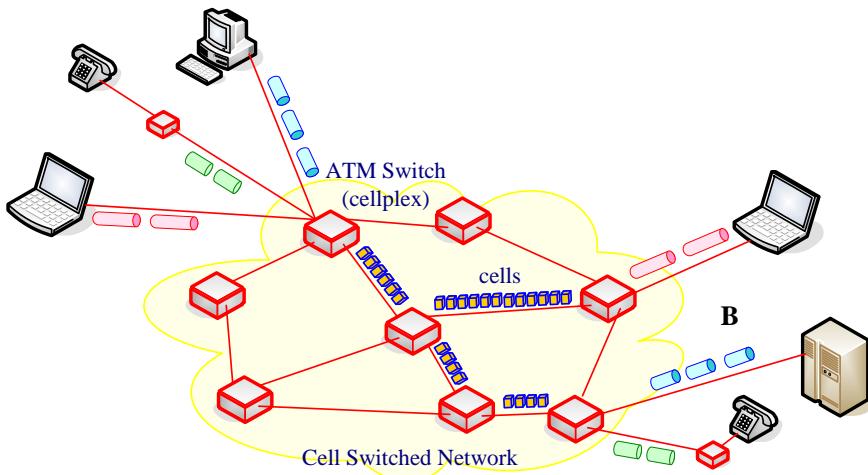


Figure 3.13: Cell switching network

3.8 Internetworking (Internet)

Internet is a collection of interconnected networks that provides universal service among heterogeneous communication networks. The series of interconnected networks includes local area, regional and national backbone networks.

The Internet was originally formed in the 1970's as a military network. Quickly, universities and companies involved with defense-related research were given access. In the late 1980's, the Internet became the global network for most universities and many businesses around the world. In 1993, when commercial providers were first permitted to sell Internet connections to individuals, usage of the network exploded. Millions of new users came on-line within months, and a new era of computer communications began.

The Internet Engineering Task Force document (RFC 2026) defines the Internet as following:

A loosely organized international collaboration of autonomous interconnected networks.

This definition encompasses several key aspects of what the Internet is:

- **Loosely organized:** No single organization has authority over the Internet. As a result, the Internet is not highly organized. No one exercises that kind of control over the Internet. As a result, you can find just about any kind of material imaginable on the Internet. No one guarantees the accuracy of information that you find on the Internet.
- **International:** The Internet is a network of resources, the international linking of tens of thousands of businesses, universities, and research organizations with millions of individual users. The Internet provides users with an enormous amount of information on a wide variety of topics. In addition, the

Internet provides the means to allow communications between computers and share computer program, databases, manuscripts, and spreadsheets across the world, or even do video conferencing. Internet uses the communication and networking infrastructure all around the world. More than 100 countries are represented on the Internet.

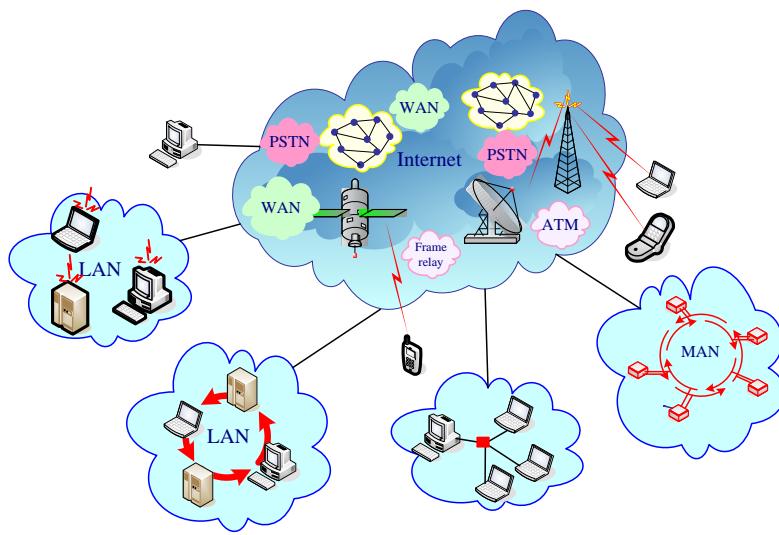


Figure 3.14: Different Network Technologies can be connected to create an Internetwork.

- **Collaboration:** The Internet is by no means the only way by which computer users can communicate with others. Several commercial on-line services provide connections to members who pay a monthly connect-time fee. Internet provides a tremendous range of information and services, including on-line conferencing, electronic mail transfer, program downloading, current weather and stock market information, travel and entertainment information, access to encyclopedias and other reference works, and electronic forums for specific user groups such as PC users, sports fans, musicians, and so on. The Internet exists only because many different organizations cooperate to provide the services and support needed to sustain it.
- **Autonomous:** The Internet community respects that organizations that join the Internet are free to make their own decisions about how they configure and operate their networks.
- **Interconnected:** The Internet is a network of networks. The whole key to the Internet is the concept of *interconnection*, which is using standard protocols that enable networks to communicate with each other. Networks in the Internet use the same telecommunications protocol (TCP/IP) and provide various services such as electronic mail, remote login, and file transfer services to the host computers. Without the interconnection provided by the TCP/IP protocol, the Internet would not exist. The TCP protocol coordinates

the overall flow of data during a data communication session between points (nodes) in the Internet. IP is an addressing structure that allows packets of data to be routed (redirected) as they migrate through different networks to reach their ultimate destination.

- **Networks:** The Internet would be completely unmanageable if it consisted of hundred million individual users, all interconnected. That's why the Internet is often described as a *network of networks*. Most of the individual users who are on the Internet don't access the Internet directly. Instead, they access the Internet indirectly through another network, which may be a LAN in a business or academic environment or a dialup or broadband network provided by an Internet service provider (ISP). In either case, however, the users of the local network access the Internet via a gateway IP router.

3.8.1 Connecting to the Internet Backbone

3.8.1.1 Internet Services Provider (ISP) and Network Access Points (Naps)

Internet users are connected to the global Internet via the hosts of their ISPs. Networks of national ISPs are connected and this interconnection is extended to the networks of ISPs of neighboring countries, and these networks together make up the global Internet.

National ISPs are connected together through complex switching stations called network access points (NAPs). Each NAP has its own system administrator. The different NAPs are actually connected by a set of trunk lines, which are part of the Internet backbone. Each of the NAPs rests on one of the Internet trunk lines, and these trunk lines allow the Internet access providers to communicate with each other.

In contrast, regional Internet service providers are smaller ISPs connected to a national ISP in a hierarchical chart. A router can operate as a device to connect to ISPs. Figure 3.15 explains how two end user in different countries can communicate with each other making use of ISPs.

Each regional ISP can give services to part of a city. The lowest networking entity of the Internet is a local Internet service provider. A local ISP is connected to a regional ISP or directly to a national service provider and provides a direct service to end users.

3.8.1.2 Common Internet Accessing Methods

Access the Internet can be loosely divided into three categories:

3.8.1.2.1 Residential Access Networks

Probably the most common access the Internet from residential areas is using a **modem** over a POTS (plain old telephone system) dialup line to an Internet service provider (ISP). A modem (modulation/demodulation unit) is a device that converts the digital data to a modulated form of signal that takes less bandwidth. A modem is required to create an appropriate digital signal to access the Internet.

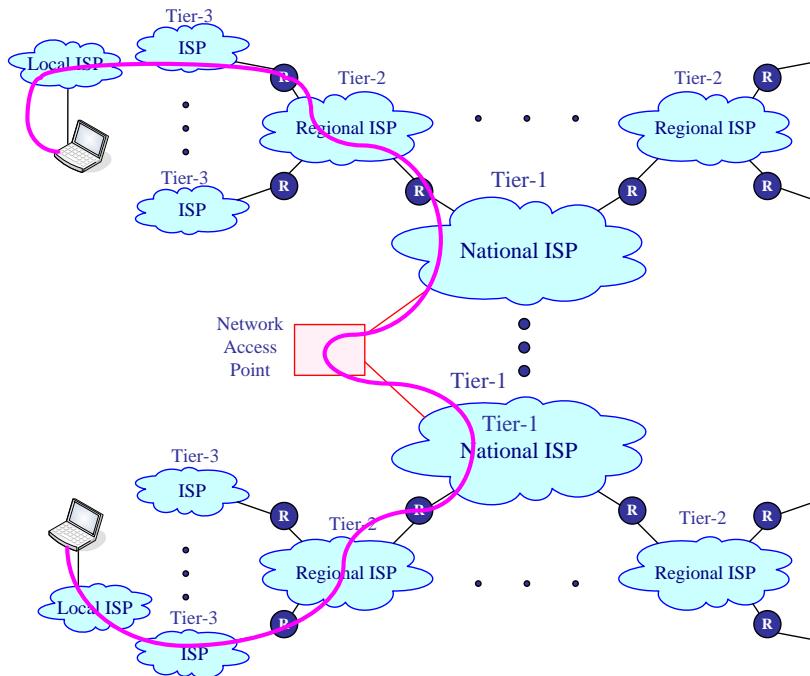


Figure 3.15: making use of different tier of ISPs to connect users in different countries.



Modems available these days are typically rated at up to 56Kbps but you can't achieve 56Kbps over standard telephone lines, even if you have matched 56Kbps modems at both ends; the maximum you will get is 33.6Kbps in both directions over standard telephone lines.

ISDN users, on the other hand, have the choice of either connecting to an ISDN capable ISP or to ISDN “modems” hosted on the LAN. Through a process called *bonding*, ISDN users can achieve speeds up to 128Kbps.

Asymmetric Digital Subscriber Line (ADSL)

ADSL is conceptually similar to dialup modems: it is a new modem technology again running over existing twisted pair telephone lines, but can transmit at rates of up to about 8 Mbps from the ISP router to a home end system. The data rate in the reverse direction, from the home end system to the central office router, is less than 1 Mbps.

Hybrid fiber coaxial cable (HFC)

While ADSL, ISDN and dialup modems all use ordinary phone lines, HFC access networks are extensions of the current cable network used for broadcasting cable television. In a traditional cable system, a cable head end station broadcasts through a distribution of coaxial cable and amplifiers to residences. Typically, the cable modem is an external device and connects to the home PC through a 10-BaseT Ethernet port. Cable modems divide the HFC network into two channels, a downstream and an upstream

channel. As with ADSL, the downstream channel is typically allocated more bandwidth and hence a larger transmission rate.

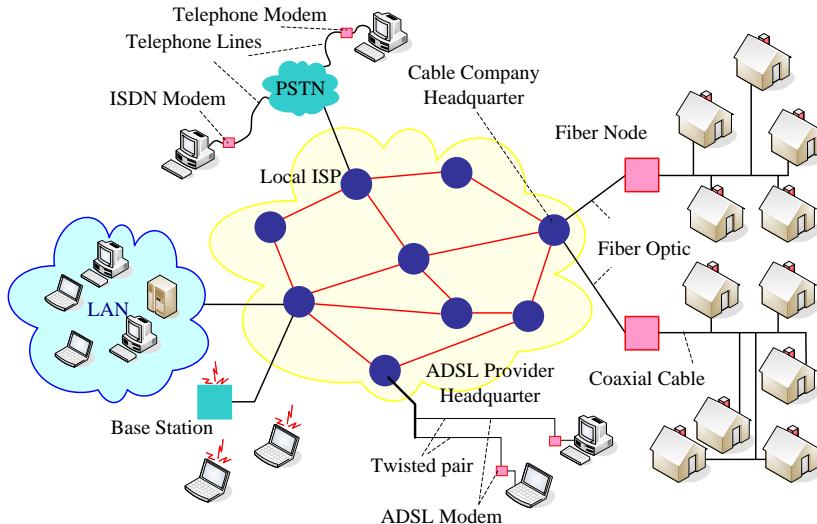


Figure 3.16: different Access Networks types

3.8.1.2.2 Institutional Access Networks, (Enterprise Access Networks)

In enterprise access networks, a local area network (LAN) is used to connect an end system to an edge router. The edge router is responsible for routing packets that have destinations outside of that LAN.

For small networks, it can often be easiest simply to add a modem or two to a computer set up to accept remote connections, and then let the users use those modems to connect. You can set up the modems on special LAN-connected interfaces built for the purpose of providing remote node connections. You can also build your own “modem farms” with tens or hundreds of modems, using special hardware that supports such uses.

3.8.1.2.3 Mobile Access Networks

Mobile access networks use the radio spectrum to connect a mobile end system (e.g., a laptop PC or a PDA with a wireless modem) to a Base station, as shown in Figure 3.16. This Base station, in turn, is connected to an edge router of a data network. This technology is expected to revolutionize the way Internet service is provided.

A mobile technology is capable of delivering very high data rates over long distances. Indeed, this would seem an ideal technology to apply to the problem space of the residential wireless local loop, where low-rate wired infrastructure often limits the types of capabilities that can be enjoyed by the residential consumer.

3.8.2 Intranet

An intranet is a private computer network based on the communication standards of the Internet. It is a smaller version of the Internet that can only be used by members of an organization. Companies can create, within their walls, a manageable, secure version of the World Wide Web. Using Intranets

Intranets allow an organization to spend less time on things that bring no value such as chasing down the right information to solve a problem. Productivity increases as corporate knowledge is more accessible and the data is more accurate.

Intranets are useful for companies for many reasons including:

1. Flexibility in time of delivery of knowledge is gained as information is always a click away.
2. Intranets can help users to locate and view information faster and use applications relevant to their roles and responsibilities.
3. Employees can link to relevant information at a time which suits them rather than being deluged indiscriminately by emails.
4. Intranets can serve as powerful tools for communication within an organization, vertically and horizontally.
5. Using hypermedia and Web technologies employees make use of manuals, benefits documents, company policies, business standards, newsfeeds, and even training.
6. Intranets are also being used as a platform for developing and deploying Business operations and management.
7. Intranet reduces the cost improving timeliness of distributed information
8. Intranet provides a secure medium for the distribution of confidential information
9. Intranet provides interactive services – surveys, training, data base access, inter-company communication

3.8.3 Extranet

Extranet is an extension of internal network that allows outside users to provide and access information in a secure environment. It is a private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

Like the intranet, it is web browser based, making information available on any computer without any special equipment. However, an extranet does require extensive security and may need special software to provide user authentication and to encrypt data.

Companies can use an extranet to:

- Exchange large volumes of data using Electronic Data Interchange (EDI)
- Share product catalogs exclusively with wholesalers or those "in the trade"
- Collaborate with other companies on joint development efforts
- Jointly develop and use training programs with other companies

- Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks
- Share news of common interest exclusively with partner companies

An extranet requires security and privacy. These can include firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of virtual private networks (VPNs) that tunnel through the public network.

3.9 Quick Review

- ❖ Networks are classified depending on the geographical coverage, the network topology, the ownership, the switching mechanism, the transmission speed, etc.
- ❖ A *LAN* is a form of limited-distance, shared packet network for computer communications over a common medium.
- ❖ Topology is the overall physical layout of a network.
- ❖ Bus topologies typically use a passive network architecture, where the computers connected through one cable.
- ❖ Star topology is a LAN topology where each computer or device on the network is connected with its own cable to a central device called a hub.
- ❖ Ring topology is a LAN topology where computers are arranged in a physical circle. The ring topology moves information on the wire in one direction and is considered an active topology.
- ❖ In Tree architecture the "star of stars" topology interconnects hubs in a hierarchy.
- ❖ In mesh topologies large networks often use combinations of the above network topologies.
- ❖ MAN is an interconnected group of data networks that are totally or partially segregated from other networks and have geographic boundaries of a metropolitan area.
- ❖ WAN are network made up of a number of LANs. It can be defined as a collection of LANs that extend over a wide geographic area.
- ❖ A Public Data Network is a network established and operated by a telecommunications administration, or a recognized private operating agency, for the specific purpose of providing data transmission services for the public.
- ❖ Private network is a high-performance and reliable communications infrastructure gives the user a vital competitive edge. It describes a wide area network that crosses public areas.
- ❖ An alternative to the private network is the VPN which is used to move information between trusted and it is built on packet- or cell-switching networks.
- ❖ Switched network is a strategy that allows multiple users to take advantage of the same line. It can take advantage of two different strategies: circuit switching and packet switching.
- ❖ Connection-Oriented means that when devices communicate, they perform handshaking to set up an end-to-end connection.
- ❖ Connectionless (Datagram transmission) means that no effort is made to set up a dedicated end-to-end connection.

- ❖ Packet switching allows the multiplexing of data packets from different sources on the same transmission path.
- ❖ A virtual circuit is a point-to-point communication link between two end stations on a switched network. It emulates the characteristics of a physical circuit on a switched network.
- ❖ Frame Relay offers a high speed version of packet switching and is well suited to high speed data applications, but not suited for delay sensitive applications.
- ❖ Cell Relay is a transmission mechanism that combines the benefits of time division multiplexing with packet switching using a fixed cell size.
- ❖ Internetworking is the process of interconnecting computers and their networks to form a single network.
- ❖ The Internet is a network of computer networks and computers spans across almost all countries in the world interconnecting all types of computer networks. The one thing that binds them onto one single network is the Internet Protocol suite TCP/IP.
- ❖ An ISP provides an Internet connection to users or companies. National ISPs are connected together through complex switching stations called network access points (NAPs).
- ❖ The different NAPs are actually connected by a set of trunk lines, which are part of the Internet backbone.
- ❖ A lot of companies use intranets/ extranets as a powerful tool to manage their resources and work in a systematic manner. An intranet is a private computer network based on the communication standards of the Internet. An Extranet is an Intranet that people outside your formal organization can have access to.

3.10 Self Test Questions

A- Answer the following questions

1. Classify networks by Geographical Coverage
2. What are the shared LAN characteristics?
3. List some of LANs advantages.
4. List the most popular LAN topologies.
5. List the main advantages and drawbacks of every one of these topologies.
6. Distinguish between LAN and MAN?
7. Where can MANs be applied?
8. Distinguish between WAN and MAN?
9. Where can WANs be useful?
10. How can you distinguish private WAN from public WAN?
11. State the differences between Switched and dedicated WANs?
12. What are the differences between circuit switched networks and packet switched networks?
13. Explain the role of nodes in networking?
14. State the difference between packet switching and frame switching?
15. State the difference between packet switching and cell switching?
16. State the difference between Internet and intranet?
17. State the difference between Internet and Extranet?
18. State the difference between Extranet and intranet?

19. The Internet can be defined as a loosely organized international collaboration of autonomous interconnected networks. Explain that.
 20. What is the role of ISP?
 21. Classify the tiers of ISPs?
 22. List the common Internet accessing methods.
 23. What are the uses of intranet in companies?
 24. What are the uses of extranet in companies?

B- Identify the choice that best completes the statement or answers the question.

1. Which of the following allows external agents to have access to corporate computing resources?
a. Internet
b. intranet
c. extranet
d. CRM service
 2. Which of the following network is a data network connection that makes use of the public telecommunications infrastructure but maintains privacy through the use of a tunneling protocol and security procedures?
a. private
b. virtual
c. virtual private
d. virtual secure
 3. In an ATM network, _____ bit rate applications often send bursts of data, and the ATM network guarantees that the traffic is delivered on time.
a. constant
b. variable
c. available
d. unspecified
 4. ATM can carry _____ over the same facilities.
a. voice and data
b. voice and video
c. data and video
d. voice, data, and video
 5. _____ would be most likely to use ATM.
a. an individual
b. a school
c. a large telephone and Internet service provider
d. a small business
 6. Which of the following communications networks were designed to support computer data transmissions?
a. Circuit-switched
b. Broadcast
c. Packet-switched
d. Data-centered
 7. Which of the following communications networks were designed to support voice data?
a. Circuit-switched
b. Broadcast
c. Packet-switched
d. Data-centered
 8. A dial-up telephone system uses a _____ communications network.
a. circuit-switched
b. packet-switched
c. broadcast
d. virtual

9. Which of the following communications networks are the most flexible?
 - a. Datagram
 - b. Virtual
 - c. Broadcast
 - d. Circuit
10. A node has to examine each packet individually and determine each packet's next path in a ____ subnet.
 - a. virtual
 - b. datagram
 - c. circuit-switched
 - d. broadcast
11. What is the type of wide area network in which information follows a dedicated path from node to node within the network?
 - a. packet-switched
 - b. circuit-switched
 - c. broadcast
 - d. virtual-switched
12. MAN topologies are very often based on a ____.
 - a. ring.
 - b. bus.
 - c. star.
 - d. hierarchy.
13. Transferring a file using the Internet's FTP software over a dial-up telephone line with a modem is an example of a ____ subnet supporting a connection-oriented application.
 - a. circuit-switched
 - b. datagram packet-switched
 - c. virtual packet-switched
 - d. broadcast
14. In which of the following communications network each circuit is dedicated to only one connection?
 - a. datagram packet-switched
 - b. virtual packet-switched
 - c. circuit-switched
 - d. broadcast
15. Users connect to the Internet via a(n) ____.
 - a. ISP.
 - b. IMP.
 - c. ATM.
 - d. CSMA/CD.
16. When a large message is sent via a packet-switched network ____.
 - a. only a small portion is actually sent
 - b. it is broken up into smaller pieces
 - c. it is rejected
 - d. message size is irrelevant; it is put into one packet
17. A client/server system is a form of a ____ network configuration.
 - a. microcomputer-to-local area
 - b. local area network-to-local area
 - c. microcomputer-to-mainframe computer
 - d. local area network-to-wide area
18. ____ is a high-speed network that interconnects multiple sites within a close geographic region.
 - a. local area network.
 - b. metropolitan area network.
 - c. wide area network.
 - d. personal area network.
19. ____ converts digital data to analog signals.

- a. modem.
 - b. codec.
 - c. encoder.
 - d. tuner.
20. What is the high-speed communications service that allows high-speed access to wide area networks?
- a. ISDN
 - b. DSL service
 - c. modem pool
 - d. cable modem
21. Which of the following can provide voice and data transmissions at speeds up to 128 kbps?
- a. T-1 lines
 - b. Cable television networks
 - c. ISDN
 - d. DSL
22. Which of the following can provide data transmission at speeds of hundreds of thousands up to millions of bits per second?
- a. T-1 lines
 - b. Cable television networks
 - c. ISDN
 - d. DSL
23. Which of the following is a digital telephone service that provides voice and data transfer services over standard twisted pair wire into a home or small business?
- a. T-1
 - b. DSL
 - c. SONET
 - d. ISDN
24. The _____ circuit is a point-to-point connection across the WAN.
- a. physical
 - b. logical
 - c. virtual
 - d. dynamic
25. _____ cells follow the same path for the duration of the connection.
- a. ISDN
 - b. ATM
 - c. LAPB
 - d. Frame Relay
26. _____ use WAN technologies to interconnect LANs in a specific geographic region.
- a. WPANs
 - b. MANs
 - c. Internetworks
 - d. Peer-to-peer networks
27. Which of the following is a network of networks or a networked collection of LANs tied together by devices such as routers?
- a. internetwork
 - b. Internet
 - c. MAN
 - d. WAN
28. Which of the following is recommended if the network use and security factors don't require using a router?
- a. LAN
 - b. MAN
 - c. WAN
 - d. internetwork
29. Which of the following consists of interconnected computers, printers, and other computer equipment in close physical proximity?
- a. WAN
 - b. MAN
 - c. WWAN
 - d. LAN
30. One_____ is composed of two or more LANs (or MANs) connected across a distance of more than approximately 48 kilometers.

- a. WLAN
b. WAN

c. DAN
d. WMAN

31. ____ or station is any device connected to a network.
a. array
b. node
c. server
d. transmitter

32. A network ____ has two components: the physical layout of network cables, and devices and the logical path followed by the network packets or frames.
a. protocol
b. operating system
c. interface card
d. topology

33. Which network is owned and maintained by a private organization?
a. public
b. local
c. private
d. global

34. The main network topologies are bus, ring, star, and ____.
a. mesh
b. hypercube
c. tree
d. mixed

35. Which of the following topologies consists of running cable from one PC or file server to the next, like links in a chain?
b. mesh
a. star
d. bus
c. ring

36. Which of the following topologies is a continuous path for data with no logical beginning or ending point?
a. hypercube
b. grid
c. star
d. ring

37. Which of the following topologies is the oldest communications design method, with roots in telephone switching systems?
a. star
b. mesh
c. ring
d. bus

38. ____ are connected together through complex switching stations called network access points (NAPs).
a. Regional ISPs
b. Local ISPs
c. National ISPs
d. Tier-3 ISPs

39. The smallest ISP is ____.
a. Tier-1 ISPs
b. Tier-2 ISPs
c. Tier-3 ISPs
d. Local ISPs

40. A ____ is a high-capacity communications medium that joins networks and central network devices across long distances.
a. router
b. backbone
c. hub
d. switch

41. A ____ is most likely to employ a mesh topology.
a. MAN
b. LAN
c. WLAN
d. DAN

CHAPTER 4

DATA TRANSMISSION

4.1 About This Chapter

Information might be a page of text, a conversation or a television picture. The information must first be encoded in an electrical manner, as electrical signal. Only such signals can be conveyed over the transmission medium, as wires. Information conveyed over communications systems is usually classed as either analog or digital signals.

Data transmission can be effectively used to describe the transfer of information (*communications*) from a sender to a receiver across a network. Some form of energy is used to represent the data, usually through a physical medium, such as electrical, electromagnetic and light.

The *transmission* must be at acceptable levels in terms of certain key criteria such as speed of connection, speed of information transfer, freedom from error, speed of response (two-way), and cost. The information can be transmitted in its original, or *native*, form. Or it can be altered in some way to affect compatibility between the transmitting and receiving devices and/or with the various elements of the network. Examples include analog voice or video converted to a digital (data) bit stream, digitized voice or video converted to analog voice or video, and digital data converted to an analog format.

This chapter examines a number of concepts and defines a fundamental set of elements that apply universally to data transmission networks. The concept of signal is explored in both analog and digital terms, with the advantages and disadvantages of each being explained. The concept of encoding is discussed in detail, with variations on the theme detailed and illustrated. Finally, this chapter explores the various types of modulation techniques used to transmit analog and digital signal through digital and analog circuitry.

4.2 Learning outcome

After this chapter, you should be able to:

1. Distinguish between analog and digital, signals, channels and transition techniques
2. Determine signal types, parameters and characteristics.
3. Explain Data transmission modes and make a comparison between them.
4. Determine Signal Impairments and their influence on data transmission quality.
5. Describe channel characteristics
6. Understand the importance of line coding in data transmission theory and practices.
7. Understand that both clocking requirements and the frequency limitations of different medium influence the choice of encoding method used.
8. Classify and explain line coding types and techniques.
9. Understand the role, the techniques, and the importance of analog transmission of digital data.

10. Understand the principles of digital transmission of analog data including analog to digital and digital to analog conversion.
11. Understand the modulation types used in transmission of analog signals.

4.3 Transmission Signals

In computer networks and communication, information is transferred in the form of signals. A signal is usually a time dependent value attached to an energy propagation phenomenon used to convey information.

4.3.1 Signal Parameters

Signals can be simple or complex. A simple signal, or a sine wave, cannot be decomposed into simpler signals. A complex signal is composed of multiple sine waves.

Signals can be periodic or random. The sine wave is the most fundamental form of a periodic signal. Visualized as a simple oscillating curve, its change over the course of a cycle is smooth and consistent, a continuous, rolling flow. Sine waves can be described by three characteristics:

4.3.1.1 Amplitude

The amplitude is the maximum value of the signal. It is equal to the maximum amplitude of a sine wave that is the highest value it reaches on the vertical axis as shown in Figure 4.1.

Amplitude is measured in volts, amperes or watts, depending on the type of signal. Volts refer to voltage, amperes refer to current and watts refer to power.

4.3.1.2 Frequency

Frequency is the period that refers to the amount of time in seconds a signal needs to complete one cycle. Frequency refers to the number of periods a signal makes over the course of one second. The frequency of a signal is its number of cycles per second. Mathematically, the relationship between frequency and period is that they are the inverse of each other's; if one is given, the other can be derived.

Electric signals are oscillating waveforms; that is, they fluctuate continuously and predictably above and below a mean energy level. The rate at which a sine wave moves from its lowest to its highest level is its frequency. Frequency is measured in cycle per second (One cycle per second = one Hertz).



Frequency and wavelength are inversely related—as the frequency of the signal (number of cycles per second) increases, the wavelength (length of the electromagnetic waveform) of the signal decreases. In other words, the more waveforms per second, the shorter the length, or cycle, of each individual wave

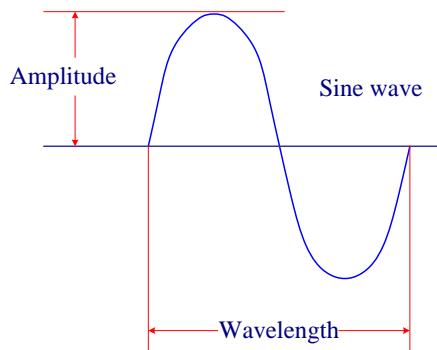


Figure 4.1: Sine wave

4.3.1.3 Phase

The term phase describes the position of the waveform relative to time zero. The wave is something that can be shifted backwards or forward along the time. Phase describes the amount of that shift. It indicates the status of the first cycle.

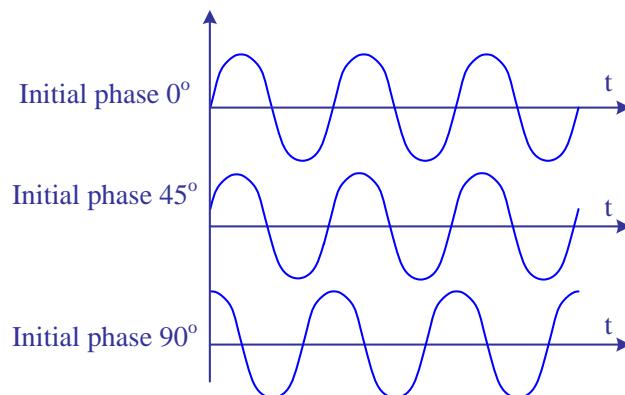


Figure 4.2: A different phase shift for the sine wave

Phase is measured in degrees or radians (360 degrees is 2π radians). A phase shift of 360 degrees corresponds to a shift of a complete period; a phase shift of 180 degrees corresponds to a shift of half a period; and a phase shift of 90 degrees corresponds to a shift of a quarter of a period. Figure 4.2 shows a different phase shift for the sine wave.

We can represent signals in time domain and in the frequency domain as in figure 4.3. Signals in general contain a multitude of frequencies. Adding two sinusoidal signals we get the time domain signal depicted in the left-hand side plot. We have added to the 1 kHz signal a signal of 3 kHz with amplitude equal to $1/3$ of the 1 kHz signal. The frequency domain picture shows the two frequencies each with its amplitude value. We then have added 4 signals together. The signals with higher frequencies, called harmonics, have successively smaller amplitudes: $1/3, 1/5, 1/7$, etc..

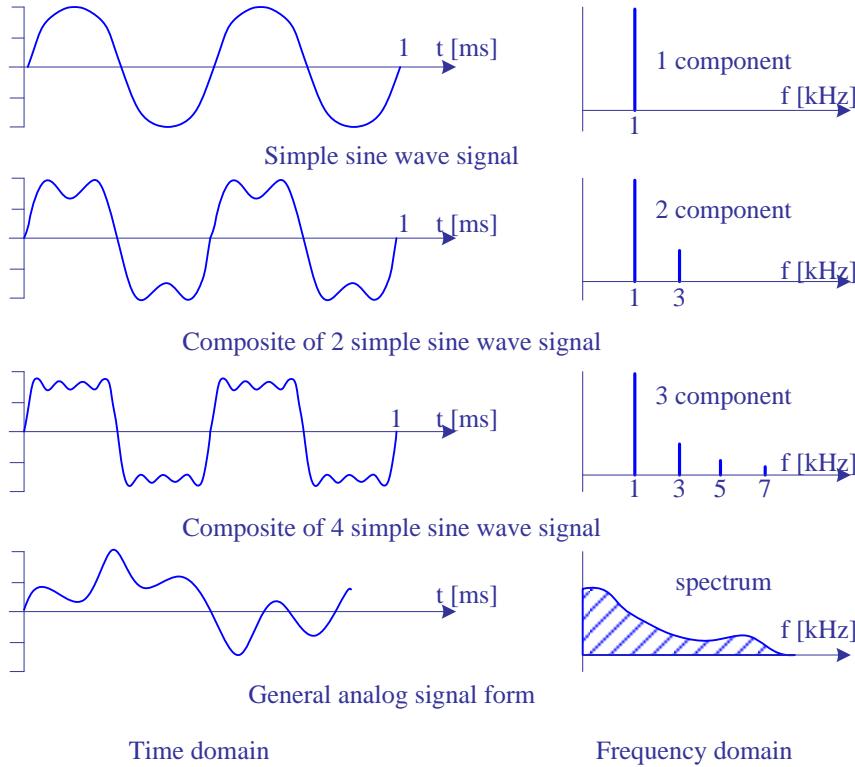


Figure 4.3: representation of different signals in time and frequency domains

In practice, we transmit the signal with a random form. The frequency domain shows that such signal contains a range of frequencies. As a matter of fact, every frequency between 0 and some upper value is represented. The resulting is the spectrum of the signal which is the signal presentation in the frequency domain. The bandwidth of the signal is the range between its lowest and the highest frequency components of its spectrum.



Bandwidth is a measure of the capacity of a circuit or channel. More specifically, bandwidth refers to the total frequency that is available on the *carrier* for the transmission of data. There is a direct relationship between the bandwidth of a circuit or a channel and both its frequency and the difference between the minimum and maximum frequencies supported. While the information (data) signal does not occupy the total capacity of a circuit, it generally and ideally occupies most of it. The more information to be sent in a given period of time, the more bandwidth required

Human voice spectrum for example mostly is in the range of 100 Hz to 3,000 Hz; the energy in the speech spectrum peaks at approximately 500 Hz. The human ear can distinguish signals as low as 20 Hz and as high as 20 kHz, and is most sensitive in the range of 1,000 Hz to 3,000 Hz. Public switched telephone networks provide reliable, raw,

voice-grade bandwidth of 4 kHz; with 3,300 Hz (200 Hz to 3,500 Hz) usable for signal transmission.

4.3.2 Signal Types

Two types of signals are used to transfer information:

4.3.2.1 Analog Signals

Analog is best explained by examining the transmission of a natural form of information, such as sound or human speech, over an electrified copper wire. Analog signals use continuously variable electric currents and voltages to reproduce data being transmitted. Since data is sent using variable currents in an analog system, it is very difficult to remove noise and wave distortions during the transmission. For this reason, analog signals cannot perform high-quality data transmission.

In its native form, human speech is an oscillatory disturbance in the air which varies in terms of its volume or power (amplitude) and its pitch or tone (frequency). As sound compression waves fall onto a transmitter, analogous (approximate) variations in electrical waveforms are created over an electrical circuit. Those waveforms maintain their various shapes across the wire until they fall on the receiver or speaker, which converts them back into their original form of variations in air pressure.

4.3.2.1.1 Advantages of Analog Signals

There are many good things to say about analog transmission:

- It was compatible with the electro-mechanical and later electronic analog switches in the first half of the century.
- Its electronics were proven in over time and it provided relatively reliable service for voice and multimedia.
- It was relatively simple and inexpensive to install.
- The signals could be frequency multiplexed over both wire and coaxial cable, making it an efficient medium to connect central offices.
- Technological advances in analog microwave transmission helped keep up with the demands for voice and low-throughput data.

4.3.2.1.2 Disadvantages of Analog Signals

- They are prone to electrical interference from outside sources that range from power lines to thunder storms to solar flare-ups from the sun, as well as noise from the telephone network itself.
- On the subscriber line, they can only transmit up to about 1,400 bits of information. Any throughput higher than that is due to signal encoding, including bit compression.
- With the growing use of digital switching, an economic break-even point was reached where it was more cost effective to remove the analog trunks between central offices, as well as their expensive analog-to-digital converters, and go all digital.

- As the cost of digital electronics continued to drop, all-digital facilities became even more economical.
- In voice networks, as the number of Optical fiber facilities grew in the '80s and '90s, analog facilities could no longer compete in throughput, reliability, or service;
- In data networks, analog throughput was quickly surpassed by the much higher rates of digital wire and later Optical fiber facilities.

4.3.2.2 Digital Signals

Digital describes electronic technology that generates, stores, and processes data in terms of two states. Thus, data transmitted or stored with digital technology is expressed as a string of 0's and 1's. Each of these state digits is referred to as a bit.

A bit is the smallest unit of data in a computer. It has a single binary value, either 0 or 1 as shown in Figure 3.4. Although computers usually provide instructions that can test and manipulate bits, they generally are designed to store data and execute instructions in bit multiples called bytes. In most computer systems, there are eight bits in a byte. The value of a bit is usually stored as either above or below a designated level of electrical charge in a single capacitor within a memory device.

Prior to digital technology, electronic transmission was limited to analog technology, which conveys data as electronic signals of varying frequency or amplitude that are added to carrier waves of a given frequency. Broadcast and phone transmission has conventionally used analog technology.

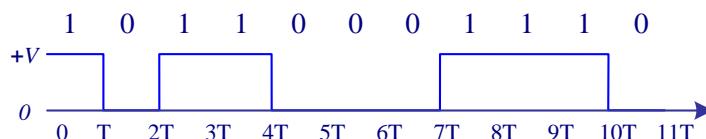


Figure 4.4: Digital Signals

Digital technology is primarily used with new physical communications medium, such as satellite and Optical fiber transmission. A modem is used to convert the digital data in your computer to analog signals for your phone line and to convert analog phone signals to digital data for your computer.

Two new terms, bit interval (instead of period) and bit rate (instead of frequency) are used to describe digital signal. The bit interval is the time required to send one single bit. The bit rate is the number of bit intervals per second. It means that the bit rate is the number of bits sent in one second, usually expressed in bps (bits per second).

Digital transmission offers many key benefits over analog transmission.

- Digital transmission produces fewer errors than analog transmission.
- Digital transmission is more efficient.
- Digital transmission permits higher maximum transmission rates.
- Digital transmission is more secure because it is easier to encrypt.
- Simplicity in multiplexing and signaling.

- Integrating voice, video and data on the same circuit is far simpler with digital transmission.
- Integrated management and control of the entire network.
- Creation of a new era of Intelligent Network (IN) services and signaling systems.



Electric light or electromagnetic encoding of data, signals representing digital data typically varies between two different voltage levels; one represents logical 0 and the other represents logical 1

4.4 Data Transmission

Data can be transmitted through a circuit in the same form they are produced. Data can also be converted from one form into the other for transmission over network circuits. Likewise, it is possible to translate analog voice data into digital form for transmission over digital computer circuits:

4.4.1 Transmission Modes

Data transmission can be classified according to the following transmission factors:

4.4.1.1 Transmission Modes According to Data flow

Techniques used to handle data flow between users are:

4.4.1.1.1 Simplex Transmission

Here data is transmitted in one direction only. No transmission in the opposite direction is possible. Examples are monitoring devices in factories and hospitals television and radio broadcasts. Only one transmission channel is required for this type, as shown in Figure 4.5.

4.4.1.1.2 Half-duplex Transmission

Half-duplex transmission: Transmission takes place in either direction on a circuit. However, transmission is possible only in one direction at a time. Examples: data processing applications two-way radios such as CBs. Only one transmission channel is required for this type, as shown in Figure 4.5.

4.4.1.1.3 Full-duplex Transmission

Data is transmitted in both directions simultaneously. A significant amount of information on both ends of the circuit is required to perform the necessary line control functions. Full-duplex transmission is generally used in computer-to-computer communication. Two-transmission channel is required for this type, as shown in Figure 4.5.

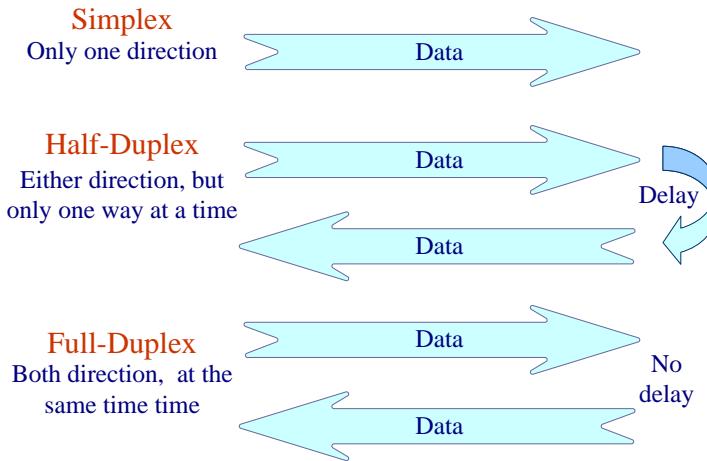


Figure 4.5: Transmission Modes

4.4.1.2 Transmission Modes According to Type of physical connection

Data can be transferred in two modes depending on type of transmission medium and distance:

4.4.1.2.1 Parallel Mode

Data can be transferred in a block of bits as shown in Figure 4.6. Data transfer inside a computer takes place in the parallel mode. In addition to that some computer devices can be connected in parallel to computer when data need to be transferred for high speed and short distance as in parallel printer. However, much of the data transfer outside the computer takes place in a serial mode. Problems with parallel transmission are reliability and distance limitations.

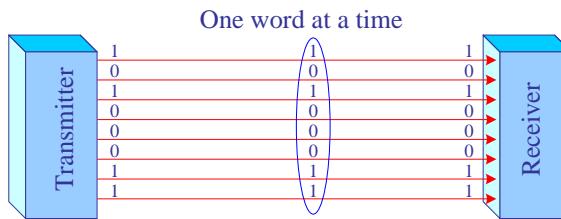


Figure 4.6: Parallel transmission Mode

4.4.1.2.2 Serial Mode

Serial Mode is the predominant method of transferring data by using a serial configuration. In this mode data transmits as a stream of one bit a time as illustrated in Figure 4.7.

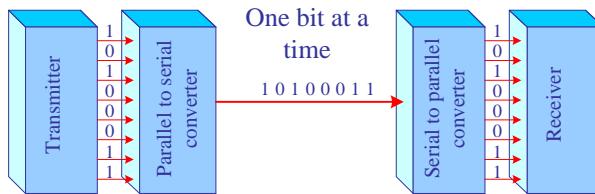


Figure 4.7: Serial transmission Mode

Two types of serial transmission depend on time:

- ❖ **Asynchronous Transmission:** Transmits any time makes it more convenient. It is also called start-stop transmission, because the transmission device can transmit a character any time. Each character is transmitted independently. It uses the start and stop bits for each character. Synchronization at the receiver is done with the help of the start bit. It is cheap and widely implemented with high overhead in terms of start and stop bits. Data in this type is transmitted one frame by a time, where a frame consisting of a character together with synchronization of information as illustrated in Figure 4.8. Meanwhile the receiver can resynchronize its clock at the beginning of each character.

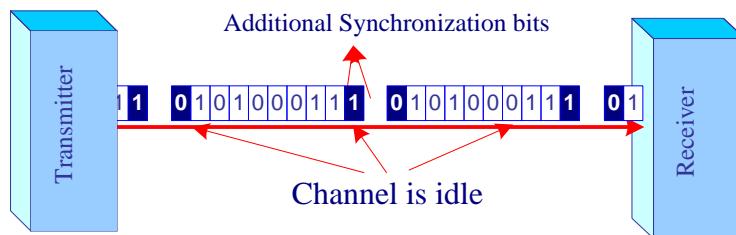


Figure 4.8: Asynchronous Transmission

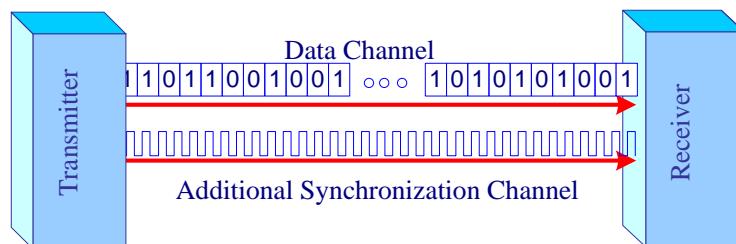


Figure 4.9: Synchronous Transmission

- ❖ **Synchronous Transmission:** It is a high-speed transmission of blocks of data. In this mode, the receiver & transmitter synchronized for a block of data as shown in Figure 4.9. Synchronization is maintained or reestablished while the line is idle. Predetermined group of sync characters are sent, and each block of data contains

sync characters at the beginning (and sometimes at the end) of the block. There are fewer control bits compared to asynchronous and overhead is less than of the asynchronous, but a given pattern of noise can affect more bits. Of course, these errors are detected and corrected. Synchronous transmission can be achieved by using additional synchronization channel which controls the stream between transmitter and receiver.



In Asynchronous connections clocking information needs to be sent as well as the data so that receiving station can synchronize its own clock with the sender's clock.

Synchronous connections use a separate clocking line to transmit clocking information.

4.4.1.3 Transmission Modes According to the Bandwidth Requirements

There are two generic transmission techniques according to bandwidth requirements Baseband and broadband.

4.4.1.3.1 Baseband Transmission

Baseband transmission can be loosely defined as the direct application of the Baseband signal to the transmission medium. The signal has frequency content extending into the direct current region. Baseband data can be transmitted hundreds and even thousands of feet. This is commonly done on wire pair and coaxial cable. Transmission distance is limited because of several factors. The data signal suffers loss due to the length and characteristics of the medium. It can be corrupted by noise, which can often be related to length of the medium. The signal itself will become distorted due to the electrical characteristics of the medium, and distances can be extended by the use of regenerators.

4.4.1.3.1 Broadband Transmission

Broadband transmission is where the Baseband signal from the data device is translated in frequency to a particular band of frequencies in radio-frequency spectrum and applied to a transmission medium. Broadband transmission requires a modem to carry out the translation. Baseband transmission may require some sort of signal conditioning device. With broadband transmission we usually think of simultaneous multiple carriers that are separated in the frequency domain.

Broadband transmission is a method of transmitting data. Modems are required to modulate digital data streams onto the channel. Broadband in this context is used in contrast with Baseband. In simple terms, broadband refers to a multichannel, high-bandwidth transmission line. The most common use of the term today is to refer to a channel capable of high-speed transmission. The term is often used to refer to Internet access via cable modems, DSL, fiber options, and wireless alternatives, all of which are much faster than dialup.

4.5 Transmission Impairments

The main purpose of communication is to be able to send and receive information to any place in no time and error free. In reality hard work must be done to achieve this goal. One of the main difficulties we account for is transmission impairment. Main types of transmission impairments are:

4.5.1 Attenuation

As a signal propagates along a transmission medium line, its amplitude decreases, as shown in Figure 4.10. If a transmission distance exceeds the required limit one or more amplifiers (repeaters) must be inserted to restore signal to its original level.

The signal becomes weaker or degrades as it travels farther from its point of origin. This could be due to the fact that the signal is a digital signal on a cable or the reduction in amplitude of an electrical signal, without the appreciable modification of the waveform. Attenuation is usually measured in decibels. Attenuation of a signal transmitted over a transmission medium is corrected by a repeater or an amplifier. A repeater is used with digital signals to amplify and clean up an incoming signal before sending it farther along the medium. An amplifier boosts an attenuated analog signal back up to its original power level so it can continue to make its way across the network.

Copper cabling has much greater attenuation than fiber-optic cabling; therefore, copper is suitable only for relatively short cable runs.

4.5.2 Dispersion

Signals tend to spread as they travel, with the amount of spreading dependent on the frequency as in Figure 4.10. This type of impairment especially affects Optical fiber cables.

Within a given channel, different wavelengths of signals have different propagation characteristics and therefore travel with different velocities causing a longer temporal pulse at the end of the channel. This variance with wavelength is known as dispersion and can cause pulse broadening. However dispersion does not alter the wavelength (frequency) content of the pulse. From a communications point of view dispersion is a very important factor because it directly affects the bit rate.

4.5.3 Distortion

Transmission medium can cause two types of distortion:

Amplitude Distortion which is caused by the variation of transmission loss with frequency. The effect of non uniform attenuation across the channel on data communications is to distort the received spectrum and, in turn, the data signal waveform. A reasonable amount of amplitude distortion can be tolerated on a voice channel transporting data. Provided that the loss is not actually infinite at any important signal frequency, it is theoretically possible to construct linear compensating networks that equalize amplitude characteristics over the frequency band of interest.

Phase Distortion constitutes the most limiting impairment to data transmission. It results from different velocities of propagation at different frequencies across the channel. A signal takes a finite time to traverse the telecommunications network end-to-end. If two tones are keyed exactly at the same time at the near end, one at 400 Hz and one at 1800 Hz, the 1800-Hz tone will arrive at the far end before the 400-Hz tone. We can say that the 400-Hz tone was delayed relative to the 1800-Hz tone. Thus we have come to use the term **delay distortion**.

Delay distortion is critical in particular for digital data, because signal components of bit positions spill into other bit positions, and so limiting the allowed rate of transmission. Figure 4.10 illustrate the effect of delay distortion.

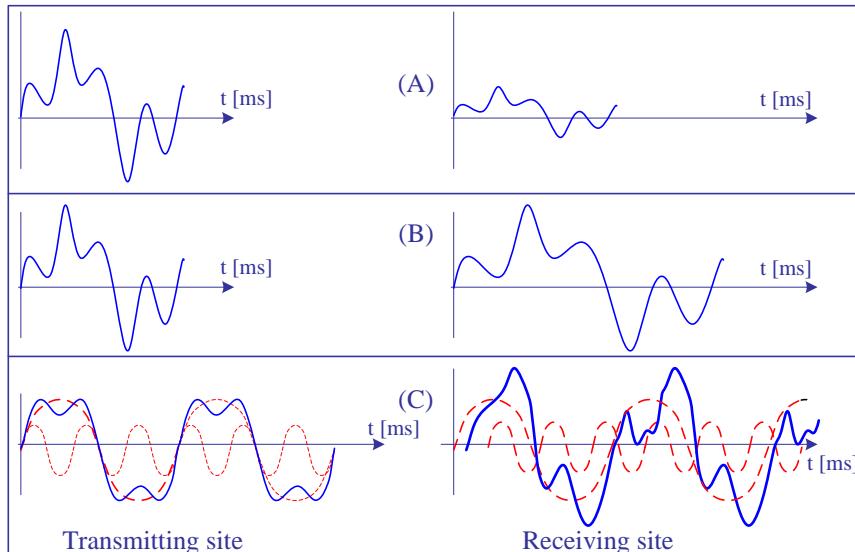


Figure 4.10: (A) Attenuation, (B) Dispersion, and(C) Delay Distortion

4.5.4 Noise

In the absence of signal being transmitted, channel will ideally have zero electrical signals presented, but in practice there is a random noise present on the line even when no signal is transmitted, as illustrated in Figure 4.11.

Noise sources may be divided into four categories: Thermal noise, Intermodulation noise, Crosstalk, and impulse noise.

4.5.4.1 Thermal Noise

Thermal noise is caused by thermal agitation of electrons in conductors. It is presented in all electronic devices a transmission medium and is considered as a function of the temperature. It is often referred to as white noise, because it affects uniformly the different frequencies. Thermal noise cannot be eliminated and therefore places an upper bound on communications systems performance.

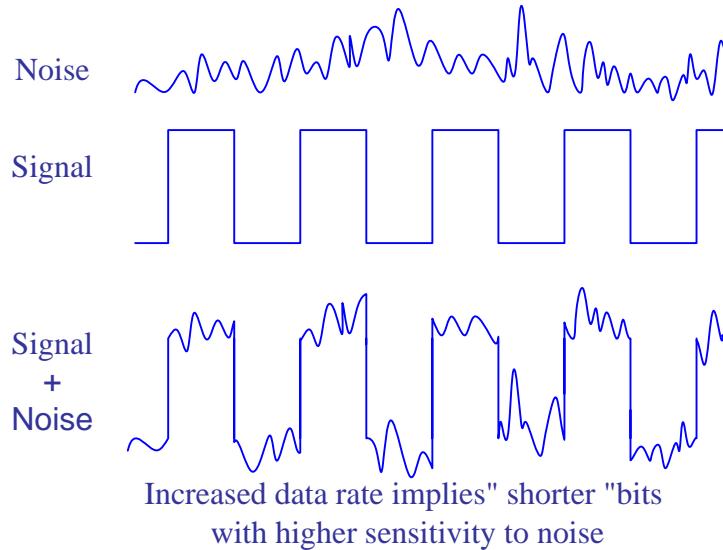


Figure 4.11: Signal with noise

4.5.4.2 Intermodulation Noise

Intermodulation noise results from the interference of different frequencies sharing the same medium. It is caused by a component malfunction or the use of a signal with excessive strength.

For example, the mixing of signals at frequencies f_1 and f_2 might produce energy at the frequency $f_1 + f_2$. This derived signal could interfere with an intended signal at frequency $f_1 + f_2$.

4.5.4.3 Crosstalk

Crosstalk is an unwanted coupling between signal paths. It occurs in neighboring channels when a foreign signal enters the path of the transmitted signal due to electromagnetic interferences.

In crosstalk one line induces a signal into another line as in Figure 4.12. In voice communications, we often hear this as another conversation going on in the background. In digital communication, this can cause severe disruption of the data transfer. Cross talk can be caused by the overlapping of bands in a multiplexed system, or by poor shielding of cables running close to one another. There are no specific communications standards that are applied to the measurement of crosstalk.

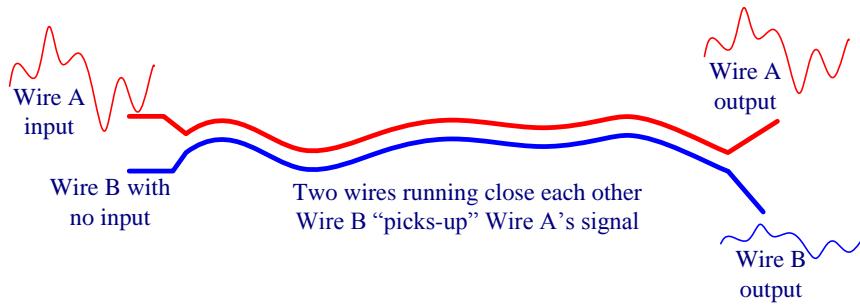


Figure 4.12: Crosstalk Noise

4.5.4.4 Impulse Noise

Impulse noise is usually caused, by irregular disturbances, such as lightning, running machines and flawed communication elements. It is a primary source of error in digital data. For example, a sharp spike of energy of a .01 second duration would not destroy any voice data, but would wash out about (96) bits of digital data being transmitted at 9600 bps.



The presence of noise or other types of impairments leads to the use of amplifiers and repeaters.

An amplifier is an analog device that simply boosts the power level of a signal.

A repeater is a digital device that interprets an incoming signal, then regenerates or reconstructs it - i.e. it makes a new copy that is a faithful reproduction of the original in every way.

4.6 Data Channel Characteristics

Data channels are characterized by their capacity, available bandwidth, transmission rate, signal to noise ratio (SNR), error probability and efficiency.

4.6.1 Channel Capacity

The capacity of a channel (transmission medium) is the maximum data rate measured in bits per second (bps). If the channel is noise free, then the maximum data rate depends on the bandwidth of the channel and encoding levels are used. This relationship is given by Nyquist's formula.

$$C = 2W \log_2 M$$

Where,

- C = Bits per second
- W = Bandwidth in Hertz
- M = Number of encoding levels in the signal

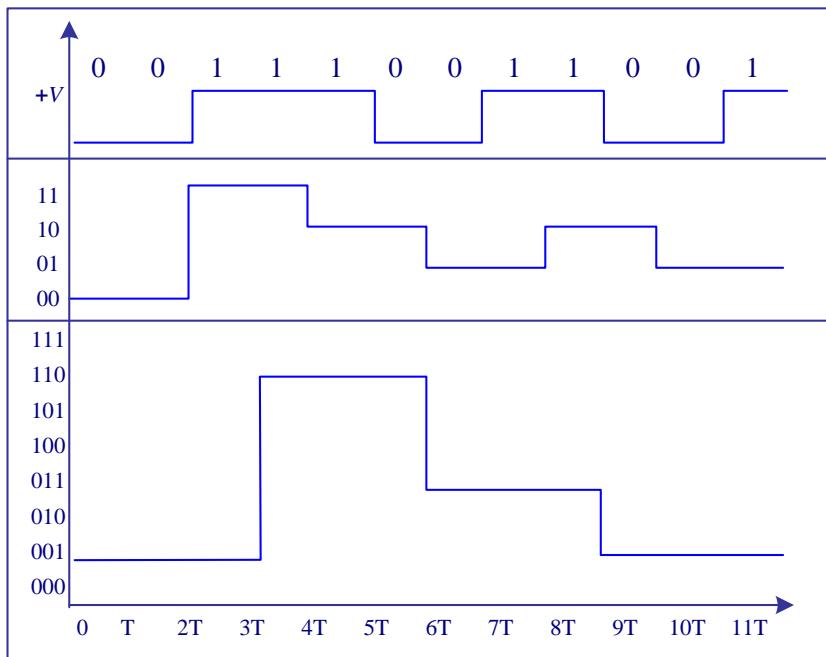


Figure 4.13: Bi-level, Four-levels and Eight-levels Digital Signals

Example:

A 5 kHz channel with Bi-level binary signals can transmit at most 10,000 bps

A 5 kHz channel with four-level binary signals can transmit at most 20,000 bps

A 5 kHz channel with Eight-level binary signals can transmit at most 30,000 bps

If the noise level of the channel is known, then we can use the Shannon formula to calculate the capacity. Note that both formulas ignore other channel impairments. Therefore what can be achieved in practice is always less than what is predicted by these formulas.

Shannon formula implies that channel capacity is limited by two things:

1. Available bandwidth or data rate: Limitations arise from the physical properties of the transmission medium and from deliberate limitations at the transmitter to prevent interference from other resources.
2. Signal to noise ratio (SNR) which is the ratio of the power in a signal to the power contained in the noise that is presented at a particular point in the transmission.



Typically SNR is measured at the receiver, because it is the point where the noise is to be removed from the signal. (SNR) is measured by decibels (dB) by the following formula:

$$SNR = 10 \log (\text{Signal Power}/\text{Noise Power}) [\text{dB}]$$

The channel capacity can be calculated using Shannon's formula:

$$C = 2W \log_2(1 + S/N)$$

Where,

- S = signal power in watts
- N = Thermal noise in watts
- W = Bandwidth in Hertz



Shannon's formula calculates the theoretical maximum capacity that can be achieved. Actual capacity will be much lower because this formula assumes thermal noise only.

4.6.2 Efficiency

Efficiency of a digital transmission is measured by the ratio of (C/W), which is the bps per hertz that is achieved.

Example

For public telephone wire and by assuming thermal noise only:

Bandwidth = 3100 Hz

Typical SNR = 30 dB

$$\text{SNR} = 10 \log_{10} (\text{S/N})$$

$$30 = 10 \log_{10} (\text{S/N})$$

$$\text{S/N} = 1000$$

$$\text{Capacity} = 3100 \log_2 (1 + 1000)$$

$$= 30,894 \text{ bps}$$

$$\text{Line efficiency} = C / W = 30,894 / 3100 = 9.966 \text{ bps/hertz.}$$

Successful transmission of data across a communication medium requires cooperation between the sending and the receiving device, a high level of synchronization between the receiver and sender, the receiver must know when each bit begins and ends so that it can keep pace with the transmitter.

4.6.3 Transmission Rate

4.6.3.1 Baud Rate (Modulation rate)

Is the circuit-signaling rate, which is the number of times per second that the signal on the circuit changes, whether in amplitude, frequency or phase? If signal is changed 1000 per second, it is said to be signaling at 1000 baud.

4.6.3.2 Circuit Speed (Data signaling rate)

It is the number of bits the circuit can carry in one second. It is measured in bits per second (bps). Bits per second and baud are not always the same. The two measures approximate each other only when one bit is sent with each signal. It is now possible to send two or more bits per signal. At a signaling rate of 2400 baud it is possible to send 2400, 4800, 7200, 9600 bits per second.



Baud is the number of signal intervals, or pulses, that are transmitted per second. **Baud** characterizes the carrier signal.

Bps stands for **b**its **p**er **s**econd. Bps is a measure of how many bits can be transmitted during one pulse (one baud). Each symbol may carry one or more (or even less) data bits, depending on the modulation technique so,
 $\text{bps} = \text{baud} * \text{number of bits per baud.}$

4.6.4 Bit Error Rate

The most common measure of data connectivity's performance is error rate. Transmission impairments are random and affect bits at random locations. The way we characterize a channel with respect to its impairment effect is by the probability of error, called *bit error rate (BER)*. For example, if the BER for a link is 2.10^{-6} , then, on the average, two out of every 10^6 bits could be expected in error. This does not say which bit number could be in error, or whether there is always an error for each of the 10^6 bit strings. Protocols for error control are designed based on these probabilities. We will return to error detection and correction in details in the later chapters.

4.6.5 Data Transmission Channels

The type of signal used to transmit data sent from one point to another. It can be either analog or digital and may represent either analog or digital data. It is possible to convert information from analog into digital form and back again without losing details. There are four possible combinations depicted in Figures 4.14, each of them represents one type of data transmission channels. We can list these combinations as follows:

- Digital transmission of digital Data
- Analog Transmission of Digital Data
- Digital Transmission of Analog Data
- Analog Transmission of Analog Data

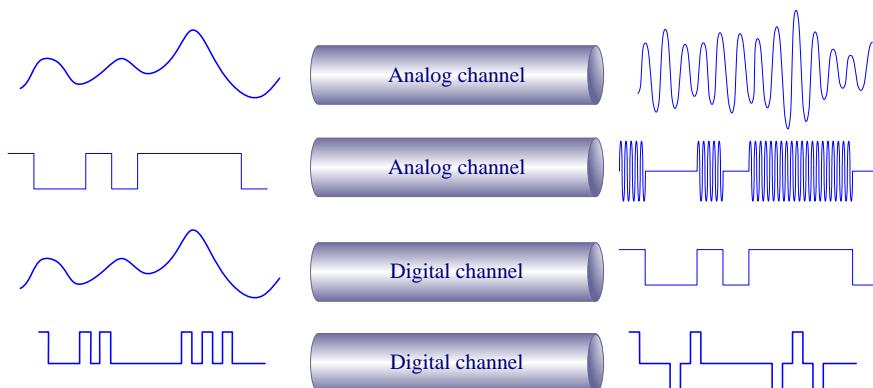


Figure 4.14: Digital and Analog Transmission Channels

In the rest of this chapter we will examine the techniques involved in each of these four combinations.

4.7 Digital Transmission of Digital Data

Digital signals are commonly referred to as **Baseband signals**. In order to successfully send and receive a Baseband signals message, both the sender and receiver have to agree how often the sender can transmit data (data rate) and how to represent the binary data (line coding).

4.7.1 Purposes of Line Coding

Line coding is the process of arranging symbols that represent binary data in a particular pattern for transmission. It is the process of converting binary data (text, numbers, graphical images, audio and video that are stored in computer memory) to a digital signal.

Below is a list of some important factors, which can improve encoding:

- To correctly interpret the signals received from the sender, the receiver's bit intervals must correspond exactly to the sender's bit intervals. If the receiver clock is faster or slower, the bit intervals are not matched and the receiver might interpret the signals differently than the sender has intended. Self synchronization is one of the characteristics of line coding.
- Interference and distortion can be reduced by
 - Avoiding direct current (dc) components
 - Concentrating the transmission power at the center of the bandwidth
- Bit error rate increases with: Data rate, and (noise strength) to (signal strength) ratio. Data rate can be increased with: Bandwidth and Encoding



A self synchronization digital signal includes timing information in the data being transmitted. This can be achieved if there are transitions in the signal that alert the receiver to the beginning, middle or end of the pulse. If the receiver's clock is out of synchronization, these alerting points can reset the clock.

4.7.2 General Classification of Line Coding

The most common types of line coding used include non-return-to-zero (NRZ), return-to-zero (RZ), and bi-phase, or Manchester. Figure 4.15 illustrates NRZ, RZ, and bi-phase encoding.

4.7.2.1 Non-Return-To-Zero (NRZ)

NRZ code represents binary 1s and 0s by two different voltage levels that are constant during bit duration. The presence of a high voltage level signal in the bit duration represents a binary 1, while a low level signal represents a binary 0. NRZ codes make the

most efficient use of system bandwidth. However, when there are long runs of bits that are the same, there are no *voltage level transitions*, making it difficult for the receiving station to know if it is **clocking** the signal correctly and so deducing the correct number of bits.

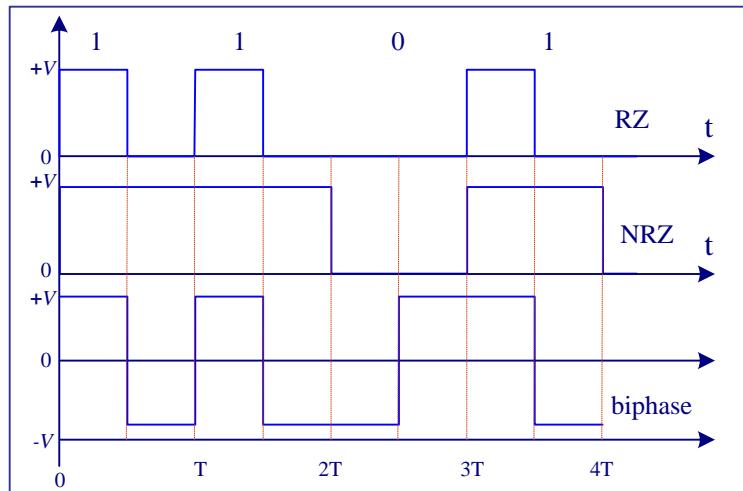


Figure 4.15: The most common types of line coding

4.7.2.2 Return-To-Zero (RZ)

In RZ encoding, a half period of pulse present in the first half of the bit duration represents a binary 1, while the voltage level returns to zero during the second half. A binary 0 is represented by the absence of a pulse during the entire bit duration. Because RZ coding uses only half the bit duration for data transmission, it requires twice the bandwidth of NRZ coding. Loss of timing can occur if long strings of 0s are present.

4.7.2.3 Bi-phase Encoding

Bi-phase, (Manchester), encoding incorporates a transition into each bit period to maintain timing information. In biphase encoding, a high-to-low voltage level transition occurring in the middle of the bit duration represents a binary 1. A low-to-high voltage level transition occurring in the middle of the bit duration represents a binary 0.

4.7.3 Signaling Techniques

Depending on the type of voltage being used, signaling can be classified as:

4.7.3.1 Polar Signaling

With polar signaling we use a positive and negative voltage to represent 0s and 1s, as shown in Figure 4.16. A separate clock signal is used to keep sender and receiver synchronized. This technique is fairly resistant to interference because of the great voltage distance between 1 and 0 signals.

4.7.3.2 Unipolar Signaling

With Unipolar signaling technique, the voltage is always positive or negative (like a dc current). Because of low voltage variance, unipolar systems are more given to interference problems. Most use separate clocking signals as polar systems because long streams of 0s and 1s may be confusing if clocks are not exactly synchronized at sender and receiver. Figure 4.16 illustrates unipolar signaling.

4.7.3.3 Bipolar

In bipolar signaling, the 1's and 0's vary from a plus voltage to a minus voltage (like an ac current) as shown in Figure 4.16. In general bipolar signaling experiences fewer errors than unipolar signaling because the signals are more distinct.

4.7.3.4 Multi-Level Signaling

Multi-level signaling can be used to increase the data rate. Returning to example in Figure 4.13, where each sequence of 2 data bits is encoded into four-level pulses for transmission. At the receiving end decoding is carried out and the original bits, 2 for each received symbol, are regenerated. Note that the symbol rate on the line is half of the bit rate seen by the data source and the destination and thus the required bandwidth of the channel is reduced to half compared to binary transmission.

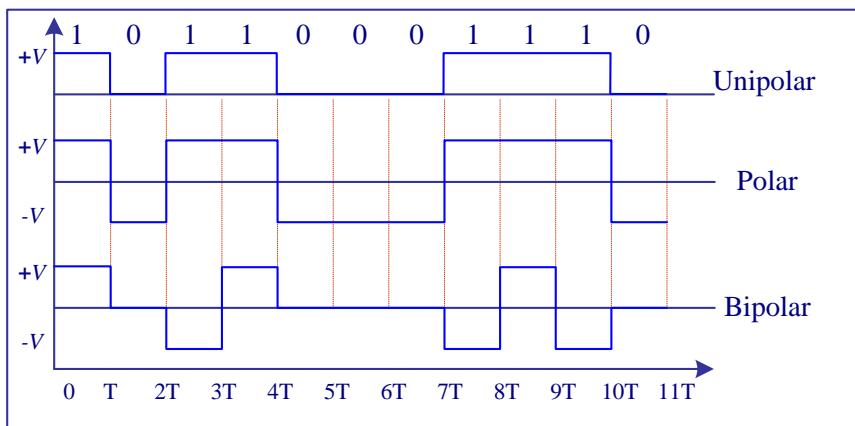


Figure 4.16: Signaling Technique



Increasing the number of levels (M) multi-level signaling increases the data rate (k) times where:

$$k = \log_2(M)$$

4.7.4 Types of Line Codes

Techniques used to convert digital data, to digital signal are:

4.7.4.1 Nonreturn-to-Zero-Level (NRZ) Signal Encoding

Transmit digital signals by using two different levels for the two binary digits. Codes that follow this technique share the property that the voltage level is constant during a bit interval. Two techniques of NRZ can be used:

4.7.4.1.1 Nonreturn-to-Zero-Level (NRZ-L)

This code is represented binary (0) for high level, and binary (1) for low level as shown in Figure 4.17.

Characteristics

- Easy to engineer
- Make efficient use of bandwidth
- Suffers from the presence of dc component
- Lack of synchronization capabilities due to potential of long runs of unchanged voltage levels.
- Attractive for digital magnetic recording, but not for signal transmissions.

4.7.4.1.1 Nonreturn-to-Zero-Inverted (NRZ-I)

NRZI is a differential encoding in which the signal is decoded by comparing the polarity of adjacent signal levels: Binary (1) encoded by transition between levels and 0 encoded by a lack of transition as shown in Figure 4.17. Similar advantages and disadvantages as NRZ-L.

4.7.3.2 Bipolar AMI Signal Encoding

A **multilevel binary** approach in which binary 0 is represented by a lack of pulse, and a binary 1 is represented by a positive or a negative pulse as shown in Figure 4.17. The binary 1 pulse must alternate in polarity. AMI stands for alternate mark inversion, whereas mark and space historical references to binary digits 1 and 0.

Characteristics

- Each 1 introduces a transition that can be used for synchronization
- Error detection is possible for a single added or lost pulse.
- Since 1 signal alternate in voltage, there is no dc component.
- Bandwidth considerable smaller than in the NRZ encoding.
- Long runs of 0's don't allow synchronization.

4.7.4.3 Manchester Signal Encoding

Manchester encoding is a **biphase** encoding in which the transition takes place in the middle of the bit period: a low-to-high transition for 1, and a high-to-low transition for 0.

Characteristics

- Allows for clocking mechanism for both kinds of bits.
- Modulation rate twice than that of NRZ, implying a greater bandwidth
- There is no dc component and the bandwidth is relatively narrow
- Noise on the line has to invert the signal before and after the inverted bit to avoid detection.

- Has been specified for the IEEE 802.3 standard for Baseband coaxial cable and twisted-pair CSMA/CD bus LAN's.
- Require high signaling rate relative to data rate, making it too costly for long-distance applications.

4.7.4.4 Differential Manchester

A **biphase** encoding in which transition at the start of the bit period represents 0, and a lack of transition at the start of the bit represents 1. In addition, a transition occurs at the middle of each bit period just for the purpose of clocking. It has been specified for the IEEE 802.5 token ring LAN, using shielded twisted pair.



One purpose of line coding is to make the form of the spectrum of a digital signal suitable for a certain communication medium.

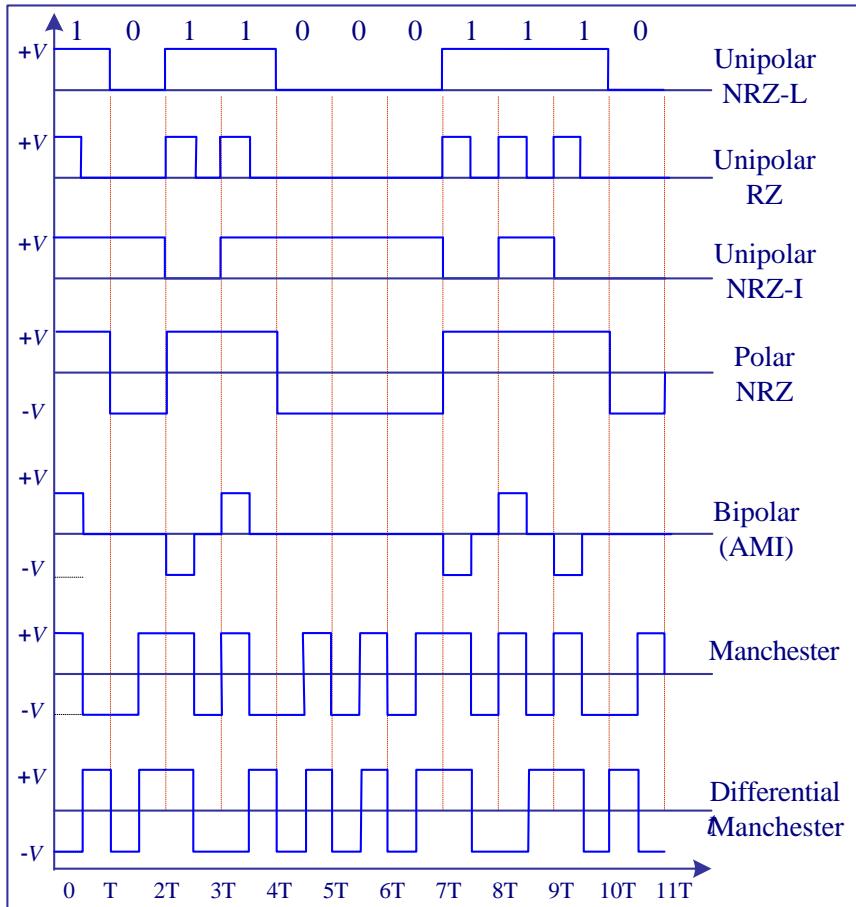


Figure 4.17: Different Encoding Techniques

4.7.5 Some Intermediate Encoding Techniques

In some situations we need to design a data pattern in that manner to ensure that at least one voltage level transition occurs for every n bits of data especially in a high speed transmission medium, prior to applying the final line coding. In networking there are many techniques used to achieve that intermediate encoding. The most popular of them are:

4.7.5.1 4B/5B Encoding

In this method every group of 4 bits is replaced by a 5-bit code in that manner to ensure that at least one voltage level transition occurs for every 5 bits. The codes are shown below:

4-bit Nibble	5-bit Code						
0000	11110	0100	01010	1000	10010	1100	11010
0001	01001	0101	01011	1001	10011	1101	11011
0010	10100	0110	01110	1010	10110	1110	11100
0011	10101	0111	01111	1011	10111	1111	11101

As an example of 4B/5B encoding, let's encode the data stream **0111010000100000**. As shown below, the data is first grouped into 4-bit nibbles. Then a 5-bit code is applied to each separate 4-bit group.

Data stream:	0111010000100000
4B/5B stream:	01111010101010011110

After applying a 4B/5B encoding method to a data stream, the physical layer then applies NRZ-I or another line coding method depending on the transmission medium.

4.7.5.2 5B/6B Encoding

Same idea as 4B/5B but you can have DC balance (3 zero bits and 3 one bits in each group of 6) to prevent polarisation. 5B/6B Encoding is the process of encoding the scrambled 5-bit data patterns into predetermined 6-bit symbols. This creates a balanced data pattern, containing equal numbers of 0's and 1's, to provide guaranteed clock transitions synchronization for receiver circuitry, as well as an even power value on the line.

For 100VG-AnyLAN for instance, the clock rate on each wire is 30MHz, therefore 30Mbits per second are transmitted on each pair giving a total data rate of 120Mbits/sec. Since each 6-bits of data on the line represents 5 bits of real data due to the 5B/6B encoding, the rate of real data being transmitted is 25Mbits/sec on each pair, giving a total rate of real data of 100Mbits/sec. For 2-pair STP and fiber, the data rate is 120Mbits/sec on the transmitting pair, for a real data transmission rate of 100Mbits/sec.

4.7.5.3 8B10B Encoding

This type of encoding is designed to be used in very fast data transmission over Optical fiber cables i.e. Gigabit Ethernet. The 8B10B encoding method is similar to 4B5B in that a group of bits are replaced with code words. The difference is that with 8B10B, each group of 8 bits is replaced with a 10-bit code word. The use of 10 bits for each 8 bits

of data drops the data rate speed relative to the line speed, for instance in order to gain a data rate of 1Gbps the line speed has to be $10/8 \times 1 = 1.25\text{Gbps}$.

The 8B10B encoding eliminates any possibility of long sequences of 1's or 0's and also eliminates DC bias, so the signal is first encoded using 8B10B and then the simple NRZ encoding method is applied after.

4.7.5.4 8B/6T Encoding

The incoming data stream is split into 8-bit patterns. Each 8-bit data pattern with two voltage levels 0 volts and V volts is examined. This 8-bit pattern is then converted into a 6-bit pattern but using three voltage levels -V, 0 and V volts, so each 8-bit pattern has a unique 6T code. For example the bit pattern 0000 0000 (8B) uses the code +00+ and 0000 1110 (8B) uses the code -+0-0+, where + represents a positive pulse and - represents a negative pulse. The rules for the symbols are that there must be at least two voltage transitions (to maintain clock synchronization) and the average DC voltage must be zero which stops any polarisation on the cable. The carrier just needs to be running at 3/4 of the speed of the data rate.



The systems that use only line coding, but not modulation, are called Baseband transmission systems. The spectrum of the line signal is still in the frequency range of the original message's "Baseband." In radio systems both coding and modulation are used.

4.8 Analog Transmission of Digital Signal

Analog Transmission occurs when the signal sent over the transmission medium continuously varies from one state to another in a wave-like pattern.

In a modulation process, the amplitude, phase, or frequency of a carrier signal varies with the variations of a digital information signal.

Perhaps the most common device associated with signal conversion today is the modem. We need modems for the transmission of digital messages over analog channels. The modems receive a message from the terminal in the form of binary data and send it as an analog waveform to the speech channel as shown in Figure 4.18. Current modems do not modulate or change the analog waveform at the rate of the binary data they receive from the terminal.

Instead they encode a set of bits into a digital symbol that may get many more values than just two. Each multilevel symbol corresponds to a set of bits and it is sent as one analog waveform to the line. When receiving a certain analog signal on the other end, the receiver detects a set of bits defined to correspond to that signal. Use of more than two signals increases the data rate through the speech channel compared with the binary principle, in which only two different signals are used. Speech channels have quite a narrow bandwidth, but a good S/N, which allows use of many different signals.

 A modem receives digital data and converts to an analog form for transmission over a medium, most typically a phone line. Modem is a shortened form of MOdulator-DEModulator, which means that the device is involved in both creating analog signals from digital data and changing analog signal back to digital data (demodulating)

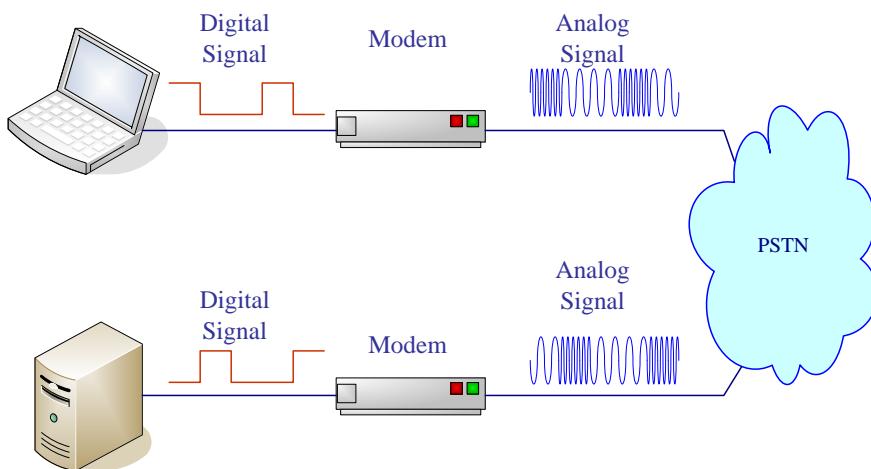


Figure 4.18: Modem connects DTE to analog networks

1. A modem receives its signal from a computer, also known as a DTE (Digital Terminal Equipment).
2. The digital signal is used to modulate an analog carrier signal by any of the shift keying techniques, as we will see below.
3. The analog signal travels over telephone lines or another medium.
4. The analog data is detected by another modem, which receives and decodes the data on the analog signal.
5. A digital signal is generated by the modem and transmitted to the DTE.

Modems are not limited to telephone line use. As mentioned above, other mediums can be used to carry the analog data generated by a modem as well. Broadband LANs utilize modems to allow several different types of data to share the same piece of cable. Each discrete type of data, whether it is computer data, video, or audio may share the cable because each type of data is transmitted using its own unique frequency.

Depending on the nature and objective of a modem, the following schemes can be used:

- Amplitude shift keying (ASK)
- Frequency shift keying (FSK)
- Phase shift keying (PSK)
- Quadrature amplitude modulation (QAM)



Modems may be used to carry data on broadband LANs in specific frequencies. Modems utilized for broadband networks are very high-speed modems.

4.8.1 Amplitude-Shift Keying (ASK)

In amplitude modulation two or more different amplitudes of the carrier frequency represent two or more binary values. Number of binary digits for each segment depends on the number of different frequencies being used. The ASK techniques are used to transmit digital data over a digital carrier. The resulting signal is:

$$S(t) = A_i \cos(2\pi f_c t)$$

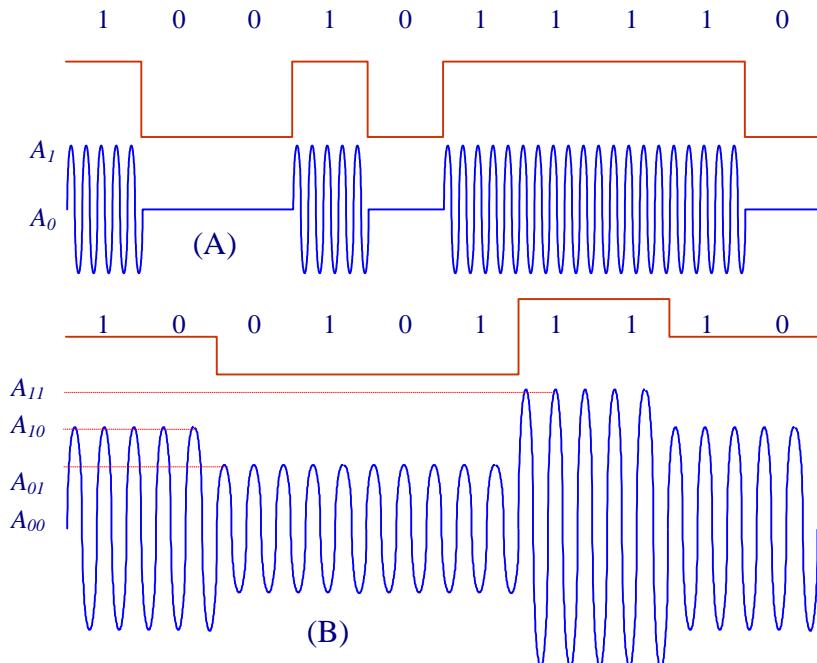


Figure 4.19: Amplitude Shift Keying: (A) Data density one bit, (B) (Data density 2 bits)

Where,

f_c = carrier frequency

t = Time

A_i = Amplitude, i depends on the number of bits as shown in Figure 4.19.

4.8.2 Frequency-Shift Keying (FSK)

The FSK techniques are less susceptible to error than ASK. Two or more binary values are represented by two or more different frequencies near the carrier frequency. On voice-grade lines, it is typically used up to 1200 bps. Commonly used for high-frequency

(3 to 30 MHz) radio transmission. It can also be used at even higher frequencies on local area networks that use coaxial cable. The resulting signal is:

$$S(t) = A \cos(2\pi(f_c + \delta_i)t)$$

Where:

δ_i = Frequency,

i depends on the number of bits.

Frequencies centered on 1200 Hz and 2200 Hz may be used for representing binary digits through frequency shifts of 100 Hz. Figure 4.20 illustrates frequency modulation for one bit data density by using two different frequencies.

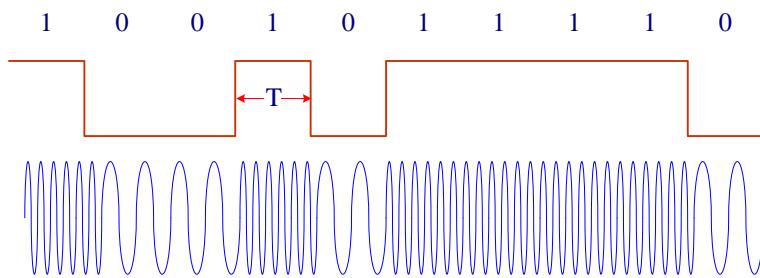


Figure 4.20: Frequency modulation (Data density 1 bit)

4.8.3 Phase-Shift Keying (PSK)

The phase of the carrier signal is shifted to represent data. The binary 0 is represented by sending a signal burst of the same phase as the previous signal burst. The binary 1 is represented by sending a signal burst of opposite phase to the preceding one; and known as differential PSK, as the phase shift is with reference to the previous bit transmitted rather than to some constant reference signal. The resulting signal is:

$$S(t) = A \cos(2\pi f_c t + \alpha_i)$$

Where:

α_i = Phase

i depends of number of bits

A two-phase system may use a shift in phase to represent the digit, 1 and no shift in phase to represent the digit 0 as shown in the following formula and Figure 4.21.

4.8.4 Multi level Sift Keying

It is possible for each modulated pulse to represent k bits instead of one bit. If the number of amplitude values used in ASK for example is M , then each carrier signal interval could be used to represent k bits of data. The bit rate is k times the baud rate in this case, and this type of modulation is M-ASK. If the number of frequencies or the number of phases values used in FSK or PSK is M , then each carrier signal interval could be used to

represent k bits of data too. The bit rate is k times the baud rate in this case, and this type of modulation is M-FSK and M-PSK respectively.

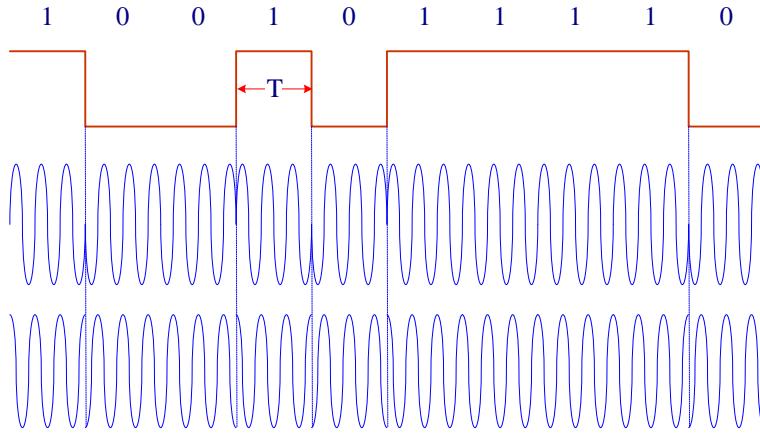


Figure 4.21: Phase modulation (Data density 1 bit)

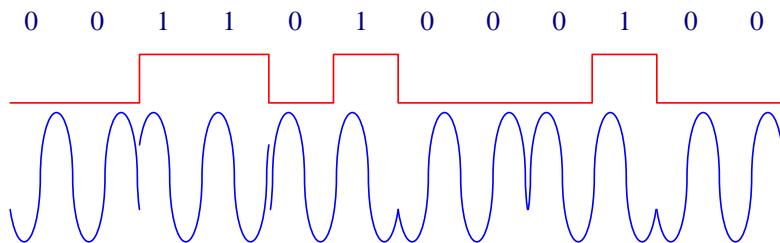


Figure 4.22: Phase modulation (Data density 2 bits)

Another type of multi level shift keying is quadrature phase-shift keying (QPSK) which represents two bits as shown in the following formula and Figure 4.22.

$$S(t) = \begin{cases} A \cos(2\pi f_c t + 45) & \text{for } 11 \\ A \cos(2\pi f_c t + 135) & \text{for } 10 \\ A \cos(2\pi f_c t + 225) & \text{for } 00 \\ A \cos(2\pi f_c t + 315) & \text{for } 01 \end{cases}$$

As more different phase shifts and magnitudes levels are used the more bits of information can be incorporated into each point or symbol. The problem arises when the phases are so close together so that it is impossible for the receiving end to distinguish from one point to the next due to noise on the line.

4.8.5 Quadrature Amplitude Modulation (QAM)

QAM is a special form of multi level shift keying where both the amplitude and phase of carrier signal are modulated, yielding a higher spectral efficiency than binary digital modulation and thus providing more bits per second using the same channel. The

number of levels of amplitude and the number of phase angles are a function of line quality. Cleaner lines translate into more spectral efficiency or more bits per Hertz.

4.9 Digital Transmission of Analog Data

A digital signal can be transmitted over a dedicated connection between two or more users. In order to transmit analog data, it must first be converted into a digital form. These processes are called sampling and encoding. Sampling involves two steps:

- Sample the analog data: by sampling at more than twice the frequency of any component of the analog signal, we capture all of the data in the signal [this is completely reversible].
- Quantized the sample: for each sample value, approximate this by some digital number [quantizing error or quantizing noise therefore irreversible]

The communication process of sampling and quantizing analog signals (pulses) is known as pulse amplitude modulation (PAM).

4.9.1 Sampling

The amplitude of a signal is measured at regular intervals. The interval is designated as Δt , and is called the sample interval. The sample interval must be chosen to be short enough that the signal does not change greatly between measurements. The sampling rate, which is the inverse of the sample interval, should be greater than twice the highest frequency component of the signal, which is being sampled. This sample rate is known as the Nyquist frequency. If you sample at a lower rate, you run the risk of missing some information, known as aliasing. Figure 4.23 illustrated digital sampling.

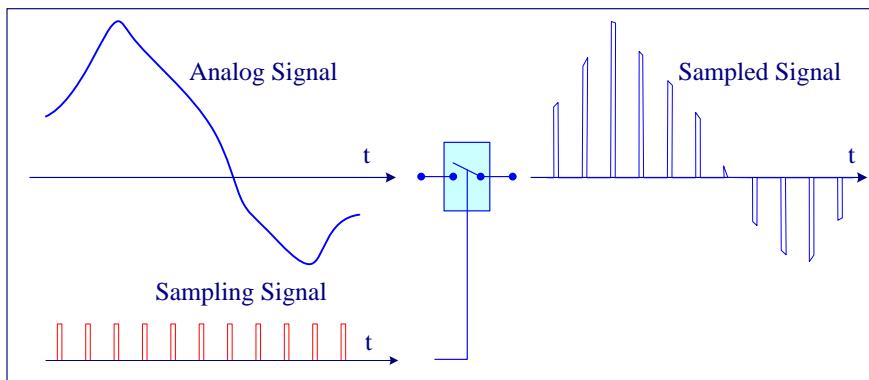


Figure 4.23: Signal sampling

4.9.2 Encoding

Once the samples are obtained as shown in Figure 5.18 and quantized, they must be encoded into binary as shown in Figure 4.24. For a given number of bits, each sample may take on only a finite number of values. These limits the resolution of the sample. If more bits are used for each sample, then a higher degree of resolution is obtained. For example, if the sampling is 8-bit, each sample may only take on 256 different values. 16-bit

sampling would give 65,536 unique values for the signal in each sample interval. Higher bit sampling requires more storage for data and requires more bandwidth to transmit.

The communication process of coding signals with binary codes to carry the information is known as pulse code modulation (PCM)

The fidelity of this modulation scheme depends upon the number of bits used to represent the amplitude. The frequency range that can be represented through PCM modulation depends upon the sample rate. To prevent "aliasing", the sample rate must be at least twice that of the highest supported frequency.

A device used to convert analog signals into a digital form is Analog to Digital Converter (ADC) and the device used to convert Digital signals into analog is Digital to Analog Converter (DAC).

To digitize a voice signal for example, 8000 samples per second are taken. These 8000 samples are then transmitted as a serial stream of 0s and 1s. Eight bits per sample times 8000 samples, requires a 64000 bps transmission rate.

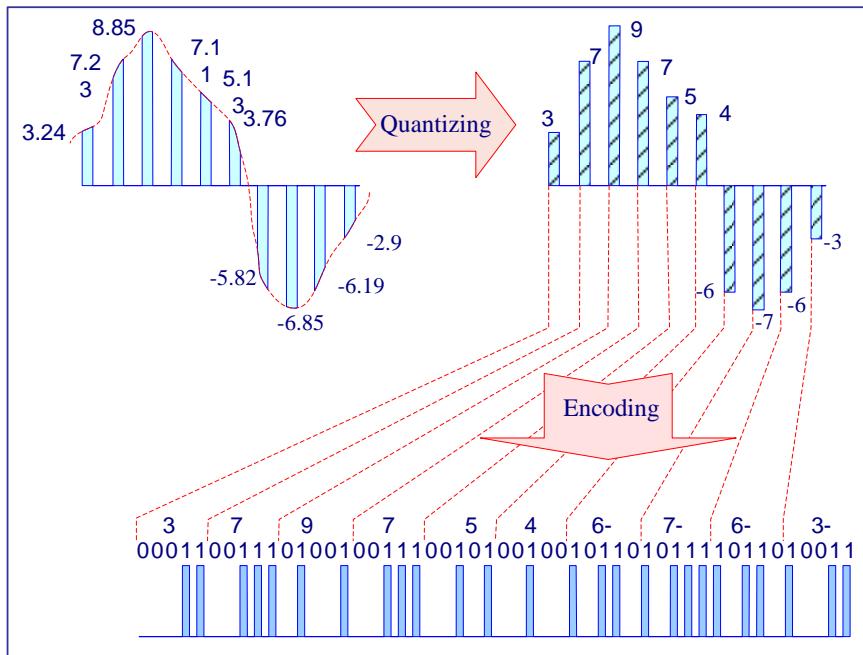


Figure 4.24 Digital Encoding

Audio compact disk stores analog information (music) as a digital signal. The amplitude of the music is sampled at a high rate, about 41,000 samples/sec. The highest frequency component in any audio signal is 20 kHz. Therefore the Nyquist rate is 40 kHz, which explains the reason for a sampling rate of 41,000 samples/sec.



Analog-to-digital conversion (A/D): An analog signal is sampled at the sampling frequency and the sample values are then represented as numerical values by the encoder.

Digital-to-analog conversion (D/A): The decoder receives numerical values of the samples that indicate the values of the analog signal at sampling instants. The sample pulses that have amplitudes corresponding to the values of the original signal at sampling instants are reconstructed to produce an analog signal close to the original one.

4.10 Analog Transmission of Analog Data

Information which is analog in its native form (voice and image) can vary continuously in terms of intensity (volume or brightness) and frequency (tone or color). Those variations in the native information stream are translated in an analog electrical network into variations in the amplitude and frequency of the carrier signal. In other words, the carrier signal is *modulated* (varied) in order to create an analog of the original information stream.

Carrier can be varied in amplitude at a fixed frequency, using Amplitude Modulation (AM). Alternatively, the frequency of the sine wave can be varied at constant amplitude, using Frequency Modulation (FM). Finally, the position of the sine wave can appear to be manipulated, adding the third technique of *Phase Modulation*.

In this section we will discuss analog modulation of analog signal. This technique is needed for two reasons:

- Transmission medium may need to use a higher frequency than that used by the data (such as voice)
- Modulation permits frequency-division multiplexing.

There are different modes of analog modulation of an analog signal:

4.10.1 Amplitude Modulation (AM)

In amplitude modulation, the strength (amplitude) of the carrier from a transmitter is varied according to how a modulating signal varies.

When you speak into the microphone of an AM transmitter, the microphone converts your voice into a varying voltage. This voltage is amplified and then used to vary the strength of the transmitter's output. Amplitude modulation adds power to the carrier, with the amount added depending on the strength of the modulating voltage. Amplitude modulation results in three separate frequencies being transmitted: the original carrier frequency, a lower sideband (LSB) below the carrier frequency, and an upper sideband (USB) above the carrier frequency. That's why AM modulation is called also **double-sideband transmitted carrier (DSBTC)**.

The sidebands are "mirror images" of each other and contain the same information. When an AM signal is received, these frequencies are combined to produce the sounds you hear as shown in Figure 4.26.

Each sideband occupies as much frequency space as the highest audio frequency being transmitted. If the highest audio frequency being transmitted is 5 kHz, then the total frequency space occupied by an AM signal will be 10 kHz (the carrier occupies negligible frequency space).

AM has the advantages of being easy to produce in a transmitter and AM receivers are simple in design. Its main disadvantage is its inefficiency. About two-thirds of an AM signal's power is concentrated in the carrier, which contains no information. One-third of the power is in the sidebands, which contain the signal's information.

While about two-thirds of an AM signal's power is concentrated in the carrier, which is essentially "wasted.", we can suppress the carrier prior to transmit the modulated signal. The modulation technique used to produce an AM signal in this case is named **Double Sideband-Suppressed Carrier (DSB-SC)**. Figure 4.26 illustrates the frequency presentation of this type of modulation.

Since the sidebands contain the same information, however, one is essentially "wasted." Of the total power output of an AM transmitter, only about one-sixth is actually productive, useful output!

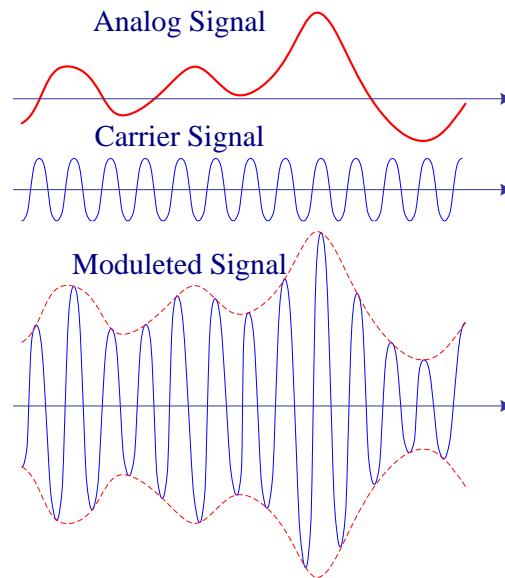


Figure 4.25: AM Modulation

Other disadvantages of AM include the relatively wide amount of frequency space an AM signal occupies and its susceptibility to static and other forms of electrical noise. Despite this, AM is simple to tune on ordinary receivers, and that is why it is used for almost all-shortwave broadcasting.

4.10.2 Single Sideband (SSB)

Since so much power is wasted in AM, radio engineers devised a method to transmit just one sideband and put all of the transmitter's power into sending useful information. This method is known as single sideband (SSB) as illustrated in Figure 4.26. In SSB transmitters, the carrier and one sideband are removed before the signal is amplified. Either the upper sideband (USB) or lower sideband (LSB) of the original AM signal can be transmitted.

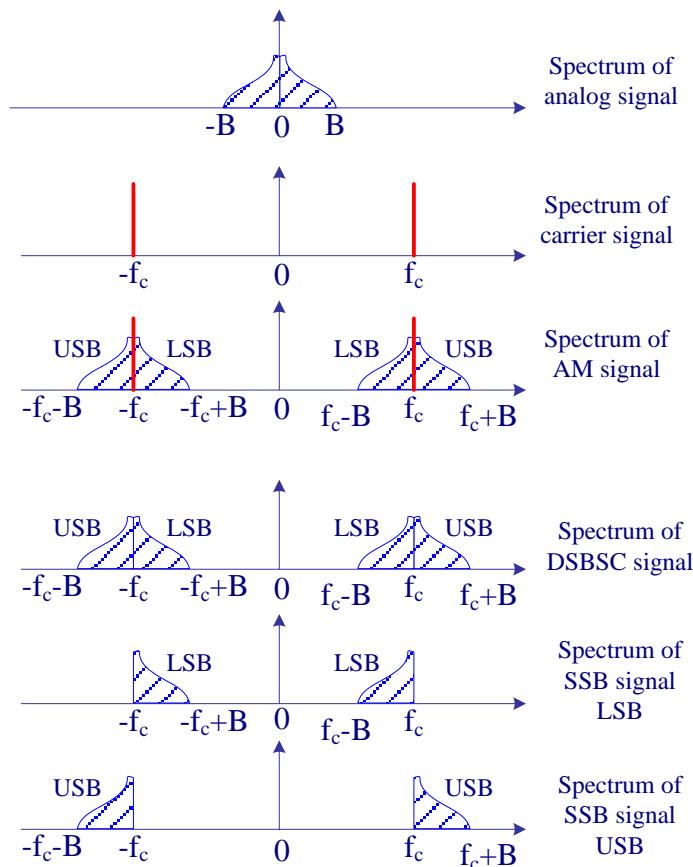


Figure 4.26: Frequency presentation of various types of AM Modulation

SSB is a much more efficient mode than AM since all of the transmitter's power goes into transmitting useful information. SSB signal also occupies only about half the frequency space of a comparable AM signal. However, SSB transmitters and receivers are far more complicated than those for AM. In fact, a SSB signal cannot be received intelligibly on an AM receiver; the SSB signal will have a badly distorted sound. This is because the carrier of an AM signal does play a major role in demodulating (that is, recovering the transmitted audio) the sidebands of an AM signal. To successfully demodulate SSB signal, you need a "substitute carrier."

For best performance, a SSB receiver needs more precise tuning and stability than an AM receiver, and it must be tuned more carefully than an AM receiver. Even when precisely tuned, the audio quality of SSB signal is less than that of an AM signal.

Mainly ham radio operators, military services, maritime and aeronautical radio services, and other situations use SSB where skilled operators and quality receiving equipment are common. There have been a few experiments in using SSB for shortwave broadcasting, but AM remains the preferred mode for broadcasting because of its simplicity.

4.10.3 Frequency Modulation (FM)

In AM, and SSB, the carrier of the signal will not change in a normally operating transmitter. However, it is possible to modulate a signal by changing its frequency in accordance with a modulating signal. This is the idea behind frequency modulation (FM) as shown in Figure 5.21.

The unmodulated frequency of a FM signal is called its center frequency. When a modulating signal is applied, the FM transmitter's frequency will swing above and below the center frequency according to the modulating signal. The amount of "swing" in the transmitter's frequency in any direction above or below the center frequency is called its deviation. The total frequency space occupied by a FM signal is twice its deviation.

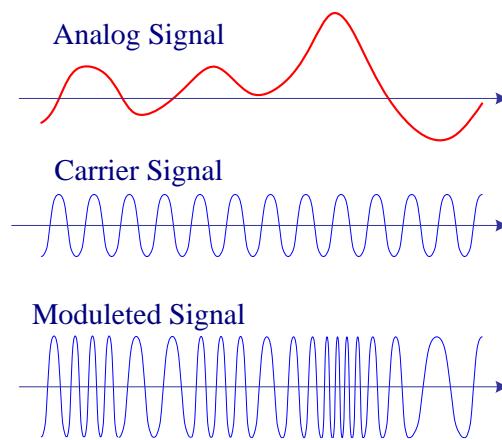


Figure 4.27: Frequency Modulation

As we might suspect, FM signals occupy a great deal of frequency space. The deviation of a FM broadcast station is 75 kHz, for a total frequency space of 150 kHz. Most other users of FM (police and fire departments, business radio services, etc.) use a deviation of 5 kHz, for a total frequency space occupied of 10 kHz. For these reasons, FM is mainly used on frequency above 30 MHz, where adequate frequency space is available. This is why most scanner radios can only receive FM signals, since most signals found above 30 MHz are FM.

The big advantage of FM is its audio quality and immunity to noise. Most forms of static and electrical noise is naturally AM, and a FM receiver will not respond to AM

signals. FM receivers also exhibit a characteristic known as the capture effect. If two or more FM signals are on the same frequency, the FM receiver will respond to the strongest of the signals and ignore the rest. The audio quality of a FM signal increases as its deviation increases, which is why FM broadcast stations use such large deviation. The main disadvantage of FM is the amount of frequency space a signal requires.

4.10.4 Phase Modulation

The **phase** of a carrier wave can be varied in response to the vibrations of the sound source in phase modulation (PM). This form of modulation is a variation of FM. The two processes are closely related because phase cannot be changed without also varying frequency, and vice versa. The rate at which the phase of a carrier changes is directly proportional to the frequency of the audio signal.

4.11 Quick Review

- ❖ An analogue system is designed for transmitting analogue signals. A digital system is designed to transmit digital signals.
- ❖ A digital signal is a discontinuous signal that changes from one state to another in discrete steps. Binary signal is a popular form of this type.
- ❖ An analogue system can transmit digital signals. This is the function of the modem used to connect computers to the different network medium.
- ❖ The use of digital signals and modulation has great advantages over analogue systems (high fidelity, time independence, source independence, signals may be coded).
- ❖ The signal that comes out of the far end of a system will never exactly match the one that was inserted into the near end because of the influences of channel impairments.
- ❖ The ratio of signal strength to noise strength has a special name: signal-to-noise ratio denoted SNR. SNR is usually measured at the receiving end, as this is where it will be at its maximum.
- ❖ The way we characterize a digital channel with respect to its impairment effect is by the probability of error, called bit error rate (BER).
- ❖ The presence of noise or other types of impairments can be handled using amplifiers and repeaters.
- ❖ The information transfer rate for a data channel is defined as the speed at which binary information (bits) can be transferred from source to destination. Units of Information Transfer Rate bits/second
- ❖ The rate at which the signal state changes when observed in the communications channel and is equal to the information transfer rate only in case of binary transmission. Units of Symbol Rate symbols/second (baud)
- ❖ The waveform pattern of voltage or current used to represent the 1s and 0s of a digital signal on a transmission link is called line encoding. The common types of line encoding are unipolar, polar, bipolar and Manchester encoding.
- ❖ The best encoding technique, leads effective self-clocking and the eliminating of DC components

- ❖ Some types of encoding (4B5B, 5B6B, 8B/6T and 8B10B) are designed to eliminate any possibility of long sequences of 1's or 0's and also eliminate DC bias. These types must be followed by another type of encoding method such as NRZ or Manchester. These types are designed to use in very fast data transmission medium.
- ❖ Line coded signal, can be transferred over a lowpass channel such as a serial bus or a wired local area network.
- ❖ Analogue modulation describes the modulation of an analogue signal onto the analogue carrier.
- ❖ Digital modulation describes the modulation of a digital signal onto the analogue carrier.
- ❖ Analog and digital modulation facilitate frequency division multiplex (FDM), where information signals are transferred simultaneously over the same shared physical medium.
- ❖ The most fundamental digital modulation techniques are:
 - PSK where a finite number of phases are used.
 - FSK where a finite number of frequencies are used.
 - ASK where a finite number of amplitudes are used.
- ❖ In the case of Multi-level digital modulation, it is possible for each modulated pulse to represent k bits instead of one bit. The bit rate is k times the baud rate.
- ❖ If the message source is analogue, like speech, then it must first be converted to a digital message by an ADC.
- ❖ In amplitude modulation (AM), the frequency and the phase of the carrier are kept constant, but its amplitude is altered in accordance with variations in the audio signal being sent.
- ❖ In a SSB transmission, only one sideband is radiated - both the carrier and the other sideband (of AM) are suppressed.
- ❖ In frequency modulation (FM), unlike AM, the amplitude of the carrier is kept constant, but its frequency is altered in accordance with variations in the audio signal being sent.
- ❖ FM is less susceptible than is AM to certain kinds of noise.

4.12 Self Test Questions

A- Answer the following questions

1. What is digital signal?
2. What is analog signal?
3. Where is digital transmission preferred?
4. Where is analog transmission preferred?
5. What are the differences between Baseband and Broadband signals?
6. What is communications channel?
7. What is the spectrum of the signal and how can it be affected by the channel bandwidth?
8. What is the channel bandwidth and how can it affect the transmission rate?

9. What is the channel capacity and how can it be affected by the influence of channel impairments and channel bandwidth?
 10. How can the use of multilevel signaling increase the transmission rate?
 11. How can you distinguish between baud and bps?
 12. What is line coding?
 13. How can the loss of timing occur in NRZ line coding?
 14. What are the advantages and disadvantages of Manchester, NRZ, RZ encoding?
 15. How does multilevel signaling affect the transmission rate?
 16. How does every type of impairments affect the receiving signals?
 17. What are the differences between unipolar, polar, and bipolar signaling?
 18. What are the advantages and disadvantages of intermediate encoding?
 19. What are the transmission modes according to data flow, type of physical connection and bandwidth requirements?
 20. Why is it necessary to convert between signal types?
 21. What is basis of term modem?
 22. Why do we need modems?
 23. How we can transmit digital signals over analog networks?
 24. What is the sampling and what is the relation between the sampling rate and the spectrum of the signal to be sampled?
 25. What is the quantization and why do we use it?
 26. What is the aim of digital modulation?
 27. What is the aim of analog modulation?
 28. What are the most fundamental digital modulation techniques?
 29. What are the differences between AM, DSB-SC, and SSB?
 30. What are the differences between AM, FM, and PM?
 31. Which type of analog modulation technique is preferred to be used in noisy channels?

B- Identify the choice that best completes the statement or answers the question.

1. Which transmission type uses a digital encoding scheme at a single fixed frequency?
 - a. Analog
 - b. Electromagnetic
 - c. Baseband
 - d. Broadband
 2. Which transmission systems use analog techniques to encode binary 1s and 0s across a continuous range of values?
 - a. Direct sequence
 - b. Electromagnetic
 - c. Baseband
 - d. Broadband
 3. What is the type of data transmission that occurs in a computer bus?
 - a. serial
 - b. parallel
 - c. analog
 - d. digital
 4. What is the type of data transmission that occurs in any form of networking medium?
 - a. serial
 - b. parallel
 - c. analog
 - d. digital
 5. What is the number of times a signal makes a complete cycle within a given time frame called?

- a. bandwidth.
b. frequency.
c. amplitude.
d. spectrum.
6. What is height of the signal wave above (or below) a given reference point called?
a. bandwidth.
b. frequency.
c. amplitude.
d. spectrum.
7. What is the range of frequencies that a signal spans from minimum to maximum called?
a. bandwidth.
b. spectrum.
c. phase.
d. amplitude.
8. What is the absolute value of the difference between the lowest and highest frequencies called?
a. spectrum.
b. amplitude.
c. bandwidth.
d. phase.
9. What is the position of the waveform relative to a given moment of time or relative to time zero?
a. bandwidth
b. spectrum
c. amplitude
d. phase
10. _____ is the loss of signal strength.
a. amplitude.
b. attenuation.
c. noise.
d. crosstalk.
11. _____ is the digital encoding scheme that checks whether there is a change at the beginning of the bit to determine if it is a 0 or a 1.
a. 4B/5B.
b. AMI.
c. NRZ-L.
d. Manchester.
12. What is the class of digital encoding schemes that solves the synchronization problem by ensuring that each bit has some type of signal change?
a. Manchester
b. NRZ-L
c. 4B/5B
d. AMI
13. What is the simplest modulation technique?
a. frequency
b. phase
c. amplitude
d. pulse code
14. Which modulation is susceptible to sudden noise impulses such as static charges created by a lightning storm?
a. Frequency
b. Phase
c. Amplitude
d. Pulse code
15. Which modulation is subject to intermodulation distortion?
a. Frequency
b. Phase
c. Amplitude
d. Pulse code
16. Which modulation is less susceptible to noise than frequency shift keying and can be used at higher frequencies?
a. Frequency
c. Amplitude

- b. Phase d. Pulse code

17. With which modulation, a codec tracks the incoming analog data by assessing up or down "steps."?
a. amplitude c. delta
b. pulse code d. frequency

18. Frequency is represented by _____.
a. amp. c. volts.
b. Hertz. d. watts.

19. What is the digital encoding scheme that transmits 1s as zero voltages and 0s as positive voltages?
a. NRZ-L c. 4B/5B
b. AMI d. Manchester

20. Which of the following techniques represents encoding?
a. analog data-to-analog signal
b. digital data-to-digital signal
c. analog data-to-digital signal
d. digital data-to-analog signal

21. Which of the following techniques represents digitizing?
a. analog data-to-analog signal
b. digital data-to-analog signal
c. analog data-to-digital signal
d. digital data-to-digital signal

22. What the conversion of digital data to analog signals requires?
a. modem . c. encoder.
b. codec. d. tuner.

23. What the conversion of analog data to digital signals requires?
a. modem. c. encoder.
b. codec. d. tuner.

24. Which of the following conversion technique uses a modem?
a. pulse code modulation c. delta modulation
b. phase shift keying d. differential Manchester

25. The number of times a signal changes value per second is called the
a. bit rate. c. frequency rate.
b. baud rate. d. byte rate.

26. What is the bandwidth for a data transmission line that can transmit within a frequency range of 100 Hz to 3,500 Hz?
a. 3,000 Hz. c. 3,500 Hz.
b. 3,400 Hz. d. 3,600 Hz.

27. What is the baud rate with the Manchester codes?
a. one-half c. equal to
b. one-third d. twice

28. What is the baud rate with with the NRZ codes?
- a. one-half
 - b. one-third
 - c. equal to
 - d. twice
29. What is the baud rate using the Manchester codes, if data is transmitted at 56,000 bps?
- a. 28,000.
 - b. 56,000.
 - c. 112,000.
 - d. 224,000.
30. What is the baud rate with amplitude modulation, if data is transmitted at 56,000 bps?
- a. 28,000.
 - b. 56,000.
 - c. 114,000.
 - d. 224,000.
31. When the frequencies of two or more signals mix together and create new frequencies the result is intermodulation.
- a. interference
 - b. noise
 - c. distortion
 - d. static
32. The bps rate of the transmitted data using quadrature amplitude modulation is _____ times the baud rate.
- a. 3
 - b. 2
 - c. 4
 - d. 8
33. What is the data transfer rate of a signal with a baud rate of 2400 when using quadrature amplitude modulation?
- a. 1200
 - b. 2400
 - c. 4800
 - d. 9600
34. Which of the following uses frequency hopping and direct sequence techniques?
- a. Frequency modulation
 - b. Pulse code modulation
 - c. Differential Manchester
 - d. Spread spectrum
35. Using Nyquist's theorem, a signal is sampled at _____ time(s) the greatest frequency.
- a. three
 - b. two
 - c. five
 - d. eight
36. When converting analog data to a digital signal, the frequency at which the "snapshots" are taken is called the
- a. quantizing rate.
 - b. snapshot rate.
 - c. snap frequency.
 - d. sampling rate.
37. What are the most difficult errors to detect?
- a. White noise
 - b. Crosstalk
 - c. Impulse noise
 - d. Attenuation
38. What is the type of noise that is always present to some degree in transmission medium and electronic devices and depends on the temperature?
- a. White noise
 - b. Impulse noise
 - c. Crosstalk
 - d. Attenuation
39. What is the type of noise that is a non-constant noise and can occur randomly?

- a. White noise
 - b. Impulse noise
 - c. Delay distortion
 - d. Crosstalk

40. What is the continuous loss of a signal's strength as it travels through a medium?

 - a. Delay distortion
 - b. Impulse noise
 - c. Thermal noise
 - d. Attenuation

41. Which of the following is NOT a type of error?

 - a. Crosstalk
 - b. Attenuation
 - c. Echo
 - d. Delay distortion

42. What is the type of transmission in which data can be transmitted from sender to receiver and from receiver to sender in both directions at the same time?

 - a. simplex
 - b. half duplex
 - c. full duplex
 - d. echo

43. What is the type of transmission in which data can be transmitted from the sender to the receiver and from the receiver to the sender in only one direction at a time?

 - a. simplex
 - b. half duplex
 - c. full duplex
 - d. echo

44. What is the type of transmission in which data can be transmitted in one direction only?

 - a. simplex
 - b. half duplex
 - c. full duplex
 - d. echo

45. What type of ports can be used to connect devices such as modems and mice to personal computers?

 - a. Parallel
 - b. USB
 - c. Serial
 - d. Centronics

46. What type of ports has eight data lines transmitting an entire byte of data at one moment in time?

 - a. parallel
 - b. USB
 - c. serial
 - d. DIN

47. What is the type of connections supports the more traditional peripheral devices such as modems and printers?

 - a. isochronous
 - b. asynchronous
 - c. synchronous
 - d. parallel

CHAPTER 5

TRANSMISSION MEDIUM

5.1 About This Chapter

The conveyance, or transmission, of information across a distance necessarily involves some form of transmission medium. The selection of physical transmission medium which serve to transport that information is critical to its successful conveyance. More than in some data transmission systems, the medium can be critical to the transferred data such in interactive system.

This chapter addresses all transmission medium commonly used in traditional voice, data, video, and image networks, whether analog or digital in nature. Those medium can be grouped into two distinctive categories, the first of which includes all wired medium, also referred to as conducted, guided, bounded medium or guided medium. The second category includes all wireless medium, also referred to as radiated, unguided, or unbounded.

This chapter focuses on twisted-pair, coaxial cable, Optical fibers, as a guided medium and microwave satellite broadcasting radio cellular communication infrared and Bluetooth as unguided medium. This chapter provides also an overview of differences and purposes of the emerging technologies in these medium.

The transmission medium is an essential part of transmission system, so we begin by providing a brief description of transmission system and its essential elements. We then examine most guided and unguided link alternatives, briefly discuss their applications, and summarize key transmission characteristics.

5.2 Learning Outcome

After this chapter, you will be able to:

1. Describe the transmission system characteristics and determine the role of every of its essential part.
2. Understand the importance of choosing the suitable transmission medium in the conveyance of data signals.
3. Distinguish between guided an unguided transmission medium.
4. Describe the various guided an unguided transmission medium.
5. Explain the general transmission characteristics of guided and unguided link alternatives.
6. Generally determine the application area of every type of transmission medium.
7. Determine the appropriate transmission medium for specific applications.

5.3 Fundamentals of Transmission Systems

Each specific transmission system is distinguished by unique properties, limitations, and appropriate applications. The application to be supported, clearly, must be of primary consideration in designing a network and in selecting the transmission medium, assuming one has the freedom of choice. As the application must support users effectively, it places certain demands on the transmission system components.

Traditional transmission systems include the following basic components as it is shown in Figure 5.1:

- Data Terminal Equipments (DTE)
- Physical Interface
- Data Communication Equipments (DCE)
- Transmission Medium

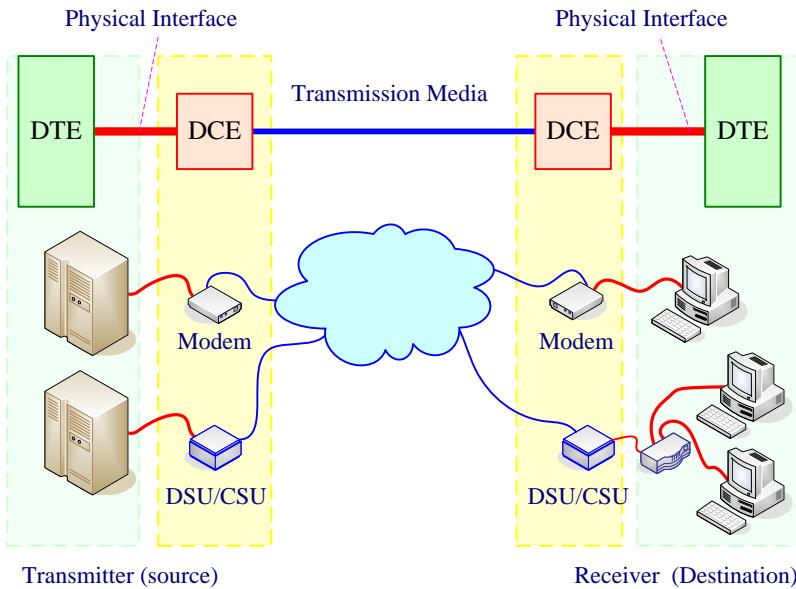


Figure 5.1: The general structure of the traditional transmission systems

5.3.1 Data Terminal Equipments (DTE)

The term “DTE” specifically refers to a data input and output devices that are used to communicate with a remotely located computer or other data communication device.

Typically, data terminal equipment (DTE) is used to describe multiple types of devices including personal computers (PCs), dedicated “dumb” terminals, scientific workstations, printers, and LAN interconnection devices such as routers or some similar device that can communicate with other computers or a host computer.

The DTE main responsibilities are to transmit and receive information and to perform error control; it captures and organizes information for communication to other

communication devices. The DTE generally supports the end-user applications program, data files, and data bases.

5.3.2 Physical Interface

Physical interface defines the characteristics of physical connection to DTE. It specifies the nature of the boundary between two devices and determines the procedures and protocols that make it possible for the devices to exchange data. In particular interface defines the connector signal levels, impedance, timing, sequence of operation, and meaning of signals how many pins are in the connector, how many wires are in the cable, and what signal is carried over which of the pins and over which of the wires, to ensure that the information is viewed compatibly.

There are two main types of networking and communication interfaces serial and parallel interfaces:

- **Serial interfaces**, which transfer data one bit at a time. The most common serial interface is the RS-232 interface. Serial interfaces are commonly used for connecting data terminal equipment (DTE) to data communications equipment (DCE).
- **Parallel interfaces**, which transfer data several bits at a time, usually one or more bytes at a time. The most common parallel interface is DB-9, DB-25 and 36-pin connector.

5.3.3 Data Communication Equipments (DCE)

The role of DCE is to accept a stream of serial data from a DTE and convert it to a form that is suitable for the particular transmission line medium being used. On the other site the DCE also works in reverse, converting data from the transmission line to a form the DTE can use.

The DCE is responsible for ensuring that the signal that comes out of the DTE is compatible with the requirements of the transmission medium. So DCE is responsible of the signal coding, the determination of voltage level to be assigned to data bits, how many of one type of bit can be sent in a row, and so on. DCE establishes, maintains, and terminates a connection between the DTE and the transmission medium. For instance, with an accessing the network using analog voice-grade line, the DCE would be responsible for translating the digital data coming from the PC into an analog form that could be transmitted over that voice-grade line.

The purpose of a DCE is to provide termination for the telecommunications link and an interface for connecting data terminal equipment (DTE) to the link. DCE refers to any device that supports data transmission over a serial telecommunications link such as modems, Channel Service Unit/Data Service Units (CSU/DSUs), multiplexers, and similar devices.

5.3.4 Transmission Medium

A transmission medium is any material substance or free space that can be used for the propagation of suitable signals, usually in the form of electromagnetic (including light waves), or acoustic waves, between transmitter and receiver. The characteristics and quality of data transmission are determined by both of the nature of the signal and the nature of the medium.

The selection of the most effective transmission medium for a given application must be made in the context of a number of key design considerations including:

- A Bandwidth capability, which refers to the raw amount of bandwidth the medium supports. The greater the bandwidth, the higher the data rate that can be achieved.
- Error performance refers to the number or percentage of errors which are introduced in the process of transmission.
- The ability to handle either analog or digital signals.
- Number of receivers - Guided medium can be used to construct a point- to-point link or a shared link with multiple attachments.
- Distance refers to the minimum and maximum spatial separations between devices that can carry data while this data still recoverable.
- Cost including cost of acquisition, deployment, operation and maintenance, and upgrade or replacement.
- Propagation delay refers to the length of time required for a signal to travel from transmitter to receiver across a transmission system.
- Security, in the context addresses the protection of data from interception as it transverses the medium.
- Mechanical strength, this issue applies to guided medium, it includes the amount of bending and twisting the conductors can tolerate, as well as the amount of weight or longitudinal stress they can support without breaking. In airwave systems, reflective dishes, antennae, and other devices must be mounted securely to deal with wind and other forces of nature.
- Other factors such like local availability and physical dimensions.



Every data network is a data circuit that has seven parts: the originating DTE, its physical interface, the originating DCE, the transmission channel, the receiving DCE, its physical interface, and the receiving DTE.

5.4 Transmission Medium General Classification and Characteristics

5.4.1 General classification of Transmission Medium

Transmission medium can be classified as guided or unguided. With guided medium, the waves are guided along a solid medium such as paired metallic wire cable,

coaxial cable, and Optical fiber cable. The atmosphere and outer space are examples of unguided medium that provide a means of transmitting electromagnetic signals but do not guide them; this form of transmission is usually referred to as wireless transmission.

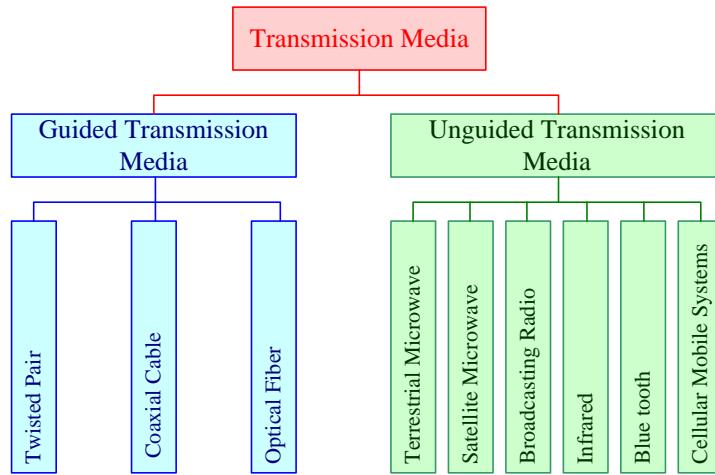


Figure 5.2: general classification of transmission medium

5.4.2 Frequency Considerations

The electromagnetic spectrum ranges from extremely low-frequency radio waves of 30Hz, with wavelengths nearly double the earth's diameter, to high-frequency cosmic rays of more than 10 million trillion Hz, with wavelengths smaller than the nucleus of an atom. Although the electromagnetic spectrum represents an enormous range of frequencies, not all the frequencies are suitable for human communications. While human voice frequencies mostly are in the range of 100 Hz to 8,000 Hz; the energy in the speech spectrum peaks at approximately 500 Hz, with most articulation being at higher frequencies. The human ear can distinguish signals as low as 20 Hz and as high as 20 kHz, and is most sensitive in the range of 1,000 Hz to 3,000 Hz. Public switched telephone networks, as we have discussed previously, provide reliable, raw, voice-grade bandwidth of 4 kHz; with 3,300 Hz (200 Hz to 3,500 Hz) usable for signal transmission. This range of frequencies provides a band of intelligibility which is considered to be good, although not complete. Because of the problems with very low and very high frequencies, we primarily use the middle of the electromagnetic spectrum for communication the radio, microwave, infrared, and visible light portions of the spectrum. We do this by modulating the amplitudes, frequencies, and phases of the electromagnetic waves. Bandwidth is actually a measure of the difference between the lowest and highest frequencies being carried. Each of the communications bands offers differing amounts of bandwidth, based on the range of frequencies they cover. The higher up in the spectrum, the greater the range of frequencies involved.

In an electrical cable system, the range of carrier frequencies depends on the nature of the medium and the requirements of the applications supported. For instance, twisted pair can support bandwidths of 10 Hz to 10^5 Hz, and coaxial cable of 10^6 Hz to 10^8 Hz. The actual range of frequencies supporting a given communication is known as a

passband, which is accomplished through the use of band-limiting filters. Figure 5.2 shows the electromagnetic spectrum and where some of the various transmission medium operate.



The radio, microwave, infrared, and visible light portions of the spectrum can all be used to generate electromagnetic waves that carry information.

5.5 Guided Transmission Medium

For guided transmission medium, the transmission capacity, in terms of either data rate or bandwidth, depends critically on the distance and on whether the medium is point-to-point or multipoint.

The term guided medium refers to the fact that the signal is contained within an enclosed physical path. Also known as conducted systems, wired medium generally employ a metallic or glass conductor which serves to conduct, or carry on, some form of electric, electromagnetic or light energy. For example, twisted pair and coaxial cable systems conduct electrical energy, employing a copper medium; Optical fiber systems conduct light, or optical, energy, generally using a glass or plastic conductor.

5.5.1 Twisted Pair

Twisted pair cables have been used for connecting telephones to local exchanges ever since telephones were invented, the size and thickness have changed but they are basically the same as they were in the early twentieth century.

Twisted pair is much less expensive than other commonly used guided transmission medium, it is easier to work with, and it is more limited in terms of data rate and distance.

5.5.1.1 Twisted Pair Physical Description

- Twisted pair consists of two insulated copper wires arranged in a regular spiral pattern as shown in Figure 5.4 (A). There are two types of twisted-pair: UTP Figure 5.2 (B) and STP Figure 5.2 (C). STP has an extra metallic wrapper around the inner cables which will further reduce RFI and EMI; this sometimes surrounds all the pairs or could surround each individual pair. This gives more bulk to the cable.
- STP is available with two impedances, 100 ohm and 150 ohm impedance - the later is more expensive. The lower impedance gives the same performance as UTP but the higher impedance STP can deal with speeds up to 100Mbps and more. Most implementations today use UTP.

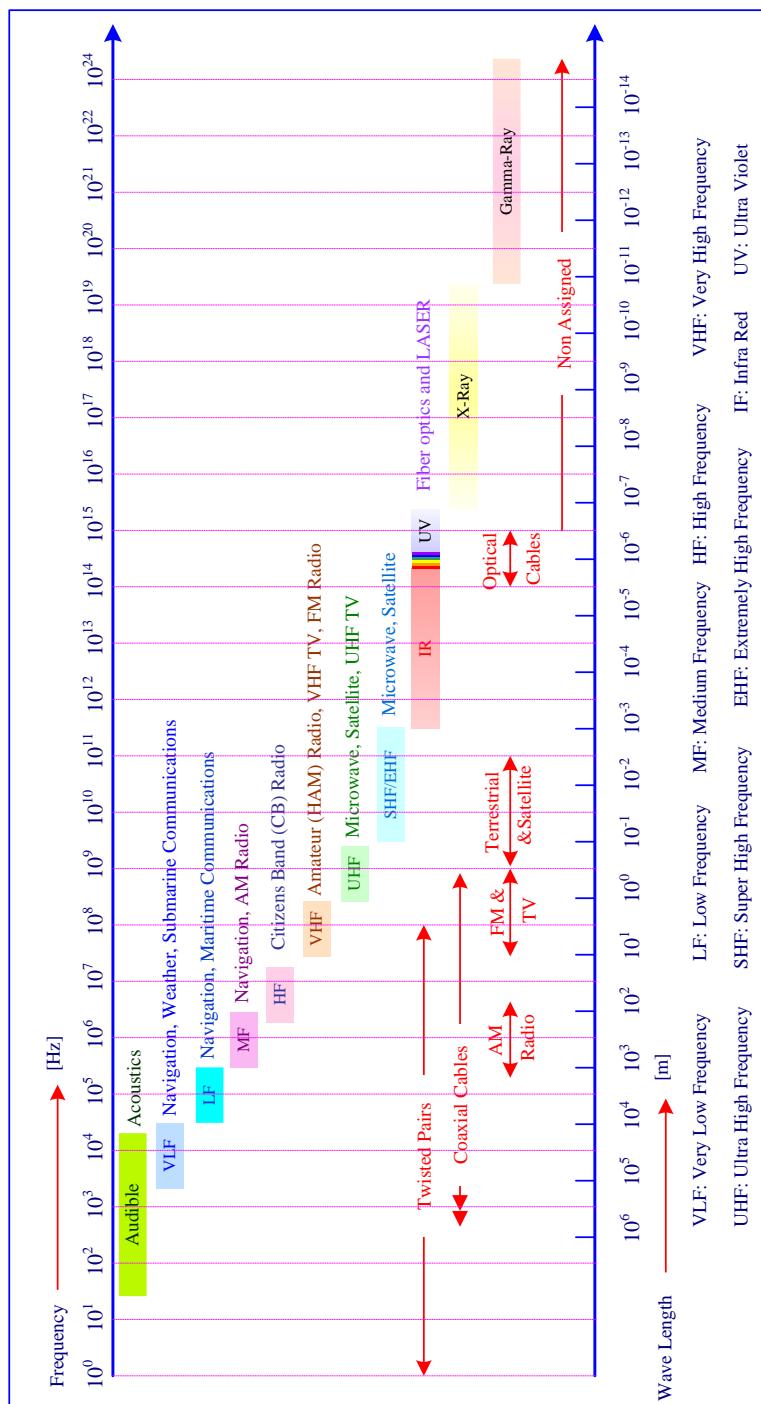


Figure 5.3: The electromagnetic spectrum

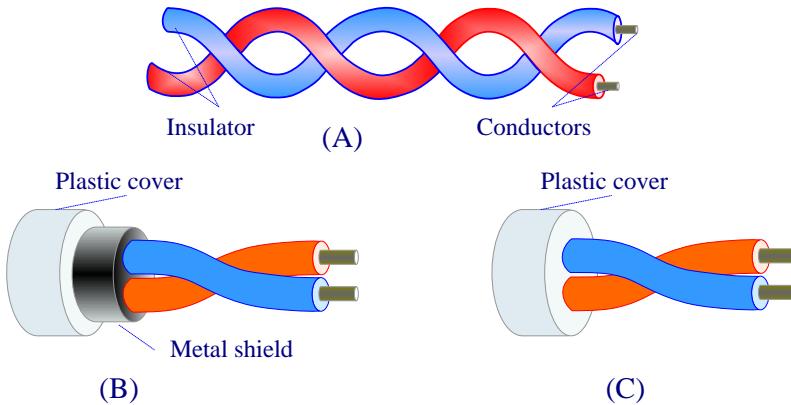


Figure 5.4: General description of twisted pair cables

- Wire pair acts as single communication link. The number of actual twisted pair cables held in one sheath varies. The one used for connecting Networks is generally 4 pairs (8 wires) but the cables laid in the road to feed telephones may have hundreds or thousands of pairs of cables. Each cable is identified by the main color of the cable and a tracing color.

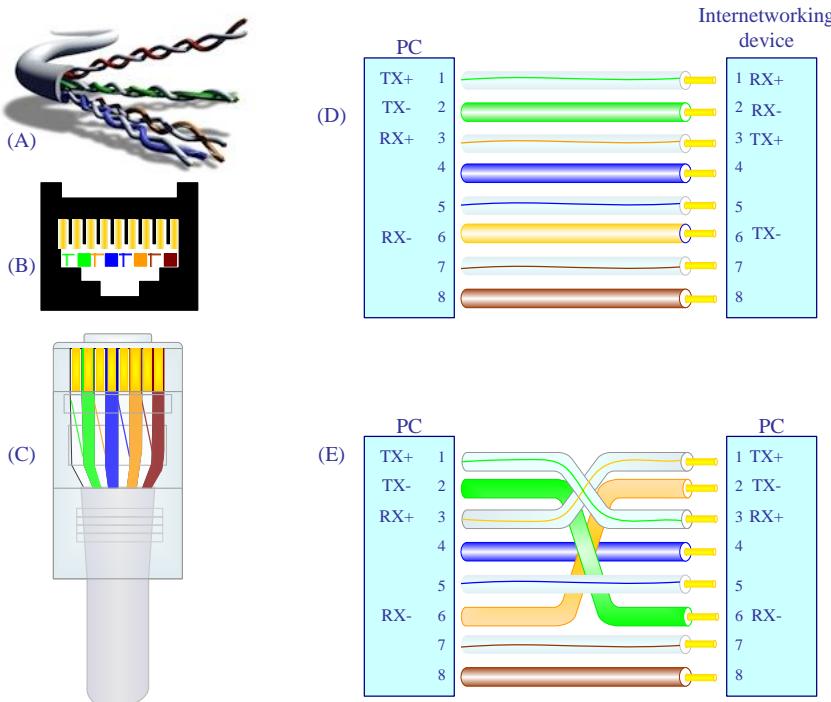


Figure 5.4: Twisted pair cables connecting methods (A) Twisted pair cable, (B) RJ 45 Female Connector, (C) RJ 45 male Connector, (D) Straight-Through Wiring using the 568A Standard and (E) Cross-Over Wiring using the 568A to 568B Standards

- Twisting tends to decrease Crosstalk interferences, electromagnetic interference (EMI), and radio frequency interference (RFI) between adjacent pairs in a cable.
- A family of push-and-click connectors for twisted-pair wiring in telephone and network wiring. RJ stands for Registered Jack. RJ types define both a jack or receptacle (female) and a plug (male) type of connector. The most common types of RJ connectors are as follows:
 - **RJ-11 connector:** A 4-wire or 6-wire telephone-type connector that connects telephones.
 - **RJ-45 connector:** An 8-wire telephone-type connector used with twisted-pair cabling for connecting computers, wall plates, patch panels, and other networking components. Figure 5.5 illustrates the wiring methods of twisted pairs using RJ45.
 - **RJ-48 connector:** An 8-wire telephone-type connector used with twisted-pair cabling for connecting T1 and 56-KB digital data service (DDS) lines.

5.5.1.2 Categories of Twisted-Pair

Twisted Pair cables are divided into different categories which vary in the number of twists per foot and quality, allowing the higher categories to transmit data at higher speeds, e.g. Category 3 cables has 2 twists per foot whereas Category 5 has 12.

Table (5.1) summarizes the maximum data rate and the usual application of the cable categories.

Category	Maximum data rate	Usual application
CAT 1	Up to 1 Mbps (1MHz)	<ul style="list-style-type: none"> ▪ Voice telephony ▪ Long-range Ethernet and DSL, operating at 10Mbps ▪ Integrated Services Digital Network (ISDN)
CAT 2	4 Mbps	<ul style="list-style-type: none"> ▪ token-ring LANs
CAT 3	16 Mbps	<ul style="list-style-type: none"> ▪ Voice and LAN applications include 10Mbps Ethernet and 4Mbps token-ring LANs.
CAT 4	20 Mbps	<ul style="list-style-type: none"> ▪ Used in 16 Mbps Token Ring ▪ Otherwise not used much
CAT 5	100 Mbps 1000 Mbps (4 pair)	<ul style="list-style-type: none"> ▪ LAN applications include 100BASE-TX, 1000BASE-T, ATM, CDDI, and No longer supported; replaced by 5E
CAT 5E	1000 Mbps (10000 Mbps prototype)	<ul style="list-style-type: none"> ▪ LAN applications include 100BASE-TX, 1000BASE-T, ATM, CDDI, and Gigabit Ethernet ▪ Offers better near-end crosstalk than CAT 5
CAT 6	Up to 400 MHz	<ul style="list-style-type: none"> ▪ Super-fast broadband applications

		Most popular cabling for new installs
CAT 6E	Up to 625 MHz (field-tested to 500 MHz)	<ul style="list-style-type: none"> ▪ Support for 10 Gigabit Ethernet (10GBASE-T)
CAT 7	600-700 MHz 1.2 GHz in pairs with special connector	<ul style="list-style-type: none"> ▪ Ultra Fast Ethernet ▪ Full-motion video ▪ Teleradiology ▪ Government and manufacturing environments ▪ Shielded system

Table (5.1): Summation twisted pair categories.

5.5.1.3 Twisted Pair Application

- In the telephone, where the telephone sets are connected to local telephone exchange. Within a building, each telephone is also connected to a twisted pair, which goes to an in-house private branch exchange (PBX). In a modem, twisted pairs are used to handle the digital traffic.
- Digital Signaling, where cables are used within a building for Local Area Network (LAN) supporting Personal Computer (PC). The data rates are typically of 10 and 100 Mbps. Recently; data rates of more than 1000 Mbps have been implemented. In long distance application of twisted pair can be used at data rates of 4Mbps or more.

5.5.1.4 Twisted Pair Transmission Characteristics

- Twisted pair transmits both analog and digital signals. Twisted Pair is limited in distance, bandwidth, and data rates (when compare to other guided transmission medium).
- Twisted-pair requires short distances between repeaters, which lead to higher costs.
- Twisted-pair is also highly susceptible to Impulse noise, interference and distortion, including electromagnetic interference (EMI), radio frequency interference (RFI), and the effects of moisture and corrosion.
- The attenuation for twisted pair is very strong function of frequency.
- For point-to-point analog signaling, a bandwidth of up to about 250 kHz is possible. This accommodates a number of channels.
- For long distance digital point-to-point signaling, data rates of up to a few Mbps are possible.

 The greatest use of twisted-pair in the future is likely to be in enterprise premises, for desktop wiring. Eventually, enterprise premises will migrate to fiber and forms of wireless, but in the near future, they will continue to use twisted-pair internally.

5.5.2 Coaxial Cable

Coaxial cable consists of a single insulated inner wire surrounded by a cylindrical conductor, which is covered with a shield; it transmits electromagnetic signals. Coaxial cable is classified into two categories: Baseband (uses digital signals) and broadband (uses analog signals). Baseband Coaxial Cable known as a 50-ohm cable commonly used for digital transmission, while a broadband Coaxial Cable is 75-ohm cable and is commonly used for analog transmission.

5.5.2.1 Coaxial Cable Physical Description

- It operates over a wider range of frequencies.
- It consists of a hollow outer cylindrical conductor that surrounds a single inner conductor. The inner conductor is held in place by either regularly spaced insulating rings or a solid dielectric material. The outer conductor is covered with a jacket or shield as shown in Figure 5.5.
- Diameter of a single coaxial cable is between 0.4 to about 1 in.
- Coaxial cable is much less susceptible to interference and crosstalk than twisted pair.
- It can be used in longer distance and support more station and shared line.
- Coaxial cable is most versatile transmission medium and is enjoying widespread use in a wide variety application.

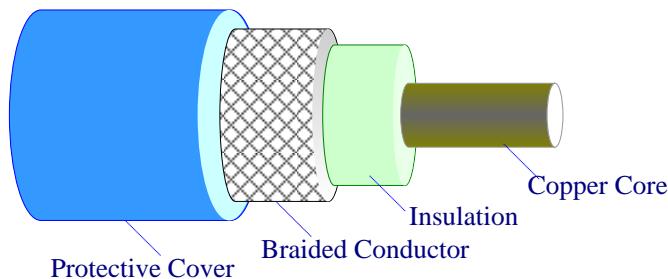


Figure 5.5: Coaxial Cable

- The most common types of coaxial cabling are
 - RG-8 and RG-11 are 50 ohm cables required for thick wire Ethernet. (ThikNet)
 - RG-58 is a smaller 50 ohm cable required for use with thin wire Ethernet. (ThinNet)
 - RG-59 is a 75 ohm cable which is most familiar when used to wire cable TV. RG-59 is also used to cable broadband 802.3 Ethernet.
 - RG-62 is a 93 ohm cable used for ARCnet. It is also commonly employed to wire terminals in an IBM SNA network.
- Coaxial cables use a special type of connectors as shown in figure 5.6 include the following:
 - **BNC cable connector:** Soldered or crimped to the ends of a thinnet cable
 - **BNC T-connector:** Used to connect a network interface card (NIC) to a thinnet cable segment

- **BNC terminator:** Provides a 50-ohm termination for the free end of a thinnet cable

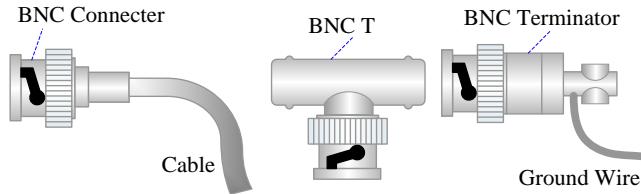


Figure 5.6: Thin Coaxial Cable Connectors

- To connect a computer to a thicknet cable, you attach a **vampire tap** to the cable. The tap pierces the cable's insulation layers and makes contact with the signal-carrying copper core as it is shown in figure 5.7.

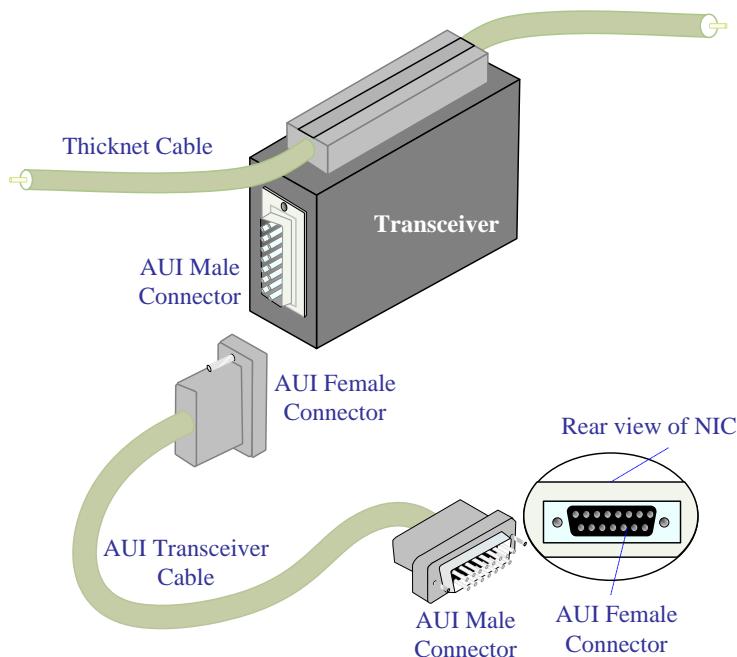


Figure 5.9: Thick Cable Connections

5.5.2.2 Coaxial Cable Application

- Television Distribution - distributing TV signals to individual homes - cable TV.
- Long-Distance telephone transmission - Coaxial cable has been traditionally an important part of long-distance telephone network. Using frequency division multiplexing (FDM) a coaxial cable can carry over 10,000 voices channels simultaneously.
- Short-run computer system links - Using digital signaling; coaxial cable can be used to provide high-speed I/O channels on computer systems.

- Local Area Network (LAN) - Coaxial cable can support a large number of devices with a variety of data and traffic types, over distances that encompass a single building or a complex of building.

5.5.2.3 Coaxial Cable Transmission Characteristics

- It is used to transfer both analog and digital signals.
- Has a frequency characteristic that is superior to twisted pair, and can be used effectively at higher frequencies and data rates.
- Much less susceptible to interference and crosstalk than twisted pair because of its shielded and concentric construction.
- Principal of constraints on performance are attenuation, thermal noise, and Intermodulation noise.
- For long distance transmission of analog signals, amplifiers or repeaters are required every kilometer, with closer spacing required if higher frequencies are used.
- The usable spectrum for analog signaling extends to about 400MHz.

5.5.3 Optical Fiber

In recent years Optical fiber Cables have been used increasingly as a transmission medium for data. Optical fiber cables have replaced a lot of the twisted pair cables being used to carry voice conversations because it is thin and light, e.g. two Optical fiber cables will carry more capacity than one thousand twisted pair cables. If the cables are 1Km long the twisted pair will also weigh 8000Kg.

An optical transmission system has three components: the light source, the transmission medium (optical fiber) which transmits optical signals and the detector which must transform optical signals back to electrical signals as illustrated in Figure 5.8.

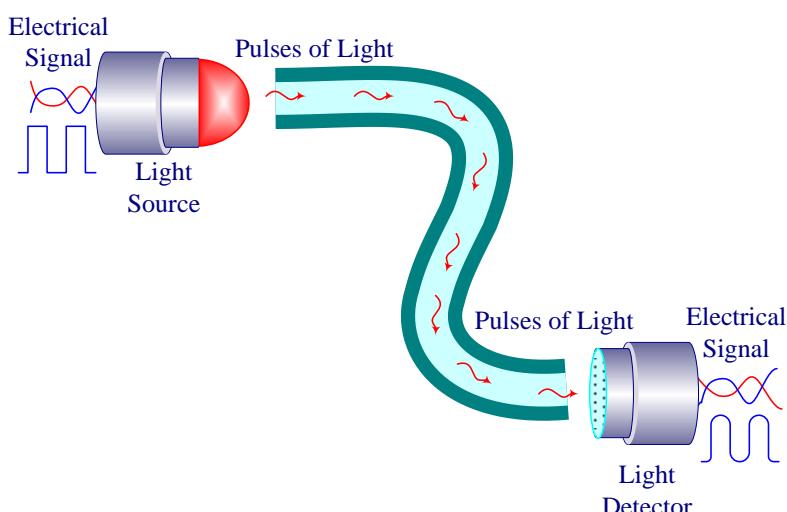


Figure 5.8: Optical Fiber

5.5.3.1 Optical Fiber Physical Description

- Optical fiber cable consists of thin glass or plastic fibers that can carry information at frequencies in the visible light spectrum and beyond.
- The typical optical fiber consists of a very narrow strand of glass or plastic as thin as a human hair called a core.
- The core is surrounded by concentric layer of glass called the cladding which ensures that the light energy remains within the fiber rather than bouncing out into the exterior.
- A typical core diameter is 62.5 microns (1 micron = 10^{-6} meters). Typically Cladding has a diameter of 125 microns.

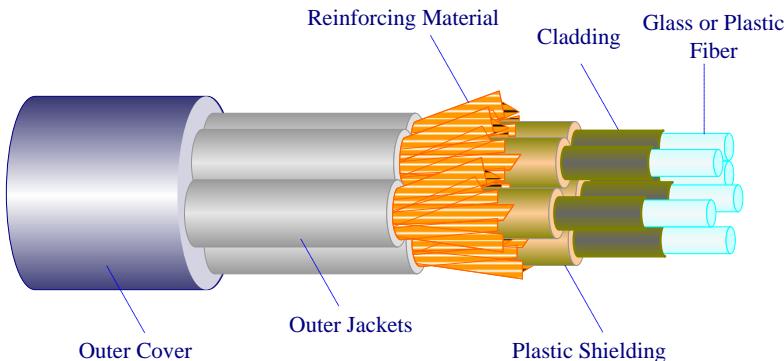


Figure 5.8: The basic components of optical fiber cable

- Optical fiber cable is available in many sizes. It can have as few as a couple pairs of fiber or it can have bundles that contain upward of 400 or 500 fiber pairs. Figure 5.8 shows the basic.
- The cladding is surrounded by plastic shielding, which, among other things, ensures that you can't bend the fiber to the point at which it would break; the plastic shielding therefore limits how much stress you can put on a given fiber.
- The plastic shielding is then further reinforced with reinforcing material that is five times stronger than steel to prevent other intrusions.
- Outer jackets cover the reinforcing material, and the number and type of outer jackets depend on the environment where the cable is meant to be deployed (e.g., buried underground, used in the ocean, strung through the air).
- Lowest losses obtained using fibers of ultra pure fused silica, but difficult to manufacture; higher loss multicomponent, glass fibers are more economical and still provide good performance. Plastic fiber even costly and can be used for short-haul links.
- Two types of light source are used to generate the light used for transmission - LED and semiconductor laser.

5.5.3.2 Types of Optical Fiber Cable

Each ray of light which travels through a fiber is called a Mode. By altering the diameter of the fiber two different transmission operating modes can be achieved - Single mode and Multimode.

➤ **Multimode Cable:** The Multimode cable is thicker than the single and more than one light ray can pass through. Because the ray travels at the same speed but each one can travel a different distance, the signal will spread over time and introduce data errors over long distances. This problem is known as dispersion. To reduce this problem there are two different types of Optical fiber cable:

- **Step-index:** This is a single fiber and cladding. It has a large core, so the light rays tend to bounce around inside the core, reflecting off the cladding. This causes some rays to take a longer or shorter path through the core. Some take the direct path with hardly any reflections while others bounce back and forth taking a longer path. The result is that the light rays arrive at the receiver at different times. The signal becomes longer than the original signal. LED light sources are used. Typical Core: 62.5 microns.
- **Graded-index:** This type of cable has a gradual change in the core's refractive index. This causes the light rays to be gradually bent back into the core path. This is represented by a curved reflective path in the Figure 5.9. The result is a better receive signal than with step index. LED light sources are used.
- The most common Multimode Optical fiber cable is 62.5/125 graded-index. The first figure is the core diameter and the second is the cladding diameter.

➤ **Single Mode Cable:** This type has separate distinct refractive indexes for the cladding and core. The light ray passes through the core with relatively few reflections off the cladding. Single mode is used for a single source of light (one color) operation. It requires a laser and the core is very small: 9 microns. Currently available Single Mode cables can transmit data at several Gbps over distances of 30Km.

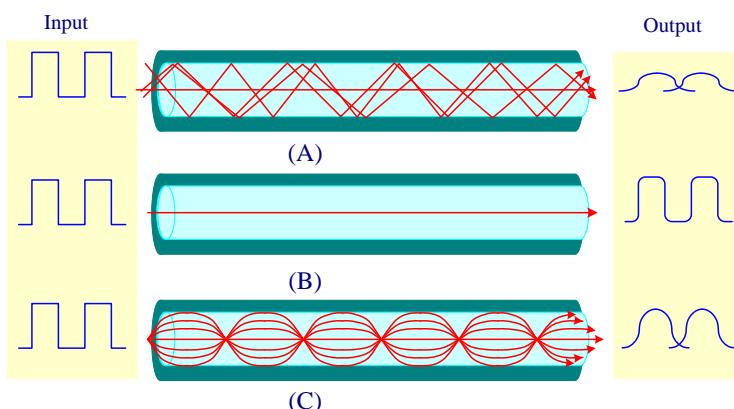


Figure 5.9: Optical Fiber Types, (A) Step-index multimode, (B) Single mode and (C) Graded-index multimode

 Optical fiber cable is the unchallenged winner in the Transmission Medium sweepstakes comparing it to other guided medium

- ❖ Greater capacity (potential bandwidth)
- ❖ Smaller size and lighter weight
- ❖ Lower attenuation
- ❖ Electromagnetic isolation
- ❖ Greater repeater spacing

There are many types of optical connectors. The connector is a mechanical device mounted on the end of a fiber-optic cable, light source, receiver, or housing allowing it to be mated to a similar device. The connector must direct light and collect light and must be easily attached and detached from equipment. Commonly used fiber-optic connectors are

- **FC Connector:** It offers extremely precise positioning of the fiber-optic cable with respect to the transmitter's optical source emitter and the receiver's optical detector.
- **SC Connector:** It offers low cost, simplicity, and durability. SC connectors provide for accurate alignment via its ceramic ferrules.
- **LC Connector:** It is constructed with a plastic housing and provide for accurate alignment via their ceramic ferrules.
- **MT-RJ Connector:** It is constructed with a plastic housing and provide for accurate alignment via its metal guide pins and plastic ferrules.

All these types of connectors are used for single-mode and multimode fiber-optic cables.

5.5.3.3 Optical Fiber Application

Optical fiber already enjoys considerable use in long distance telecommunications, and its use in military applications is growing. The continuing improvements in performance and decline prices, together with the inherent advantages of optical fiber have made it increasingly attractive for local area network. Five categories of the application of optical fiber are:

- Long-haul Trunks: It is becoming increasingly common in the telephone network. Long-haul routes average about 900 miles in length and offer high capacity (20,000 - 60,000 voices channels). These systems compete economically with microwave and have so under price coaxial cable in many developed countries that coaxial cable is rapidly being phased out of the telephone network.
- Metropolitan Trunks: It has an average length of 7.8 miles and may have as many as 100,000 voice channels in a trunk group. Most facilities are installed underground conduits and area repeaterless, joining telephone exchanges in a metropolitan or city area.

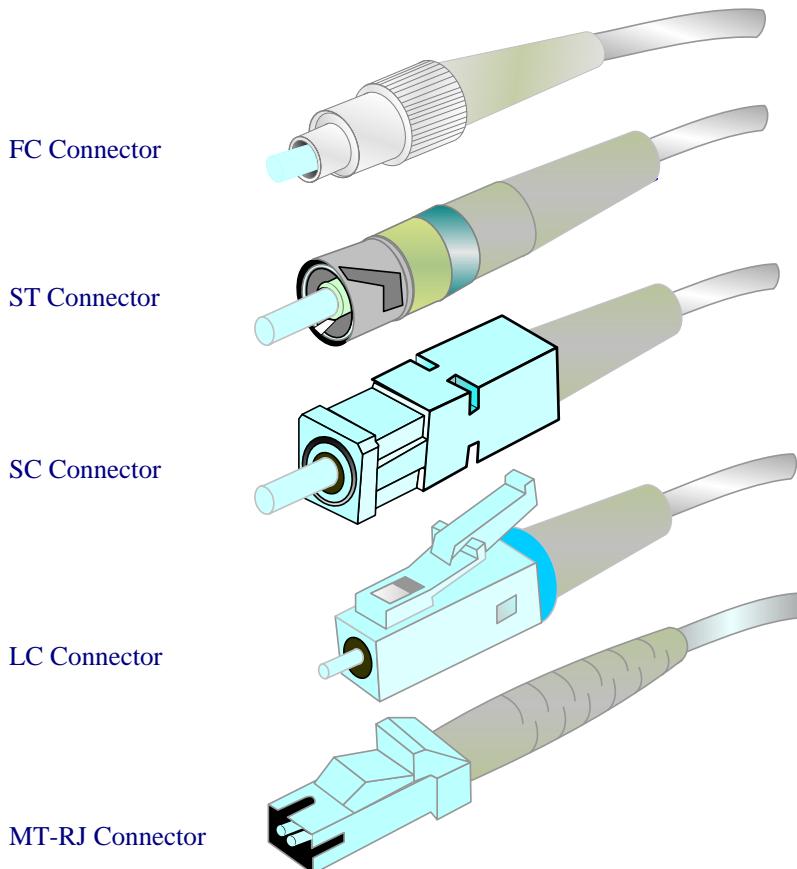


Figure 5.9: Some Types of Optical fiber Connectors

- Rural-exchange Trunks: It has circuit length ranging from (25– 100) miles that links town and villages. In U.S they often connect the exchange of different telephone companies. Most of these systems have fewer than 5, 00 voice channels. This technology application competes with microwave facilities.
- Subscriber Loops: Fiber circuits run directly from the central exchange to a subscriber. These facilities are beginning to displace twisted pair and coaxial cable links as the telephone networks evolve into full-service network capable of handing not only voice and data but also image video. The initial penetration of optical fiber in this application is for the business subscriber, but for home transmission is soon begin to appear.
- Local Area Network: Standards have been developed and products introduced for optical fiber networks that have total capacity of 100 Mbps and more which can support hundreds or even thousands stations in very large buildings.

5.5.3.4 Optical fiber Transmission Characteristics

- EMI does not affect the signals running in a Optical fiber cable as they are not electrical and they are more secure as the signals do not leak out either and cannot be picked up by an outside source.
- Optical fiber system operates range of about $(10)^{14}$ to $(10)^{15}$ Hz; cover the infrared and visible spectrum proportion.
- The principle of optical fiber transmission is that a light from the source enters the cylindrical glass or plastic core. Rays at shallow angles are reflected and propagated along the fiber; the surrounding material absorbs other rays.
- In multimode transmission, propagation paths exist with each carry a different paths length and time to traverse the fiber. These cause signal elements to spread out in time, which reduce the data transmission rate and increase distortion.
- Because of a single transmission with single-mode transmission, such distortion cannot occur.
- Both single mode and multimode can support several different wavelengths of light and can employ laser or LED light source.
- In optical fiber, light propagates best in three distinct wavelengths "windows" centered on 850, 1300, and 1550 nanometers (nm). Most local application today uses 850- nanometers (nm) LED light sources. Although this combination is relatively inexpensive, it is generally limited to data rates under 100 Mbps and distance of a few km.
- To achieve higher data rates and longer distance a 1300-nm LED or a laser source is needed. Higher data rates and distance require a 1500-nm laser source.



Both step index and graded index allow more than one light source to be used (different colors simultaneously), so multiple channels of data can be run at the same time

5.6 Unguided Transmission Medium

Rather than relying on electric energy, unguided medium generally makes use of radio or light waves that are transmitted and received across space, and are referred to as *airwave* systems.

Unguided transmission medium includes atmosphere and outer space used in terrestrial microwave radio transmission systems, satellite, mobile telephone, and personal communications systems.

5.6.1 Terrestrial Microwave

Microwave is the name given to radio waves falling in the 1GHz to 100GHz frequency band. In fact, current microwave systems largely operate up to the 50GHz range. Given the growing demand for wireless access to all forms of medium, we can

expect to see many developments in coming years that take advantage of the high-bandwidth properties of this frequency bands and higher.

Microwave systems are commonly used as high capacity, point-to-point transmission systems in telecommunications networks, such as high-capacity trunk telephone network connections between major exchanges, or on smaller scale between buildings. The high frequency and short wavelength of microwave radio allows high capacity radio systems to be built using relatively small but highly directional antennas. The small scale yields benefits in terms of cost, installation, and maintenance.

Transmissions and receptions are achieved by means of an antenna. Antenna can be:

- **Directional:** Point-to-point focused beams employing high frequencies as illustrated in Figure 5.10 (A).
- **Omnidirectional:** Waves propagating in all directions using signals of lower frequencies as shown in Figure 5.10 (B).

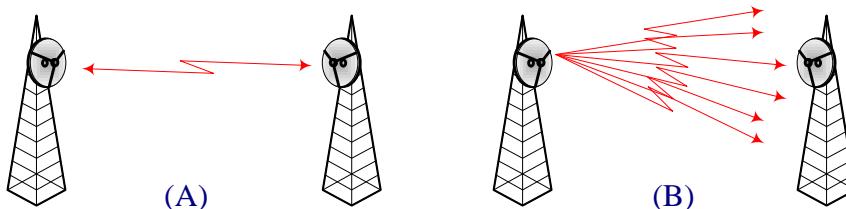


Figure 5.10: (A) Directional Transmission and (B) Omnidirectional Transmission

Terrestrial microwave radio transmission systems consist of at least two radio transmitter/ receiver connected to high-gain antennas (directional antennas that concentrate electromagnetic or radio wave energy in narrow beams) focused in pairs on each other, as illustrated if Figure 4.7.

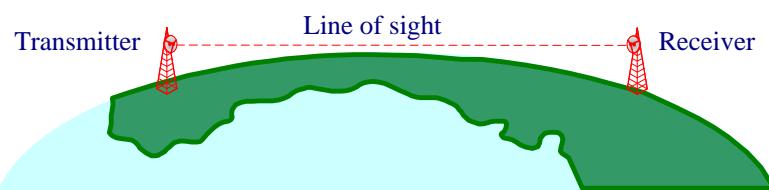


Figure 5.11: Terrestrial Microwave

The important design criterion is that microwave requires line of sight and is a highly directional beam. Microwave requires a clear, unobstructed view, and can't move through any obstacles, even things you wouldn't think would be obstacles, such as leaves on a tree. Technologies that depend on line of sight may work brilliantly in areas that have the appropriate terrain and climate, and they may not perform very well where there are many obstacles or where there is a lot of precipitation. Furthermore, line of sight is restricted by the curvature of the earth, which interrupts the line of sight at about 144 km.

5.6.1.1 Terrestrial Microwave Physical Description

- The most common microwave antenna is the parabolic "dish".

- The antenna is fixed rigidly and focuses a narrow beam to achieve line-of-sight transmission to the receiving antenna.
- Microwave antenna is usually located at substantial heights above ground level in order to extend the range between antennas and be able to transmit over intervening obstacles.
- The maximum distance between antennas conforms to:

$$d = 4.14\sqrt{Kh}$$

d = distance between antennas,

h = antenna height in meters.

K= adjustment factor, K usually assumed to be = 3/4 adjustment factor for curvature of earth.

- To achieve a long-distance transmission, a series of microwave relay towers is used; point-to-point microwave links are strung together over the desired distance as shown in Figure 5.12.

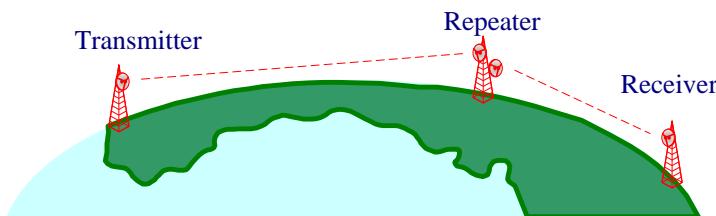


Figure 5.12: Achieve long-distance transmission using repeaters

5.6.1.2 Terrestrial Microwave Application

Most applications for terrestrial microwave are:

- Long-haul telecommunication service as an alternative to coaxial cable or optical fiber. Microwave facilities require far fewer amplifiers or repeaters, but require line-of-sight transmission. Commonly for both voice and television transmission.
- Short point-to-point links between buildings; this can be used for closed circuit TV as a data link between local area networks. It can also be used for the so-called bypass application. A business can establish a microwave link to a long-distance telecommunications facility in the same city, bypassing the local telephone company.
- The role of microwave has been greatly expanded since the 1980s, with applications in just about every network domain. The following are examples of the wireless systems that rely on microwave:
 - Wireless wide area networks (WWANs)
 - Wireless metropolitan area networks (WMANs)
 - Wireless local area networks (WLANs)
 - Wireless personal area networks (WPANs)

5.6.1.3 Terrestrial Microwave Transmission Characteristics

- Microwave Transmission covers a substantial portion of the electromagnetic spectrum. The common frequency is between 2 - 40 GHz.

- The higher frequency used higher potential bandwidth and the higher potential data rates.
- As with any transmission system, a main loss source of energy is due to attenuation.

$$\text{Loss} = 10 \log(4\pi d / \lambda)^2 \text{ [dB]}$$

Where,

d = distance

λ = wavelength

- Repeater spacing with microwave varies depending on the frequency of transmission. In microwave systems that operate in the 2GHz, 4GHz, and 6GHz bands, towers can be separated by 70 km. In the higher-frequency allocations, such as 18GHz, 23GHz, and 45GHz, the spacing needs to be much shorter, in the range of 1.5 to 8 km. This is an important issue in network design and, depending on the scope over which you want to deploy these facilities; it can have a significant impact on the investment required.
- Microwave is subject to the uncertainties of the physical environment. Metals in the area, precipitation, fog, rainfall, and a number of other factors can cause reflections and therefore degradations and echoes. The higher we move away from land-based systems, the better the performance because there is less intrusion from other land-based systems, such as television, radio, and police and military systems.
- With the growing popularity of microwave, transmission areas overlap and interference is always a danger. So assignment of frequency bands is strictly regulated. Before you can deploy a microwave system outside your own private campus, you have to be licensed to operate that system in all environments.
- The most common band for long-haul telecommunication is the 4 GHz - 6GHz bands. The 11 GHz band is now coming into use. 12GHz band is used as a component of cable TV system. Microwave link used to provide TV signals to local CATV installation. Signal then distribute to the subscribers. A 22 GHz band is used for short point-to-point links between buildings.
- The higher microwave frequency are less useful for longer distance because of increase attenuation but quite adequate for shorter distance. The higher frequencies, the smaller and cheaper antennas are needed.



Line-of-sight (LOS) microwave provides broadband bearer connectivity over a link or series of links in tandem. We can take advantage of this “line-of-sight” phenomenon at frequencies from 150 MHz and upwards into the millimeter spectrum. Each link can be up to 46 km long or more depending on terrain topology. Some links extend over 160 km.

5.6.2 Satellite Microwave

A communication satellite is used to link two or more ground-based microwave transmitter/receivers (transceivers), known as earth stations, or ground stations. International telecommunication is usually carried by commercial satellite.

Satellites operate in the microwave frequency spectrum. So microwave and satellite signals are really the same thing. The difference is that with satellite, the repeaters for augmenting the signals are placed on platforms that reside in high orbit rather than on terrestrial towers.

5.6.2.1 Satellite Microwave Physical Description

The power levels associated with satellite communications are greater than those of terrestrial microwave networks. If the satellite has a lot of power, you don't need as big a dish on the ground.

The transponder is the key communications component in satellite. It accepts the signal coming from the earth station and then shifts that signal to another frequency. When the signal is on the new frequency, it is amplified and rebroadcast downlink.

Footprint is a very important thing and unique to satellites. It refers to the area of earth that the satellite's beams cover.

Another important factor that affects the use and application of satellites is the orbits in which they operate. As shown in Figure 5.13, there are three major orbits: geosynchronous orbit (GEO), middle earth orbit (MEO), and low earth orbit (LEO). The majority of communications satellites in use are GEOs.

- **GEO Satellites:** A GEO satellite is launched to 22,300 miles (36,000 km) above the equator. GEO satellites have the benefit of providing the largest footprint of the satellite types. Just three GEO satellites can cover the entire world, but the delay factor in getting to that orbit inhibits its use with the continuously growing range of real-time applications that are very sensitive to delay. Satellite period of rotation equals the earth's period of rotation at height of 34,784 km.
- **MEO Satellites:** MEO satellites orbit at an elevation of about 6,200 to 9,400 miles (10,000 to 15,000 km). MEO satellites are closer to the earth than GEO satellites, so they move across the sky much more rapidly in about one to two hours. As a result, to get global coverage, you need more satellites (about five times more) than with GEO systems. But because the altitude is lower, the delay is also reduced.
- **LEO Satellites:** LEOs are a lot like cellular networks, except that in the case of LEOs, the cells as well as the users are moving. LEOs orbit at about 400 to 1,000 miles (640 to 1,600 km). LEOs can be used with smaller terminals than can the other satellites because they are much closer to the earth (40 times closer). But, again, because they are closer, you need many more LEOs than other satellites to get the same coverage (about 20 times more LEOs than GEOs and 5 times more LEOs than MEOs). A user must always be able to see at least one LEO satellite that is well clear of the horizon.

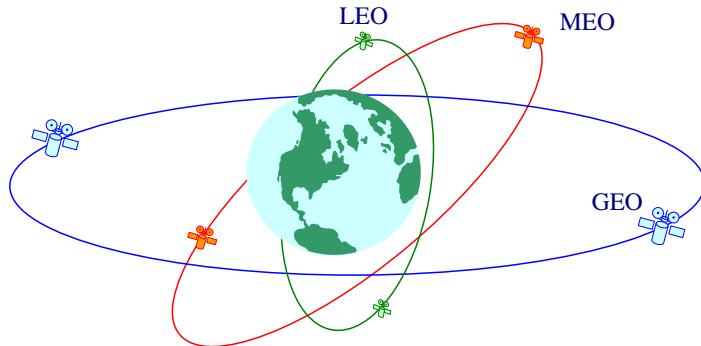


Figure 5.13: Orbits of satellites

- The satellite receives transmissions on one frequency band (uplink), amplifies or repeats the signal, and transmits it on another frequency (downlink). A single orbiting satellite will operate on a number of frequency bands, called transponder channels, or simply transponders.
- In satellite communications, the frequency allocations always specify two different bands: One is used for the uplink from earth station to satellite and one for the downlink from satellite to earth station.

The most dominant frequency bands used for communications are C-band, Ku-band, Ka-band, and L-band.

- **C-Band:** C-band transmits uplink around the 6GHz range and downlink around the 4GHz range.
- **Ku-Band:** Ku-band was introduced in the early 1980s, and it revolutionized how we use satellite communications. It operates on the uplink at around 14GHz and on the downlink at around 11GHz.
- **Ka-Band:** Ka-band offers a wide frequency band about 30GHz uplink and about 20GHz downlink. This expanded bandwidth means that Ka-band satellites are better prepared than satellites operating at other bands to accommodate telemedicine, tele-education, telesurveillance, and networked interactive games.
- **L-Band:** L-band operates in the 390MHz to 1,550MHz range, supporting various mobile and fixed applications. It is largely used to support very-small-aperture terminal (VSAT) networks and mobile communications, including handheld terminals (such as PDAs), vehicular devices, and maritime applications.

5.6.2.2 Satellite Microwave Application

Among the important application for satellites are:

- Television distributing: Satellites are well suited to television distribution and being used extensively throughout the world. In its traditional use, a network provides programming from a central location. Program then transmitted to the satellite and then broadcast down to a number of stations, which then distribute the programs to individual viewers. The Public Broadcasting Service (PBS), distribute its television programming almost exclusively by the use of satellite channels. Other commercial networks also make substantial use of satellite in the cable television system which are receiving most of their broadcasting from satellites. The most recent application of satellite technology to television distribution is direct broadcast satellite (DBS) in which satellite video signals are transmitted directly to home user. DBS is economically feasible, and a huge number of channels are already in service in both analog and digital systems.
- Long-distance telephone transmission: Point-to-point trunks between telephone exchange offices in public telephone networks. It is the optimum medium for high usage international trunks and is competitive with terrestrial systems in long distance international links.
- Private business networks: The satellite provider can divide the total capacity into a number of channels and lease these channels to individual business users. A user equipped with the antennas at a number of sites can use a satellite channel for a private network. Traditionally, such applications have been quite expensive and limited to larger organizations with high-volume requirements. Recent development is the very small aperture terminal (VSAT) system, which provide low cost alternative. Numbers of subscriber stations are equipped with low cost VSAT antennas. Using some protocol, these stations share a satellite transmission capacity for transmission to a hub station. The hub station exchange messages with each of the subscribers as well as relay messages between subscribers.

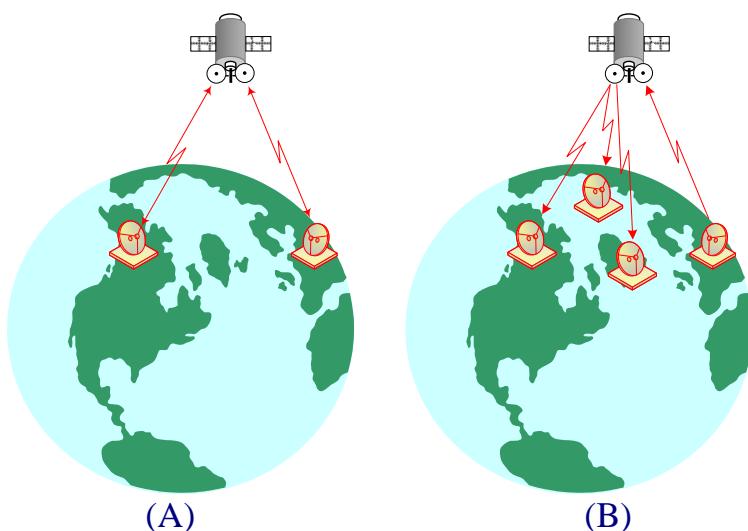


Figure 5.14: (A) Point-to-Point transmission and (B) Broadcasting transmission

- The application of the satellite microwave is related to the orbit of the satellite for example:
 - The main applications of GEO systems are one-way broadcast, VSAT systems, and point-to-multipoint links. There are no delay factors to worry about with one-way broadcasts from GEO systems. As a result, international television is largely distributed over these satellite networks today.
 - The main applications for MEOs are in regional networks, to support mobile voice and low-speed data, in the range of 9.6Kbps to 38Kbps.
 - The key applications for LEOs are support for mobile voice, low-speed data, and high-speed data.
- Several properties of satellite must be noted:
 - Long distance is involved, propagation delay of about a quarter second between transmission from earth station and reception to another earth station. This delay is noticeable in ordinary telephone conversation. Also introduce problem in the areas of error control and flow control.
 - Satellite microwave is inherently a broadcast facility. Many stations can transmit to the satellite, and many stations can receive a transmission from a satellite. And it can be designed for special needs as a point-to-point transmission. Figures 5.14 (A) and (B) illustrate the two types.

5.6.3 Broadcasting Radio

Unlike microwave transmission that is directional Broadcast radio transmission is omnidirectional Broadcast. The signals in radio broadcasting need simpler antennas, and it may not be rigidly mounted to a precise alignment.

Current broadcasting systems such as radio and TV use technologies that were originally developed in the 1940s. Even though some updates have been made such as color TV, stereo sound, and radio data system (RDS), current systems do not meet the quality requirements of the future. Another problem with these systems is that they do not utilize radio frequencies as efficiently as more modern technologies do.

Broadcast radio frequencies range of 30 MHz to 1 GHz covers FM radio as well as UHF and VHF television. This range is also used for a number of data-networking applications.

Range of 30 MHz to 1 GHz is an effective one for broadcast communications. Unlike the case for lower-frequency electromagnetic waves, the ionosphere is transparent to radio waves about 30 MHz. Transmission is limited to line of sight, and distant transmitters will not interfere with each other due to reflection from the atmosphere. Broadcast radio waves are less sensitive to attenuation from rainfall.

Prime source of impairment for broadcast radio waves is multipath interference. Reflection from land, water and natural or human-made objects can create multiple paths between antennas. This effect is frequently evident when TV reception displays multiple images as an airplane passes by.



High Performance Radio LAN is the wireless personal area networks (WPANs) that occupy the space surrounding an individual or device, typically involving a 10m radius. This is referred to as a personal operating space (POS).

5.6.4 Infrared

Infrared communication is achieved using transmitters/receivers (transceivers) that modulate noncoherent infrared light. The most important difference between infrared and microwave transmission is the former does not penetrate walls. Thus the security and interference problem encountered in microwave systems are not present. There is no frequency allocation issue with infrared, because no licensing required.

Infrared portion is below the visible light portion (400 – 700) nanometers (nm). The loss is lower at higher wavelength allowing greater data rates over longer distances.

Three alternative transmission techniques are used for infrared data transmission:

- The directed beam involves point-to-point connections. The range of communications is limited by the transmitted power and the direction of focus. With proper focusing, ranges up to a kilometer can be achieved. This technology can be used in token-ring LANs and interconnections between buildings.

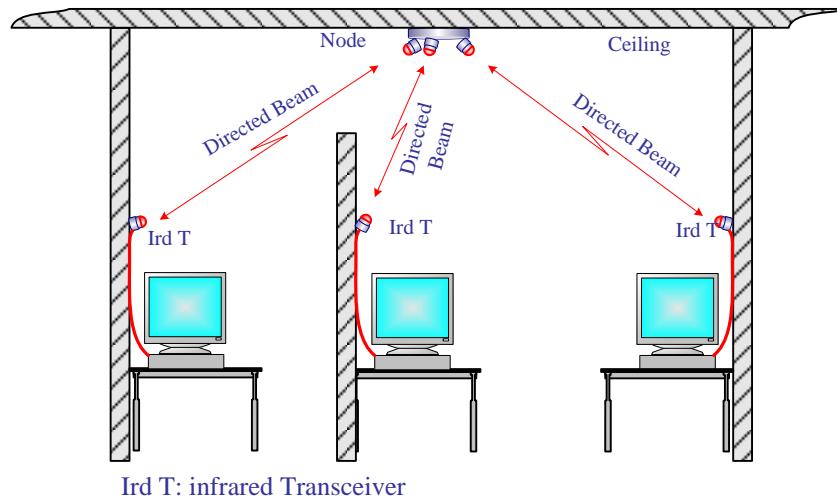


Figure 5.15: Infrared directed beam technique

- The omnidirectional configuration consists of a single Base station that is normally used on ceilings. The Base station sends an omnidirectional signal, which can be picked up by all transceivers. The transceivers in turn use a directional beam focused directly at the Base-station unit.

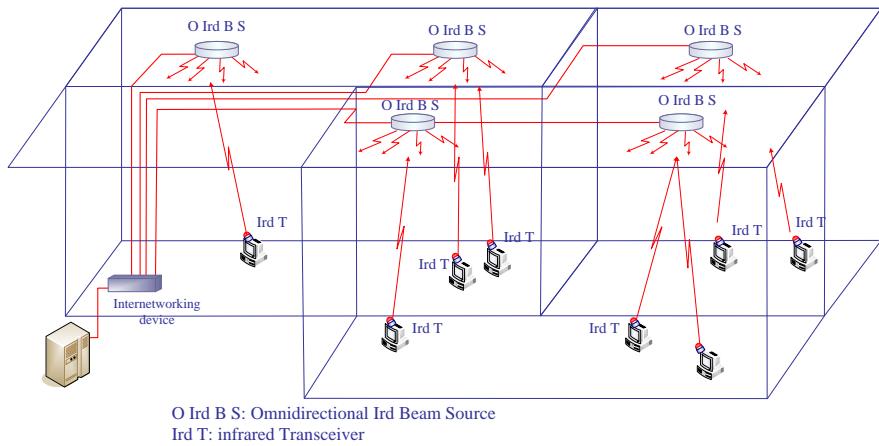


Figure 5.16: Infrared omnidirectional configuration technique

- In the diffused-configuration method, the infrared transmitters direct the transmitted signal to a diffused reflecting ceiling. Light is diffusely reflected and scattered in the room from a wide-angle source or a diffusing spot formed on a reflector. It is received by wide-acceptance-angle photodetector portable units located anywhere in the room. The advantages of this configuration are that there are no alignment requirements and that there is freedom of movement. The signal is reflected in all directions from this ceiling. The receivers can then pick up the transmitted signal.

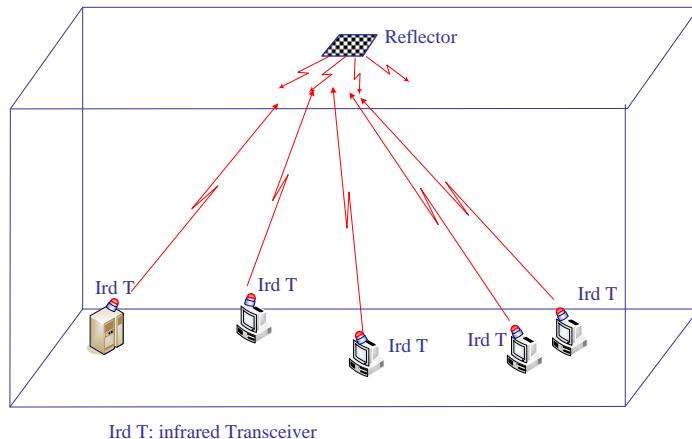


Figure 5.17: Infrared diffused-configuration technique

The use of infrared has several advantages:

- The bandwidth for infrared communication is large and can therefore achieve high data rates.
- Also, because infrared rays are reflected by lightly colored objects, it is possible to cover the entire area of the room with reflections from objects. Since infrared cannot penetrate through walls and other opaque obstacles, it becomes very

difficult for any adversary to carry out a passive attack or to eavesdrop. Hence, communication with infrared technology is more secure.

- Also, separate infrared networks can be used in adjacent rooms without any interference effects.
- Finally, equipment for infrared communication is much cheaper than microwave communication.

The one major disadvantage of infrared technology is that background radiation from sunlight and indoor lighting can cause interference at the infrared receivers.



An optical wireless system basically is defined as any system that uses modulated light to transmit information in open space or air using a high powered beam in the optical spectrum. It is also referred to as free space optics (FSO), open air photonics, or infrared broadband.

5.6.5 Bluetooth

Bluetooth technology allows for the replacement of proprietary cables that connect one digital device such as mobile computers, cellular handsets, printers, keyboards, and many other devices to another with a universal short-haul radio link.

A small wireless Bluetooth network connecting, for example, a user's computer to its peripherals is called a personal area network (PAN). In PAN You can network up to eight Bluetooth devices together in a master-slave relationship, called a piconet. In a piconet, one device becomes the designated master for the network with up to seven slaves directly connected. The master device controls and sets up the network, which includes defining the network's hopping scheme. The master may have a total of 256 connections, but only seven can be active at any time. A master can suspend its connection to a slave by parking it and taking another slave. Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence.

Although only one device may perform as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. And, a device can act as a slave in two piconets. By linking a series of piconets, you can create scatternets, which allow the internetworking of several devices over an extended distance. This relationship also allows for a dynamic topology that may change during any given session: As a device moves toward or away from the master device in the network, the topology and therefore the relationships of the devices in the immediate network change. Figure 5.18 shows the relationship of piconets and scatternets.

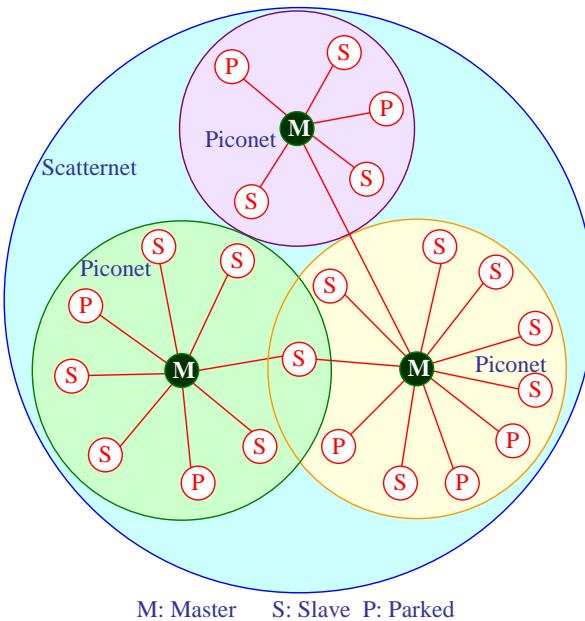


Figure 5.18: Bluetooth network topology

Bluetooth systems use the same 2.4-GHz license free frequency band as WLANs and they can coexist in the same area. The wideband WLAN signals and narrowband Bluetooth signals do not interfere much.

Bluetooth-enabled devices will automatically locate each other, but making connections with other devices and forming networks may require user action. Sometimes they connect automatically, which a feature is called unconscious connectivity.



Bluetooth technology was named after Harold Blaatand (Bluelooth) II, who was the King of Denmark from 940–981 and was generally considered a “unifying figurehead” in Europe during that period. The unification of Europe and the unification of PDAs and computing devices is the parallelism that the founders of this technology sought to create when they chose the name Bluetooth.

5.6.6 Cellular Mobile Systems

The term cellular describes how each geographic region of coverage is broken up into cells. Within each of these cells is radio transmitter and control equipment. Each cell is assigned a small frequency band and is served by a Base station. Neighboring cells are assigned different frequencies to avoid interference.

Oriented in a honeycomb fashion shown in Figure 5.19, each cell is kept small, so that the radio transmitting power required at the transmitting Base station can be kept low.

This limits the area over which the radio signal is effective, and therefore reduces the area over which radio signal interference can occur.

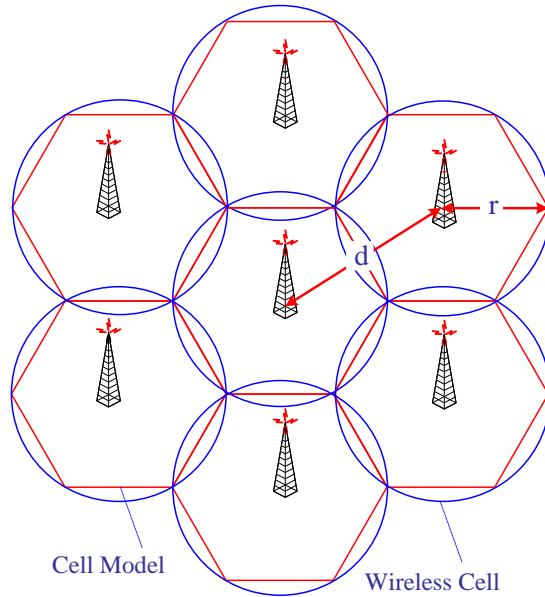


Figure 5.19: The hexagonal pattern of cellular network

The hexagonal pattern of a cell is chosen so that the distance d between the centers of any two adjacent cells becomes the same. Distance d is given by

$$d = \sqrt{3}r$$

where r is the wireless cell radius. A typical practical value for the cell radius is 3 km to 5 km.

The exact shape of the cells (cell model) actually varies quite a bit due to several factors, including the topography of the land, the anticipated number of calls in a particular area, the number of man-made objects (such as the buildings in a downtown area), and the traffic patterns of the mobile users. This maximizes the number of mobile users.

A lower powered antenna is placed at a strategic place, but it is not in the center of the cell, as you might think. The tower then uses directional antennas that point inward to each of the adjacent cells. By using the appropriately sized transmitter, frequencies in one particular cell are also used in nearby cells. The key to success is making sure cells using the same frequency cannot be situated right next to each other, which would result in adverse effects. Figure 5.20 illustrates the principle of frequency reuse. The benefit is that a service provider is able to reuse the frequencies allotted to them continually so long as the system is carefully engineered. Figure 5.20 illustrates the principle of frequency reuse.

As a cell phone moves through the cells, in a car for example, the cell switching equipment keeps track of the relative strength of signal and performs a handoff when the signal becomes more powerful to an adjacent cell site. If a particular cell becomes too congested, operators have the ability to subdivide cells even further.

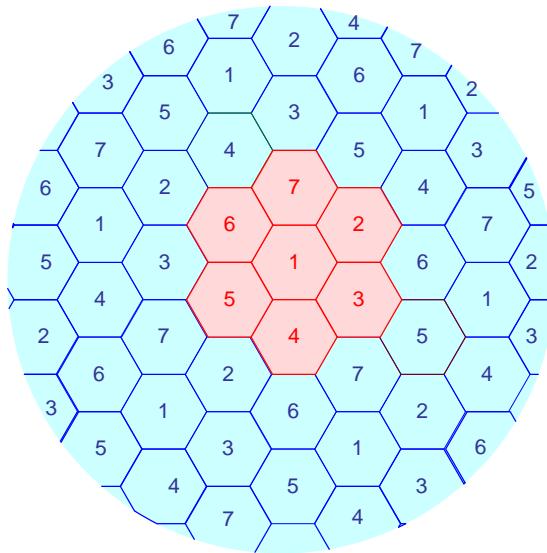


Figure 5.20: Illustration of frequency reuse principle

Signals from the mobile user terminal arrive at an antenna that provides an RF interface to the fixed wireless infrastructure, and that infrastructure in turn provides an interface to the fixed wired infrastructure. In the case of cellular systems, the fixed wired infrastructure will typically be a public-switched telephone network (PSTN) or a public-switched data network , PSDN (PSDN). In the case of WLAN systems, the fixed network will typically be a wired Ethernet LAN in an office building, office complex, or university campus.

In the case of cellular systems, the fixed wireless infrastructure includes antennas, radio Base stations (BSs) , mobile switching centers (MSCs), and terrestrial lines (typically, coaxial cable or optical fiber) to make connections among BSs and MSCs as well as between MSCs and the PSTN. The fixed wireless infrastructure will also include computers and a variety of instrumentation needed for operation and maintenance of the cellular network. All of the equipment and software in place, from the antennas to the PSTN connections, will be owned and operated by the cellular service provider.

A wireless local area network transmits over the air by means of Base stations, or access points, that transmit a radio frequency; the Base stations are connected to an Ethernet hub or server. Mobile end-users can be handed off between access points, as in the cellular phone system, though their range generally is limited to a couple hundred feet. Figure 5.20 shows the connectivity of two mobile users in cellular systems. The Base station is connected to the mobile switching center (MSC). An MSC serves several Base stations and is responsible for connecting calls between mobile units. An MSC is also connected to the public telephone system to enable communication between a fixed subscriber and mobile subscriber. An MSC also manages mobility and accounting for user billing.

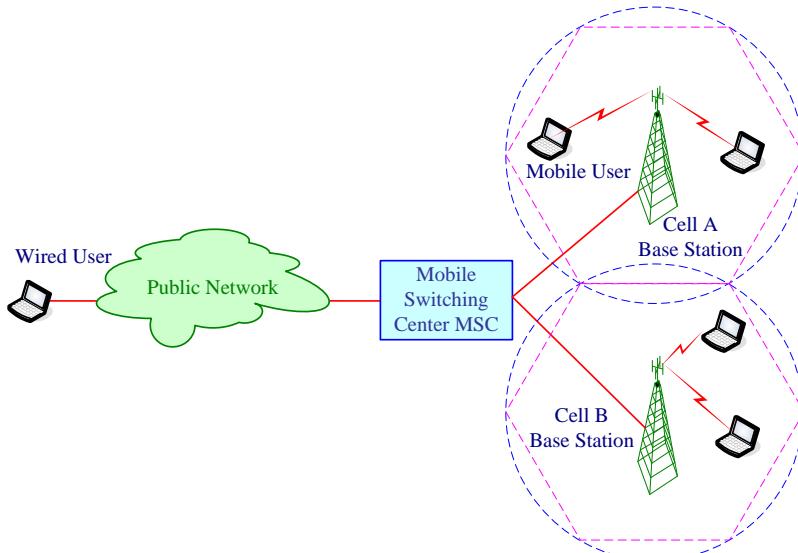


Figure 5.20: The connectivity of two mobile users in cellular systems.



Since 1980, mobile radio communication has taken on a more personal flavor. Cellular radio systems have extended the telephone network to the car, to the pedestrian, and even into the home and office. A new and widely used term in our vocabulary is personal communications. It is becoming the universal tether. No matter where we go, on land, at sea, and in the air, we can have near instantaneous two-way communications by voice, data, and facsimile. At some time it will encompass video.

5.7 Summary

- ❖ Traditional transmission systems include DTE, physical interface, DCE and transmission medium
- ❖ Modern long-distance links use either radio or fiber-optic cable as the medium. The decision on which one to use is driven by economics more than any other factor. However, capacity can well be another deciding factor.
- ❖ Data can travel on guided links, such as twisted pairs, coaxial cables and optical fiber cables, and unguided links, such as certain types of wireless links such as microwave links, satellite links, cellular networks, infrared links and Bluetooth nets.
- ❖ Network cabling consisting of copper wire has been the predominant network connectivity medium since the very beginning of the local area network.
- ❖ Every type of guided medium requires special equipment to connect the computer to the network backbone.

- ❖ Twisted-pair wire comes in two major flavors: unshielded twisted pair (UTP) and shielded twisted pair (STP). The big difference between UTP and STP is that the STP wires are encased in a foil wrap that protects them from interference.
- ❖ UTP cable has been placed in different categories based on data-transmission capabilities.
- ❖ Fiber-optic cable is a high-speed alternative to copper wire it uses pulses of light as its data-transfer method and is often employed as the backbone of larger corporate networks. Fiber-optic cable is more expensive and more difficult to install than copper cable. On networks where security is an issue, fiber-optic cable provides a more secure environment.
- ❖ We can summarize the main characteristics of guided transmission medium in the following table:

Cable Type	Cable Cost	Installation Cost	EMI Sensitivity	Data Bandwidth
UTP	Lowest	Lowest	Highest	Lowest
STP	Medium	Moderate	Low	Moderate
Coax	Medium	Moderate	Low	High
Optical fiber	Highest	Highest	None	Very high

- ❖ Wireless network connections take advantage of radio signals, infrared light, or lasers. For longer distances, wireless communications can also take place through cellular telephone technology through microwave transmission, or via satellite.
- ❖ Bluetooth replaces the cables necessary for short-range communication within 10 meters and operates at 2.4 GHz frequency band and supports data rates of 700 Kb/s.
- ❖ Infrared systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Infrared can be used as unguided transmission medium using one of three techniques, the directed beam, the omnidirectional and the diffused-configuration
- ❖ The radio-frequency spectrum is shared with others and requires licensing. Metallic and fiber medium need not be shared and do not require licensing.
- ❖ A cellular network includes a networked array of Base stations, each located in a hexagonal cell to cover networking services.
- ❖ Frequency reuse in a certain region of a wireless network occurs when the same frequency used in one area could be reused to cover another area.
- ❖ Deployment of wireless medium is faster and less costly than deployment of cable, particularly where there is little or no existing infrastructure. And where environmental circumstances make it impossible or cost-prohibitive to use cable.
- ❖ Wireless is greatly affected by external impairments, such as the impact of adverse weather, so reliability can be difficult to guarantee.

5.8 Self Test Questions

A- Answer the following questions

1. What is transmission in telecommunication?

2. What is message in telecommunication?
3. List the transmission medium types.
4. How can data transmission be divided depending on the nature of sent message format?
5. What is communications channel?
6. Name the transmission modes
7. What are the guided transmission medium?
8. List the types of guided transmission medium
9. What are the unguided transmission medium?
10. List the types of unguided transmission medium
11. List the twisted-pair categories.
12. What are the main applications of coaxial cable?
13. What are the types of Optical fiber cable?
14. What are the main applications of Optical fiber cable?
15. What are the main characteristics that make the Optical fiber cables superior in comparison with coaxial cables and twisted pair?
16. List the types of unguided medium.
17. Where are terrestrial microwave links applicable?
18. What are the three major satellite orbits?
19. What are the most dominant frequency bands used for communications?
20. What are the infrared configurations?
21. How a small wireless Bluetooth network can be configured?
22. Illustrate the connectivity of two mobile users in cellular systems.

B- Identify the choice that best completes the statement or answers the question.

1. _____ is the simplest and most common type of conducted medium
 - a. broadband coaxial cable.
 - b. Baseband coaxial cable.
 - c. twisted pair wire.
 - d. Optical fiber cable.
2. Optical fiber cable can transmit data at over _____.
 - a. 100 MHz.
 - b. 100 Kbps.
 - c. 100 Mbps.
 - d. 100 Gbps.
3. _____ is NOT an example of conducted medium.
 - a. Optical fiber cable
 - b. AM radio
 - c. twisted pair wire
 - d. Baseband coaxial cable
4. Which of the following technologies has the potential to replace infrared for short-distance wireless connections?
 - a. WAP
 - b. Pager
 - c. Bluetooth
 - d. PCS
5. _____ can accept both analog and digital signals.
 - a. GEO satellite
 - b. terrestrial microwave
 - c. cellular
 - d. Personal Communication Systems

29. Fiber-optic cables can handle network transmissions from 100 Mbps to ____.
- a. 1 Gbps
 - b. 10 Gbps
 - c. 100 Gbps
 - d. 1 Tbps
30. A ____ cable consists of a single cable sheath that contains fibers and copper cables in different combinations for different implementations
- a. coax
 - b. twisted-pair
 - c. hybrid fiber/coax
 - d. fiber-optic
31. ____ uses twisted-pair cable with an extra foil shield to guard against EMI?
- a. Thinnet
 - b. UTP
 - c. Thicknet
 - d. STP
32. Regarding crosstalk problems, what is the effect of having more twists per inch in a pair of wires?
- a. The cable is less resistant to crosstalk
 - b. There is no effect
 - c. The cable is more resistant to crosstalk
 - d. The cable is less resistant but thicker
33. With respect to twisted-pair cabling, coaxial cables can carry signals:
- a. for more distance
 - b. for less time
 - c. for less distance
 - d. for equal distance
34. ____ is a form of UTP that contains four wire pairs and can carry up to 10 Mbps of data with a possible bandwidth of 16 MHz.
- a. CAT 3
 - b. CAT 5
 - c. CAT 4
 - d. CAT 7
35. ____ is a form of UTP that contains four wire pairs and supports up to 1000 Mbps throughput and a 100 MHz signal rate
- a. CAT 4
 - b. CAT 6
 - c. CAT 5
 - d. CAT 7
36. ____ is the significant drawback in using fiber.
- a. Its cost
 - b. It is susceptible to noise
 - c. It is not reliable
 - d. Low security levels
37. Fiber-optic cabling is resistant to ____.
- a. Regeneration
 - b. Attenuation
 - c. Segmentation
 - d. EMI
38. What are the satellites that found between 100 and 1,000 miles from Earth?
- a. GEO
 - b. LEO
 - c. MEO
 - d. HEO
39. What are the satellites that found between 1,000 and 22,300 miles from Earth?
- a. GEO
 - b. LEO
 - c. MEO
 - d. HEO
40. What are the satellites that found at 22,300 miles from Earth?
- a. GEO
 - c. MEO

CHAPTER 6

DATA LINK SERVICES AND LAN PROTOCOLS

6.1 About This Chapter

Protocols designed for LANs are normally concerned with the data-link layer and the physical layer. Link-layer protocols including Ethernet, token ring, FDDI, PPP, ATM and frame relay are used to move a datagram over an individual link. These protocols in general define the format of the data unit exchanged between the nodes at the ends of the link, as well as the actions taken by these nodes when sending and receiving this data unit. Data unit exchanged by a link-layer protocol is called frame which encapsulates one network-layer datagram. It is the network adaptor that enables the nodes to exchange frames. The actions taken by a link-layer protocol when sending and receiving frames include error detection and sometimes correction, retransmission, flow control and medium access control.

Link-layer protocol has the node-to-node job of moving a network-layer datagram over a single link in the path. But the details of the link-layer service depend on the specific link-layer protocol that is employed over the link. In this chapter we will introduce possible services that can be offered by a link-layer protocol including framing, medium access control, reliable delivery, flow control, error detection, and error correction.

6.2 Learning outcome

After this chapter, you will be able to:

1. Understand the role, and the importance of data link protocols and the services provided by them.
2. Understand the role and the structure of physical addresses in LANs.
3. Understand the role of framing in data transmission and explain the frame structure.
4. Understand the shared medium access problem.
5. Classify and explain the most popular MAC methods.
6. Understand the importance of reliable data transmission.
7. Classify and explain flow control methods used by data link layer.
8. Classify and explain error detection type methods used in LANs.
9. Understand the principles of error detection and correction of data.

6.3 The Services Provided by the Data Link Layer

The IEEE 802 standard subdivides the data-link layer of the protocol model into the logical-link control (LLC) layer and the medium access control (MAC) layer as it was previously illustrated (see Figure 2.7).

The LLC layer implements flow and error control apart from providing an interface to the network layer. The MAC layer primarily controls the access to transmission medium

and is responsible for framing. LLC has the option of choosing from various types of MAC layers.

Logical-Link Control Layer (LLC): Data to be transmitted from the higher layers is passed down to the logical-link layer, which

- Determines the mechanism for addressing users across the medium.
- Controls the exchange of data between each two users.
- Manages communications between devices over a single link of a network
- Performs flow and error control
- Supports both connectionless and connection-oriented services used by higher-layer protocols

The LLC appends its header to form the LLC protocol data unit, which is then sent to the MAC layer, which appends the header and the frame check sequence to create the MAC frame.

Medium Access Control (MAC): A LAN is required to provide sharing access to the transmission medium. To ensure efficient access to a medium, users have to comply with some rules. The MAC protocol

- Assemble data into frames with addresses and error detection-fields.
- Manages protocol access to the physical network medium.



The LLC sublayer performs tasks such as call setup and termination and data transfer. The MAC sublayer handles frame assembly and disassembly, error detection and correction, and addressing.

The data-link layer defines standards that assign meaning to the bits carried by the physical layer. It establishes a reliable protocol through the physical layer so the network layer can transmit its data. The data elements carried by the data-link layer are called frames. Examples of frame types include X.25 and 802.x (802.x includes both Ethernet and Token Ring networks).

LLC	<ul style="list-style-type: none"> ○ 802.2 ○ (Un) acknowledged connectionless service ○ Connection-oriented service 						
MAC	CSMA/CD 802.3	Token bus 802.4	Round robin priority 802.12	Token Ring 802.5	Token Ring FDDI	DQDB 802.6	CSMA?CA 802.11
Physical	Base band/ Broad band Coaxial Twisted pair Optical fiber	Broad band/ Carrier Band Coaxial Optical fiber	Twisted pair	Twisted pair	Twisted pair Optical fiber	Optical fiber	Infrared Spread Spectrum
topology	Bus/Tree/Star topologies		Ring topology		Dual bus topology		Wireless

Figure 6.1: IEEE 802 standard for LAN protocols

The two most common MAC protocols are 802.3 Ethernet and 802.5 Token Ring. Other MAC protocols include 100BaseVBG (802.12) and wireless 802.11. On most

systems, drivers for the NIC perform the work done at the data-link layer. Figure 6.1 summarizes IEEE 802 standard for LAN protocols.



The LLC uses the MAC services to provide two types of data-link operations to the network layer above it: LLC1 for connectionless and LLC2 for connection-oriented data-link communication services (known as Type 1 and Type 2, respectively).

6.4 Framing

Almost all link-layer protocols encapsulate each network-layer datagram within a link-layer frame before transmission onto the link. Frames are exchanged between nodes. When node A wishes to transmit a frame to node B, it tells its adaptor to transmit a frame from the node's memory. This results in a sequence of bits being sent over the link. The adaptor on node B then collects together the sequence of bits arriving on the link and deposits the corresponding frame in B's memory. Recognizing exactly what set of bits constitutes a frame—that is, determining where the frame begins and ends—is the central challenge faced by the adaptor.

A frame consists of a data field, in which the network-layer datagram is inserted, and a number of header fields. A frame may also include trailer fields; however, sometimes both header and trailer fields are called header fields. A data link protocol specifies the structure of the frame, as well as a channel access protocol that specifies the rules by which a frame is transmitted onto the link.

6.4.1 Frame Structure

The formatting of the data is a critical part of a LAN protocol. Data formats let the receiving device logically determine what is to be done with the data and how to go about doing it. Data formats include code type, message length, and transmission validation techniques. Figure 6.2 shows a generic MAC frame. The fields of the frame format are as follows:

- TCP header specifies the TCP header of the original packet. IP header specifies the IP header of the original packet (in later chapter we will explain these two header in details).
- LLC header contains the data from the logical-link layer.
- MAC header gives the MAC control information, such as the MAC source and destination addresses and the priority level.
- Frame check sequence is used for error checking.

LLC forms the upper half of the data link layer, with the MAC sub layer below it. The LLC layer implements flow and error control apart from providing an interface to the network layer. LLC header includes the option of choosing from various types of MAC layers and how to control the exchange of data between each two users. So LLC hides the differences between the various kinds of 802 networks by providing a single format and

interface to the network layer. The LLC appends its header to form the LLC protocol data unit, which is then sent to the MAC layer, which appends the header and the frame check sequence to create the MAC frame.

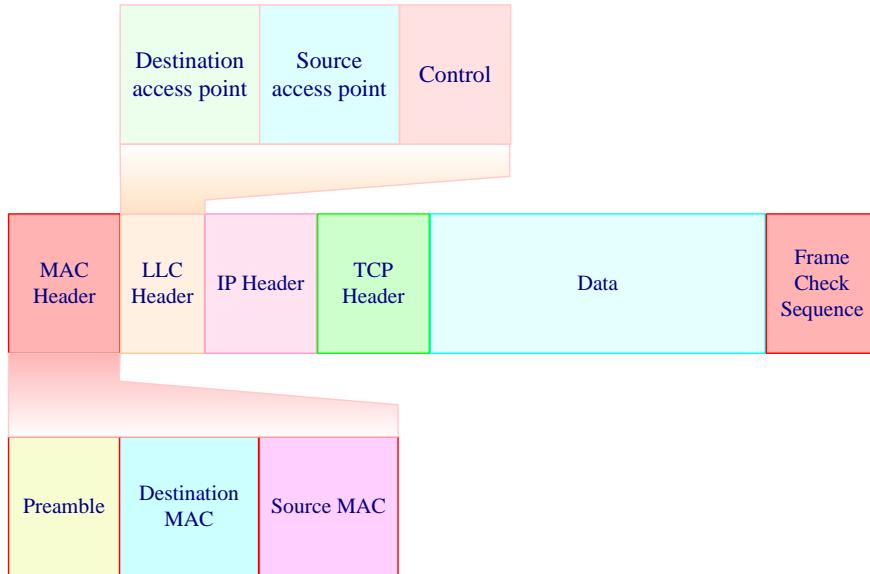


Figure 6.2: generic MAC frame format

The network layer on the sending machine passes a packet to LLC, using the LLC access primitives. The LLC sub layer then adds an LLC header, containing sequence and acknowledgement numbers. The resulting structure is then inserted into the payload field of an 802 frame and transmitted. At the receiver, the reverse process takes place.

LLC provides unreliable datagram service, acknowledged datagram service, and reliable connection-oriented service. The LLC header contains the following fields:

- **Destination access point field:** tells from which process did the frame came from
- **Source access point field:** tells to which process the frame will be delivered
- **Control field:** contains sequence and acknowledgement numbers

These fields are primarily used when a reliable connection is needed at the data link level as in wireless transmission used. In other application as the Internet, best-efforts attempts to deliver IP packets are sufficient, so no acknowledgements at the LLC level are required.



Each particular local area network (LAN) or wide area network (WAN) data-link protocol has its own method of framing data for transmission over the network or telecommunications line. The format in which data frames are constructed depends on the particular data-link layer protocol being used.

6.4.2 MAC Addressing

A MAC address is as wide as 6 bytes and is normally shown in hexadecimal notation (48 bits in length and are expressed as twelve hexadecimal digits), such as 25-00-4A-C3-85-BB. The MAC address is unique for each device and is permanently stored in the adapter's read-only memory. As it is shown in Figure 6.3, the first six hexadecimal digits, which are administered by the IEEE, identify the manufacturer or vendor and thus comprise the Organizational Unique Identifier (OUI).

Consequently, networking manufacturers need to purchase MAC addresses for their products. The remaining six hexadecimal digits comprise the interface serial number, or another value administered by the specific vendor. MAC addresses are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the NIC initializes.



Unlike an IP address, a MAC address is not hierarchical. The advantage of MAC addressing is that a device may not need to have an IP address in order to communicate with the surrounding devices in its own LAN.

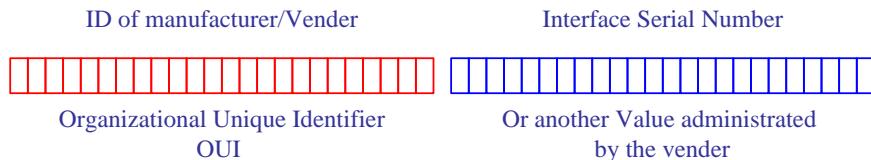


Figure 6.3: MAC Address Structure

Each destination address specified in an IP header is the logical address and is different from the physical (MAC) address. For a packet from a source host to be delivered successfully to its destination, the host needs to identify both the IP address and the MAC address. The source uses the address resolution protocol (ARP) and Reverse Address Resolution Protocol (RARP) to match the logical and physical address of a destination (we will return to these protocols in the coming chapters).

Each node adapter that receives a frame checks whether the MAC address of the frame matches its own MAC address. If the addresses match, the adapter extracts the inner packet and passes it up the protocol stack.

6.5 Shared medium and multiple access problem

The different types of LAN may be characterized by their distinctive topologies, but all comprise a single shared medium transmission path interconnecting all the data terminal devices. Multiple computers must share access to the medium that connects them. However, if two computers were to put data onto the medium at the same time, the data frame from one computer would collide with the frames from the other computer, and both sets of data frame would be destroyed. A unique characteristic of a shared medium is its ability to support atomic broadcast, in which all devices on the medium can monitor network activities and receive the information transmitted on the shared medium.



There are two major classes of shared-medium networks: local area networks mainly used to construct computer networks that span physical distances no longer than a few kilometers, and backplane buses, mainly used for internal network communication.

Typically, when there is a collision, none of the receiving nodes can make any sense of any of the frames that were transmitted; in a sense, the signals of the colliding frame become inextricably tangled together.

In order to ensure that the broadcast channel performs useful work when multiple nodes are active, it is necessary to somehow coordinate the transmissions of the active nodes. This coordination job is the responsibility of the **multiple access protocol**.

We can broadly classify any multiple access protocol as belonging to one of three categories: **channel partitioning protocols**, **random access protocols**, and **taking-turns protocols**.

6.5.1 Channel Partitioning Protocols

Time Division Multiple Access (TDMA) and Frequency Division Multiplexing (FDMA) are two techniques that can be used to partition a broadcast channel's bandwidth among all nodes sharing that channel. TDMA divides time into **time frames** and further divides each time frame into N **time slots**. Each slot time is then assigned to one of the N nodes.

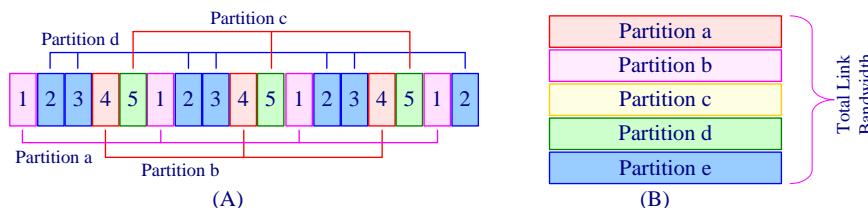


Figure 6.4: A four-node TDMA (A) and FDMA (B) example

Whenever a node has a frame to send, it transmits the frame's bits during its assigned time slot in the revolving TDMA frame. Typically, frame sizes are chosen so that

a single frame can be transmitted during a slot time. Figure 6.4 shows a simple four-node TDMA and FDMA examples.

FDMA divides the channel into different frequencies and assigns each frequency to one of the N nodes. FDMA shares both the advantages and drawbacks of TDMA. It avoids collisions and divides the bandwidth fairly among the N nodes.

A third channel partitioning protocol is **Code Division Multiple Access (CDMA)**. While TDMA and FDMA assign times slots and frequencies, respectively, to the nodes, CDMA assigns a different code to each node. Each node then uses its unique code to encode the data bits it sends. CDMA allows different nodes to transmit simultaneously and yet have their respective receivers correctly receive a sender's encoded data bits.

6.5.2 Random Access Protocols

In a random access protocol, a transmitting node always transmits at the full rate of the channel. When there is a collision, each node involved in the collision repeatedly retransmits its frame until the frame gets through without a collision. If a node experiences a collision, it doesn't necessarily retransmit the frame right away. Instead it waits a random delay before retransmitting the frame. Each node involved in a collision chooses independent random delays. Because after a collision the random delays are independently chosen, it is possible that one of the nodes will pick a delay that is sufficiently less than the delays of the other colliding nodes, and will therefore be able to "sneak" its frame into the channel without a collision.

The most commonly used random access protocols are the **ALOHA**, **Slotted ALOHA**, and **Carrier Sense Multiple Access (CSMA)**

6.5.2.1 ALOHA, Slotted ALOHA

In both slotted and pure ALOHA, a node's decision to transmit is made independently of the activity of the other nodes attached to the broadcast channel. In particular, a node neither pays attention to whether another node happens to be transmitting when it begins to transmit, nor stops transmitting if another node begins to interfere with its transmission.

In the basic Aloha scheme, each transmitter sends data frames whenever it has data available to send. This naturally leads to a large number of collisions, and hence a number of data frames have to be retransmitted. Hence, the effective throughput of the Aloha channel is very low because the probability of frames collisions is high. The slotted Aloha scheme was developed to deal with the collision problem. In slotted Aloha, the time is divided into slots, and frames transmission is restricted to these time slots. Thus, the number of collisions is reduced significantly. The throughput with slotted Aloha is double that with basic Aloha.

6.5.2.2 CSMA - Carrier Sense Multiple Access

Carrier Sense Multiple Access (CSMA) is a protocol that lets only one user at a time transmits, on a first come, first served basis. A user needing to transmit data first listens to the medium and senses for a carrier on the medium to determine whether other users are transmitting: the carrier-sense phase. If the medium is busy, the user has to wait until the

medium is idle. The amount of time a user must wait depends on the particular type of the protocol. If no other users transmit data, the user proceeds to transmit its data onto the medium.

If two or more users simultaneously try to transmit, a collision of frames occurs, and all data is corrupted. In such a case, all corresponding users stop transmitting. Thus, after a collision, all the users involved will start contention, each after a randomly chosen amount of time. After finishing the transmission of data, a user waits for an acknowledgment from the destination user. If the acknowledgment does not arrive, the user retransmits the data.

The main disadvantage of CSMA when a collision occurs is that other users cannot use the medium until all corrupted frames finish transmission. This problem increases in the case of long frames. However, this issue can be resolved with the use of CSMA/CD, whereby:

- A user listens to the channel while transmitting data. In case of a collision, the transmission is halted, and a jamming signal is transmitted to inform the other users that a collision has occurred.
- In the networking world, this is termed as **carrier sensing** - a node listens to the channel before transmitting. If a frame from another node is currently being transmitted into the channel, a node then waits ("backs off") a random amount of time and then again senses the channel.
- If the channel is sensed to be idle, the node then begins frame transmission. Otherwise, the node waits another random amount of time and repeats this process. In the networking world, this is termed as **collision detection** - a transmitting node listens to the channel while it is transmitting.
- If it detects that another node is transmitting an interfering frame, it stops transmitting and uses some protocol to determine when it should next attempt to transmit.

These rules are embodied in the family of **CSMA** (Carrier Sense Multiple Access) and **CSMA/CD** (CSMA with Collision Detection) protocols

6.5.2.3 Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier-sense multiple access with collision avoidance (CSMA/CA) is the least popular of the three major access methods. Collision detection and carrier sensing are very difficult in a wireless environment. Shadow-fading effects impair collision detection, as objects obstruct the direct signal path between users. Path loss and shadow-fading effects result in signals being hidden between users. Thus, collision-avoidance schemes are normally used in wireless networks, especially in wireless LANs.

In CSMA/CA, each computer signals its intent to transmit before it actually transmits data by sending a busy tone a frame. This busy tone is broadcast to all the nearby transmitters. A transmitter that receives a busy tone from any receiver refrains from transmitting. Once the busy tone ends, the transmitter waits for a random amount of time before sending frame. This random back-off scheme is used to prevent all transmitters

from transmitting at the same time when the busy signal ends. In this way, computers sense when a collision might occur; this allows them to avoid transmission collisions.

6.5.3 Taking-Turns Protocols

The two most important **taking-turns protocols** are **token-passing protocol** and the **polling protocol**.

6.5.3.1 Polling Protocol

The polling protocol requires one of the nodes to be designated as a master node. The master node **polls** each of the nodes in a round-robin fashion. In particular, the master node first sends a message to node 1, saying that it can transmit up to some maximum number of frames. After node 1 transmits some frames, the master node tells node 2 it can transmit up to the maximum number of frames. The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.

The polling protocol eliminates the collisions and the empty slots that plague the random access protocols. This allows it to have a much higher efficiency. But it also has a few drawbacks

- The first drawback is that the protocol introduces a polling delay, the amount of time required to notify a node that it can transmit.
- The second drawback, which is potentially more serious, is that if the master node fails, the entire channel becomes inoperative.

6.5.3.2 Token-passing Protocol

In this protocol a small, special-purpose frame known as a **token** is exchanged among the nodes in some fixed order. When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node. If a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node. Token passing is decentralized and has a high efficiency. But it has a few drawbacks

- The failure of one node can crash the entire channel.
- If a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.

6.5.3.3 Demand Priority (Round-Robin) Access Method

Unlike contention-access MAC, the round-robin-access scheme is deterministic, and there is no random allocation of a time slot to a frame. This scheme is not as popular as the others used in LANs, it is a relatively new access method designed to be used effectively when most users have large amounts of data to transmit.

Each user is given a chance to transmit data in a round-robin fashion. Each user may transmit data; if it has no data to transmit, the user passes its turn to the next user. The internetworking device manages network access by doing round-robin searches for requests to send from all nodes on the network. It is responsible for noting all addresses, links, and end nodes and verifying that they are all functioning.

With demand priority, it is possible to implement a scheme in which certain types of data will be given priority if there is contention. If the hub or repeater receives two requests at the same time, the highest priority request is serviced first. If the two requests are of the same priority, both requests are serviced by alternating between the two.



An access control or channel allocation algorithm is typically implemented in hardware on the network adaptor. Numerous channel allocation algorithms have been devised. Channel partitioning algorithm are sometimes called static channel allocation other algorithms are called dynamic channel allocation.

6.6 Reliable Transmission and Flow Control

Frames are sometimes corrupted while in transit. Even when error-correcting codes are used, some errors will be too severe to be corrected. As a result, some corrupt frames must be discarded. If a link-layer protocol provides the reliable-delivery service, then it guarantees to move each network-layer datagram across the link without error.

A link-layer reliable-delivery service is often used for links that are prone to high error rates, such as a wireless link, with the goal of correcting an error locally, on the link at which the error occurs, rather than forcing an end-to-end retransmission of the data by transport- or application-layer protocol. However, link-layer reliable delivery is often considered to be unnecessary overhead for low bit-error links, including fiber, coax and many twisted pair copper links. For this reason, many of the most popular link-layer protocols do not provide a reliable delivery service.

Even if the transmission is error free, at a certain point the receiver simply may not be able to handle the frames as they arrive because it has a limited buffering capacity especially when the transmitter start to send frames at a rate slightly higher than the receiver can handle and accept. In the result receiver will start to lose some frames. Transmission systems must use flow-control techniques on their links to guarantee that when a transmitter wants to transmit frames faster than the receiver can accept them will, it not overwhelm a receiver with data. Otherwise the receiver's buffer can overflow and frames can get lost.

The protocol contains well-defined rules about when a sender may transmit the next frame. These rules often prohibit frames from being sent until the receiver has granted permission, either implicitly or explicitly. This is usually accomplished using a combination of two fundamental mechanisms acknowledgments and timeouts.

An acknowledgment (ACK) is a small control frame (header without any data) that a protocol sends back to its peer saying that it has received an earlier frame. The receipt of an acknowledgment indicates to the sender of the original frame that its frame was successfully delivered. If for some reasons the sender does not receive an acknowledgment after a reasonable amount of time, it will mean that the receiver didn't correctly receive the original frame or the transmitter couldn't be able to receive the ACK frame. In this case the

transmitter retransmits the original frame again. This action of waiting a reasonable amount of time is called a timeout.

Using acknowledgments and timeouts to implement reliable delivery is called automatic repeat request (ARQ). Two widely used flow-control protocols are stop and wait and sliding window.

6.6.1 Stop-and-Wait Flow Control

The stop-and-wait algorithm is the simplest ARQ scheme and the least expensive technique for link-overflow control. The idea behind this protocol is straightforward; the transmitter waits for an acknowledgement after transmitting one frame, see Figure 6.5 which depict a protocol's behavior. If the acknowledgment is not received by the transmitter after a certain agreed period of time, the transmitter retransmits the original frame.

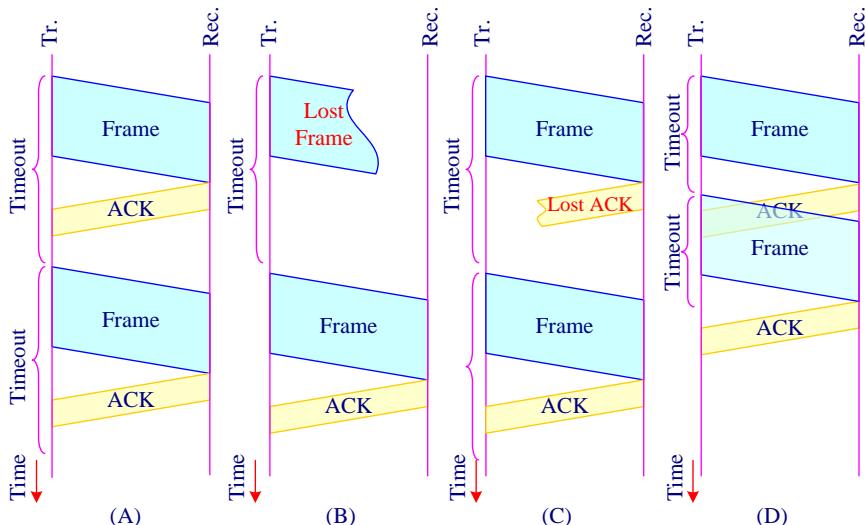


Figure 6.5: Stop-and-wait algorithm scenarios. (A) The ACK is received before the timer expires; (B) the original frame is lost; (C) the ACK is lost; (D) the timeout fires too soon.

The retransmission of a certain frame is take place in one of the following situations:

- the original frame is lost or unacknowledged
- the ACK is lost
- the timeout fires too soon

Now suppose the transmitter sends a frame and the receiver acknowledges it, but the acknowledgment is either lost or delayed in arriving. This situation is illustrated in timelines (C) and (D) of Figure 6.5. In both cases, the sender times out and retransmit the original frame, but the receiver will think that it is the next frame, since it correctly received and acknowledged the first frame. This has the potential to cause duplicate copies of a frame to be delivered. To address this problem, the header for a stop-and-wait protocol usually includes a 1-bit sequence number—that is, the sequence number can take

on the values 0 and 1—and the sequence numbers used for each frame alternate, as illustrated in Figure 6.6. Thus, when the sender retransmits frame 0, the receiver can determine that it is seeing a second copy of frame 0 rather than the first copy of frame 1 and therefore can ignore it.

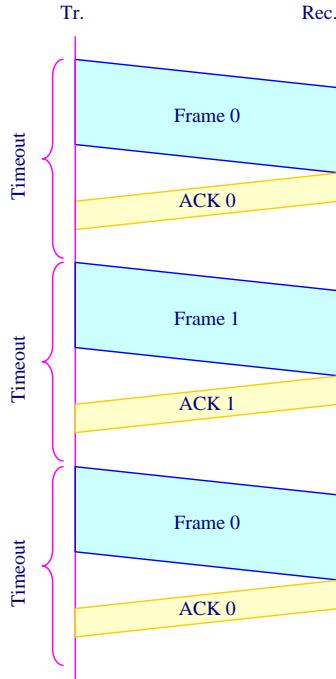


Figure 6.6: Using 1-bit sequence number to guarantee the correct stop and wait ACK.

6.6.2 The Sliding Window Flow Control

Using the sliding window algorithm, first the sender assigns a sequence number, to each frame, and maintains three variables:

- The send window size (SWS), gives the upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit;
- The sequence number of the last acknowledgment received (LAR) (see Figure 6.7 (A));
- The sequence number of the last frame sent (LFS)

The sender also maintains the following invariant:

$$LFS - LAR \leq SWS$$

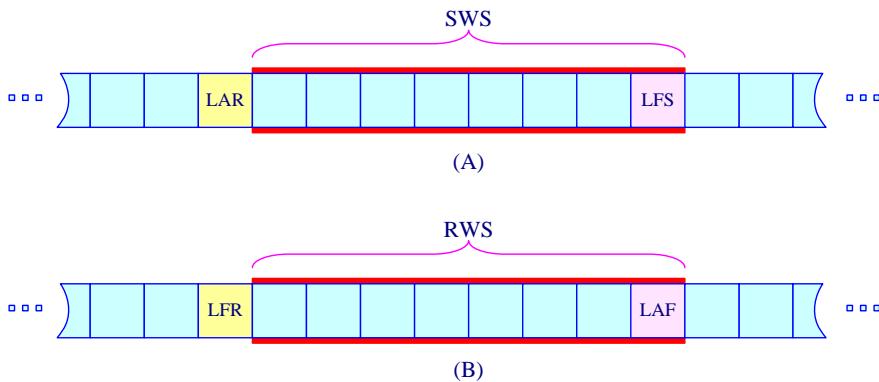


Figure 6.7: Sliding windows, (A) on sender and (B) on receiver.

When an acknowledgment arrives, the sender moves LAR to the right, thereby allowing the sender to transmit another frame. Also, the sender associates a timer with each frame it transmits, and it retransmits the frame should the timer expire before an ACK is received. Notice that the sender has to be willing to buffer up to SWS frames since it must be prepared to retransmit them until they are acknowledged.

The receiver maintains the following three variables:

- The receive window size (RWS), gives the upper bound on the number of out-of-order frames that the receiver is willing to accept;
- The sequence number of the largest acceptable frame (LAF) (see Figure 6.7 (B))
- The sequence number of the Last frame received (LFR)

The receiver also maintains the following invariant:

$$LAF - LFR \leq RWS$$

When a frame with sequence number seqN arrives, the receiver takes the following action.

- If $\text{SeqN} \leq \text{LFR}$ or $\text{SeqN} > \text{LAF}$, then the frame is outside the receiver's window and it is discarded.
- If $\text{LFR} < \text{SeqN} \leq \text{LAF}$, then the frame is within the receiver's window and it is accepted.

Now the receiver needs to decide whether or not to send an ACK. Let SeqNToAck denote the largest sequence number not yet acknowledged, such that all frames with sequence numbers less than or equal to SeqNToAck have been received. The receiver acknowledges the receipt of SeqNToAck, even if higher-numbered packets have been received. It then sets $\text{LFR} = \text{SeqNToAck}$ and adjusts $\text{LAF} = \text{LFR} + \text{RWS}$.

Figure 6.8 shows an example of sliding-window flow control. With this protocol, a transmitter (Tr) and a receiver (Rec) agree to form identical-size sequences of frames. Let the size of a sequence be 6. Thus, a transmitter allocates buffer space for $SWS=6$ frames, and the receiver can accept up to $RWS=6$ frames. The transmitter can then send up to 6

frames without waiting for any acknowledgment frames. Each frame in a sequence is labeled by a unique sequence number. For every k frames forming a sequence, the transmitter attaches a sequence-number field to each frame. Therefore, as many as 2^k sequence numbers exist.

First, a transmitter opens a window of size $SWS = 6$, as the figure shows. The receiver also opens a window of size $RWS = 6$ to indicate how many frames it can expect. In the first attempt, let's say that frames with sequence number 0, 1, and 2 are transmitted. The transmitter then shrinks its window to 3 but keeps the copy of these frames in its buffer just in case any of the frames is not received by the receiver. At the receipt of these three frames, the receiver shrinks its expected window to 3 and acknowledges the receipt of frames by sending an acknowledgment ACK 3 frame to the transmitter meaning that the receiver has successfully received all frames including the frame with sequence number 2, and ready to receive new frames starting with the frame with sequence number 3.

At the release of ACK 3, the receiver changes its expected window size back to 6 since it has the ability to receive 3 additional frames. This acknowledgment also carries information about the sequence number of the next frame expected and informs that the receiver is prepared to receive the next 6 frames. At the receipt of ACK 3, the transmitter maximizes its window back to 6, discards the copies of frames 0, 1, and 2, and continues the procedure. In this protocol, the window is imagined to be sliding on coming frames.

In our example, suppose $LFR = 5$ i.e., the last ACK the receiver sent was for sequence number 5, and $RWS = 6$. This implies that $LAF=11$. Should frames 7 and 8 arrive, they will be buffered because they are within the receiver's window. However, no ACK needs to be sent since frame 6 is yet to arrive. Frames 7 and 8 are said to have arrived out of order. (Technically, the receiver could resend an ACK for frame 5 when frames 7 and 8 arrive.) Should frame 6 then arrive-perhaps it is late because it was lost the first time and had to be retransmitted, or perhaps it was simply delayed-the receiver acknowledges frame 8, bumps LFR to 8, and sets LAF to 14. If frame 6 was in fact lost, then a timeout will have occurred at the sender, causing it to retransmit frame 6.



Sequence number is implemented by a finite-size header field. This makes it necessary to reuse sequence numbers or, stated another way, sequence numbers wrap around.

6.7 Error detection

Error detection is important whenever there is a non-zero chance of your data getting corrupted. Whether it's an Ethernet frames or a file error sources are present when data is transmitted over a medium. These errors are introduced by signal attenuation and noise. Even if all possible error-reducing measures are used during the transmission, the receiver can incorrectly decide that a bit in a frame to be a zero when it was transmitted as a one (and vice versa). Any network must deliver accurate messages.

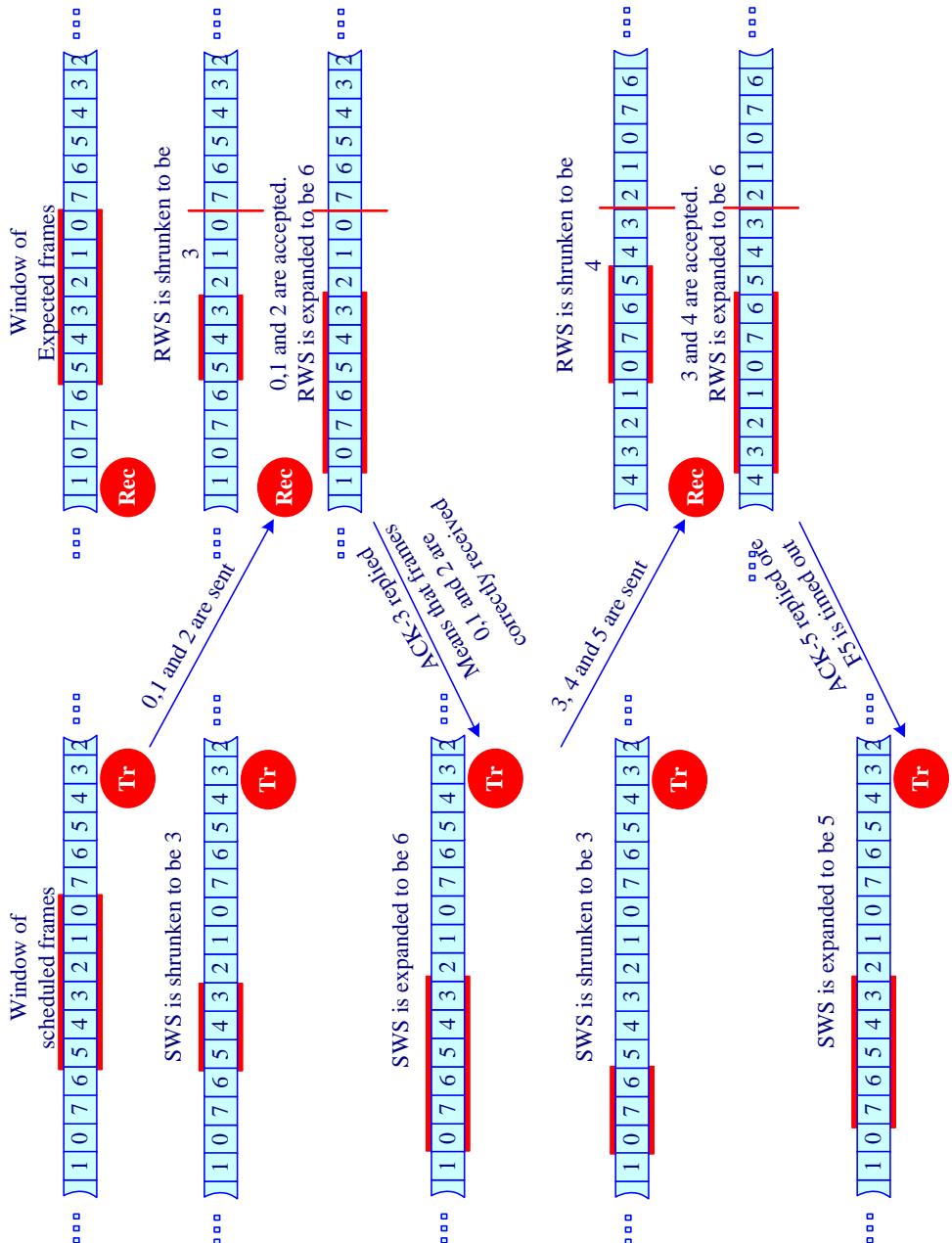


Figure 6.8: Sliding windows algorithm operation.

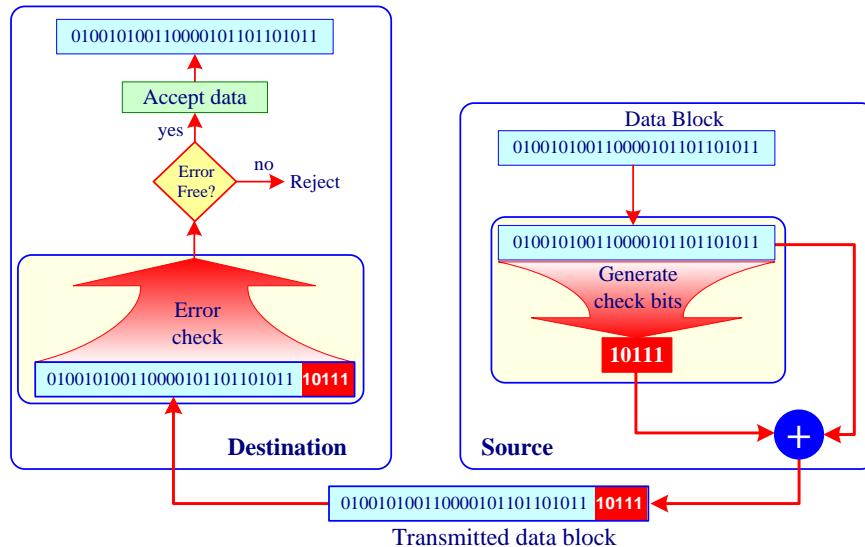


Figure 6.9: Error check mechanism.

Most networking equipment at the data-link layer inserts some type of error-detection code as it is shown in Figure 6.19. The basic idea behind any error detection scheme is to add redundant information to a frame that can be used to determine if errors have been introduced.

We say that the extra bits we send are redundant because they add no new information to the message. Instead, they are derived directly from the original message using some well-defined algorithm well known to both the sender and the receiver. The sender applies the algorithm to the message to generate the redundant bits. It then transmits both the message and those few extra bits. The receiver applies the same algorithm to the received message. If it comes up with the same result as the sender, the receiver accept it, otherwise it can be sure that either the message or the redundant bits were corrupted, and it must take appropriate action, that is, discarding the message, or correcting it if that is possible.

The most common approaches to error detection are

- Parity check
- Two dimensional parity check
- Internet checksum
- Cyclic redundancy check (CRC)

6.7.1 Parity Check

The simplest form of error detection is the use of a single **parity bit**. The sender includes one additional bit and chooses its value such that the total number of the original information plus a parity bit is even or odd. So there are two variants of parity bits: **even parity bit** and **odd parity bit**. An even parity bit is set to 1 if the number of ones in a given set of bits is odd (making the total number of ones even). An odd parity bit is set to 1 if the number of ones in a given set of bits is even (making the total number of ones

odd). Figure 6.10 illustrates an even and odd parity scheme for some combination of data code, with the single parity bit being stored in a separate field

On the receiving side the receiver needs only count the number of 1's in the received set of bits. If an odd number of 1-valued bits are found with an even parity scheme (or an even number of 1-valued bits are found with an odd parity scheme), the receiver knows that at least one bit error has occurred. Of course, if two bits are corrupted this system will not detect it.

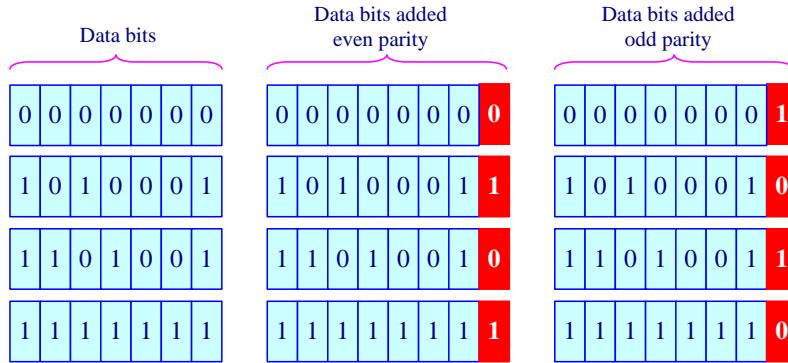


Figure 6.10: Parity check example.

6.7.2 Two-Dimensional Parity

Two-dimensional parity is a two-dimensional generalization of the single-bit parity scheme. Here, the set of bits in a frame are divided into i rows and j columns. A parity value is computed for each row and for each column. The resulting $i+j+1$ parity bits are the data link frame's error detection bits.

Figure 6.11 illustrates how two-dimensional even parity works for an example frame containing 6 bytes of data. Suppose now that a single bit error occurs in the original set bits of data. With this two-dimensional parity scheme, the parity of both the column and the row containing the flipped bit will be in error. Notice that the fourth bit of the parity byte is 1 since there are an odd number of 1s in the third bit across the 6 bytes in the frame. Figure 6.12 shows that the receiver can thus not only detect the error, but can use the column and row indices of the column and row with parity errors to actually identify the bit that was corrupted and correct that error! Notice that we have added 14 bits of redundant information to a 42-bit message, and yet we have stronger protection against common errors than the method described above.

6.7.3 Internet Checksum Algorithm

Although this algorithm is not used at the link level, nevertheless it provides the same sort of functionality as CRCs and parity, so we discuss it here. We will see later that we use this algorithm to detect possible errors in TCP and IP headers.

The idea behind it is very simple. The transmitter adds up all the words of a message, typically the asserted bits, and storing the resulting value at the end of data unit. The receiver can later perform the same operation on the data, compare the result with the

received checksum and decides if the message was corrupted or not. If any transmitted data, including the checksum itself, is corrupted, then the results will not match, so the receiver knows that an error occurred. Figure 6.12 gives a simple example of the checksum for four 16-bit words.

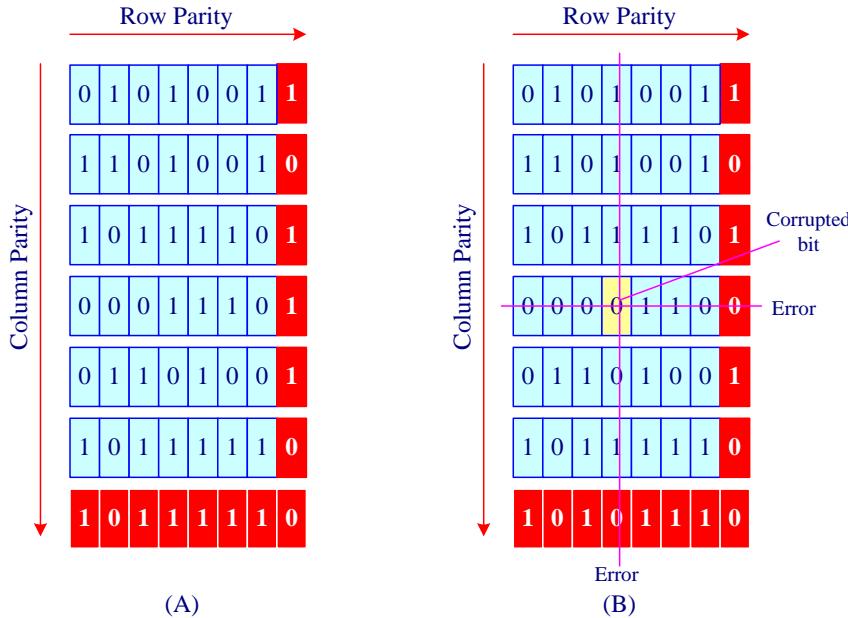


Figure 6.11: two dimensional parity check example.

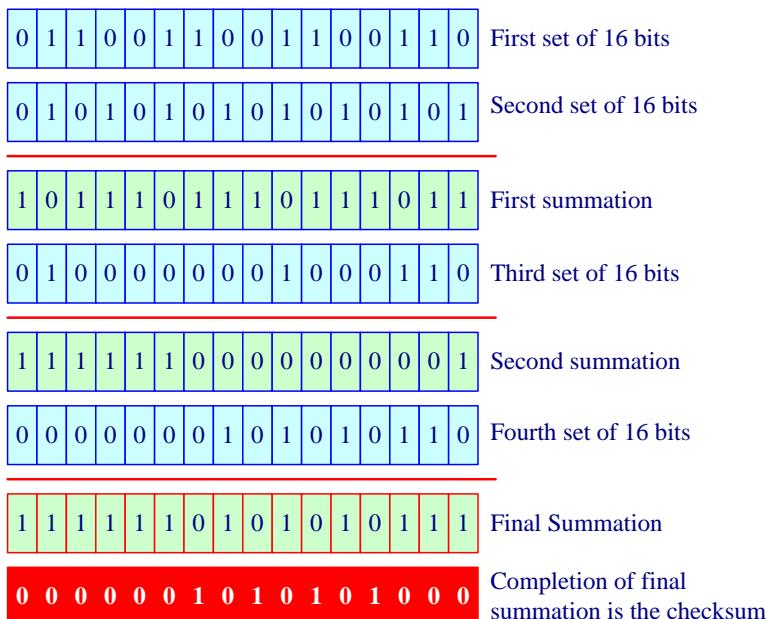


Figure 6.12: Internet checksum example.

The 1's complement is obtained by converting all the 0s to 1s and converting all the 1s to 0s. Thus the 1's complement of the sum becomes the checksum. At the receiver, all four 16-bit words are added, including the checksum. If no errors are introduced into the segment, then clearly the sum at the receiver will be 1111111111111111. If one of the bits is a zero, then we know that errors have been introduced into the segment.

6.7.4 Cyclic Redundancy Check (CRC)

The parity and Internet checksum are not foolproof, even if the parity bit is the same as it is transmitted, or the sum for checksum equals 1111111111111111; it is still possible that there are undetected errors in the data unit. For this reason, a number of protocols use more sophisticated error detection techniques than these simple methods.

A powerful method for detecting errors in the received data is by grouping the bytes of data into a block and calculating a Cyclic Redundancy Check (CRC). This is usually done by the data link protocol and calculated CRC is appended to the end of the data link layer frame as FCS.

The CRC is calculated by performing a modulo 2 division of the data by a generator polynomial and recording the remainder after division.

Calculating a Cyclic Redundancy Check is a much more robust error checking algorithm.

$\sum_0^n a \cdot x^n ; a = 0 \text{ or } 1$	
CRC-8 for ATM	$x^8 + x^2 + x + 1$ 1 0 0 0 0 0 1 1 1
CRC-CCITT	$x^{16} + x^{15} + x^5 + 1$ 1 0 0 1 0 0 0 0 0 1 0 0 0 1
CRC-12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$ 1 1 0 0 0 0 0 0 1 1 1 1
CRC-16	$x^{16} + x^{15} + x^2 + 1$ 1 1 0 0 0 0 0 0 0 0 0 0 0 1 0 1
CRC-32 used in IEEE 802:	$x^{32} + x^{26} + x^{23} + x^{22} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ 1 0 0 0 0 0 1 0 0 1 1 0 0 0 0 0 1 0 0 0 1 1 1 0 1 0 1 1 0 1 1 0 1 1 1

The algorithm treats all bit streams as binary polynomials

$$\sum_0^n a \cdot x^n ; a = \begin{cases} 0 \\ 1 \end{cases}$$

For example data stream 10011101 represents a polynomial $1.x^7 + 0.x^6 + 0.x^5 + 1.x^4 + 1.x^3 + 1.x^2 + 0.x^1 + 1.x^0$. Given the original frame, the transmitter generates the FCS for that frame. The FCS is generated so that the resulting frame (the cascade of the original frame and the FCS), is exactly divisible by some pre-defined polynomial. This pre-defined polynomial is called the divisor or CRC Polynomial or generator.

Figure 6.13 illustrates that CRC algorithm in both transmitting and receiving sides operate as the following:

1. Get the raw frame
2. Left shift the raw frame by n bits and divide it by generator.
3. The remainder of the last action is the FCS.
4. Append the FCS to the raw frame. The result is the frame to transmit

At the receiving side the receiver will do the same operation on the cascade of the original frame and the FCS to check the presence of errors as the following:

1. Receive the frame.
2. Divide it by the generator.
3. If the remainder is not zero then there is an error in the frame. Otherwise the frame is error free.

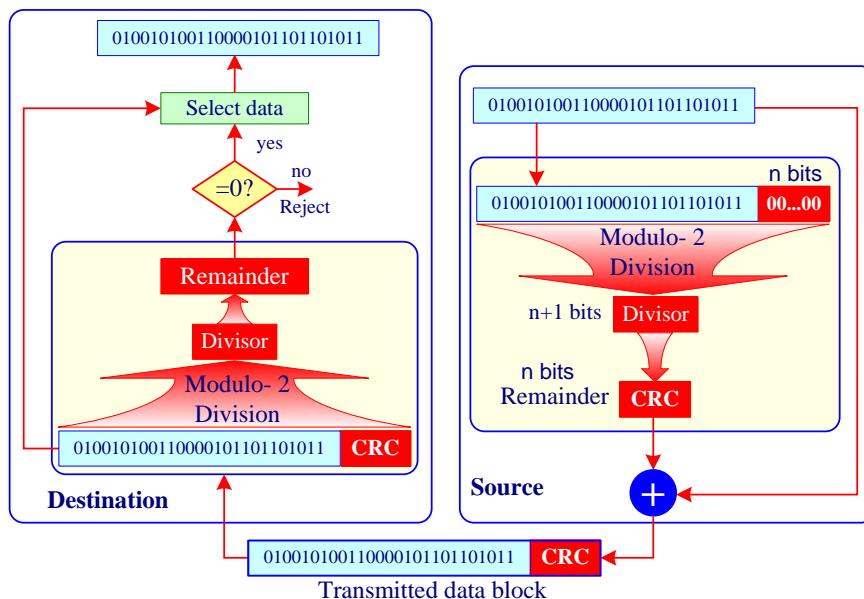
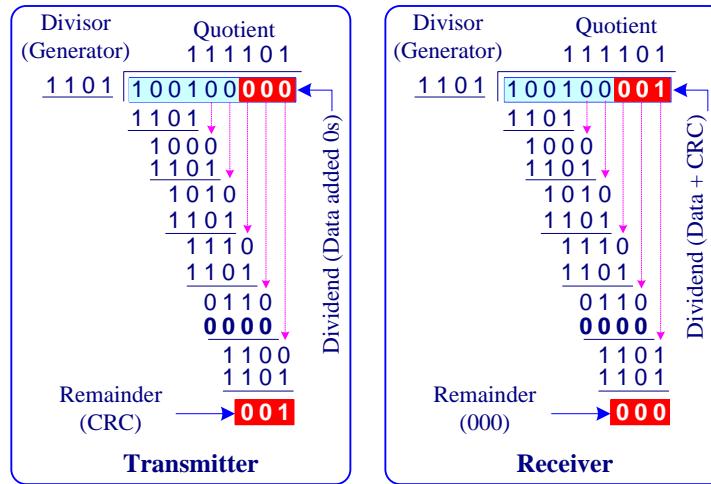


Figure 6.13: CRC algorithm.

For more illustration you can follow the depicted example in figure 6.14.



Data Block: 100100

Generator: 1101

CRC: 001

Transmitted data block: 100100001

Figure 6.14: CRC example.

In general, we can provide quite strong error detection capability while sending only k redundant bits as FCS for an n -bit message, where $k \ll n$. On an Ethernet, for example, a frame carrying up to 12,000 bits (1500 bytes) of data requires only a 32-bit CRC code, or as it is commonly expressed, uses CRC-32. Such a code will catch the overwhelming majority of errors, as we will see below. Following is a list of the most used generators.

The CRC-12 is used to generate 12-bit FCS. Both CRC-16 and CCRC-CCITT are used to result in 16 bit FCS. Applications that need extra protection can make use of the CRC-32 which generates 32 bit FCS. The CRC-32 is used by the local network standards committee (IEEE-802) and in some DOD applications.

$\sum_0^n a \cdot x^n ; a = 0 \text{ or } 1$	
CRC-8 for ATM	CRC-CCITT
$x^8 + x^2 + x + 1$	$x^{16} + x^{15} + x^5 + 1$
1 0 0 0 0 0 1 1 1	1 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 1
CRC-12	
$x^{12} + x^{11} + x^3 + x^2 + x + 1$	CRC-16
1 1 0 0 0 0 0 0 1 1 1 1	$x^{16} + x^{15} + x^2 + 1$
CRC-32 used in IEEE 802:	
$x^{32} + x^{26} + x^{23} + x^{22} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	
1 0 0 0 0 0 1 0 0 1 1 0 0 0 0 1 0 0 0 1 1 0 1 1 0 1 0 1 1 1	

6.7.5 Error Correction

Error correction is similar to error detection, except that a receiver can not only detect whether errors have been introduced in the frame but can also determine exactly where in the frame the errors have occurred (and hence correct these errors). Some protocols (such as ATM) provide link-layer error correction for the packet header rather than for the entire packet.



Although the most common place to have error detection is data link layer; nevertheless it may be applied in most layers. The data unit of the layer may include some sort of error-detection scheme which can be performed on the data unit header only.

6.8 Quick Review

- ❖ Data link layer converts frames of data into raw bits for the physical layer. It converts the raw bit stream offered by the physical layer into a stream of frames for use by the network layer. MAC addresses are used at this layer. As a consequence of having multiple nodes share a single broadcast channel was the need to provide node address at the data link level. Physical addresses are quite different from network-layer addresses, and in the case of the Internet, a special protocol (ARP - the address resolution protocol) is used to translate between these two forms of addressing.
- ❖ Methods of accessing shared medium deal with how to access to a shared link so that all users eventually have a chance to transmit their data. The simplest access methods are channel partitioning methods (TDM, FDM, CDMA). These are efficient when the number of stations is small and fixed and the traffic is continuous. When the number of stations is large and variable or the traffic is fairly bursty, the ALOHA protocol, with and without slotting, are suitable. When the state of the channel can be sensed, stations can avoid starting a transmission while another station is transmitting. This technique, carrier sensing, has led to a variety of protocols that can be used on LANs and MANs.
- ❖ Wireless LANs have their own problems and solutions. The biggest problem is caused by hidden stations, so CSMA does not work. One solution is to use CSMA/CA.
- ❖ Taking-turns approaches (polling and token passing) are popular and used in VG Any LAN and token ring networks.
- ❖ Flow control is provided by data link layer protocols to prevent a fast sender from overrunning a slow receiver. The sliding window mechanism is widely used to integrate error control and flow control in a convenient way.
- ❖ Sliding window protocols can be categorized by the size of the sender's window and the size of the receiver's window. When both are equal to 1, the protocol is stop-and-wait. When the sender's window is greater than 1, for example, to prevent the sender from blocking on a circuit with a long propagation delay, the receiver

can be programmed either to discard all frames other than the next one in sequence or to buffer out-of-order frames until they are needed.

- ❖ The most link-control schemes used by LAN protocols are stop and wait and sliding window. In the stop-and-wait method, a sender waits for an acknowledgment after transmitting one frame. This flow-control method is significantly improved in the sliding window method, which lets multiple frames travel on a transmission link.

- ❖ The data-link layer establishes and maintains the data link for the network layer above it. It ensures that data is transferred reliably between two stations on the network.
- ❖ A link-layer reliable-delivery service is often used for links that are prone to high error rates, such as a wireless link, with the goal of correcting an error locally, on the link at which the error occurs, rather than forcing an end-to-end retransmission of the data by transport- or application-layer protocol.
- ❖ Error detection methods determine whether transferred bits are in fact correct or whether they possibly were corrupted in transit. The parity check method involves counting all the 1 bits in the data and adding one extra bit, called the parity bit. This makes the total number of 1 bits even (even parity) or odd (odd parity).
- ❖ The parity-check method is the simplest error-detection technique but is not effective. Internet checksum is error-detection method used at the network and transport layers.
- ❖ The cyclic redundancy check (CRC) method is one of the most elaborate and practical techniques but is more complex, adding 8 to 32 check bits of error-detection code to a block of data. With the cyclic redundancy check (CRC) method, some frames arriving at the destination node contain errors and thus have to be discarded.

6.9 Self Test Questions

A- Answer the following questions

1. What are the main services provided by the link layer
2. Explain the general data link frame structure
3. How the MAC address is guaranteed to be unique for each device?
4. Explain the shared medium access problem?
5. List the access problem solution technique.
6. List the random access protocols.
7. Explain the carrier-sense multiple access with collision avoidance (CSMA/CA) protocol.
8. Explain the carrier-sense multiple access with collision detection (CSMA/CD) protocol.
9. Explain the token passing protocol.
10. How does the round robin protocol work?
11. Where is the flow control supposed to be used at the data link layer level?
12. Name the widely used flow-control protocols.

13. How does sliding window algorithm work?
14. What are the most common approaches to error detection?
15. What is the basic idea behind any error detection scheme?
16. List the most common approaches to error detection.
17. How does the CRC algorithm in both transmitting and receiving sides operate?

B- Identify the choice that best completes the statement or answers the question.

1. What is the purpose of a network's access method?
 - a. Control traffic
 - b. Avoid collisions
 - c. Make the bandwidth unlimited for the network
 - d. Limit the network bandwidth
2. CSMA/CD stands for ____.
 - a. Carrier Service Multiple Access with Collision Detection
 - b. Carrier Sense Multiple Access with Collision Determine
 - c. Carrier Sense Multiple Access with Collision Detection
 - d. Control Sense Multiple Access with Collision Direction
3. In the case of a collision a NIC on an Ethernet will ____.
 - a. immediately stop transmitting
 - b. keep transmitting
 - c. wait for 10 minutes before transmitting again
 - d. wait for 2 minutes before transmitting again
4. The statement that is true about collisions is:
 - a. A collision rate greater than 5% of all traffic is pretty common
 - b. Collisions do not occur on Ethernet
 - c. Collisions cannot corrupt data on transit
 - d. On heavily trafficked networks, collisions are fairly common
5. CSMA/CA ____.
 - a. eliminates collisions
 - b. is faster than CSMA/CD
 - c. has less collisions occurrence
 - d. has less overhead than CSMA/CD
6. ____ is used to ensure data integrity further in the connection-oriented protocols.
 - a. digital signature
 - b. digital certificate
 - c. symmetric encryption algorithm
 - d. checksum
7. MAC address contains ____ parts.

a. 1	c. 2
b. 3	d. 4
8. ____ is the size of a full MAC address.

a. 10 characters	c. 11 characters
------------------	------------------

- b. switching d. demand priority

19. All computers have equal access to the medium, when using the ____ channel access method.
a. CSMA/CA c. token passing
b. CSMA/CD d. demand priority

20. What are the fundamental unit of data for network transmission and reception in the NIC.?
a. bits c. packets
b. segments d. frames

21. How many parts of two hexadecimal numbers separated by colons forms the MAC address?
a. four c. six
b. five d. seven

22. One feature that separates the CSMA/CD protocol found on wired LANs from the CSMA/CA found on wireless networks is that_____
a. a priority is assigned to transmissions
b. there are no collisions
c. it is guaranteed that only one workstation will transmit at a time
d. it is a round robin protocol

23. 1101011, would be transmitted as____ using odd parity.
a. 00101001. c. 11010011.
b. 11010010. d. 11010110.

24. The Internet uses ____ CRC.
a. 8-bit c. 64-bit
b. 16-bit d. 32-bit

25. The receiver responds with____ if a packet of data arrives without error.
a. ACK. c. REJ.
b. NAK. d. COP.

26. Extended sliding window systems can support ____ packets.
a. 12 c. 128
b. 27 d. 127

27. In a sliding window scheme, acknowledgements always contain a value ____ the number of the next expected packet.
a. greater than c. less than
b. equal to d. equal to or greater than

28. ____ ARQ is the most efficient error control technique.
a. Go-back-N c. Selective-reject
b. Stop-and-wait d. Send-and-wait

29. What is the most common places to perform error detection?
a. data-link layer c. application layer
b. network layer d. physical layer

30. Individual characters are grouped together in a block in _____ parity,
a. odd c. vertical redundancy
b. CRC d. longitudinal

31. The data 110101100 is equivalent to the polynomial
a. $x^6+x^3+x^2+x^0$. c. $x^6+x^5+x^4+x^3+x^1$.
b. $x^6+x^4+x^3+x^1$. d. $x^8+x^7+x^5+x^3+x^2$.

32. _____ percent of errors will be undetected when using simple parity.
a. 20 c. 50
b. 30 d. 80

33. Which of the following is a valid MAC address?
a. 00:B0:A1:8C:32:65:BB
b. 01:DB:7F:86:E4:6G
c. 00:D0:B7:AD:1A:7B
d. 03:BC:5A:E6:E4

34. Most Token Ring networks today run at _____.
a. 4 Mbps c. 16 Mbps
b. 100 Mbps d. 1000 Mbps

35. A Token Ring system that is waiting to capture a free token is said to be in _____.
a. transmit mode c. passive mode
b. repeat mode d. stripping mode

CHAPTER 7

LAN TECHNOLOGY

7.1 About This Chapter

The LAN system has grown over the years, becoming even larger and more complex. It now includes a wide variety of medium systems, each based on its own particular set of hardware and each with its own configuration guidelines.

The goal of this chapter is to describe the entire range of LAN technology specified in the IEEE standard. This includes wide variety of Ethernet technology, Token ring, FDDI, VG-Any LAN, WLAN and others and descriptions of all LAN medium systems and Access control.

The design of complete LAN systems to carry data between computers is a major subject, and a number of books are needed to describe all of the issues that can be encountered. Since this chapter will focus on the most popular LAN technologies, Ethernet, IEEE 802.12, Token Ring, Fiber Distributed Data Interface (FDDI), Wireless LANs and ATM LAN. Ethernet easily has the largest installation base, which continues to expand into the foreseeable future; it took the largest part of this chapter.

7.2 Learning Outcome

After this chapter, you will be able to:

1. Understand the differences between LAN technologies
2. Classify and explain the 802 LAN standards
3. Identify the frame structure used by every standard
4. Identify the coding methods and data rate for each of these standards
5. Summarize the general physical characteristics of each standard.
6. Identify the most popular application to use every standard
7. Describe the MAC protocol used by various LAN standards
8. understand auto negotiation process
9. Identify the advantages and disadvantages of various LAN standards

7.3 Ethernet LAN Architecture

The actual development of Ethernet occurred at the Xerox Palo Alto Research Center (PARC) in Palo Alto, California. A development team had to connect over 100 computers on a one km cable. The resulting system, which operated at 2.94 Mbps using the CSMA/CD access protocol, was referred to as "Ethernet". It is named after the aluminiferous ether through which electromagnetic radiation was once thought to propagate.

During its progression from a research based into a manufactured product, Ethernet suffered several identify crises. During the 70s, it endured such temporary names as the "Alto Aloha Network" and the "Xerox Wire". After reverting to the original name, Xerox decided, quite wisely, that the establishment of Ethernet as an industry standard for

local area networks would be expedited by an alliance with other vendors. A resulting alliance with Digital Equipment Corporation (DEC) and Intel Corporation resulted in the development of a 10-Mbps Ethernet network. It also provided Ethernet with significant advantages over other networks known at that time as ARCnet and Wangnet.

Ethernet is the most widely used local area network (LAN) technology. The original and most popular version of Ethernet supports a data transmission rate of 10 Mb/s. Newer versions of Ethernet called "Fast Ethernet" support data rates of 100 Mb/s, "Gigabit Ethernet", 10 Gb/s and above. An Ethernet LAN may use coaxial cable, special grades of twisted pair wiring, or Optical fiber cable. "Bus" and "Star" wiring configurations are supported. Ethernet devices compete for access to the network using a protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

7.3.1 Ethernet Frame Format

Ethernet Frame Format was developed by DEC, Intel, and Xerox. It is slightly different from the IEEE 802.3 format. The specific field are shown if Figure 7.1. The Ethernet frame field length is in 8 bit octets (bytes) and described as the following:

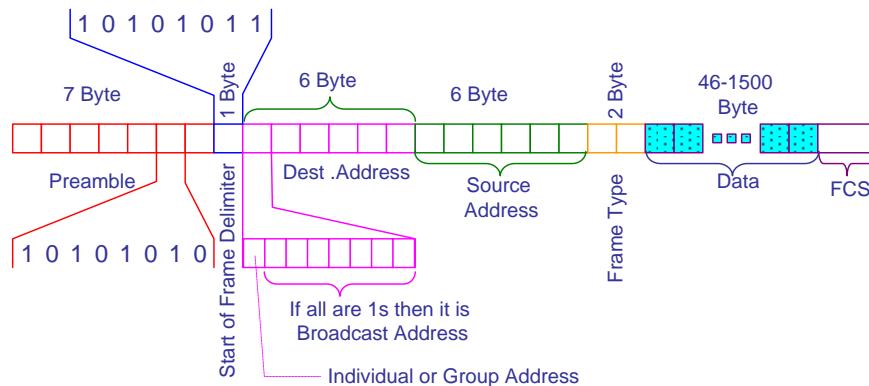


Figure 7.1: Ethernet Frame Format

- **Preamble field:** A sequence of seven octets with the bit pattern 10101010 to allow bit synchronization. They serve to give components in the network time to detect the presence of a signal, and being reading the signal before the frame data arrives.
- **Start of frame delimiter (SFD):** Bit pattern 10101011 - signals start of a valid frame to receiver.
- **Destination and source addresses:** Ethernet addresses for each of source and destination computers are six bytes long, the first bit of the destination address can be set to indicate either an individual address or a group address (frame is aimed at a logical grouping of machines). If a group address is followed by all 1's then this frame is intended for all machines on the LAN, this is a broadcast or global address.
- **Frame Type:** A two-octet field indicating the number of octets in the data fields in the IEEE 802.3 standard OR a two-octet field indicating the type of frame in the IEEE 802.3 standard.

original Digital-Intel-Xerox Ethernet (Ethernet I and II). If the length is less than the minimum frame size then padding is added at the end of the data field

- **Frame data:** The data field is the only variable-length field, and can range from a minimum of 46 to a maximum of 1500 octets. The contents of this field are completely arbitrary, and are as determined by the higher-layer protocol in use. If the size of this field is less than 46 bytes, then use of the subsequent "Pad" field is necessary to bring the frame size up to the minimum length. A minimum Ethernet frame size is 64 bytes from the Destination MAC Address field through the Frame Check Sequence.
- **Frame check sequence (FCS):** This is a four octet field used for error detection. It contains a Cyclic Redundancy Checksum (CRC) which provides a check of the integrity of the data in the entire frame. The CRC is a unique number that is generated by applying a polynomial to the pattern of bits that make up the frame. The same polynomial is used to generate another checksum at the receiving station. The receiving station checksum is then compared to the checksum generated at the sending station. This allows the receiving Ethernet interface to verify that the bits in the frame survived their trip over the network system intact.



A *multicast* address allows a single Ethernet frame to be received by a group of stations. The special case of the multicast address known as the *broadcast* address, which is the 48-bit address of all ones.

7.3.2 Ethernet Networks (IEEE 802.3 Standards)

The IEEE 802.3 standard is based on Ethernet. However, it has several significant differences, particular its support of multiple physical layer options, which include 50- and 75-ohm coaxial cable, UTP, and optical fiber. Other differences are a name given to the IEEE 802.3 standard for a bus-based broadcast system that generally follows the form "**S type L**". Here, **S** refers to the speed of the network in Mbps, type is BASE for Baseband and BROAD for broadband, and **L** refers to the maximum segment length in 100-meter multiples. Thus, 10BASE5 refers to an IEEE 802.3 Baseband network that operates at 10 Mbps and has a maximum segment length of 500 meters. One exception to this general form is 10BASET, which is the name for IEEE 802.3 network that operates at 10 Mbps using UTP cables. Figure 7.2 summarizes the most popular types of IEEE 802.3 standard.

7.3.2.1 10Base5 - "Thick Ethernet"

10Base5 or Thick Ethernet, ThickNet gets its name from the thick coaxial cable it uses. As its name implies it is a 10Mbps Baseband transmission with a range of 500 meters. This type of network typically uses bus topology as shown in Figure 7.3. Its greater range made it a viable choice for larger campuses where LANs were needed. It has largely been supplanted by Optical fiber cable however. The cable for ThickNet - RG-8 or RG-11 is very expensive (the most expensive of the copper choices), not at all resilient (making it extremely difficult to work with) but also has very good shielding (the best shielding in copper medium). It was often the only choice in secure applications.

Speed of the network	Type (Base or Broad band)	Maximum Segment length *100 [m] Or type of cabling technology used
Conventional Ethernet	Fast Ethernet	Gigabit Ethernet
10 Base	5	100 Base T4
10 Base	2	100 Base TX
10 Base	T	100 Base FX
10 Base	FB	100 Base VG-AnyLan
10 Base	FL	100 Base T
10 Base	FP	1000 Base LX
10 Broad	36	1000 Base EX
		10 G Base SX
		10 G Base LX
		10 G Base EX
		10 G Base LX4
		10 G Base CX4

CX: stands for short-haul copper.
 LX: stands for long-wavelength transmissions over long cable runs of fiber-optic cabling
 SX: stands for short-wavelength transmissions over short cable runs of fiber-optic cabling
 SX : (for 10G) SR stands for short range, SW stands for short wave
 LX:: (for 10G) LR stands for long range, LW stands for long wave
 EX: ER stands for extended range, EW stands for extra long wavelength
 LX4: 4- separate laser sources
 CX4 : 4-lines copper

T: stands for (UTP)
 T4: stands for TP using four telephone-grade pairs
 TX: stands for TP two data-grade pairs
 F: stands for fiber-optic link
 FP: stands for Fiber Passive
 FL: stands for Fiber-Optic Inter-Repeater Link (FOIRL)
 FB: Fiber-Optic for extending a backbone system
 FX: stands for fiber-optic link using two strands of fiber-optic cable
 VG :stands for Voice Grade

Figure 7.2: IEEE 802.3 standard.

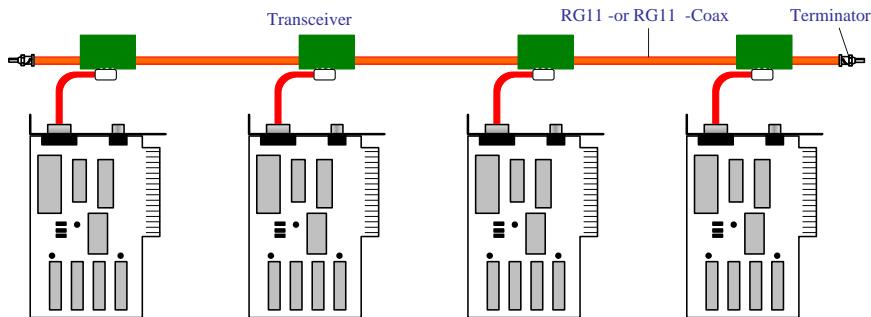


Figure 7.3: Thick Ethernet with RJ-11 Coaxial Cable

7.3.2.2 10Base2 - "Thin Ethernet"

10Base2, also ThinEthernet, ThinNet or CheaperNet, draws its nicknames from the cable it uses, RG 58 Coaxial cable, which is quite inexpensive. The overall cost of running a 10Base2 network is the smallest, largely in part of its linear (bus) topology. Really only one long cable is used and "snaked" to every machine, so no cable "runs" are necessary.

A ThinNet does not really need a hub (see Figure 7.4), thus decreasing the cost further and has almost twice the range of a 10BaseT network thus not requiring as many repeaters, again reducing costs. It has been primarily used in temporary networks or in small office or home networks. The overall performance is not on par with 10BaseT, primarily because of its linear topology. One computer addresses every computer between it and its target thus greatly reducing the network capacity.

Like 10BaseT the Network Interface Card (NIC) serves as a transceiver, so external transceivers are not necessary. Since it is a bus topology, termination is very important to prevent signal reflection.

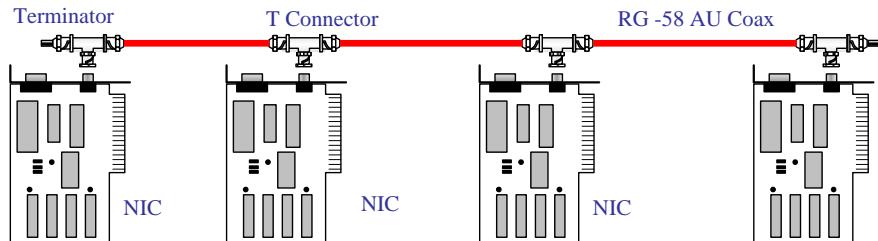


Figure 7.4: Thin Ethernet with RJ-58-AU Coaxial Cable

7.3.2.3 10BaseT - "Standard Ethernet"

10BaseT is the most prevalent network schematic in use today. It uses inexpensive UTP cable, which is fairly low cost and quite easy to work with. It requires the use of a HUB or Concentrator.

The network card (NIC) has transceiver capabilities so no external transceivers are needed. As mentioned before, 10BaseT uses Unshielded Twisted Pair cable as illustrated in Figure 7.8. Currently the requirement is a minimum of Category 3 UTP, but most

installations today are done in Category 5, thus allowing future upgrades to "Fast Ethernet".

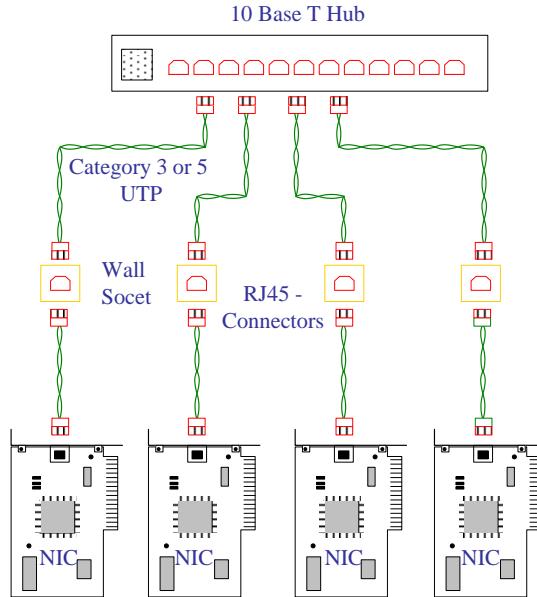


Figure 7.5: 10BaseT Ethernet

UTP cable uses a RJ45 connector, with pins 1 and 3 used to transmit data and pins 2 and 7 to receive. Usually the cables are run with all pins connected, again for future 100BaseX upgrades.

Like its name suggests it supports 10Mbs traffic and is a Baseband transmission, meaning it will use repeaters to extend its range, not amplifiers.

7.3.2.4 10BaseF - "Fiber Ethernet"

10BaseF gets its name from the Optical fiber cable it uses. It was released to enhance the prior Optical fiber Inter-Repeater Link (FOIRL) standard. It is actually composed of a few variations: 10BaseFB, 10BaseFL and 10BaseFP. 10BaseFB is not for true LAN applications but rather for "Backbone" connections between LAN segments. 10BaseFL is the most used application of 10BaseF family because it can be used for standard LAN and Backbone applications, and 10BaseFP is simply a more "LAN" oriented application. Both 10BaseFL and FB have a 2000-meter maximum segment length and 10BaseFP has a 500-meter limit.

10Base-FL is ideal for connecting between buildings. The Optical fiber cable typically used with 10Base-FL is multi-mode fiber (MMF) known as "62.5/125". This designation indicates the Optical fiber core of the cable is 62.5 microns in diameter, and the outer cladding is 125 microns in diameter. Other types of multi-mode Optical fiber cable such as 50/125, 85/125, and 100/140 may be used in 10Base-FL links, but they may not achieve the same distance as 62.5/125. The wavelength of light used with 10Base-FL is 850 nanometers. The transceiver attaches to the two Optical fiber cables through connectors that are commonly known as "ST" connectors.

The independent transmit and receive paths of the 10Base-FL medium allow the full-duplex mode of operation to be optionally supported. When operating in full-duplex mode, 10Base-FL can support segment lengths longer than 2000 meters. In full-duplex mode, segment lengths are no longer restricted by the round trip timing requirements of a CSMA/CD collision domain. High quality multi-mode fiber and transceivers can support segment lengths of 5 km. Even longer distances can be supported with the more expensive single mode fiber (SMF).

10Base-FB is restricted to use as a point-to-point link between repeaters. The repeaters on both ends of the link must be specifically designed to support 10Base-FB. 10Base-FB cannot be used to connect a computer directly to a repeater. 10Base-FB supports the same cable and connector types as 10Base-FL. However a 10Base-FB port on one repeater cannot be directly connected to a 10Base-FL port on another repeater as the signaling protocols are not compatible. 10Base-FB is also not capable of supporting the full-duplex mode of operation.

10Base-FP uses "Optical fiber passive star" system, a single "Star" may link up to 33 computers.

The 10Base-FP Star is passive device which implies it requires no power. It is ideal for use in locations where no active power supply is available. The Star acts as a passive hub that receives optical signals from special 10Base-FP transceivers. This type is not capable of supporting the full-duplex mode of operation.

The reason for choosing 10BaseF implementations is its clearly superior range and it's extremely high clarity. This is of course due to its use of Optical fiber cable. Added to the fact the fiber becomes the clear choice in high end and high security applications. However it's high price and the difficulty to work with, still prevent its widespread use. Connections in fiber have to be absolutely perfect as to prevent the light from refracting at connection points. Microscopic instruments need to be used to properly cut and assemble a cable. So most applications rely on ready-made cable and connectors, and thus driving the price even higher. As pricing for fiber cable and related connectors and devices dropped, more and more implementations appeared.



In order for each transmitter to reliably detect collisions, the minimum transmission time for a complete frame must be at least one slot time, and the time required for collisions to propagate to all stations on the network must be less than one slot time.

7.3.2.5 10Broad36

10Broad36 uses inexpensive 75 ohm broadband cable. It supports transmission of multiple channels over a single cable using frequency division multiplexing (FDM) dividing the bandwidth into separate frequencies, each channel uses a different frequency range.

Single 10Broad36 segments can be as long as 1800 meters. With multiple segments the broadband cable medium can span a total distance of up to 3600 meters. Computers are

connected to cable using transceivers. Computers attach to the transceivers through an AUI cable that can be up to 50 meters in length.

10Broad36 networks use either a "single cable" or "dual cable" configuration terminated by a "head end" device. In a single cable configuration, the cable carries transmissions over two channels, each using a different frequency range. One channel is used to transmit signals, and the other is used to receive it. The head end includes a frequency converter that changes the frequency of the signal and re-transmits it in the opposite direction along the same cable. The signal is then received by all devices on the cable. In a dual cable configuration, when a signal is transmitted, it reaches the head end where it is passed via a connector to the other cable without any change in frequency.



When introduced, 10Broad36 offered the advantage of supporting much longer segment lengths than 10Base5 and 10Base2. But this advantage was diminished with introduction of the 10Base-F standards.

7.3.2.6 Traditional Ethernet Summary

The following table summarizes the general physical characteristics of several types of traditional Ethernet standards

Standard	Standard First Released	Topology	Medium	Maximum Cable Segment Length in Meters	
				Half-Duplex	Full-Duplex
10Base5	DIX 1980 802.3 1983	Bus	50-ohm coaxial cable	500	n/a
10Base2	802.3a 1985	Bus	50-ohm RG 58	185	n/a
10Broad36	802.3b 1985	Bus	Single broadband 75-ohm CATV cable	1800	n/a
FOIRL	802.3d 1987	Star	Two optical fibers	1000	>1000
1Base5	802.3e 1987	Star	Two telephone cable	250	n/a
10Base-T	802.3i 1990	Star	Two 100-ohm Cat 3 or better UTPcable	100	100
10Base-FL	802.3j 1993	Star	Two optical fibers	2000	>2000
10Base-FB	802.3j 1993	Star	Two optical fibers	2000	n/a
10Base-FP	802.3j 1993	Star	Two optical fibers	1000	n/a

7.3.3 Fast Ethernet

Fast Ethernet is a collective term for a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbit/s. Increasing the Ethernet transmission rate by a factor of ten was not a simple task, and the effort resulted in the development of four separate physical layer standards:

- 100Base-TX for two pairs of high-quality twisted pair wires
- 100Base-T4 for four pairs of normal-quality twisted pair wires
- 100Base-T2 for two pairs of low-quality twisted pair wires
- 100Base-FX for multimode optical fiber cables.

Each of these standards was defined with different encoding requirements and a different set of medium-dependent sublayers, even though there is some overlap in the link cabling.

The 802.3U (100Base-T) committee design approach kept 100-Mbps Ethernet as close to the original definition as possible. Therefore the network segment length for a 100Base-T cable is limited to 100 meters, as with 10Base-T and it utilizes the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) shared-medium access method supported in earlier versions of Ethernet. The simplicity of this medium access method might make it attractive to companies using traditional Ethernet. The challenge for developing this technology is the collision detection (CD) function. As the bandwidth is increased times ten, the collision was reduced to one tenth.

7.3.3.1 100Base-T4

The physical layer implementation for 100Base-T4 varies significantly from the physical layer definition of 10Base-T. The 100Base-T4 achieves its speed by dividing a 100-Mbps data stream into three 33-Mbps streams. These three streams are sent over three pairs of Unshielded Twisted Pair (UTP) wire. A fourth pair of wire is used for collision detection. No data is sent on the fourth pair; instead, the hub uses it to signal a workstation when a collision occurs.

Splitting the data stream across the wires helps ensure the signal integrity. However, because 100Base-T4 splits the data stream over four pairs of cable, full duplex is not supported. As it is depicted in Figure 7.6, the 100Base-T4 requires 4 pair Category 3 (CAT 3) or better cabling. The total network diameter is 205 meters, which is shorter than current 10Base-T standards.

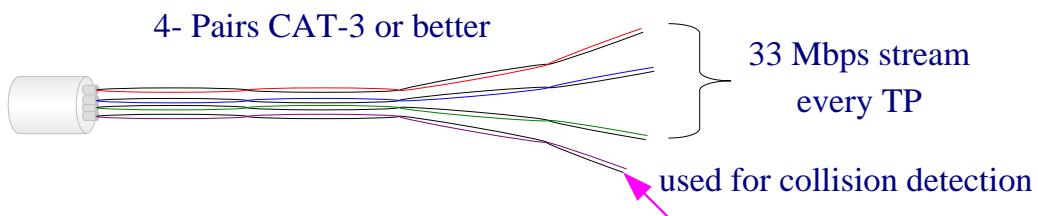


Figure 7.6: 100Base-T4 cabling

7.3.3.2 100Base-TX

The 100Base-TX is a true derivative of 10Base-T. Its 100-Mbps speed is achieved by sending the signal 10 times faster. Signal integrity is retained by shortening cable lengths and using Category type 5 (CAT 5) cabling. CAT 5 cabling increases the twist ratio of the wires to cancel the electromagnetic interference (EMI). Because 100Base-TX uses exactly the same protocol as Ethernet (no splitting of data streams), it supports full and half duplex mode.

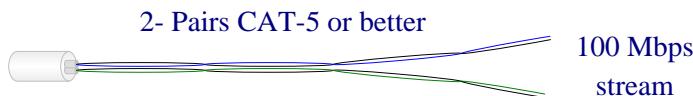


Figure 7.7: 100Base-TX cabling

7.3.3.3 100Base-T2

The 100Base-T2 specifications was developed as a better alternative for upgrading networks with installed Category 3 cabling than was being provided by 100Base-T4. Two important new goals were defined:

- To provide communication over two pairs of Category 3 or better cable
- To support both half-duplex and full-duplex operation 100Base-T2 uses a transmission scheme called as "dual duplex Baseband transmission" which transmits data over each wire pair in each direction simultaneously.
- It uses a signal encoding scheme called "Five-level Pulse Amplitude Modulation", or PAM5x5.

The 100Base-T2 standard was approved in March 1997, and is not widely used at this time. As with 100Base-T4, this technology began to fade as Category 5 cabling became more common.

7.3.3.4 100Base-FX

100Base-FX is essentially a fiber version of 100Base-TX. The Optical fiber cable typically used with 100Base-FX is multi-mode fiber (MMF) known as "62.5/125". This designation indicates the Optical fiber core of the cable is 62.5 microns in diameter, and the outer cladding is 125 microns in diameter. Other types of multi-mode Optical fiber cable such as 50/125, 85/125, and 100/140 may be used in 100Base-FX links, but they may not achieve the same distance as 62.5/125. The wavelength of light used with 100Base-FX is 1300 nanometers. Even longer distances can be supported with the more expensive single mode fiber (SMF). In full-duplex mode, segment lengths are no longer restricted by the round trip timing requirements of a CSMA/CD collision domain.

The 100Base-FX standard allows several types of Optical fiber connectors to be used. Duplex "SC" connectors are recommended, but "ST" and FDDI "MIC" connectors are also permitted. Two Optical fiber cables are used in each 100Base-FX segment. One cable is used to transmit data, and the other is used to receive data.



The most compelling reason to switch to another LAN technology, such as FDDI or ATM, was usually the higher data rate of the new technology; however, Ethernet always fought back, producing versions that operated at equal data rates or higher. Switched Ethernet was also introduced in the early 1990s, which further increased its effective data rates.

7.3.3.5 Fast Ethernet Summary

Figure 6.8 summarizes the general physical characteristics of several types of fast Ethernet standards

7.3.4 Gigabit Ethernet

Gigabit Ethernet is Ethernet that provides speeds of 1000 Mbps—one billion bits per second. It uses the same Ethernet frame format and medium access control technology as all other 802.3 Ethernet technologies.

Gigabit Ethernet is carried primarily on optical fiber, although it can be used with Cat 5 cable for short distances. Gigabit Ethernet is compatible with other Ethernet standards because it uses the same CSMA/CD MAC protocol. Many gigabit Ethernet components are backward compatible with fast Ethernet and standard Ethernet (10 Mbps), and existing Ethernet LANs with 10 and 100 Mbps cards can feed into a gigabit Ethernet backbone.

The network topology for Gigabit Ethernet follows the traditional rules of Ethernet. At Layer 2, the Spanning Tree Protocol is used to ensure that there are no logical loops in the network, creating a hierarchical tree topology. More complex LAN configurations, including parallel data paths, are created through the use of routing technology. At any speed, Ethernet is designed for transporting data in the local area environment. Like Ethernet and Fast Ethernet, Gigabit Ethernet leverages other technologies and standards to provide higher-level services such as Class of Service (CoS) traffic prioritization and Quality of Service (QoS) data delivery that limit jitter and latency.

The key objective of the 802.3z Gigabit Ethernet Task Force was to develop a Gigabit Ethernet standard that encompassed the following:

- Allowed half- and full-duplex operation at speeds of 1000 Mbps
- Used the 802.3 Ethernet frame formats
- Used the CSMA/CD access method with support for one repeater per collision domain
- Addressed backward compatibility with 10BASE-T and 100BASE-T technologies

	100 Base TX	100 Base T4	100 Base T2	100 Base FX
Transmission Rate	100 Mb/s (200 Mb/s full-duplex mode)	100 Mb/s (full-duplex not supported)	100 Mb/s (200 Mb/s full-duplex mode)	100 Mb/s (200 Mb/s full-duplex mode)
Cable Type	2 Cat 5 UTP (support STP)	4 Cat 3 or better UTP	4 Cat 3 UTP	2MMF, 62.5/125, 1300 nanometer
Maximum Segment Length	100 meters	100 meters	100 meters	Half-Duplex: 412 m Full-Duplex: 2000 m
Maximum Number of Transceivers per Segment	2	2	2	2
Connector Technology	2RJ-45 for UTP 9-pin D-type for STP	RJ-45	RJ-45	SC (preferred), ST and FDDI MIC
Signal Encoding	4B/5B	8B6T	PAM5x5	4B/5B
Standard	802.3u	802.3u	802.3y	802.3u
First Released	1995	1995	1997	1995
All these standards have a star topology				

Figure 7.8: General physical characteristics of several types of fast Ethernet standards

The IEEE 802.3z Gigabit Ethernet includes three physical layer specifications, two for Optical fiber medium—1000BASE-SX and 1000BASE-LX—and one for shielded

copper medium—1000BASE-CX. These standards use the same "8B/10B" coding scheme as Fiber Channel, and similar optical and electrical specifications. Another group, the IEEE 802.3ab Task Force, is defining the physical layer to run Gigabit Ethernet over the installed Base of Category (UTP) cabling. This 1000BASE-T effort is completed in June 1999.

7.3.4.1 1000Base-LX

The "L" in 1000Base-LX stands for "long" as it uses long wavelength lasers to transmit data over Optical fiber cable. The long wavelength lasers specified by the standard operate in the wavelength range of 1270 to 1355 nanometers. Both single mode and multi-mode optical fibers are supported. Long wavelength lasers are more expensive than short wavelength, but have the advantage of being able to drive longer distances.

7.3.4.2 1000Base-SX

The "S" in 1000Base-SX stands for "short" as it uses short wavelength lasers to transmit data over Optical fiber cable. The short wavelength lasers specified by the standard operate in the wavelength range of 770 to 860 nanometers. Only multi-mode optical fiber is supported. Short wavelength lasers have the advantage of being less expensive than long wavelength lasers.

7.3.4.3 1000Base-CX

The "C" in 1000Base-CX stands for "copper" as it uses specially shielded balanced copper jumper cables also called "twinax" or "short haul copper". Segment lengths are limited to only 25 meters that restricts 1000Base-CX to connecting equipment in small areas like wiring closets.

7.3.4.4 1000Base-T

The 1000Base-T standard supports Gigabit Ethernet over 100 meters of Category 5 balanced copper cabling. The 1000BASE-T PHY employs full-duplex Baseband transmission over four pairs of Category 5 cabling. The aggregate data rate of 1000 Mb/s is achieved by transmission at a data rate of 250 Mb/s over each wire pair. The use of hybrids and cancellers enables full-duplex transmission by allowing symbols to be transmitted and received on the same wire pairs at the same time. Baseband signaling with a modulation rate of 125 Mbaud is used on each of the wire pairs.

A five level Pulse Amplitude Modulation (PAM5) is employed for transmission over each wire pair. The modulation rate of 125 Mbaud matches the GMII clock rate of 125 MHz and results in a symbol period of 8 ns. This specification permits the use of category 5 or better-balanced cabling, installed according to ANSI/TIA/EIA-568-A. The 1000BASE-T standard makes use of two signaling methods already used in earlier IEEE standards: 100BASE-TX (125 Mbaud three level Baseband signaling) and 100BASE-T2 (25 Mbaud PAM5 Baseband signaling.) These methods were chosen to make the 1000BASE-T PHY and 100BASE-T to have 100/1000 dual speed Ethernet PHY implementations, and to make the standards development less time consuming.

7.3.4.5 The Gigabit Ethernet Extension Field

With the introduction of the 802.3z standard for Gigabit Ethernet in 1998, an extension field was added to the end of the Ethernet frame to ensure it would be long enough for collisions to propagate to all stations in the network. The extension field is appended as needed to bring the minimum length of the transmission up to 512 bytes (as measured from the Destination Address field through the extension field). It is required only in half-duplex mode, as the collision protocol is not used in full-duplex mode. Non data bits, referred to as "extension bits", are transmitted in the extension field so the carrier is extended for the minimum required time.

7.3.4.6 Gigabit Ethernet Summary

Figure 6.9 provides a summary of the general physical characteristics of several types of Gigabit Ethernet standards.



To prevent the performance lost in networks with a large amount of small packets a new concept is added called packet bursting. This allows devices to send bursts of small packets to fully utilize the bandwidth.

7.3.5 10 Gigabit Ethernet

10 Gigabit Ethernet is the most recent and fastest of the Ethernet standards recently in use. It defines a version of Ethernet with a nominal data rate of 10 Gbit/s, ten times as fast as Gigabit Ethernet. This standard was formally ratified by the IEEE on 12 June, 2002. The 10 Gigabit specifications are contained in the IEEE 802.3ae supplement to the 802.3 standard. The new 10-gigabit Ethernet standard encompasses seven different medium types for LAN, MAN and WAN.

10 Gigabit Ethernet Gigabit Ethernet systems operate in full-duplex mode only, over Optical fiber medium.

In the 10GBASE-X medium types, an "S" stands for the 850 nanometer (nm) wavelength of Optical fiber operation, an "L" stands for 1310 nm, and an "E" stands for 1550 nm. The letter "X" denotes 8B/10B signal encoding, while "R" denotes 66B encoding and "W" denotes the WIS interface that encapsulates Ethernet frames for transmission over a SONET STS-192c channel.

7.3.5.1 10 Gigabit Ethernet Types

There are several medium types, which are designed for use in either local or wide area networking. This provides the 10 Gigabit Ethernet system with the flexibility needed to operate in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN).

1. 10GBase-SR ("short range"): designed to support short distances over deployed multi-mode fiber cabling, it has a range of between 26 m and 82 m depending on cable type. It also supports 300 m operation over a new 2000 MHz multi-mode fiber. The 10GBase-SR medium type is designed for use over dark fiber, meaning

- an Optical fiber cable that is not in use and that is not connected to any other equipment.
- 2. 10GBase-CX4: also known by its working group name **802.3ak**. Copper interface using InfiniBand CX4 cables and InfiniBand 4x connectors for short-reach (15 m maximum) applications (such as aggregation switch to router). This is currently the lowest-cost per port interface at the expense of transmission range. Transmits over 4-lanes in each direction over copper cabling. Each lane of the copper carries 3.125 Gbaud of signaling bandwidth. It uses an 8 to 10 bit conversion to accommodate better line signaling.
 - 3. 10GBase-LX4: uses wavelength division multiplexing to support ranges of between 240 m and 300 m over deployed multi-mode cabling. This is achieved through the use of four separate laser sources operating at 3.125 Gbit/s in the range of 1300nm on unique wavelengths. This standard also supports 10 km over single-mode fiber.
 - 4. 10GBase-LR ("long range"): this standard supports 10 km over a 1310 nm single-mode fiber using 64B-66B Physical Coding Sublayer (PCS) to interconnect transceivers at a distance spaced at 10 km, but it can often reach distances of up to 25 km with no data loss.
 - 5. 10GBase-ER ("extended range"): this standard supports 40 km over single-mode fiber using 1550 nm. Recently several manufacturers have introduced 80-km-range ER pluggable interfaces.
 - 6. 10GBase-LRM ("Long Reach Multimode"): supports distances up to 220 m on FDDI-grade 62.5 μm multi-mode cable originally installed in the early 1990s for FDDI and 100BaseFX networks.
 - 7. 10GBase-SW, 10GBase-LW and 10GBase-EW: These varieties use the WAN PHY, designed to interoperate with OC-192/STM-64 SONET/SDH equipment. They correspond at the physical layer to 10GBASE-SR, 10GBASE-LR and 10GBASE-ER respectively, and hence use the same types of fiber and support the same distances. (There is no WAN PHY standard corresponding to 10GBase-LX4.)
 - 8. 10GBase-T or IEEE 802.3: is a standard released in 2006 to provide 10 gigabit/second connections over conventional unshielded or shielded twisted pair cables, over distances up to 100 m.

10GBASE-T works up to 55 meters with existing Category 6 cabling. In order to allow deployment at the usual 100 meters, the standard uses a new partitioned augmented Cat 6 or "6a" cable specification, designed to reduce crosstalk between UTP cables (formally known as "alien crosstalk").

Pulse-amplitude modulation with 16 discrete levels (PAM-16) is used instead of PAM-5 which is what is used in the older 1000BASE-T gigabit Ethernet standard.

	1000 Base LX	1000 Base SX	1000 Base CX	1000 Base TX
Transmission Rate	1000 Mb/s (2000 Mb/s full-duplex mode)	1000 Mb/s (2000 Mb/s full-duplex mode)	1000 Mb/s (2000 Mb/s full-duplex mode)	1000 Mb/s (2000 Mb/s full-duplex mode)
Cable Type	2 MMF 62.5/125 or 50/125 2 SMF 10 micron (1270 ~ 1355) nm	2 MMF 62.5/125 or 50/125 (770 ~ 860) nm	specialty shielded balanced copper jumper cable assemblies	4- Cat 5 or better 100-ohm
Maximum Segment Length	HD, MMF & SMF: 316 m FD MMF: 550 m FD SMF: 5000 m	HD 62.5/125; 275 m HD 50/125; 316 m FD 62.5/125; 275 m FD 50/125; 550 m	FD: 25 m HD: 25 m	100 m
Maximum Number of Transceivers per Segment	2	2	2	2
Connector Technology	SC	SC	9-pin D-type for STP	RJ-45
Signal Encoding	8B/10B	8B/10B	8B/10B	PAM5
Standard	802.3z	802.3z	802.3z	802.3ab
First Released	1998	1998	1998	1999
All these standards have a star topology. HD:Half-Duplex, FD: Full-Duplex				

Figure 7.9: Physical layer specifications defined for Gigabit Ethernet

7.3.5.2 10 Gigabit Ethernet Frame Format

The key purpose the developing 10-Gigabit Ethernet standard is to use the same MAC frame format as specified in the preceding Ethernet standards. This will allow a seamless integration of the 10-Gigabit Ethernet with the existing Ethernet networks. There is no need for fragmentation/reassembling and address translation, implying faster switching. Since the full-duplex operation is used, the link distance does not affect the MAC frame size. The minimum MAC frame size will be made equal to 64 octets as specified in the previous Ethernet standards. Carrier extension is not needed.

7.3.5.3 10 Gigabit Ethernet Applications

10 Gigabit Ethernet has applications across local-area networks (LANs), metropolitan-area networks (MANs), and wide-area networks (WANs).

7.3.5.3.1 LAN Applications

10 Gigabit Ethernet would serve well in the following network environments:

- Server interconnect for clusters of servers
- Aggregation of multiple 1000BaseX or 1000BaseT segments into 10 Gigabit Ethernet links
- Switch-to-switch links for very high-speed connections between switches in the same data center, in an enterprise backbone, or in different buildings
- 10 Gigabit Ethernet will most likely be found in service provider and enterprise data centers and LANs.

7.3.5.3.2 MAN Applications

10 Gigabit Ethernet will likely be deployed in MAN applications in over dark fiber, dark wavelength, and as a fundamental transport for facility services. 10 Gigabit Ethernet will be a natural fit with dense wave division multiplexing (DWDM) equipment as more DWDM-based systems are deployed.

- For enterprise solutions, 10 Gigabit Ethernet services over DWDM will enable serverless buildings, remote backup, and disaster recovery.
- For service provider solutions, 10 Gigabit Ethernet will enable the provisioning of dark wavelength gigabit services to customers at a competitive cost structure.

7.3.5.3.3 WAN Applications

10 Gigabit Ethernet WAN applications look similar to MAN applications because they also support dark fiber, dark wavelength, and SONET infrastructures. Multilayer switches and terabit routers will be attached via 10 Gigabit Ethernet to the SONET optical network, which includes add drop multiplexers (ADMs) and DWDM devices. When dark wavelengths are available, 10 Gigabit Ethernet can be transmitted directly across the optical infrastructure, reaching distances from 70 to 100 km.



In July 2007, the study group presented a Project Authorization Request (PAR) to the 802 Standards Executive Committee for a new IEEE 802.3ba standard which includes both 40 GBit/s and 100 GBit/s data rates.

7.3.6 Ethernet Auto-Negotiation

Ethernet LANs contain in general different devices and support different standard operations. So what happens when two computers each support a different standard want to communicate with each other? Among the things the installer needs to know are which speed should be set on the Ethernet interface and whether full-duplex mode should be enabled. However, these features are embedded in the network equipment and are invisible to the installer. One twisted-pair port looks a lot like another and it is not obvious which network options may be supported. The communicated devices need protocol allowing them to automatically select the correct speed and other features, thus relieving the installer of this configuration task.

As a solution IEEE developed an auto-negotiation process to enable devices with different technologies to choose common transmission parameters, such as speed and duplex mode. In this process, the connected devices first share their capabilities as for these parameters and then choose the fastest transmission mode they both support.

The technologies currently supported by auto-negotiation are: 10BASE-T Half Duplex, 10BASE-T Full Duplex, 100BASE-TX Half Duplex, 100BASE-TX Full Duplex, 100BASE-T4, 100BASE-T2 Half Duplex, 100BASE-T2 Full Duplex, 1000Base-T Half Duplex, 1000Base-T Full Duplex, and 10GBase-T.

Therefore, all Ethernet medium systems that use twisted-pair medium can also support the Auto-Negotiation signals. However, Optical fiber links use a variety of light sources and optical wavelengths, which do not interoperate. That, in turn, makes it impossible to develop an automatic configuration signaling system that works on all Optical fiber links. For that reason, there is no IEEE standard Auto-Negotiation support for most Optical fiber link segments. The only exception is the Gigabit Ethernet Optical fiber automatic configuration system.

Operation of the Auto-Negotiation system includes the following basic concepts:
Operation over link segments: Auto-Negotiation is designed to work over link segments only. A link segment can only have two devices connected to it—one at each end.
Auto-Negotiation occurs at link initialization: When a device is turned on, or an Ethernet cable is connected, the link is initialized by the Ethernet devices at each end of the link. Link initialization and Auto-Negotiation occurs once, prior to any data being sent over the link.

Auto-Negotiation uses its own signaling system: Each Ethernet medium system has a particular method of sending signals over the cable. However, the Auto-Negotiation system uses its own, independent signaling system designed for twisted-pair cabling. These signals are sent once, at link initialization time.

When describing the operation of Auto-Negotiation, the device at the opposite end of a link from a local device is called the link partner. Figure 7.10 shows two link segments. Each link segment has two devices: a computer at one end and a switching hub at the other.

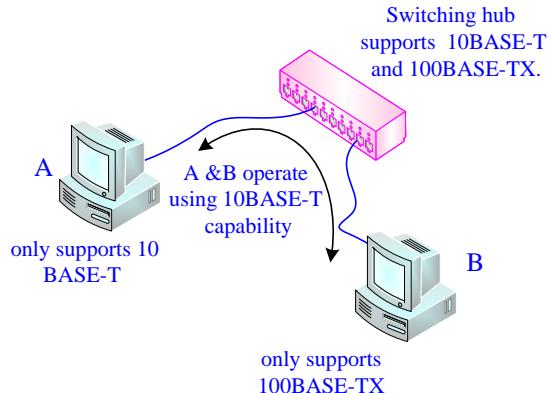


Figure 7.10: Auto-Negotiation link partners

Using the Auto-Negotiation protocol, each device advertises its capabilities to the link partner at the other end of the link. The protocol then selects the highest common denominator between the devices at each end of the link.



Half duplex Ethernet transmission is typical and allows simultaneous one-way transmission between nodes while eliminating collisions. Full duplex is an enhancement that allows simultaneous two-way transmission between nodes while eliminating collisions. Full duplex transmission increases performance and efficiency by doubling the bandwidth.

7.4 100VG-AnyLAN IEEE 802.12

While high speed Ethernet was designed to allow continued use of CSMA/CD, 100Base VG-AnyLAN uses only the same MAC layer service interface but uses different MAC methods (transmission and collision detection). One goal of this standard is to make it easy to use existing wiring and to ease its use with any LAN type. It can be used with Cat 3 - Cat 5 UTP or 2-pair STP or two optical fibers. Hubs (repeaters) can be cascaded to allow easy addition of other LAN segments to form a hierarchical or cascaded LAN.

Instead of using the technique common to Ethernet standard where each controller checks for a busy network, 100VG-AnyLAN uses a demand priority scheme. Demand priority works like a traffic signal; the hub logic determines which controller has access to the network. The hub polls each controller to determine if that controller has data to transmit and then allows transmission in port order.

For example, if there is a request waiting on port one and port three, all requests are of equal priority. The hub begins by servicing port one. Next, the hub checks to make sure

that no new requests have come in for port two, the next in line. Assuming no requests have come in, the hub proceeds to service the request on port three.

If a request came in from ports two and four while the request at port three was being serviced, port four would be the next one serviced and then the hub would start back at port one. This "round-robin technique" allows equal access to network medium.

7.4.1 Hub Priority

On a 100VG-AnyLAN network, priorities are also allowed. The network manager can set the priority from the hub. In theory, every workstation could be set to high, which negates the purpose of priorities, but in ideal network only ports using applications such as video conferencing or multimedia would be set to high. These types of applications require frequent response in real time, so they need the priority set to high. If port one has a normal priority request and ports two and three have high priority, the hub bypasses port one and services ports two and three first. Of course, if after servicing port three, high-priority requests continue to come from port two and three, station one again is bypassed. Normal requests will continue to be bypassed until that request has been waiting 200-300 ms (depending upon the configuration of the hub timer).

Once the timer has expired:

- The hub completes the processing of the current high-priority request.
- The hub changes the priority of the request on port one from normal to high.
- The hub again polls all ports and determines, using the port order, which port should be processed next.
- In the example above, the hub would finish the request from port two, complete the outstanding request from port three and then service the request waiting at port one. This handling of priorities guarantees that a maximum settable delay will not be exceeded.
- The network manager, through network management software, should ensure that a high number of users are not all configuring systems to send packets marked as high-priority. The network manager can configure each hub to treat frames from a particular port as normal, regardless of request priority assigned locally by the driver.
- In some application technology and operating system technology applications can set priority. This means that only requests from a particular application will be high priority and other requests from that port will be normal priority.

7.4.2 Hub Layers

Up to three hierarchical (cascaded) layers of hubs are allowed in a 100VG-AnyLAN network as it is shown in Figure (7.11). The root hub (first-level hub) controls which request is being serviced. When the root hub receives a request from another hub, it passes control of the network to the second-level hub. The second-level hub services its requests in port order. The root hub continues to process all requests from the second-level hub before it continues servicing the third port on its own hub.

7.4.3 100VG-AnyLAN Advantages and Disadvantages

7.4.3.1 Advantages

- Lower-cost hubs compared to the switching hubs recommended and used with 100Base-T technology.
- Provides an easier migration path from Token Ring networks than 100Base-T technology because 100VG-AnyLAN is able to use Token Ring (802.5) frame formats.
- 100VG-AnyLAN is deterministic - the longest maximum time it will take to send a packet on a network can be calculated.

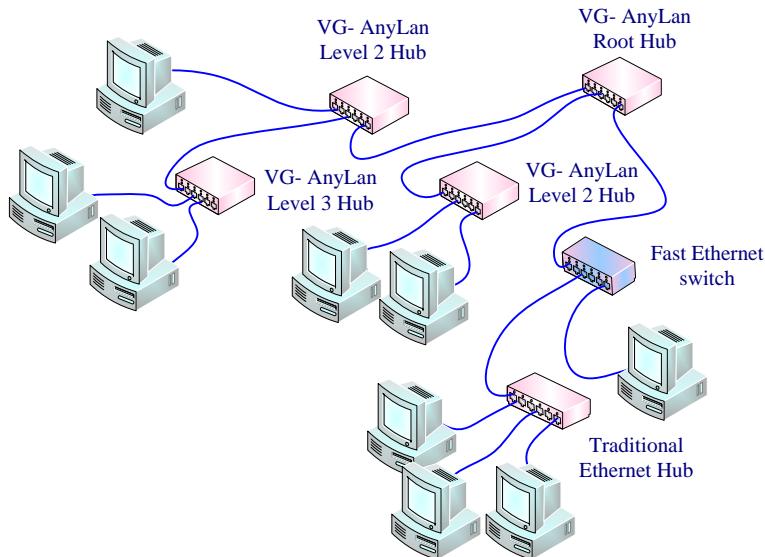


Figure 7.11: three level VG-AnyLan configuration

7.4.3.2 Disadvantages

Total throughput of 100VG-AnyLAN cannot exceed 100-Mbps. With 100Base-T and efficient switching hubs, it is possible to reach higher throughputs.

 Some times 100 VG-AnyLan is called 100Base-VG. It is intended for use by small local workgroups. It support token ring networks

7.5 Token Rings

Alongside the Ethernet, token rings are the other significant class of shared-medium network. The Token Ring was originally developed by IBM in the 1970s to provide data communication services for its mainframe computers. The term Token Ring is generally used to refer to both IBM's Token Ring and IEEE 802.5 network implementations.

7.5.1 Token Ring Topology and specifications

Although Token Ring and IEEE 802.5 networks are physically cabled in a star topology, they operate in a logical ring topology, as illustrated by Figures 7.12.

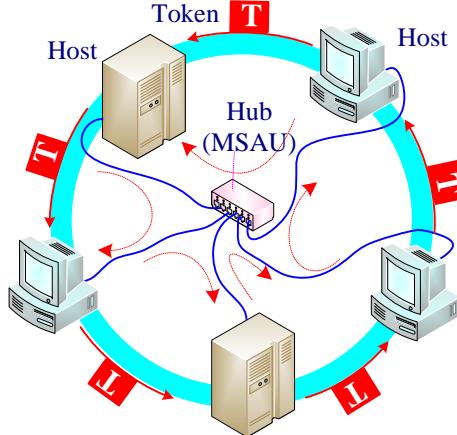


Figure 7.12: Physical Star-Logical Ring

Generally any link or host failure would make the whole network useless. The solution is to connect each host into the ring using an electromechanical relay. As long as the host is healthy, the relay is open and the host is included in the ring. If the host becomes inactive, the relay closes and the ring automatically bypasses the host, as illustrated in Figure 7.13.

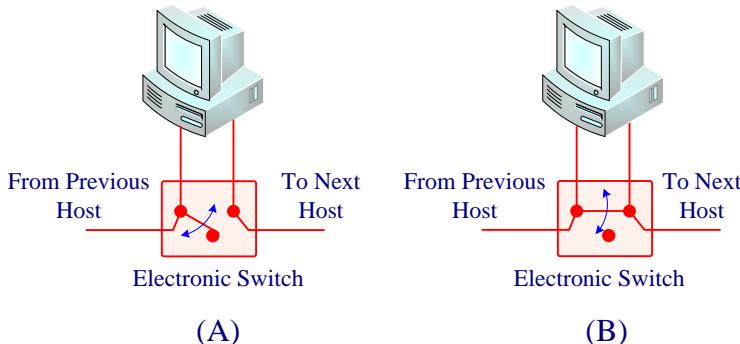


Figure 7.13 Relay Token ring with relays: (A) active host; (B) bypassed host

One of the small differences between the IBM Token Ring specification and 802.5 is that the former actually requires the use of special arrangement, whereas several of relays are usually packed into a single box, known as a multistation access unit (MSAU), while the latter does not. In practice, MSAUs are almost always used because of the need for robustness and ease of station addition and removal. It also makes it very easy to add stations to and remove stations from the network, since they can just be plugged into or unplugged from the nearest MSAU, while the overall wiring of the network can be left unchanged.

The IEEE specification includes no formal specification for transmission medium or topology for token ring. This gives the opportunity to use various medium types and topologies. On the other side there are three cable types for Baseband transmission cabling system specified by the IBM Token Ring specification as follows:

- **Type 1:** It consists of two shielded pairs with 150-ohm impedance placed in a shielded outer casing. Using this Type, each end-station can be up to 101m from the MAU. A Type 1 based ring can support up to 260 end-stations for both 4Mbps and 16Mbps operation.
- **Type 2:** It can consist of two or four (STP) twisted-wire and supports end-stations to MAU lengths up to 100m. This type can support up to 260 end stations using 4Mbps or 16Mbps.
- **Type 3:** It is a data-grade unshielded twisted-pair (UTP) with maximum cable distance between the end-station and the MAU 45m. Token Ring operates at 4Mbps on Category 3 and 4, and at 16Mbps on Category 4 and 5 UTP and supports up to 72 stations.

The hub (MAU) capacity depends on the vendor and the hub model. For example an IBM MSAU has 10 connection ports and can connect up to eight computers. You can extend a Token Ring network by connecting MAUs to ring-out and ring-in ports to form stackable MAUs that can support larger numbers of stations. You can connect up to 33 MAUs to form a network. The only rule that must be followed is that each MAU must be connected in such a way so that it becomes part of the ring. Figure 7.14 shows three MAUs connected and maintaining a logical ring. Many MAUs support being connected by fiber-optic cabling to create networks that span a building or campus.

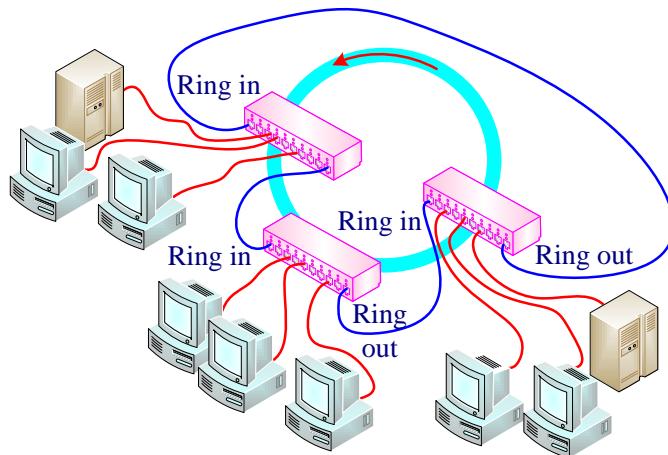


Figure 7.14: Three stackable MAUs connected and maintaining a larger ring

Data always flows in a particular direction around the ring. Each host receiving frames from its upstream neighbor and then forwarding them to its downstream neighbor. The ring is viewed as a single shared medium; and shares two key features with an Ethernet:

- The presence of distributed algorithm to control when each host is allowed to transmit

- All frames are seen by every host, and only the host with the destination address identified in the frame header saves a copy of the frame as it flows past.

7.5.2 Token Ring and IEEE 802.5 Frame Format

Token Ring and IEEE 802.5 support two basic frame types:

- Token frame which is 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter (see Figure 7-15).
- Data/command frames vary in size, depending on the size of the information field, where the data is carried.
 - Data frames carry information for upper-layer protocols
 - Command frames contain control information and have no data for upper-layer protocols (see Figure 7-16).

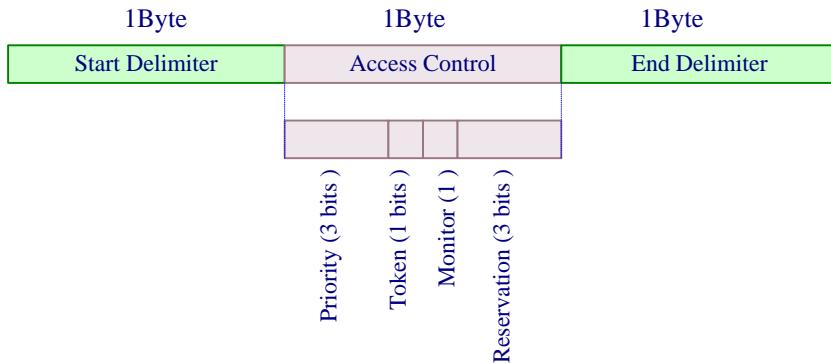


Figure 7.15: Token frame structure

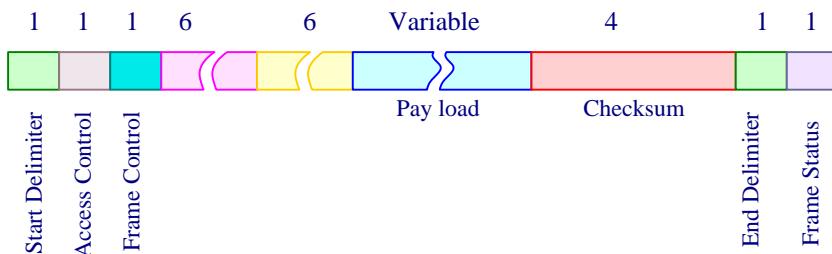


Figure 7.16: Data/command frames structure

The token frame fields are specified as follows:

- Start Delimiter (SD): Indicates start of the frame. It Alerts each host of the arrival of a token, or data/command frame.
- Access Control (AC): Indicates
 - the frame's priority (the most significant 3 bits)
 - token bit (whether it is a token or a data frame)
 - Reservation field (the least significant 3 bits).

- Monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).
- Frame Control: Contains either Medium Access Control information for all computers or "end station" information for only one computer. It indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information.
- Destination Addresses: Identify the destination host addresses (the address of the computer to receive the frame)
- Source Addresses: Identify the source host addresses (the address of the computer that sends the frame).
- Data (1 byte to 4,500 bytes or 18,000 bytes): Contains the data being sent (Token Ring MAC control information, or a standard 802.2 LLC-PDU). It indicates that the length of the field is limited by the ring token holding time, which defines the maximum time a host can hold the token.
- Frame Check Sequence (FCS): Contains CRC error-checking information. It is filled by the source host with a calculated value dependent on the frame contents. The destination recalculates the value to determine whether the frame was damaged in transit. If the frame was damaged, it is discarded.
- End Delimiter: Indicates the end of the frame. It signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame or identify the frame that is the last in a logical sequence.
- Frame Status: Tells whether the frame was recognized, copied, or whether the destination address was available. It is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

7.5.3 Token Ring Operation

Hosts in the ring are serviced in a round-robin fashion and each host gets a chance to transmit. The idea is so simple:

- A token, circulates around the ring; each host receives and then forwards the token
- If a host with a frame to transmit sees the token, it "seizes" the token. The seizing process involves simply modifying 1 bit in the second byte token; the first 2 bytes of the modified token now become the preamble for the subsequent data packet.
- After modifying the frame flows past each host on the ring.
- Each host looks inside the frame to see if it is the intended recipient. If so, it copies the frame into a buffer as it flows through the network adaptor, and forwarding the message onto the next host on the ring. Otherwise it simply forwards the frame to the neighboring host.
- When the frame makes its way back around to the sender, this host strips its frame off the ring and reinserts the token.
- Token ring uses an Interframe Gap after the data/command, which is essentially a gap between the end of one frame and the beginning of the next. This gap is typically at least 1 byte for 4 Mbps and is at least 5 bytes for 16 Mbps network implementations.
- Now, any host downstream will have the opportunity to transmit a frame.

- Unlike CSMA/CD networks (broadcast), such as Ethernet, token passing networks are deterministic, meaning that it is possible to calculate the maximum time that will pass before any host will be capable of transmitting. Before putting each frame onto the ring, the station must check that the amount of time it would take to transmit the frame would not cause it to exceed some time called the token holding time (THT). This means keeping track of how long it has already held the token, and looking at the length of the next frame that it wants to send.

7.5.4 IBM Token ring and IEEE 802.5 differences

Finally, although the IBM Token Ring and IEEE 802.5 network specifications differ slightly, the network implementations are basically compatible. The following table summarizes their specification differences

	IBM Token Ring	IEEE 802.5
Data Rates	4, 16 Mbps	4, 16 Mbps
Hosts Per Segment	260 STP 72 UTP	250
Topology	Star	Not specified
Medium	Twisted-pair	Not specified
Signaling	Baseband	Baseband
Access Method	Token passing	Token passing
Encoding	Differential Manchester	Differential Manchester
Routing Information Field (RIF) Size	2 to 30 bytes	2 to 30 bytes
Maximum Frame Size	4,550 bytes for 4 Mbps 18,200 bytes for 16 Mbps	4,550 bytes for 4 Mbps 18,200 bytes for 16 Mbps

The High-Speed Token Ring Alliance (HSTRA) wrote a specification for 100 Mbps full-duplex Token Ring to meet the challenge by Fast and Gigabit Ethernet.

Token Holding Time (THT) addresses the issue of how much data a given host is allowed to transmit each time it possesses the token, or stated differently, how long a given host on the network is allowed to hold the token. As stated previously, the default THT is 10 ms.

The important issue to address is how much data a given host is allowed to transmit each time it possesses the token? Or how long a given host is allowed to hold the token? We call this the token holding time (THT). In 802.5 networks, the default THT is 10 ms.

Token Ring is considered a half-duplex network implementation because only one host can transmit at any given time. Token Ring's full-duplex network implementation is known as Dedicated Token Ring (DTR). Token Ring hosts connect, point-to-point, to a DTR concentrator or switch and have all available link bandwidth to use for data transmission and reception.

 Token Ring networks use a sophisticated priority system that permits certain user-designated, high-priority stations to use the network more frequently. Token Ring frames have two fields that control priority, the priority field and the reservation field.

7.6 FDDI - Fiber Distributed Data Interface

FDDI is an optical fiber based network. In many respects, FDDI is similar to 802.5 and IBM Token Rings. It uses a ring topology and currently support only 100 Mbps operation. However, there are significant differences as we will see later. Due to its built-in redundancy, topological flexibility, and extensive distances make FDDI an ideal choice for use as a high-speed backbone supporting applications sensitive to network downtime. FDDI can also be used as a high-speed workgroup LAN to connect servers or desktops requiring high performance and exceptional reliability.

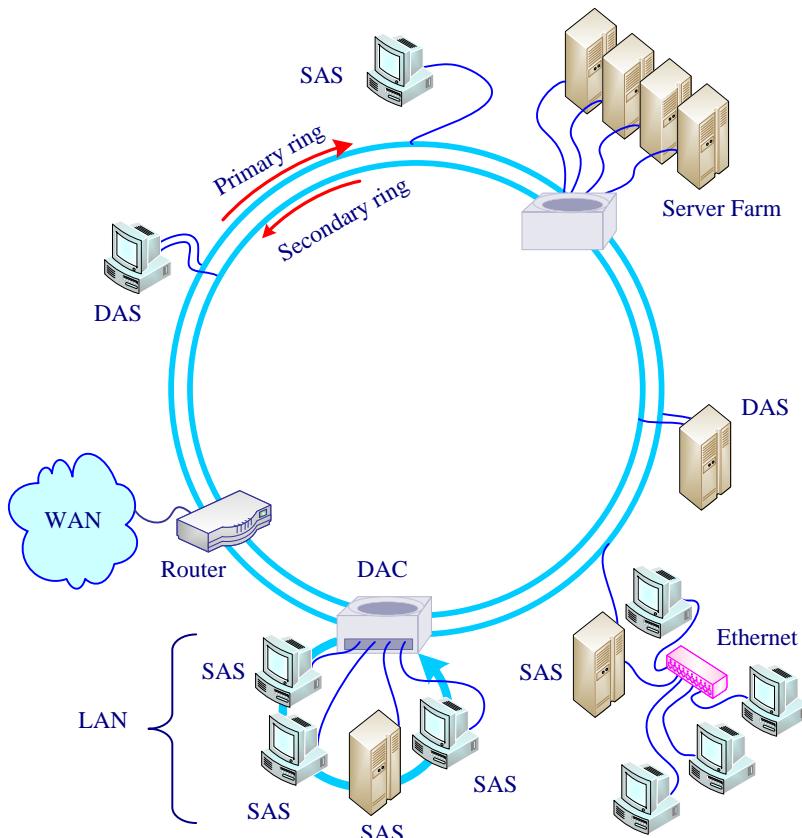


Figure 7.17: A Sample Dual ring FDDI Configuration

7.6.1 FDDI Operation and Specifications

FDDI is a LAN architecture that is based on redundant fiber rings that transmit in opposite directions. One of the rings is the primary ring and the other ring is the secondary ring. Figure 7.17 illustrates a FDDI topology with both single attachment stations (SAS) and dual attachment stations (DAS). Also illustrated is the use of FDDI concentrators, used to connect multiple stations to the FDDI LAN. To provide external access to a wide-area network (WAN), a router with dual attachment FDDI ports (ports A and B) is attached to the FDDI ring. The second ring comes into play only if the primary ring fails, as depicted in Figure 7.18. In the case of failure, the ring loops back on the secondary fiber to form a complete ring.

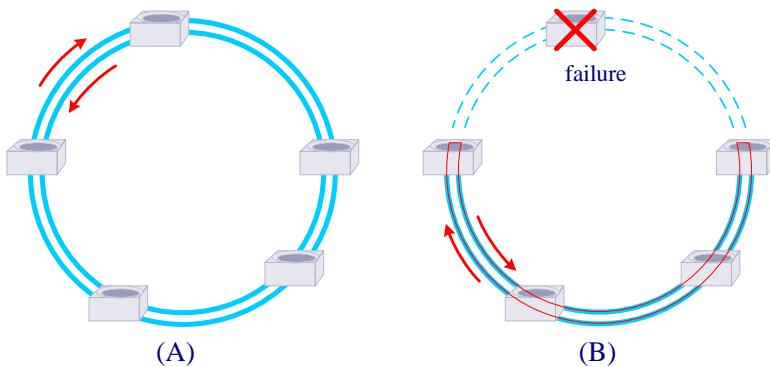


Figure 7.18: The ring operates normally (A) and loops back on the secondary fiber In the case of failure (B).

FDDI uses 4B/5B encoding, discussed in chapter 2 and supports several different types of Optical fiber cable, including the 62.5/125 micron multimode cable which provides for network segments up to 100 kilometers long with up to 500 workstations placed as far as 2 kilometers apart. Overall, the network is limited to a total of 200 km of fiber, which means that, because of the dual nature of the ring, the total amount of cable connecting all stations is limited to 100 km. Single mode Optical fiber cables provide even longer segments, with up to 60 kilometers between workstations.

A computer that is connected to both rings is called a dual attachment station (DAS), and when one of the rings is broken by a cable fault, the computer switches to the other ring, providing continued full access to the entire network. A double ring FDDI network in this condition is called a wrapped ring.

FDDI allows nodes to attach to the network by means of a single cable in a star topology using a hub called a dual attachment concentrator (DAC). The DAC creates a single logical ring, like a Token Ring MAU. A computer connected to the DAC is called a single attachment station (SAS). Should this SAS fail, the concentrator detects this situation and uses an optical bypass to isolate the failed SAS, thereby keeping the ring connected. To expand the network further, you can connect additional DACs to ports in

existing DACs without limit, as long as you remain within the maximum number of computers permitted on the network.

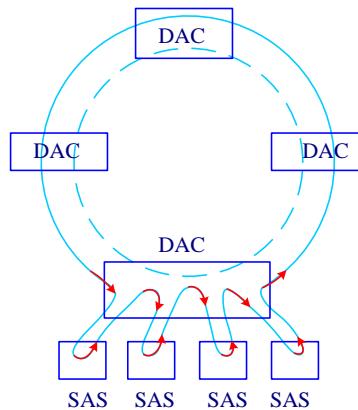


Figure 7.19: Illustration of the DAC operation

One of the most important DAC characteristics is that it converts the optical data on the FDDI system into another format that can be used to connect to other data networks. This allows one FDDI network node to connect many other data communication devices.

FDDI backbones are often installed to connect existing LANs, like Ethernet, within a building or campus-wide network to provide robust, high-performance, resilient backbone integration and transport. Integration of FDDI with ATM is also possible.

Some technology enables FDDI connected devices to potentially operate up to 200 Mb/s, twice the normal transmission rate of ordinary FDDI as a full duplex FDDI connection. This additional transmission capacity is provided with no change to your network infrastructure or cost increase.

FDDI is a token passing architecture differing from token ring in that while a station has a token it can transmit as many frames as possible before the token expires. Because of this, there can be multiple frames on the ring at any time.

FDDI uses a timed token-passing technology similar to that of token ring networks as defined in the IEEE 802.5 standard. FDDI stations generate a token that controls the sequence in which other stations will gain access to the wire.

- The token passes around the ring, in a certain direction from one node to the next.
- If one station has frames ready to transmit, it captures the token, transmits as many frames as it wants within the specified access period
- Every node on the ring checks the frames. The recipient station then reads the information from the frames
- When the frames return to the originating station, they are stripped from the ring.
- The station then releases the token.

7.6.2 FDDI Frame Format

Like Token Ring, FDDI uses several different types of frames in its communications. Data frames, token frames and station management frames.

Token frame, contains only the Preamble, plus the Starting Delimiter, Frame Control, and Ending Delimiter fields, for a total of 3 bytes. The token passing mechanism used by FDDI is virtually identical to that of Token Ring, except that the early token release feature that is optional in Token Ring is standard equipment for the FDDI protocol. The station management frame is responsible for ring maintenance and network diagnostics.

The most common of these is the data frame, shown in Figure 7.20. The functions of the fields in the FDDI data frame are as follows:

- Preamble: Indicates the beginning of the frame and contains series of alternating 0s and 1s, used for clock synchronization. And it functions as an interframe gap between data frames and tokens.
- Starting Delimiter: Indicates the beginning of the data frame or token and uses a unique data symbol, distinct from normal data symbols.
- Frame Control: Indicates the type of data found in the Data field. Some of the most common values are as follows:
 - 41, 4F—Station Management (SMT) Frame
 - C2, C3—MAC Frame (token)
 - 50, 51—LLC Frame (Data).
- Destination Address: Specifies the physical address of the computers that will receive the frame. FDDI uses the same address format as Token Ring.
- Source Address: Specifies the physical address of the computers that sent the frame.
- Information: Contains network layer protocol data, or an SMT header and data, or MAC data, depending on the function of the frame.
- Frame Check Sequence: Contains a cyclical redundancy check (CRC) value, used for error detection. The destination host recalculates the CRC value for the frame and compares it to the one contained in the frame. If the FCS sequences match, the frame is processed further.
- End Delimiter: Indicates the end of the frame. It uses a unique data symbol, distinct from normal data symbols.
- Frame Status: Contains three indicators that may be modified by intermediate systems when they retransmit the frame, the functions of which are as follows:
 - **E (Error).** Indicates that an error has been detected, either in the FCS or in the frame format.
 - **A (Acknowledge).** Indicates that the intermediate system has determined that the frame's destination address applies to itself.
 - **C (Copy).** Indicates that the intermediate system has successfully copied the contents of the frame into its buffers.
 - **End of Frame Sequence (FS, 12 bits).**

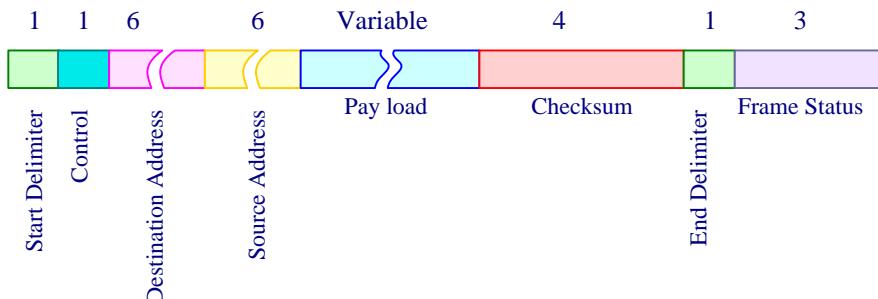


Figure 7.20: The FDDI data frame

 In a difference from the IEEE 802.5 specification in FDDI many frames from each host can exist on the ring at the same time, instead of only one frame per host. This allows FDDI networks to support higher data traffic rates than token ring networks and makes FDDI more suitable for network backbones.

7.7 Wireless LAN (IEEE 802.11)

Wireless technology has helped to simplify networking by enabling multiple computer users to simultaneously share resources in a home or business without additional or intrusive wiring. A wireless LAN, or WLAN, is simply a local area that tries to provide all the features of wired LANs, but without the wires. It can be either an extension to a current wired network or an alternative to it.

7.7.1 Wireless LANs General Characteristics

WLANs can cover areas ranging in size from a small office to a large campus, with neighborhood and city-wide ranges planned for the future.

The benefits of wireless LANs include:

- Convenience: It allows users to access network resources from nearly any convenient location within their primary networking environment
- Backup capability: It provides temporary connections to an existing, cabled network and helps provide backup to them.
- Mobility and portability: A WLAN allows users to move around while keeping their computer connected. Mobility enables users to access the network resources from any point in the geographic area.
- Productivity: Using of wireless network employee can potentially be more productive as his or her work can be accomplished from any convenient location.
- Deployment: Initial setup of an infrastructure-based wireless network requires little more than a single access point and the locations are easy to reach.

- Expandability and flexibility: Extending networks beyond the limits of physical connectivity wireless networks can increase number of clients with the existing equipment without requiring additional wiring.
- Cost: Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

Wireless LAN technology has some drawbacks; most of these have to do with the inherent limitations of the technology.

- Security: Because of using radio frequencies wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available.
- Range: The typical range of some WLAN standards equipment (802.11g) on the order of tens of meters will be insufficient in a structure larger than a typical home. To obtain additional range, repeaters or additional access points will have to be purchased.
- Reliability: Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects such as multipath, or fading that are beyond the control of the network administrator. As a result, important network resources such as servers are rarely connected wirelessly.
- Speed: The speed on most wireless networks (typically 1-108 Mbit/s) is reasonably slow compared to the slowest common wired networks (100 Mbit/s up to several Gbit/s).

7.7.2 WLAN Architecture

The possibilities for building wireless networks are almost endless, ranging from using infrared signals within a single building to constructing a global network from a grid of low-orbit satellites. While adaptable to both indoor and outdoor environments, wireless LANs are especially suited for indoor locations such as office buildings, manufacturing floors, hospitals and universities.

802.11 was designed to run over three different physical medium, two based on radio and one based on diffused infrared. The radio based on spread spectrum and run at 11 Mbps and at 54 Mbps in the 2400 MHz and 5600 MHz bands.

The idea behind spread spectrum is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices. Spread spectrum comes in one of two standards; both of them run in the 2.4-GHz frequency band:

- Frequency hopping involves transmitting the signal over a random sequence of frequencies; that is, first transmitting at one frequency, then a second, then a third,

and so on. The sequence of frequencies is not truly random, but is instead computed algorithmically by a pseudorandom number generator. The receiver uses the same algorithm as the sender—and initializes it with the same seed—and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.

- Direct sequence: For each bit the sender wants to transmit, it actually sends the exclusive-OR of that bit and n random bits. As with frequency hopping, the sequence of random bits is generated by a pseudorandom number generator known to both the sender and the receiver. The transmitted values, known as an n -bit chipping code, spread the signal across a frequency band that is n times wider than the frame would have otherwise required.

The third physical standard for 802.11 is based on diffused infrared signals. This technology has a range of up to about 10 m and is limited to the inside of buildings only.

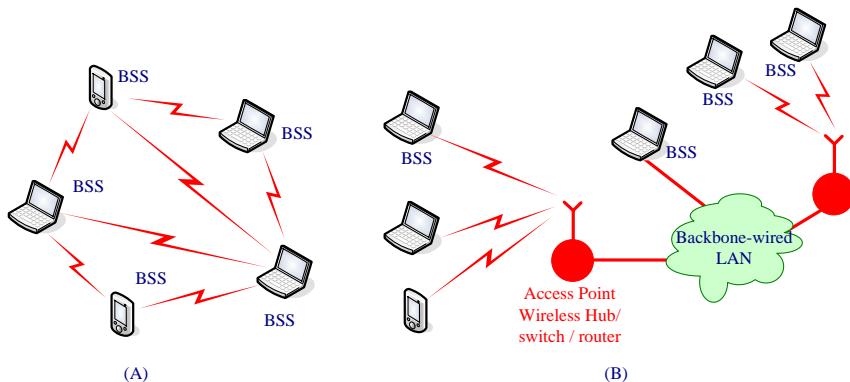


Figure 7.21: IEEE 802.11 LAN architecture, (A) ad hoc mode and (B) infrastructure mode

The 802.11 specification defines two types of operational modes: ad hoc (peer-to-peer) mode and infrastructure mode.

In **ad hoc mode**, the wireless network is relatively simple. The networked computers communicate directly with one another without the use of an access point. In ad hoc mode, also known as Independent Basic Service Set (IBSS) or peer-to-peer mode, all of the computers and workstations connected with a wireless NIC card can communicate with each other via radio waves without an access point. Ad hoc mode is convenient for quickly setting up a wireless network in a meeting room, hotel conference center, or anywhere else when sufficient wired infrastructure does not exist. An ad hoc network might be formed, for example, when people with laptops meet together and want to exchange data in the absence of a centralized AP. Figure 7.21 (A) shows IEEE 802.11 ad hoc

Infrastructure mode, all wireless devices and computers communicate with the access point which provides the connection from the wireless radio frequency world to the hard-wired LAN world. The access point is a device that links a wireless network to a wired LAN. It increases the effective range of a wireless network and provides additional network management and security features. A basic wireless infrastructure with a single

access point is called a Basic Service Set (BSS) . When more than one access point is connected to a network to form a single sub-network, it is called an Extended Service Set (ESS).

The stations, which may be either fixed or mobile, and the central Base station communicate amongst themselves using wireless technologies. APs may be connected together using any transmission medium to form a **distribution system (DS)**. Figure 7.21 (B) illustrates the principal components of the 802.11 wireless LAN architecture.

7.7.3 WLAN IEEE 802.11 Standard

WLAN IEEE 802.11 standard belongs to the same IEEE 802 family that is being increasingly deployed for wireless LAN communication. The IEEE 802.11 standard defines the physical layer and medium access control (MAC) layer for a wireless local area network.

7.7.3.1 802.11 Standard

It was the original specification of the 802.11 IEEE standard operated in the 2.4 GHz range. This specification delivered 1 to 2 Mbps using one of the following technologies:

- Direct-sequence spread spectrum (DSSS) uses seven channels
- Frequency-hopping spread spectrum (FHSS) uses a pseudonoise sequence and signal hopping from one channel to another. This technique makes use of 79 channels.
- Infrared with an operating range of about 20 meters operates on a broadcast communication paradigm. A pulse position modulation (PPM) scheme is used.
- Orthogonal frequency division multiplexing (OFDM) which is a multicarrier modulation scheme.

This specification is no longer used and has largely been replaced by other forms of the 802.11 standard.



Both direct sequencing spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) wireless technologies can operate in the unlicensed 2.4-GHz ISM band.

7.7.3.2 802.11a Standard

It is an extension to 802.11 that applies to wireless LANs using an orthogonal frequency division multiplexing (OFDM) encoding scheme which uses 12 orthogonal channels in the 5 GHz and provides up to 54 Mbps (The achievable Mb/s data rates are 6, 9, 12, 18, 24, 36, 48, and 54). It has the shortest range of the 802.11 standards. It is less able to penetrate physical barriers like walls. The 802.11a specification is also known as Wi-Fi5, and though regionally deployed, it is not a global standard like 802.11b. The 802.11a specification applies to wireless ATM systems and is used in access hubs.

7.7.3.3 802.11b Standard (Wi-Fi)

The Wireless-Fidelity 802.11b standard operates in the 2.4 GHz range with up to 11 Mbps data rates and is backward compatible with the 802.11 standard. 802.11b uses a technology known as complementary code keying (CCK) modulation, which allows for higher data rates with less chance of multi-path propagation interference (duplicate signals bouncing off walls). This standard provides a better range than 802.11a: up to 300 feet in ideal circumstances and its better able than 802.11a to penetrate physical barriers, and lower in cost, but cannot support as many simultaneous connections. Furthermore, it operates on the same frequency as many cordless phones and other appliances; therefore, it is more susceptible to interference and other things that degrade its performance. Therefore it's not considered a good technology for certain applications requiring absolutely reliable connections, such as live video streaming. The two standards 802.11a and 802.11b can operate next to each other without any interference

7.7.3.4 802.11g Standard

802.11g is the most recent IEEE 802.11 draft standard and operates in the 2.4 GHz range with data rates as high as 54 Mbps over a limited distance. Some proprietary solutions manage to get 108Mbps. This standard is close to 802.11b in certain aspects; it provides a slightly shorter range than 802.11b, but still better than 802.11a. This standard suffers from the same problems, such as interference and absolute reliability, as 802.11b

7.7.4 WLAN IEEE 802.11 Frame Format

The three frame types in IEEE 802.11 are control frames, data-carrying frames, and management frames.

Control frames ensure reliable data delivery. There are six types of control frames:

- Power save poll (PSPoll): The sender sends this request frame to the access point requesting from it a frame that had been buffered by the access-point because it has been in power-saving mode.
- Request to send (RTS): The sender sends an RTS frame to the destination before the data is sent in the four-way handshake implemented in IEEE 802.11 for reliable data delivery.
- Clear to send (CTS): The destination sends a CTS frame to indicate that it is ready to accept data frames.
- ACK frame: The destination uses this frame to indicate to the sender a successful frame receipt.
- Contention-free end (CFE): The point-coordination function algorithm (PCF) uses this frame to signal the end of the contention-free period.
- CFE/End + CFE/ACK: PCF uses this frame to acknowledge the CFE end frame.

The data-carrying frames can be categorized into:

- Data: This is the regular data frame and can be used in both the contention and contention-free periods.
- Data/CFE-ACK: This is used for carrying data in the contention-free period and is used to acknowledge received data.

- Data/CFE-Poll: (PCF) uses this frame to deliver data to destinations and to request data frames from users.
- Data/CFE ACK/CFE-Poll: This frame combines the functionalities of the previous three frames into one frame.

Management frames are used to monitor and manage communication among various users in the IEEE 802.11 LAN through access points.

All other stations hearing the RTS or CTS then know about the pending data transmission and can avoid interfering with those transmissions. The transmission process including the transmission and reception of the RTS, CTS, DATA and ACK frames are shown in Figure 7.18. An IEEE 802.11 sender can operate either using the RTS/CTS control frames, as shown in Figure 7.21, or can simply send its data without first using the RTS control frame, as shown in Figure 7.17.

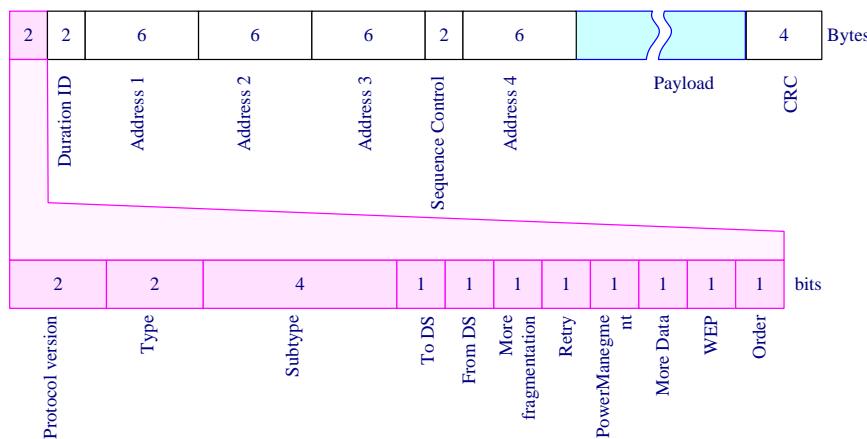


Figure 7.22: WLAN IEEE 802.11 frame structure

Beside the source and destination addresses, data field and CRC contained in all the other LAN types the frame contains other fields as it is illustrated in figure 7.22

- Frame Control
 - Protocol Version: indicates the version of IEEE 802.11 standard.
 - Type: indicates the frame type (Management, Control or Data).
 - Subtype: indicates the frame subtype (Authentication frame; De authentication frame; Association request frame; Association response frame; Re association request frame; Re association response frame; Disassociation frame; Beacon frame; Probe frame; Probe request frame and Probe response frame).
 - To DS: is set to 1 when the frame is sent to Distribution System (DS)
 - From DS: is set to 1 when the frame is received from the Distribution System (DS)
 - More Fragments: is set to 1 when there are more fragments belonging to the same frame following the current fragment
 - Retry: indicates that this fragment is a retransmission of a previously transmitted fragment. (For receiver to recognize duplicate transmissions of frames)

- Power Management: indicates the power management mode that the station will be in after the transmission of the frame.
- More Data: indicates that there are more frames buffered to this station.
- WEP: indicates that the frame body is encrypted according to the WEP (wired equivalent privacy) algorithm.
- Order indicates that the frame is being sent using the Strictly-Ordered service class.
- Duration/ID: Station ID is used for Power-Save poll message frame type. The duration value is used for the Network Allocation Vector (NAV) calculation.
- Address fields (1-4): The peculiar thing about the 802.11 frame format is that it contains four, rather than two, addresses. How these addresses are interpreted depends on the settings of the To DS and From DS bits in the frame's Control field. This is to account for the possibility that the frame had to be forwarded across the distribution system, which would mean that the original sender is not necessarily the same as the most recent transmitting node. Similar reasoning applies to the destination address. In the simplest case, when one node is sending directly to another, the DS bits are 0, Address 1 identifies the target node, and Address 2 identifies the source node. In the most complex case, both DS bits are set to 1, indicating that the message went from a wireless node onto the distribution system, and then from the distribution system to another wireless node. With both bits set, Addr1 identifies the ultimate destination, Address 2 identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination), Address 3 identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded it across the distribution system), and Address 4 identifies the original source.
- Sequence Control: consists of fragment number and sequence number. It is used to represent the order of different fragments belonging to the same frame and to recognize packet duplications.
- Data - is information that is transmitted or received, it contains MAC service data unit or control information.
- CRC - contains a 32-bit Cyclic Redundancy Check (CRC) used for error detection.

7.7.5 WLAN IEEE 802.11MAC Method

WLANS use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or Distributed Coordination Function (DCF). CSMA/CA attempts to avoid collisions by using explicit packet acknowledgments (ACKs), which means that an ACK packet is sent by the receiving station to confirm the integrity of the data packet that arrived. The algorithm works as follows.

- The sender senses the energy level on the radio frequency to determine whether or not another station is transmitting and provides this carrier sensing information to the MAC protocol.
- If the medium is sensed idle, the sender may transmit.
- If the medium is sensed busy

- The sender has to wait.
 - When the medium is sensed idle, the sender has to wait two additional time periods.
 - The first period depends on the packet to be transmitted.
 - If it is an ACK, this period is one short interframe space (SIFS);
 - Otherwise it is a DCF interframe space (DIFS).
 - The second is a random backoff period, which prevents multiple terminals from seizing the medium immediately after completion of the preceding transmission.
 - After both periods have passed and the channel has not been seized, the terminal may start transmission.
 - Otherwise, the whole process restarts.
- When a receiving station has correctly and completely received a frame for which it was the addressed recipient (if no other station's transmission has interfered with the frame's transmission), it waits a short period of time (known as the Short Inter Frame Spacing - SIFS) and then sends an explicit acknowledgment frame back to the sender. Wireless sender can not itself determine whether or not its frame transmission was successfully received at the destination.

The idea is for the sender and receiver to exchange control frames with each other before the sender actually transmits any data. This exchange informs all nearby nodes that a transmission is about to begin. Specifically:

- The sender transmits a Request to Send (RTS) frame to the receiver.
- The RTS frame includes a field that indicates how long the sender wants to hold the medium (i.e., it specifies the length of the data frame to be transmitted).
- The receiver then replies with a Clear to Send (CTS) frame; this frame echoes this length field back to the sender.
- Any node that sees the CTS frame knows that it is close to the receiver, and therefore cannot transmit for the period of time it takes to send a frame of the specified length.
- Any node that sees the RTS frame but not the CTS frame is not close enough to the receiver to interfere with it, and so is free to transmit.
- There are two more details to complete the picture.
 - First, the receiver sends an ACK to the sender after successfully receiving a frame. All nodes must wait for this ACK before trying to transmit.
 - Second, should two or more nodes detect an idle link and try to transmit an RTS frame at the same time, their RTS frames will collide with each other.

The transmission of a frame by a sending station and its subsequent acknowledgment by the destination station is shown in Figure 7.23.

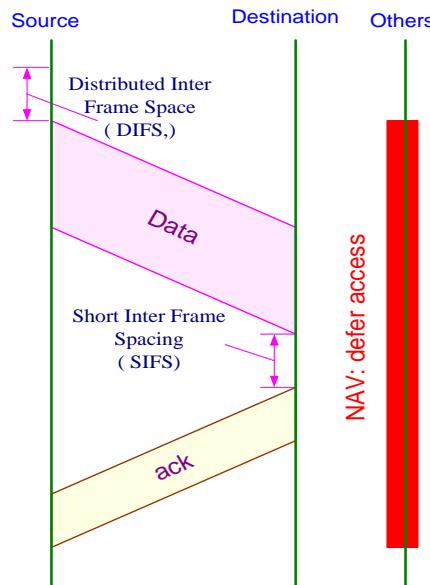


Figure 7.23: The transmission of a frame by a sending station and its subsequent acknowledgment by the destination station

A receiver that receives an RTS frame responds with a CTS frame, giving the sender explicit permission to send.

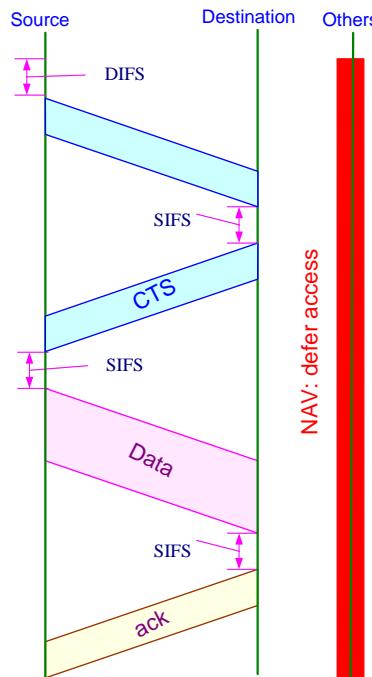


Figure 7.24: The RTS, CTS, DATA and ACK frames (4 way handshaking)

💡 Both direct sequencing spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) wireless technologies can operate in the unlicensed 2.4-GHz ISM band.

7.8 ATM LAN

ATM is designed for high-speed transmission of all types of communications, from voice to video to data, over one network. ATM provides integration of multiple dissimilar network architectures from the desktop to the wide area by converting all information to a consistent cell format.

By making these cells uniform in length, and employing innovative switch and traffic management methodologies, ATM provides unparalleled scalability, operating from Mb/s to Gb/s, and the ability to support implicit levels of Quality of Service. These two important characteristics of ATM enable networks to be built that last a long time and have the ability to significantly reduce the cost associated with the operation and support of multiple application or service specific networks.

With virtually unlimited bandwidth potential, ATM technology is currently used in network backbones (as depicted in Figure 7.25) or specific workgroup applications with heavy traffic loads and/or the need to integrate various types of traffic, such as voice, video, or compute intensive data, into a single network.

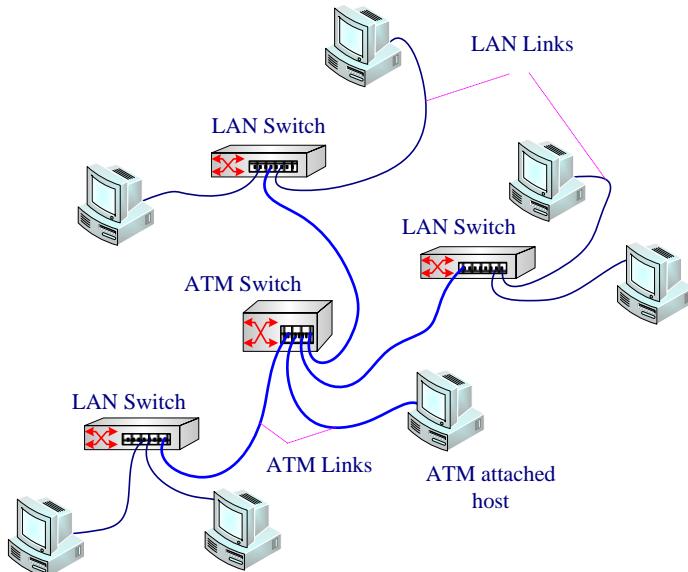


Figure 7.25: ATM used as a LAN backbone.



ATM is a high-speed, broadband transmission data communication technology based on cell switching, which uses fixed-size cells, each 53-byte. ATM is used to carry integrated data, voice, and video information and can be used as the underlying technology for Fiber Distributed Data Interface (FDDI), Synchronous Optical Network (SONET), and other high-speed networks. ATM can run on any medium including coax, twisted-pair, or fiber-optic.

7.9 Quick Review

- ❖ Today, Ethernet is by far the most prevalent LAN technology, and is likely to remain so for the foreseeable future.
- ❖ All of the Ethernet technologies, whether they use coaxial cable or copper wire, or whether they run at 10 Mbps, 100 Mbps or 1 Gbps, use the same frame structure.
- ❖ The popularity and large installed base of 10-Mb/s LANs makes it a natural springboard for faster networking technologies.
- ❖ The term *Ethernet* refers to the family of local-area networks (LANs) standardized by the IEEE 802.3 Working Group.
- ❖ Ethernet is a broad term in its own right. It has several subsets ranging from 10Base2 (10 Mbps Ethernet with a maximum segment length of 185 meters over thin coaxial cable) to 1000BaseT (1000 Mbps Ethernet or Gigabit Ethernet with a maximum segment length in excess of 500 m over fiber-optic cable).
- ❖ Anticipated in spring 2002 is the standardization of 10-Gigabit Ethernet, supporting distances up to 40 km over single-mode fiber.
- ❖ As Ethernet speeds have increased, the network diameter has shrunk proportionately. Whereas 10 Mbps Ethernet supports up to four repeater hops, 100 Mbps (Fast) Ethernet supports only one or two repeater hops. Gigabit Ethernet had to be modified a bit by the use of carrier extensions in the frame to make one repeater hop possible.
- ❖ Ethernet implementations will utilize the full-duplex features with LAN switching technology.
- ❖ The 802.3 standards are not complete yet; the 100Gbps Ethernet prototypes are in the early stages, and they promise all the benefits of a ubiquitous and inexpensive technology for use in metro and wide area service provider networks.
- ❖ Both 100Base-T and 100VG-AnyLAN technologies have a common goal: to provide 100-Mbps connectivity without modification to the network packet transferred on the wire. The main difference is in their approach to providing 10 times the bandwidth of the 10Base-T, without decreasing the 100-meter 10Base-T lobe length.
- ❖ Ethernet faced many challenges from other LAN technologies, including token ring, FDDI and ATM. Some of these other technologies succeeded at capturing a part of the market share for a few years.
- ❖ There are many reasons for Ethernet's success. First, Ethernet was the first widely-deployed high-speed LAN. Other technologies such FDDI and ATM are more

complex and expensive than Ethernet, which further discouraged network administrators from switching over. Ethernet always fought back, producing versions that operated at equal data rates or higher. Ethernet hardware in particular, network interface cards has become a commodity and is remarkably cheap.

- ❖ One other 100Base standard, which is not part of 802.3 is 100VG-AnyLan. The main characteristics of this standard, is that it attempts to leverage older, preinstalled copper wire (Category 3, 4 or 5 - so it may be an economical alternative in an upgrade process), it can accommodate both Ethernet and Token Ring packets, it uses Demand Priority Access instead of the traditional CSMA/CD and it uses hubs that can filter packets based on their address, thereby reducing traffic and enhancing privacy.
 - ❖ The WLAN standard 802.11 defines the *Medium Access Control* (MAC) and PHY layers for a LAN with wireless connectivity. Under these standard many substandards were adopted (802.11a, 802.11b, 802.11h and 802.11i). They differ from each other by their frequency range, data rate and transmission distance.
 - ❖ Wireless LAN, such as those based on IEEE 802.11, have one Base station or access point that controls communication with all of the other wireless nodes in the network.
 - ❖ The reliability of these networks is set by the quality of the RF link between the central access point and each endpoint.
 - ❖ WLANs use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) or Distributed Coordination Function (DCF) as an access method.
 - ❖ The concept of ATM LANs is very simple, use ATM switches to build a LAN and so allow users to have access extremely high network capacity.
-

7.10 Self Test Questions

A- Answer the following questions

1. Describe the ethernet frame format.
2. What is the standard Ethernet?
3. List the common types of traditional Ethernet standards?
4. List the common types of fast Ethernet standards?
5. How does every type of fast Ethernet standards achieve its speed?
6. What is the signal encoding used by every type of fast Ethernet standards?
7. What is the cable type used by every type of fast Ethernet standards?
8. What is the cable type used by every type of Gigabit Ethernet standards?
9. Why is the extension field added to the Gigabit Ethernet frame?
10. What is the encoding scheme used by every type of Gigabit Ethernet standards?
11. List some of the 10 gigabit Ethernet applications
12. List the common types of the 10 gigabit Ethernet standards?
13. What happens when two computers each support a different Ethernet standard want to communicate each other?
14. How does the hub priority work?
15. How does the MAU maintain the ring topology in the case of any host failure?
16. Explain the token ring frame format.
17. How does token ring algorithm work?

18. What is the benefit of using the secondary ring in FDDI?
19. What are the differences between the SAS and DAS devices?
20. Explain the FDDI frame format.
21. What are the benefits of using wireless LANs?
22. What are the two types of the 802.11 specification operational modes?
23. List the WLAN standards.
24. How does the Wi-Fi work?
25. Explain the WLAN IEEE 802.11 frame structure.
26. How does (CSMA/CA) work for WLANs?

B- Identify the choice that best completes the statement or answers the question.

1. One of the following can be easily scaled 10 Mbps to 100 Mbps to 1000 Mbps to 10Gbps.

a. Ethernet	c. ARPANET
b. SONET	d. Internet
2. 10 Gigabit Ethernet operates at ____.

a. simplex	c. half duplex
b. demand priority	d. full duplex
3. Gigabit Ethernet uses ____.

a. TDMA	c. CSMA/CD
b. CDMA	d. demand priority
4. ____ cables are Category 4 UTP cables capable of a maximum transmission rate of 20 Mbps.

a. 10Base2	c. 10Base20
b. 10Base5	d. 10BaseT
5. 10Base5 refers to ____.

a. thicknet	c. Category 5 UTP
b. thinnet	d. Category 6 UTP
6. What is the central device in a star-wired ring topology?

a. hub.	c. MAU.
b. switch.	d. server.
7. In a ____ W LAN, user devices communicate with the nearest access point and may move from one cell to another.

a. single-cell	c. peer-to-peer
b. multiple-cell	d. star-wired
8. In a ____ W LAN, there is no access point at the center of a cell and each user device communicates to the other user devices.

a. single-cell	c. peer-to-peer
b. multiple-cell	d. star-wired
9. In a ____ wireless LAN, all user devices communicate with one access point, competing for the same set of frequencies.

21. FDDI is a _____ topology.
a. bus
b. ring
c. dual-ring
d. star
22. In a WLAN, the _____ communicates with the wireless user device.
a. interface card
b. access point
c. modem
d. controller
23. The _____ is one of the most common standards for broadband Ethernet.
a. 10Broad5
b. 10Base2
c. 10Broad36
d. 10BaseT
24. _____ supports 100 Mbps baseband signals using two pairs of Category 5 unshielded twisted pair.
a. 100BaseTX
b. 100BaseFX
c. 100BaseT4
d. 100VG-AnyLAN
25. _____ supports older category wire such as Category 4 and 5.
a. 100BaseTX
b. 100BaseFX
c. 100BaseT4
d. 100VG-AnyLAN
26. _____ is used for short-distance (0.1 to 25 meters) jumper cables using balanced copper wire.
a. 1000BaseSX
b. 1000BaseLX
c. 1000BaseCX
d. 1000BaseT
27. The feature that separates the CSMA/CD protocol found on wired LANs from the CSMA/CA found on wireless networks is that _____
a. a priority is assigned to transmissions
b. there are no collisions
c. it is guaranteed that only one workstation will transmit at a time
d. it is a round robin protocol
28. What is the IEEE standard that covers wireless technologies?
a. 802.11
b. 802.12
c. 802.13
d. 802.14
29. What is the IEEE standard that covers Token Ring?
a. 802.2
b. 802.3
c. 802.4
d. 802.5
30. What is the IEEE standard that covers the Logical Link Control?
a. 802.2
b. 802.3
c. 802.4
d. 802.5
31. What is the IEEE standard that defines the access method used by most Ethernet networks?
a. 802.2
b. 802.3
c. 802.4
d. 802.5
32. What is the standard that describes an Ethernet network connected by twisted-pair cable that can support 100-Mbps transmissions using baseband digital signals?

CHAPTER 8

EXTENDED LAN

8.1 About This Chapter

The cable alone is not enough in large networks. Transmission medium and the protocols that regulate them have finite limits on the number of nodes that can be supported. In order to expand the size and range of a computer network, devices that amplify, connect, and segment the transmission medium need to be added. These hardware devices are called repeaters, hubs, bridges, and routers.

Depending on the type of topology your network uses and the type of cabling you use, your LAN might require some sort of connectivity device to connect the various network computers, printers, and other devices together. In cases where you need to extend your LAN (say, to the second floor of an office building) or add a large number of new users to the LAN, other connectivity devices might be required. Some of these connectivity devices merely serve to connect devices; others are used to boost the data signal traveling on the network medium, and still others actually participate in determining how data traffic should flow on the network.

Some devices with the hub, which is a device you would use on a small network, or even in a peer-to-peer networking situation, to connect computers. The other devices that we will look at, such as repeaters, switches, and routers, are often lumped under the blanket term internetworking devices. An internetwork is a network of LANs, meaning that some sort of connectivity technology is used to extend a LAN beyond its typical size or to connect different LANs together into one large network.

Local Area Network (LAN) technology has made a significant impact on almost every industry. Operations of these industries depend on computers and networking. The data is stored on computers than on paper, and the dependence on networking is so high that banks, airlines, insurance companies and many government organizations would stop functioning if there were a network failure. Since, the reliance on networks is so high and the network traffic is increasing, we have to address some of the bandwidth problems this has caused and find ways to tackle them.

Virtual LAN (VLAN) support may be attractive in banks, airlines, insurance companies and many government organizations. A VLAN is logical grouping of ports into workgroups. With VLAN support network managers can define workgroups independent of underlying network topology.

VLANs are becoming popular because of the flexibility they offer. Users can physically move but stay on the same VLAN. So in this chapter we will define VLAN's and examine the difference between a LAN and a VLAN. This is followed by a discussion on the advantages VLAN's introduce to a network.

In the past few years, we have seen an explosion of mobile devices over the world such as notebook, multimedia PDA and mobile phones. The rapidly expanding markets of cellular voice and limited data service have created a great demand for mobile

communication and computing. Mobile communications applications include mobile computing and wireless communications. We will focus in this chapter on how to wirelessly extend networks.

8.2 Learning Outcome

After this chapter, you should be able to:

1. Explain how to extend LAN using physical Layer devices
2. Explain how to extend LAN using Data link Layer devices
3. Explain how to extend LAN using Network Layer devices
4. Explain how to extend LAN using Gateway
5. Understand the necessity to extend LAN
6. Understand the capability and the advantages and disadvantages of every connectivity device while extending LANs
7. Understand the structure of VLAN and how VLAN extend the capability of LAN
8. Understand the role of wireless connectivity devices in extending LANs
9. Explain how to extend LAN using wireless connectivity devices
10. Understand the role of optical fiber cables and devices in extending LANs

8.3 Extending LAN Using Physical Layer Devices

8.3.1 Repeaters

8.3.1.1 General Description

Repeater, the simplest internetworking device, is designed primarily to connect two segments of a LAN. It is unintelligent device works at the network **Physical** layer as shown in Figure 8.1. A repeater is a Baseband device, its essential function is signal regeneration, differentiates it from a piece of cable (see Figure 8.2). Signal regeneration is needed when the LAN length is extended. When a LAN is extended, bits can be corrupted and decayed. The repeater assumes that the connecting LANs have the same protocol. It simply accepts bits from one LAN and transmits them on to the other LANs.

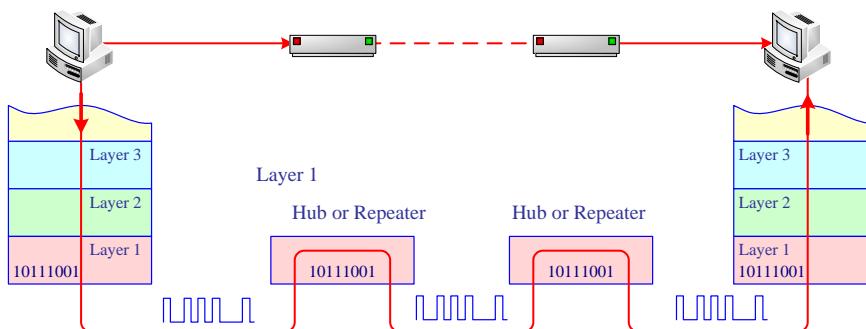


Figure 8.1: Repeater in ISO physical Layer

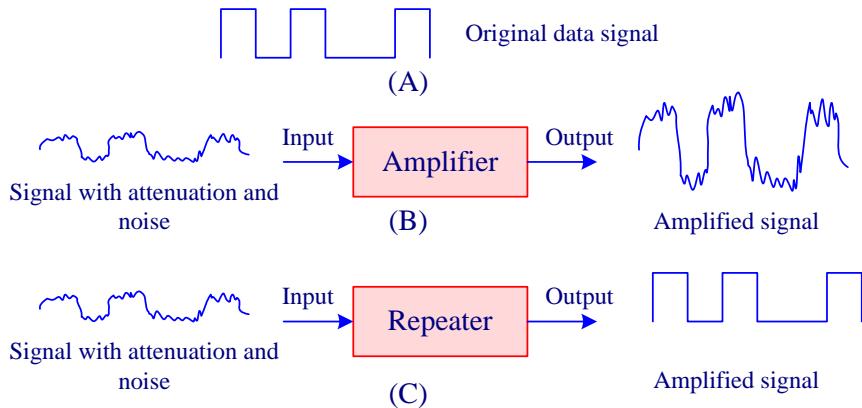


Figure 8.2: illustration of the differences between a repeater and an amplifier

Repeaters are employed in bus network topologies to connect different network segments together.

8.3.1.2 Characteristics of Repeaters:

- They connect between two LANs which are already at maximum length but which need to be interconnected into one bus.
- Receive signals from each bus to which they are attached and repeats the signal onto the other segment cleaned up and newly amplified
- Make no attempt to read frames. Just blindly repeat any signal they read, leads to the possibility of passing noise from one segment to another
- Each repeater allows the total length of a LAN to double
- Repeaters add some delay to transmission and increased LAN length adds more delay. This forms the CSMA/CD mechanism, which relies on propagation time. To avoid this problem, propagation times are calculated based on no more than four repeaters between any two workstations on a LAN - beyond this limit the CSMA/CD starts to fail.
- By careful arrangement of repeaters this condition can be met and a whole large building can be on a single extended LAN.
- Repeaters can be used to connect two groups of computers that are too far apart to be strung on a single segment. When you use a repeater like this, the repeater divides the cable into two segments. The cable length limit still applies to the cable on each side of the repeater. Figure 8.3 shows you how to use repeater to connect groups of computers.

8.3.1.3 Drawbacks of Repeaters

- No filtering of noise generated on one segment, all passes to next segment
- The entire LAN is on one bus (it becomes a single collision domain), but many more machines can be added, more contention for bus, more collisions and poorer performance.

8.3.2 Amplifiers

They serve the same purpose as repeaters but do so by amplifying the signal rather than repeating it. Amplifiers are used in Broadband technology for analog signals.

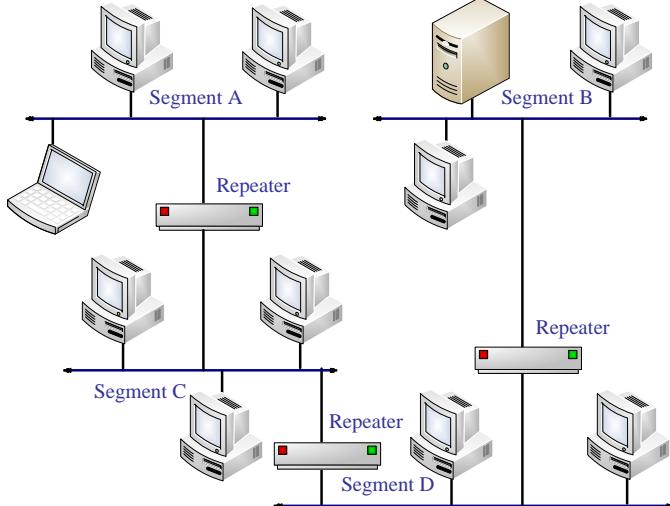


Figure 8.3: Repeater connection

When a broadband signal, which is an analog signal, is transported over a copper wire, it adds noise (see Figure 8.2). When this signal is passed through the transport segment from amplifier to amplifier, any noise it picks up along the way is added to the signal and amplified. So the longer the transmission distance, and the more times the signal is passed between amplifiers, the worse the signal will be when it reaches its destination. With audio transmission systems, it is possible to filter noise, but with data transmission systems, you cannot filter without degrading the signal, which results in corrupted data.

8.3.3 Hubs

8.3.3.1 General Description

Known as concentrators or multiport repeaters, hubs work at the physical level, to connect multiple network segments see Figure 8.4. Hubs come in all sizes and shapes and are available in a wide range of prices. Typically, the more ports on the hub, the more expensive the hub. Hubs that support faster varieties of Ethernet, such as Fast Ethernet (which were discussed earlier in the previous chapter), will also cost more.

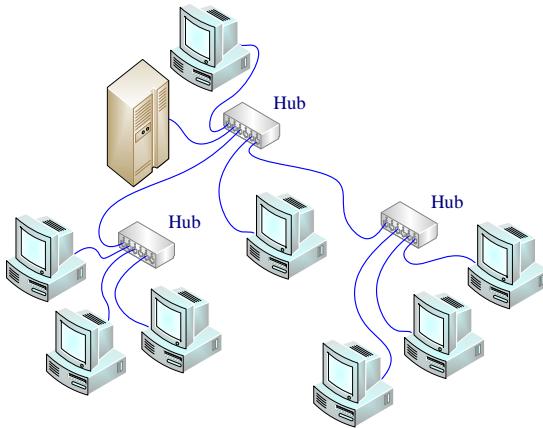


Figure 8.4: Hub connection



A device called a wiring concentrator or Multistation Access Unit (MAU) is similar to a hub but is used in Token Ring networks.

8.3.3.2 Types of Hubs

- **Passive Hub:** The most basic type, a Passive Hub does not use repeater technology; it just passes the signal along without regenerating it. Although the name Concentrator is used to define any type of hub, it is perhaps most appropriate when used to describe a passive hub
- **Active Hub:** An active hub adds repeater technology to a passive hub and serves in the dual role of concentrator and repeater. For this reason, an active hub is also called a Multiport Repeater
- **Intelligent Hub:** This term encompasses quite a few different types of hubs. It basically describes an active hub that can perform additional "intelligent" functions. These functions can be:
 - Remote management, in which the hub's status can be monitored remotely in conjunction with a monitoring software package. The term Distributed Hub is also used
 - Virtual LAN (VLAN): Virtual Segments can be created to isolate certain groups of devices as not to interfere with regular network activity.
 - 10/100 or 10/100/1000 conversions: The hub can translate signals from 10Mbps, 100Mbps, and 1000Mbps to allow the coexistence of different NIC types
 - Medium conversion: A hub can also have multiple connector types - Fiber, RJ45, AUI and convert between them. This type is **hybrid hub** which is an advanced hub that can accommodate several different types of cables.

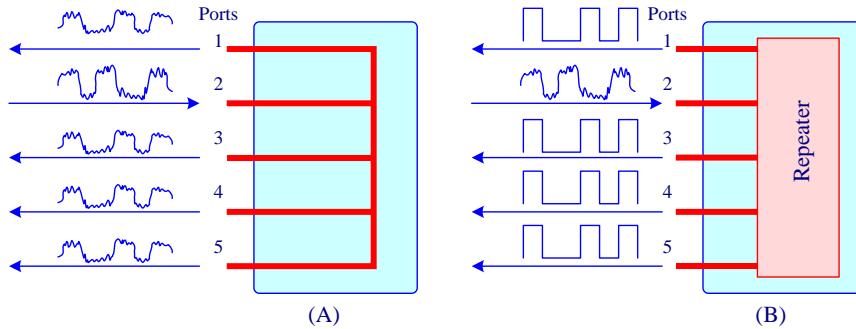


Figure 8.5: Hub Types (A) Passive and (B) Active

You can connect hubs to one another; this is called *daisy-chaining*. When you daisy-chain hubs you connect a cable to a standard port on one of the hubs and the daisy-chain port on the other hub or switch. You can daisy-chain no more than three hubs together.

➤ **Stackable Hub:** It is modular in design and can be mounted in racks and cabinets within the wiring closet and can be connected using special ribbon or DB-50 cables. Stackable hub may also have an uplink switch that can be used to convert one of the ports into an additional uplink port, allowing you to connect another hub directly to the port. Figure 8.6 shows how to use stackable hubs to connect LANs and stations with different speeds.

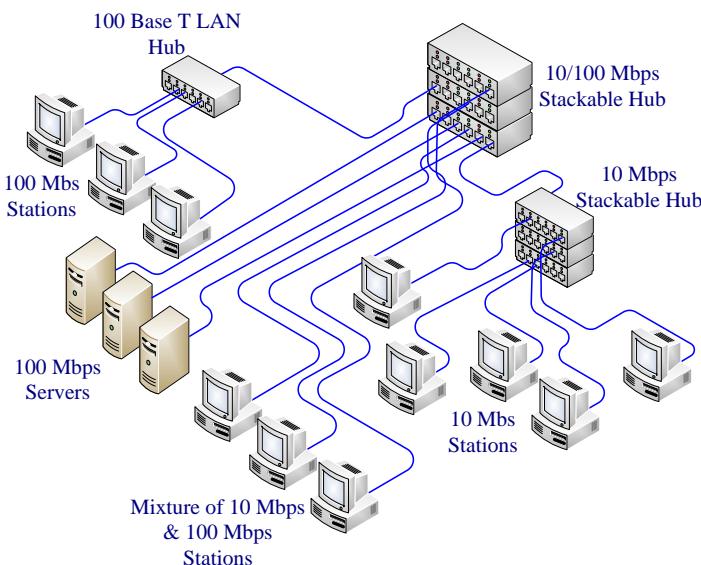


Figure 8.6: using stackable hubs to connect LANs and stations with different speeds

 Ethernet switches, which offer superior performance than Hubs, are gaining popularity in today's high-speed multimedia environments as their price continues to fall.

8.4 Extending LAN Using Data Link Layer Devices

8.4.1 Bridges

8.4.1.1 General Description

A bridge is an intelligent device that works at the Data Link Layer as illustrated in Figure 8.7. It connects two networks so that they act as if they are one network.

Most bridges have the capability to listen to the network and automatically figure out the address of each computer on both sides of the bridge. Then the bridge can inspect each message that comes from one side of the bridge and broadcast it on the other side of the bridge, but only if the message is intended for a computer that's on the other side. This key feature enables bridges to partition a large network into two smaller, more efficient networks. They can be used both to join dissimilar medium such as unshielded twisted-pair (UTP) cabling and fiber-optic cabling, and to join different network architectures such as Token Ring and Ethernet.

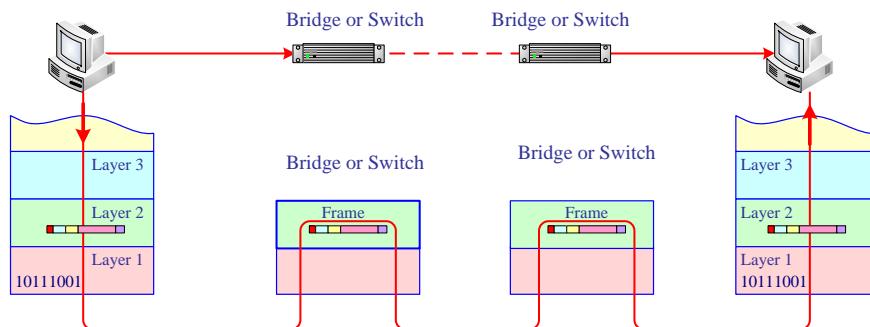


Figure 8.7: Bridge in ISO Data Link Layer

 While a single Ethernet segment can carry only 10 Mbps of total traffic for example, an Ethernet bridge can carry as much as 10n Mbps, where n is the number of ports (inputs and outputs) on the bridge.

8.4.1.2 Types of Bridges

In general, bridges can be classified into:

- **Transparent bridges:** These bridges are used to join network segments that are based on same MAC protocol. Typically they are found in Ethernet environments. The transparent bridge analyzes the incoming frames and forwards them to the appropriate segments one hop at a time.
- **Source-route bridges:** They are typically found in Token Ring environments, in source-route bridging, each ring is assigned a unique number on a source-route bridge port. Token Ring frames contain address information, including a ring and bridge numbers, which each bridge analyzes to forward the frame to the appropriate ring.
- **Source-route transparent bridges:** Source-route transparent bridging is an extension of source-route bridging, whereby non-routable protocols receive the routing benefits of source-route bridging and a performance increase associated with transparent bridging.
- **Source-route translation bridges:** These bridges are used to join network segments that are based on different MAC protocols. An Ethernet-to-Token Ring bridge is an example of a translating bridge. A variation of the translation bridge is the **encapsulating bridge**, which is used to join networks that use the same MAC protocol across a network that uses a different MAC protocol. Figure 8.8 illustrates the application of FDDI-to-Ethernet encapsulation bridges to interconnect three Ethernet LANs.

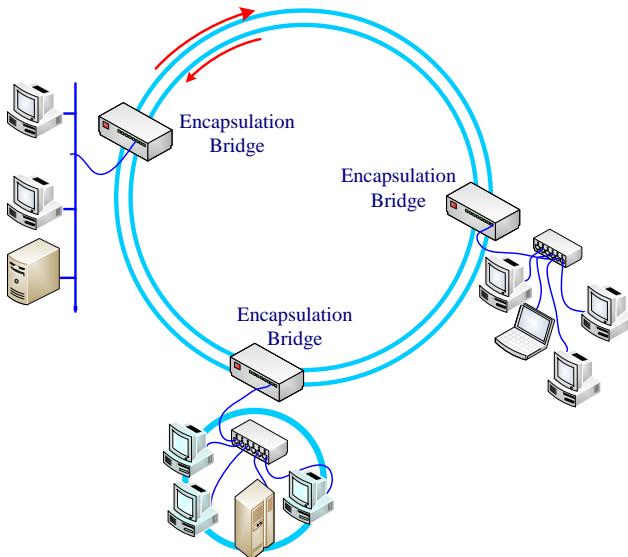


Figure 8.8: Application of FDDI-to-Ethernet encapsulation bridges

- **Remote Bridges:** They are often used to connect two geographically separated networks by telephone lines, leased lines, or a circuit-switched service (see Figure 8.9). A remote bridge has at least one local area network (LAN) port for a connection to a switch or a hub, and at least one serial port (synchronous for digital lines or asynchronous for modems or both synchronous and asynchronous

serial ports). Remote bridges can also be enabled for Simple Network Management Protocol (SNMP) and have other diagnostic and support features.

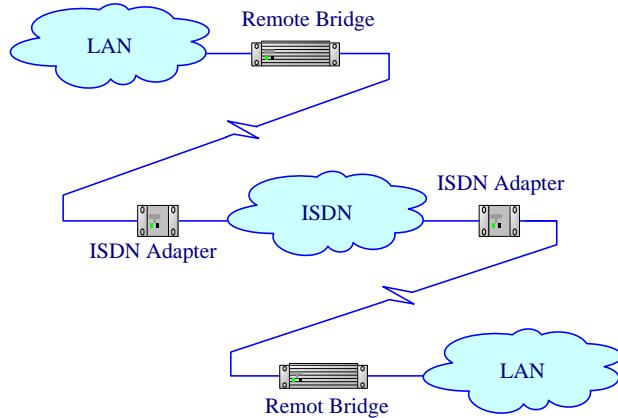


Figure 8.9: Using remote bridge to join two separate LANs located at a great distance from each other

8.4.1.3 Characteristics of Bridges

- Bridges like repeaters, add segments and total length to LAN, but bridges can also detect errors and do **frame filtering**. Read frames (place into a memory buffer) from both sides of the bridge and can take different actions depending on the frame, which was read. If an error was detected frame is thrown away.
- Buffered frames are examined to see:
 - Which machine **sent** the frame and on which side of the bridge is that machine located, this information is kept in memory from then on
 - Which machine is the **destination** for the frame and on which side of the bridge is it located. If the destination is on the other side of the bridge the frame is repeated onto that segment, otherwise no action is taken on the frame since the originator and receiver are on the same side of the bridge. This is known as **frame filtering**
 - These bridges (most) are called **adaptive or learning bridges**. A bridge learns where each machine is located by listening to all traffic on the network. Any time a machine sends a message, the bridge records the source address and location. After time it knows where each machine is located and from then on a message being sent to a machine on the same segment is not repeated (frame filtering) (see Figure 8.10)
- Frame filtering reduces traffic on both segments since local traffic is not forwarded. This reduces collisions and contention for each LAN
- A bridge provides partial separation of a LAN into two or more collision domains, leads to a design principle. Machines that communicate frequently should be placed in a separate collision domain

- To increase reliability, some sites use two or more bridges in parallel between pairs of LANs, as shown in Fig. 8-11. This arrangement, however, also introduces some additional problems because it creates loops in the topology.
- Unknown destination frames and Broadcast frames cause a cycles of bridges
 - Broadcast frames are always forwarded by all bridges since they are directed to all other machines. Unknown destination frames are forwarded when it reaches the bridge since they are directed to its destination.
 - This can present a problem in a bridged network which contains a cycle of bridges in Figure 8.11, with A simple example of these problems can be seen by observing how a frame F1, with unknown destination is handled. Each bridge, following the normal rules for handling unknown destinations, forward a copy of this frame to LANs connected to it. This cycle goes on forever unless the cycle is removed.

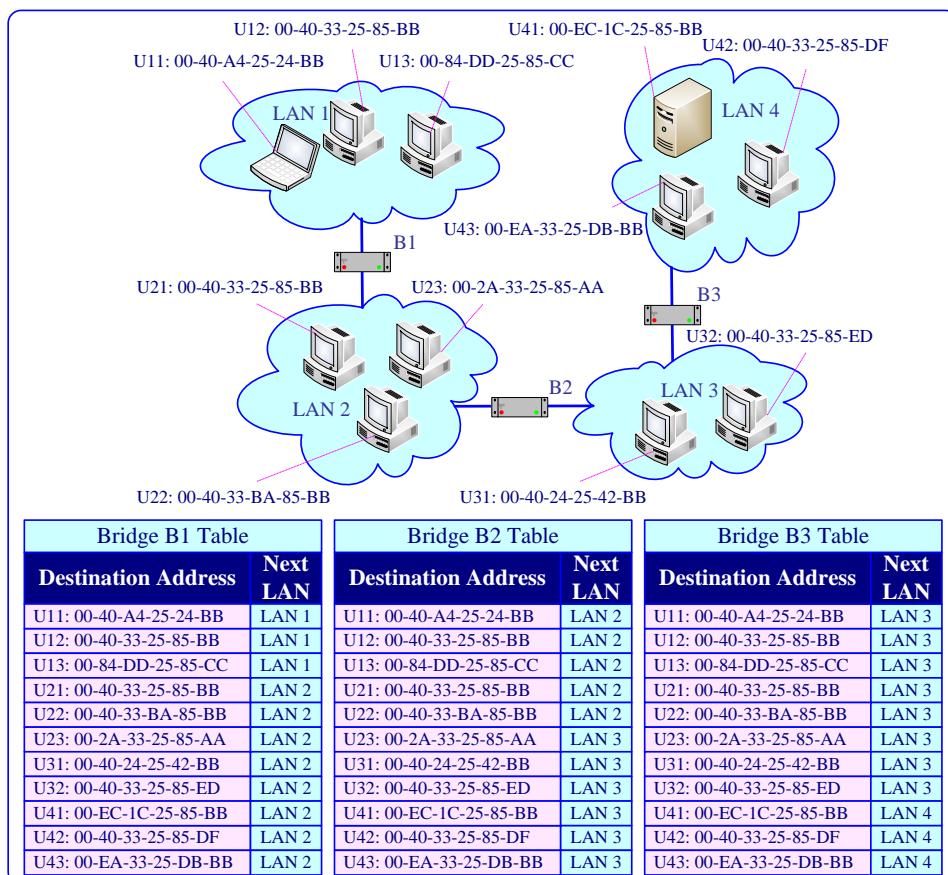


Figure 8.10: Illustration of bridge table building

- The **Distributed Spanning Tree (DST)** algorithm is implemented by many bridges and allows bridged networks to automatically decide which bridges will not be allowed to forward broadcast messages thus preventing cycles. Figure 8.7 shows a DST. The algorithm works as follows:

- Each link from a bridge to a LAN is assigned a cost. This link cost is inversely proportional to the link's bit rate. A higher bit rate implies a lower cost.
 - First the bridges have to choose one bridge to be the root of the tree. They make this choice by having each one broadcast its ID (serial number, installed by the manufacturer) and guaranteed to be unique worldwide. Any bridge with the lowest ID is selected as root.
 - Next, a tree of shortest paths from the root to every bridge and LAN is constructed. This tree is the spanning tree. If a bridge or LAN fails, a new one is computed.
 - The result of this algorithm is that a unique path is established from every LAN to the root and thus to every other LAN (not all the bridges are necessarily present in the tree to prevent loops)
- Even after the spanning tree has been established, the algorithm continues to run during normal operation in order to automatically detect topology changes and update the tree.

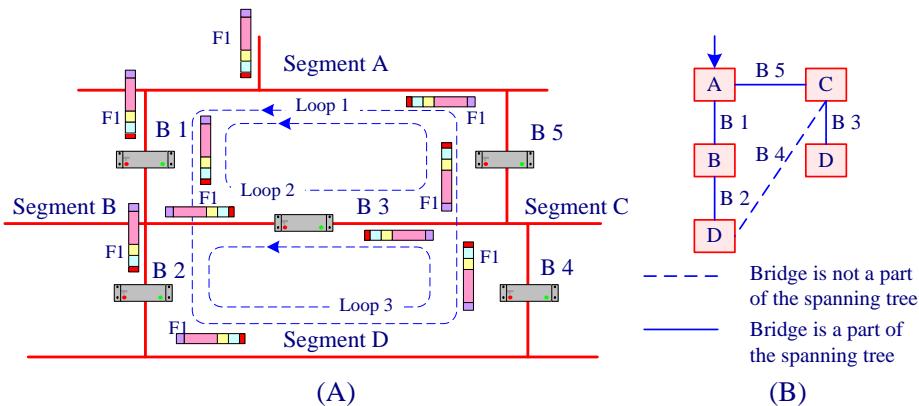


Figure 8.11: Network contains a cycle of bridges (A) Interconnected LANs.
(B) A spanning tree covering the LANs.



A bridge enhances the efficiency of networks by facilitating simultaneous transmissions within multiple LANs. But it can forward only one frame at a time in a store-and-forward fashion between two segments.

8.4.2 LAN Switches

8.4.2.1 General Description

A LAN Switch is a fundamental part of most networks used as layer 2 device. It makes it possible for several users to send information over a network at the same time without slowing each other down. Switches allow different **nodes** or **subnets** to communicate directly with one another in a smooth and efficient manner. In the simplest terms, a switch is a mechanism that allows us to interconnect links to form a larger

network. A switch is a multi-input, multi-output device, which transfers packets from an input to one or more outputs.

Recent LAN switches are evolving to multi-layer devices capable of handling protocol issues involved in high-bandwidth applications that historically have been solved by routers. Today, LAN switches are being used to replace hubs in the wiring closet because user applications are demanding greater bandwidth. They consist of many ports that connect LAN segments (Ethernet and Token Ring) and a high-speed port (such as 100-Mbps Ethernet, Fiber Distributed Data Interface (FDDI), or 155-Mbps ATM which connects the LAN switch to other devices in the network. A LAN switch has dedicated bandwidth per port, and each port represents a different segment.

A vital difference between a hub and a switch is that all the nodes connected to a hub share the bandwidth among themselves, while a device connected to a switch port has the full bandwidth all to itself. For example, if 10 nodes are communicating using a hub on a 10 Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well. But with a switch, each node could possibly communicate at the full 10 Mbps.



Switches can forward multiple frames simultaneously through multiple parallel data paths.

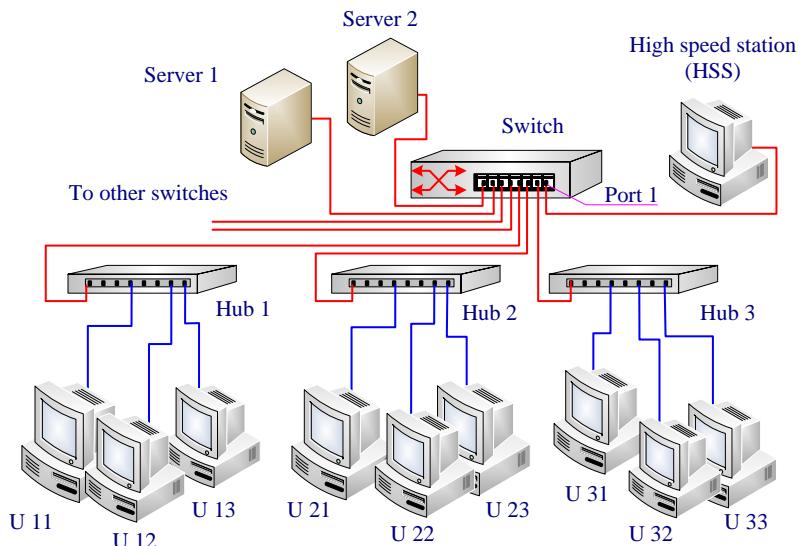


Figure 8.12: An example of a network using a switch

Switching allows a network to maintain full-duplex Ethernet. Before switching, Ethernet was half-duplex, which means that only one device on the network can transmit at any given time. In a fully switched network, nodes only communicate with the switch, never directly with each other.

Fully switched networks employ either twisted-pair or fiber-optic cabling, both of which use separate conductors for sending and receiving data. In this type of environment, Ethernet nodes can forgo the collision detection process and transmit at will, since they are the only potential devices that can access the medium. In other words, traffic flowing in each direction has a lane to itself. This allows nodes to transmit to the switch as the switch transmits to them, in a collision free environment. Transmitting in both directions can also effectively double the apparent speed of the network when two nodes are exchanging information. For example, if the speed of the network is 10Mbps, then each node can transmit simultaneously at 10 Mbps.

Switches maintain address tables just like transparent bridges. They learn the addresses of their neighbors, and when a frame is to be forwarded, they first look up the address table and broadcast only if no entry corresponding to that destination is found. Stations that have not transmitted recently are aged out. This way a small address table can be maintained and the switch can relearn if a station starts transmitting again. Referring to Figure 8.12 we can imagine the switch address table as it is shown in Figure 8.13.

Switch address tables			
Destination Address	Port	Destination Address	Port
U11: 00-40-A4-25-24-BB	2	U31: 00-40-24-25-42-BB	4
U12: 00-40-33-25-85-BB	2	U32: 00-40-33-25-85-ED	4
U13: 00-84-DD-25-85-CC	2	U33: 00-EC-1C-25-85-BB	4
U21: 00-40-33-25-85-BB	3	HSS: 00-40-33-25-85-DF	1
U22: 00-40-33-BA-85-BB	3	S 1: 00-EA-33-25-DB-BB	8
U23: 00-2A-33-25-85-AA	3	S 2: 00-CD-89-65-DB-BA	7

Figure 8.13: A switch address table for the network shown in Figure 8.12

 When a LAN switch first starts up and as the devices that are connected to it request services from other devices, the switch starts to build its table that associates the MAC address of each local device with the port number through which that device is reachable.

Whenever a device connected to the LAN switch sends a packet to an address that is not in the LAN switch's table (for example, to a device that is beyond the LAN switch), or whenever the device sends a broadcast or multicast packet, the LAN switch sends the packet out all ports except for the port from which the packet originated.

8.4.2.2 Switching Technologies

LAN switches rely on **Packet-switching**. The switch establishes a connection between two segments just long enough to send the current packet. Incoming packets (part of an **Ethernet frame**) are saved to a temporary memory area (**buffer**); the MAC address contained in the frame's header is read and then compared to a list of addresses maintained in the switch's **lookup table**. In an Ethernet-Based LAN, an Ethernet frame contains a

normal packet as the payload of the frame, with a special header that includes the MAC address information for the source and destination of the packet.

Packet-Based switches use one of three methods for routing traffic:

- **Cut-through switching:** Cut-through switches read the MAC address as soon as a packet is detected by the switch. After storing the six bytes that make up the address information, they immediately begin sending the packet to the destination node, even as the rest of the packet is coming into the switch. Cut-through switches with collision fragments detection will store the frame in the buffer and begin transmission as soon as the possibility of collision is eliminated and it can grab the outgoing channel. No Cyclic Redundancy Check (CRC) verification is done in these switches.
- **Store-and-forward switching:** A switch using **store and forward** will save the entire packet to the buffer and check it for CRC errors or other problems before sending. If the packet has an error, it is discarded. Otherwise, the switch looks up the MAC address and sends the packet on to the destination node. Many switches combine the two methods, using cut-through until a certain error level is reached and then changing over to store and forward. Very few switches are strictly cut-through, since this provides no error correction.
- **Fragment-Free:** A less common method is **fragment-free**. It works like cut-through except that it stores the first 64 bytes of the packet before sending it on. The reason for this is that most errors, and all collisions, occur during the initial 64 bytes of a packet.



Switches avoid collisions by buffering frames instead of trying to send multiple frames out the same twisted pair at the same time.

8.4.2.3 LAN Switch Physical Structure

The **switch function** is to transfer the data unit from a switch's incoming port to the appropriate outgoing port. A high level view of generic switch architecture is shown in Figure 8.14. Four components of a switch can be identified:

- **Input ports:** The input port performs several functions. It performs the physical layer functionality of terminating an incoming physical link to a switch. It performs the data link layer functionality needed to interoperate with the data link layer functionality.
- **Output ports:** An output port stores the data units that have been forwarded to it through the switching mechanism, and then transmits the data units on the outgoing link. The output port thus performs the reverse data link and physical layer functionality as the input port.
- **Switching controller (processor):** It executes the switching mechanism, maintains the switching tables, and performs network management functions, within the switch.

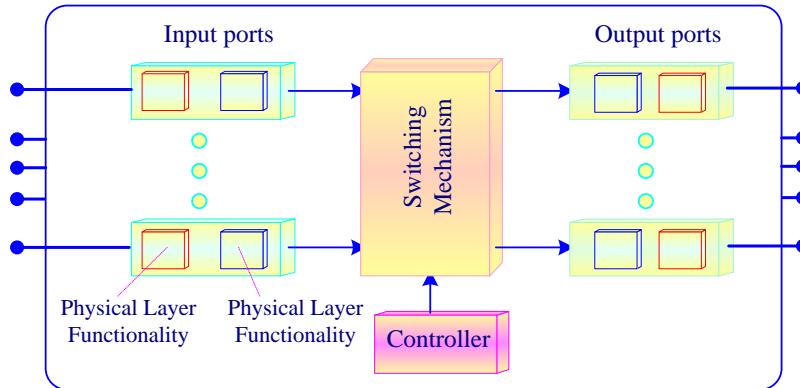


Figure 8.14: A high level view of generic switch architecture

- **Switching mechanism:** The switching mechanism connects the switch's input ports to its output ports. This switching mechanism is completely contained within the switch.

- **Matrix** (A crossbar switch): This type of switch has an internal grid with the input ports and the output ports crossing each other. When a packet is detected on an input port, the MAC address is compared to the lookup table to find the appropriate output port. The switch then makes a connection on the grid where these two ports intersect. A data unit arriving at an input port buffer travels along the horizontal bar attached to the input port until it intersects with the vertical bar leading to the desired output port. If the vertical bar leading to the output port is free, the packet is transferred to the output port. If the vertical bar is being used to transfer a data unit from another input port to this same output port, the arriving packet is blocked and must be queued at the input port. Figure 8.15 shows two types of cross bar switches.

Figure 8.15 (A) illustrates a full availability 8-port switch configuration. The full availability switch matrix of Figure 8.15(A) allows all eight of the stations to be simultaneously communicating: Port 1 with port 5; port 2 with port 8; port 3 with port 4, and port 6, port 7.

In the configuration in figure 8.15 (A), the maximum throughput of the network has been multiplied to $4 \times 10 \text{ Mbit/s} = 40 \text{ Mbit/s}$, reflecting the four simultaneous paths which may be established across the backplane of the switch. Figure 8.15(B) shows a limited availability switch matrix. In a limited availability (or partial mesh) matrix, not all of the ports can communicate at once, since insufficient paths are available.

- **Shared-memory architecture:** Stores all incoming packets in a common memory-buffer shared by all the switch **ports** (input/output connections), then sends them out via the correct port for the destination node. An input port with an arriving data unit (frame) first signaled the controller. The data unit is then copied from the input port buffer into controller memory. The controller then extracted the destination address from the header,

looked up the appropriate output port in the switch table, and copied the data unit to the output port's buffers.

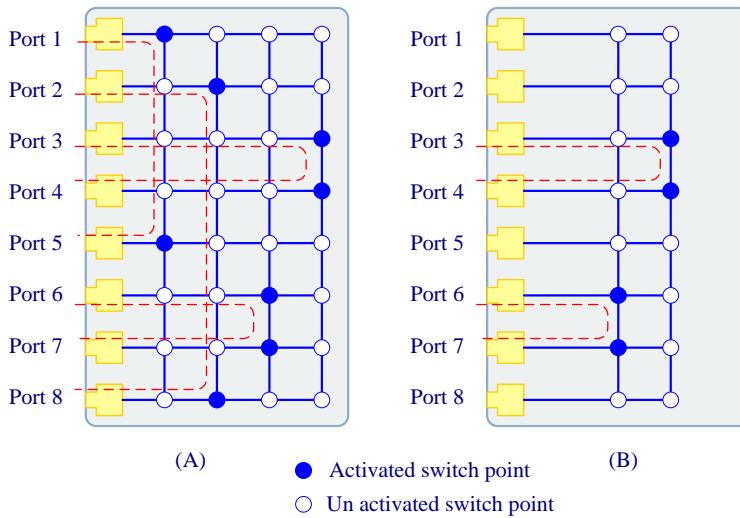


Figure 8.15: (A) Full availability (full-mesh) and (B) limited availability (partial mesh) switches.

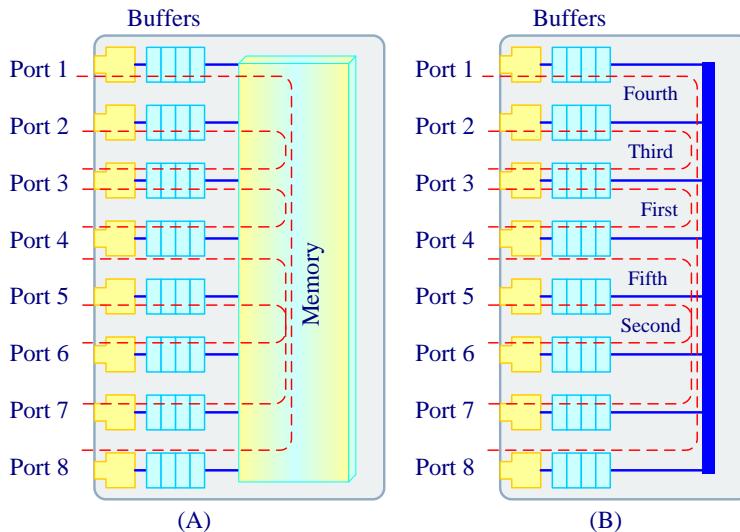


Figure 8.16: (A) Shared-memory architecture and (B) Bus-architecture.

- **Bus-architecture:** Instead of a grid, an internal transmission path (**common bus**) is shared by all of the ports using TDMA. A switch based on this configuration has a dedicated memory-buffer for each port, as well as an ASIC to control the internal bus access. A data unit arriving at an input port and finding the bus busy with the transfer of another data unit is blocked from passing through the switching fabric and queued at the input port buffer. Because every data unit must cross the single bus, the

switching bandwidth of the switch is limited to the bus speed. Given that bus bandwidths of over a gigabit per second are possible in today's technology, switching via a bus is often sufficient for switches that operate in access and enterprise networks (e.g., local area and corporate networks).

8.4.2.4 Switches Features

There are a variety of features that distinguish them, like the following:

- **Flow Control:** Flow control is necessary when the destination port is receiving more traffic than it can store and handle. Switches come with various flow control strategies depending on the vendors. Some switches upon finding that the destination port is overloaded will send jam message to the sender. This strategy works as only those frames that go to the overloaded destination port are jammed and not the others.
- **Full Duplex:** There is no contention between stations to transmit over a medium, and a station can transmit whenever a frame is queued in the adapter. The station can also receive at the same time.
- **Multiple LAN Technologies:** Switches can support ports having single LAN technology or a multiple of them namely, Ethernet, 100Base-T, FDDI, token ring, ATM and 100VGAnyLAN.
- **Network Management:** This is an important feature, as it allows the network administrator to detect a problem even before it occurs. Monitoring is mainly through Simple Network Management Protocol (SNMP) or Remote Monitoring (RMON) while diagnostics are mostly proprietary.



The switch floods frames sent to the broadcast address and unknown unicast addresses;

8.5 Extending LAN Using Network Layer Devices

8.5.1 Routers

8.5.1.1 General Description

As the complexity of the network system grows, layer 2 devices are not adequate to meet the needs of networks. Routers, known as layer 3 switches, implement the switching and forwarding functions at the network layer of the protocol stack.

Routers are conceptually similar to bridge, except that they are found in the **Network** layer of the OSI as shown in Figure 8.16. They can read the network addresses of packets and can make decisions on where to send the data according to Routing Tables.

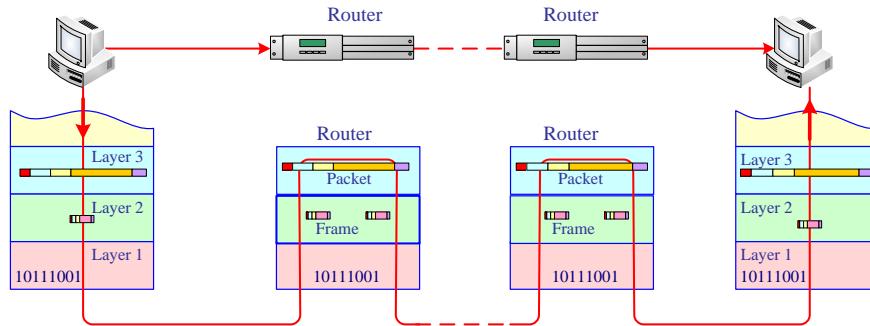


Figure 8.16: Router in ISO Network Layer

Figure 8.17 shows a typical network scenario in a large organization. The network is split up into subnets, each having a number of desktop systems connected to a layer 2 switch. Router acts as the backbone and connects layer 2 switches through higher-speed links. Servers are connected to either the layer 2 or the router.

You can configure a network with several routers that can work cooperatively together. For example, some routers are able to monitor the network to determine the most efficient path for sending a message to its ultimate destination. If a part of the network is extremely busy, a router can automatically route messages along a less-busy route.

Let's look at what a very simple router might do. Imagine a small company that makes animated 3-D graphics for local television stations. There are 10 employees of the company, each with their own computer. Four of the employees are animators, while the rest are in sales, accounting and management. The animators will need to send lots of very large files back and forth to one another as they work on projects. To do this, they'll use a network.

When one animator sends a file to another, the very large file will use up most of the network's capacity, making the network run very slowly for other users. One of the reasons that a single intensive user can affect the entire network stems from the way that Ethernet works. Each information packet sent from a computer is seen by all the other computers on the local network. Each computer then examines the packet and decides whether it was meant for their address. This keeps the basic plan of the network simple, but has performance consequences as the size of the network, or level of network activity increases. To keep the animators' work from interfering with that of the folks in the front office, the company sets up two separate networks, one for the animators and one for the rest of the company. A router links the two networks and connects both networks to the Internet.

8.5.1.2 Router Physical Structure

The simplest, earliest routers were often traditional computers, with switching between input and output port being done under direct control of the CPU. Input and output ports functioned as traditional I/O devices in a traditional operating system. An input port with an arriving datagram first signaled the CPU via an interrupt. The packet was then copied from the input port into processor memory. The routing processor then

extracted the destination address from the header, looked up the appropriate output port in the routing table, and copied the packet to the output port's buffers.

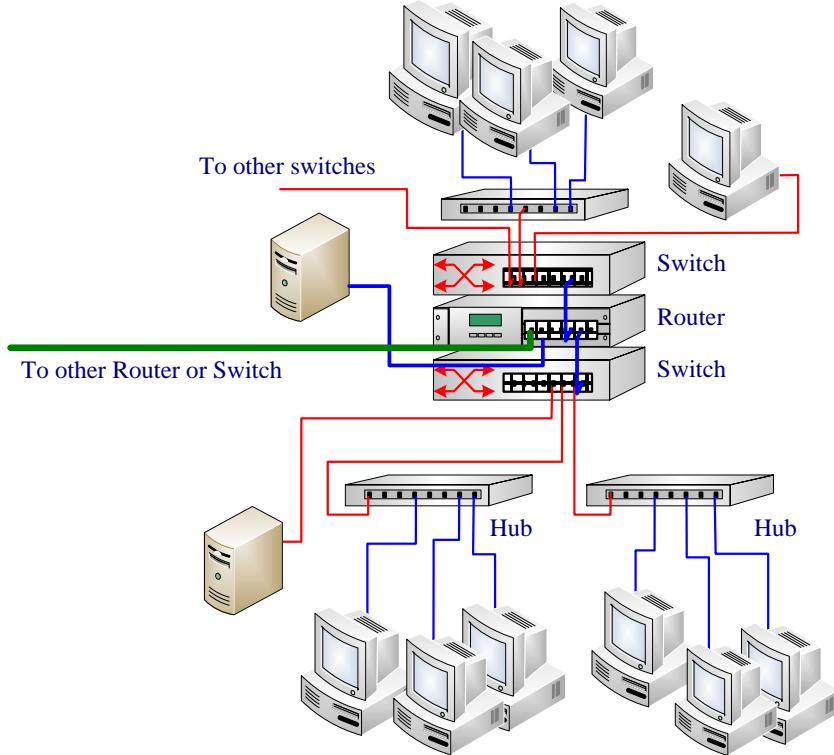


Figure 8.17: Typical network router connection in a large organization.

The architecture of a generic modern router is shown in Figure 8.18 and is comprised of the following major components:

- **Buffers:** These are first-in first-out (FIFO) buffers for storing messages in transit. The buffer size is an integral number of flow control units. Buffers may be associated with each input physical channel and each output physical channel, or may be associated only with inputs (input buffering) or outputs (output buffering).
- **Switch:** This component is responsible for connecting router input buffers to router output buffers. Routers can contain any type of switching mechanisms illustrated previously in the switch physical design. High-speed routers will utilize crossbar networks with full availability, while lower-speed implementations may utilize networks that do not provide full connectivity between input buffers and output buffers.
- **Routing and arbitration unit:** This component implements the routing algorithms, selects the output link for an incoming message, and accordingly sets the switch. If multiple messages simultaneously request the same output link, this component must provide for arbitration between them. If the requested link is busy, the incoming message remains in the input buffer. It will be routed again after the link is freed and if it successfully arbitrates for the link.

- Link controllers (LCs): The flow of messages across the physical channel between adjacent routers is implemented by the link controller. The link controllers on either side of a channel coordinate to transfer units of flow control.
- Processor interface: This component simply implements a physical channel interface to the processor rather than to an adjacent router. It consists of one or more injection channels to the processor and one or more ejection channels from the processor. Ejection channels are also referred to as delivery channels or consumption channels.

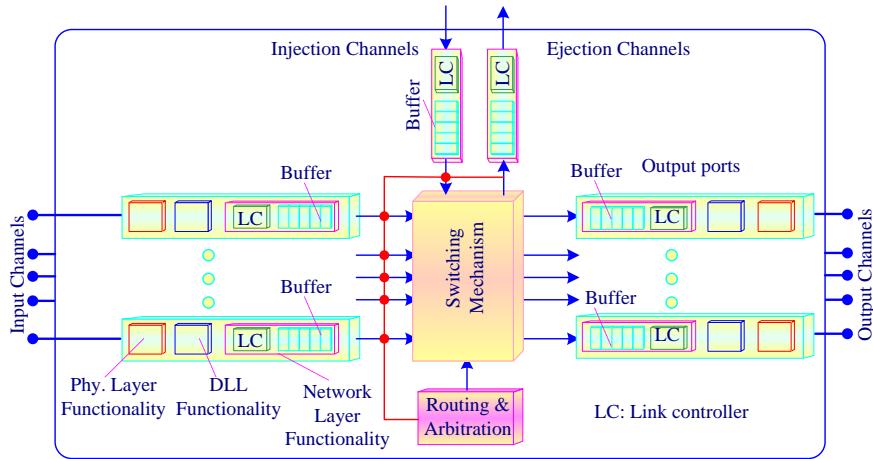


Figure 8.18: Generic modern router architecture

The router is the only device that sees every message sent by any computer on either of the company's networks. When an animator sends a huge file to another animator, the router looks at the recipient's address and keeps the traffic on the animator's network. When an animator, on the other hand, sends a message to the bookkeeper asking about an expense-account check, then the router sees the recipient's address and forwards the message between the two networks.

8.5.1.3 Router Characteristics and Functions

A router is a device that directs (routes) data from one path to another in a network. Routers base their switching information on one or more information parameters contained within the packet of data they receive. These parameters may include the destination address, availability of a transmission path or communications channel, maximum allowable amount of transmission delay a packet can accept, along with other key parameters.

When a router is initially installed into a network, it begins its life by requesting a data network address. Using this data network address, it sends (broadcasts) messages to nearby routers and begins to store address connections of routers that are located around it. Routers regularly exchange their connection information (lists of devices it is connected to) with nearby routers to help them keep the latest packet routing information.

A router can make decisions on where to forward packets dependent on a variety of factors including the maximum transmission distance or packet priority. Distance vector

routing and link state routing allow the router to select paths that match the needs of the data that is being sent through it.

Some routers may use fixed (static) routing tables that are manually programmed by the network administrator instead of dynamically created routing tables. The use of static routing tables may seem to be inflexible, however the use of static routing ensures other router's that may have corrupt routing tables are not able to change or influence the routing table.

In general a table is a collection of information, including:

- Information on which connections lead to particular groups of addresses
- Priorities for connections to be used
- Rules for handling both routine and special cases of traffic

A routing table can be as simple as a half-dozen lines in the smallest routers, but can grow to massive size and complexity in the very large routers that handle the bulk of Internet messages.

A router, then, has two separate but related jobs.

1. The router ensures that information doesn't go where it's not needed: This is crucial for keeping large volumes of data from clogging the connections of "innocent bystanders."
2. The router makes sure that information does make it to the intended destination

In performing these two jobs, a router is extremely useful in dealing with two separate computer networks. It joins the two networks, passing information from one to the other and, in some cases, performing translations of various **protocols** between the two networks. It also protects the networks from one another, preventing the traffic on one from unnecessarily spilling over to the other. As the number of networks attached to one another grows, the routing table for handling traffic among them grows, and the processing power of the router is increased. Regardless of how many networks are attached, though, the basic operation and function of the router remains the same. Since the Internet is one huge network made up of tens of thousands of smaller networks, its use of routers is an absolute necessity.

Routers can support multiple protocols (TCP/IP, AppleTalk, IPX/SPX) and they also have certain protocols defined for them. The most primitive type of router has a Static routing table that is maintained manually. In this table the network admin must enter network addresses and the corresponding destination address (i.e. for the network 129.12.13.0 send packets to 129.12.13.1) also they have a default address to which they sent the unknown packets in the hope that that router has an appropriate destination. Such methods are very cumbersome.

The more intelligent routers of today use RIP (Routing Information Protocol) in which they broadcast their own routing tables and also listen for other routers' table information and use it to dynamically build up their own routing table. Another protocol becoming popular today is OSPF (Open Shortest Path First) in which routers maintain statistical information about various routes selected in the past and can "grade" the overall quality of a certain path and use that information when making subsequent routing decisions. OSPF promises to be a very effective routing protocol. Because routers have their own network address and operating system, they can often be remotely managed.

Routers also can have multiple interface types and can connect various network types (i.e.: Ethernet, Token Ring, ATM, ISDN etc). This is possible due to the fact that routers actually strip off and recreate Data link layer information for the packets to adapt them to the new environment.

When a message first arrives at a router, it must be examined to determine the output channel over which the message is to be forwarded. This is referred to as the routing delay and typically includes the time to set the switch. Once a path has been established through a router by the switch, we are interested in the rate at which messages can be forwarded through the switch. This rate is determined by the propagation delay through the switch (interrouter delay) and the signaling rate for synchronizing the transfer of data between the input and output buffers. These delays along with contention by messages for links, determine the network throughput.

8.5.1.4 Routing Compared to LAN Switching

Switches usually work at **Layer 2 (Data or Datalink)** of the OSI Reference Model, using MAC addresses, while routers work at **Layer 3 (Network)** with Layer 3 addresses (IP, IPX or Appletalk depending on what Layer 3 protocols are being used).

The algorithm that switches use to decide how to forward packets is different from the algorithms used by routers to forward packets. One of these differences in the algorithms between switches and routers is how **broadcasts** are handled. A hub or a switch will pass along any broadcast packets they receive to all the other segments in the broadcast domain; but a router will not. Without the specific address of another device, it will not let the data packet through. This is a good thing for keeping networks separate from each other, but not so good when you want to talk between different parts of the same network. This is where switches come in.

8.5.2 Brouters

Brouters are a hybrid between a router and a bridge. It is any network device having the capabilities of both a bridge and a router. Usually, it will act as a router for one protocol (for example, TCP/IP) and a bridge for all other protocols (for example, IPX/SPX). They can route packets of a routable protocol and bridge packets of a non-routable protocol.

Brouters are not common in networks. Network services often send their announcements over every protocol on the network, which generates additional traffic and makes it generally disadvantageous to run more than one protocol on a single network. The solution adopted by most implementers today is to use a single protocol for all network communication on the main portion of the network, they use the **Network** layer for the router part and the **Data Link** Layer for the bridge part as it is illustrated in Figure 8.19.

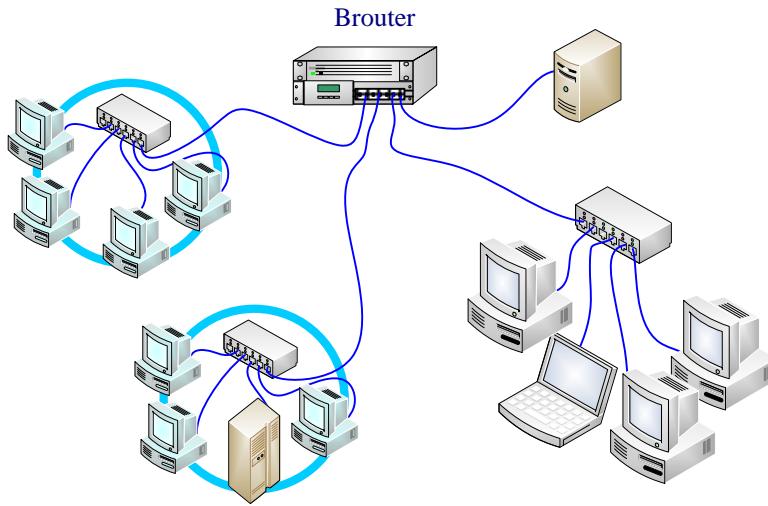


Figure 8.19: Brouter Network

8.6 Extending LAN Using Gateways

Gateway is a term used to describe a broad category of network components that allow communication between different networking architectures, different environments and different protocols. They repackage and convert data going from one environment to another so that each environment can understand the other environment's data. A gateway repackages information to match the requirements of the destination system. Gateways can change the format of a message so that it conforms to the application program at the receiving end of the transfer.

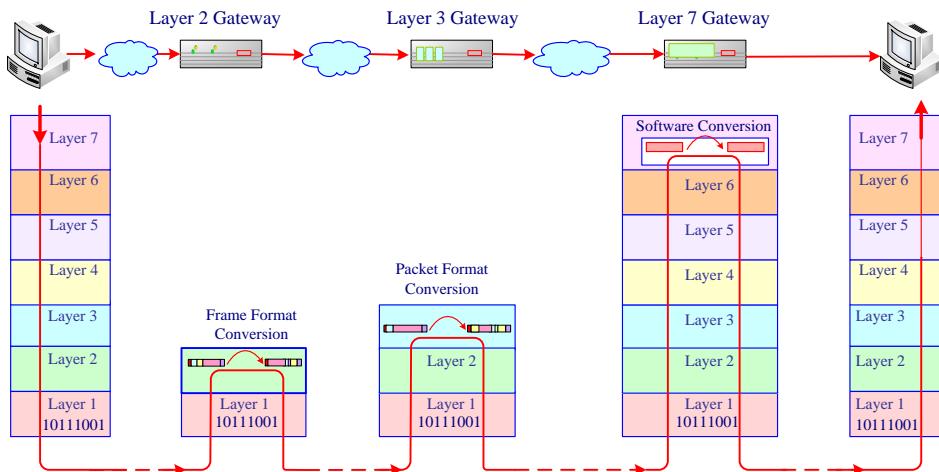


Figure 8.20: Gateway in ISO Application Layer

A gateway is usually a dedicated device or a set of services running on a dedicated computer. Some examples of gateways as it is shown in Figure 8.20 include a router that

translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself.

In General gateways link two systems that do not use the same:

- Communication protocols.
- Data-formatting structures.
- Languages.
- Architecture.

So they are task-specific, which means that they are dedicated to a particular type of transfer. They are often referred to by their task name (Windows NT Server to SNA gateway).

A gateway takes the data from one environment, strips off its old protocol stack, and repackages it in the protocol stack from the destination network.

To process the data, the gateway:

- Disassembles incoming data through the network's complete protocol stack.
- Encapsulates the outgoing data in the complete protocol stack of the other network to allow transmission.

The primary use for gateways today is for handling e-mail. POP3 and SMTP are two examples of such mail-handling protocols that are handled by gateways. Most e-mail systems that can connect to disparate systems either use a computer set up as a gateway for that chore, or let the e-mail server handle the gateway chores itself.

Gateways interconnect heterogeneous networks; for example, they can connect Microsoft Windows NT Server to IBM's Systems Network Architecture (SNA). Gateways change the format of the data to make it conform to the application program at the receiving end.

8.7 Other Techniques to Extend LANs

8.7.1 Virtual LAN (VLAN)

8.7.1.1 General Description

A VLAN is a networking technology that allows networks to be segmented logically, that is group users by logical addresses into a virtual, rather than a physical. Basically, a VLAN is a collection of nodes that are grouped together in a single broadcast domain, it supports network managers can define workgroups independent of underlying network topology. Users can physically move but stay on the same VLAN.

The LAN switches or bridges can support many virtual LANs which operate as subnets. Users within a virtual LAN are grouped either by their address or by port address, with each node attached to the switch via a dedicated circuit. Users also can be assigned to more than one virtual LAN, should their responsibilities cross workgroup domains.

VLAN's allow a network manager to logically segment a LAN into different broadcast domains. Since this is a logical segmentation and not a physical one,

workstations do not have to be physically located together. Users on different floors of the same building, or even in different buildings can now belong to the same LAN.

VLAN's also allow broadcast domains to be defined without using routers. Bridging or switching software is used instead to define which workstations are to be included in the broadcast domain. Routers would only have to be used to communicate between two VLAN's

VLAN Frame Format

The frame type used in VLAN is the latest iteration of the 802.3 frame, which is specified in the 802.3ac standard. This frame type adds a 4-byte field (VLAN tag) for the 802.1q VLAN standard, increasing the maximum frame size from 1,518 bytes to 1,522 bytes (see Figure 8.21).

When frames are sent across the network, there needs to be a way of indicating to which VLAN the frame belongs, so that the bridge will forward the frames only to those ports that belong to that VLAN, instead of to all output ports as would normally have been done. This information is added to the frame in the form of a tag header. Frames in which a tag header has been added are called tagged frames. Tagged frames convey the VLAN information across the network. Tag header:

- Allows user priority information to be specified,
- Allows source routing control information to be specified, and
- Indicates the format of MAC addresses.



VLAN tag: This is only used on 802.3 frames that are handled by 802.1q VLAN-enabled network switches (multiport bridges). The tag is used to identify a packet with a specific VLAN. When the packet leaves the switch, the tag is removed.

There are two formats of the tag header:

1. Ethernet Frame Tag Header: It consists of
 - a. tag protocol identifier (TPID) , which indicates that a tag header is following
 - b. tag control information (TCI) contains
 - i. the user priority, it is a 3-bit field, which allows priority information to be encoded in the frame. Eight levels of priority are allowed, where zero is the lowest priority and seven is the highest priority.
 - ii. the canonical format indicator (CFI) The CFI bit is used to indicate that all MAC addresses present in the MAC data field are in canonical format.
 - iii. the VLAN ID. The VID field is used to uniquely identify the VLAN to which the frame belongs. There can be a maximum of $(2^{12} - 1)$ VLAN's. Zero is used to indicate no VLAN ID, but that user priority information is present.
 2. Token Ring and (FDDI) tag header: It consists of

- iv. subnetwork access protocol encoded (SNAP-encoded) TPID and TCI.
- v. tag control information (TCI) contains (the same as in Ethernet tagged frame)

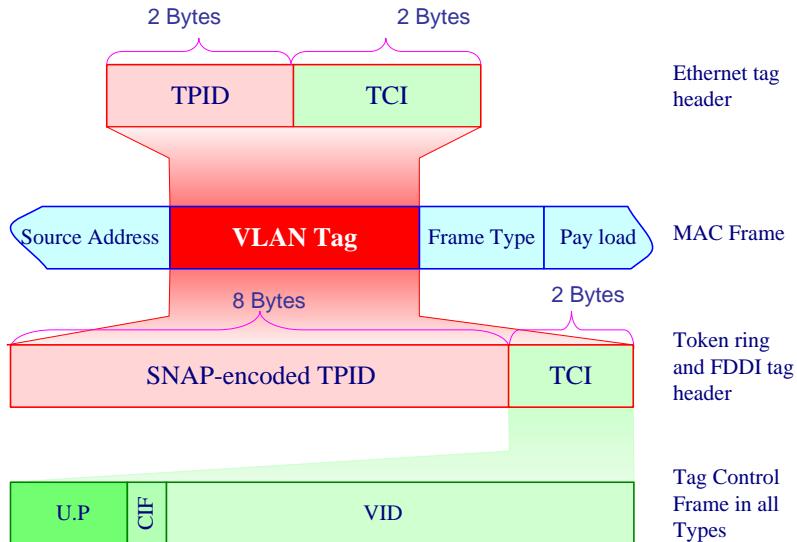


Figure 8.21: VLAN Frame format

Using a switch as the main concentrator makes for a more efficient network because the network can be partitioned into several smaller collision domains. However, broadcasts sent by any host are still received by all hosts on the network, even if all of the hosts do not need to receive them.

To overcome these problems, many switches support virtual LAN (VLAN) technologies. Using VLAN switches, the network administrator can create virtual network segments whose logical topology is independent of the physical topology of the wiring. Each station can be assigned a VLAN identification number (ID), and stations with the same VLAN ID (no matter what physical switch they are connected to) can act and function as though they are all on the same physical network segment. Broadcasts sent by one host are received only by hosts with the same VLAN ID. The assignment of VLAN IDs is done at the port level on the switches themselves and can be managed remotely using network management software. Moving a host to another department only requires the assignment of a different VLAN ID to the port on the switch to which the host is connected—no rewiring of patch cables is needed. A switch that you have implemented VLANs on has multiple broadcast domains, similar to a router. But you still need a router to route from one VLAN to another see Figure 8.22; the switch can't do this by itself.

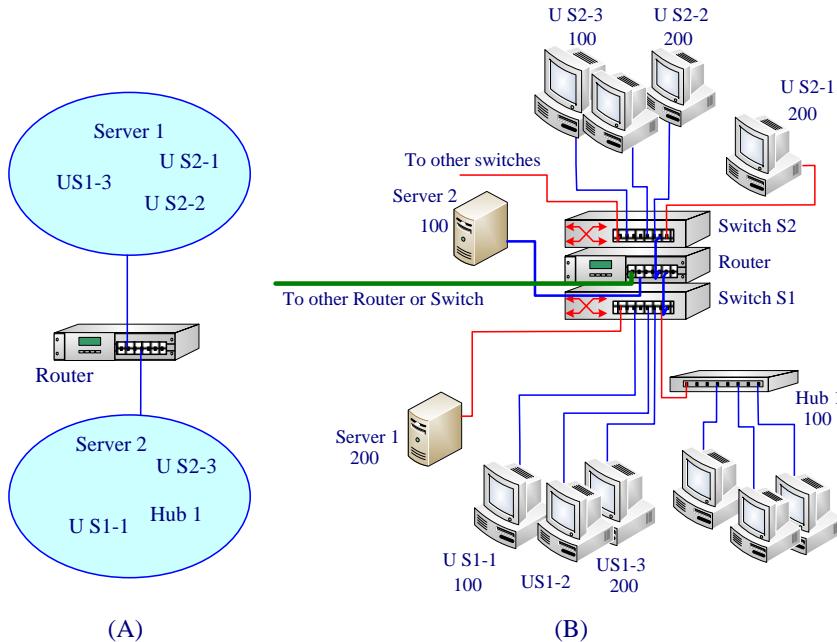


Figure: 8. 22: Virtual LAN (A) Physical View (B) Virtual (Logical) View

8.7.1.3 VLAN Advantages

The main advantages of using VLAN technologies are that:

- **Performance/Bandwidth:** In networks where traffic consists of a high percentage of broadcasts and multicasts, VLAN's can reduce the need to send such traffic to unnecessary destinations.
- Since VLAN's create broadcast domains using switches instead of routers, careful monitoring of network use allows the network administrator to create VLANs that reduce the number of router hops and increase the apparent bandwidth for network users.
- **Formation of Virtual Workgroups:** Companies may want VLANs set up for departments that are heavy network users (such as Multimedia or Engineering), or a VLAN across departments that is dedicated to specific types of employees (such as managers or sales people).
- **Managing a project** or working with a specialized application can be simplified by the use of a VLAN that brings all of the required nodes together. Without VLAN's, the only way this would be possible is to physically move all the members of the workgroup closer together.
- **Simplified Administration:** Seventy percent of network costs are a result of adds, moves, and changes of users in the network. Some of these tasks can be simplified with the use of VLAN's. If a user is moved within a VLAN, reconfiguration of routers is unnecessary. In addition, depending on the type of VLAN, other administrative work can be reduced or eliminated.

- An attractive feature of VLANs is that it is possible to change the logical topology without moving any wires or changing any addresses.
- **Reduced Cost:** VLAN's can be used to create broadcast domains, which eliminate the need for expensive routers. In addition it is more efficient and cost-effective to provide better security, uninterrupted power supply, consolidated backup, and a proper operating environment in a single area than if the major resources were scattered in a building.
- **Security:** Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data. Separating systems with sensitive data from the rest of the network decreases the chance that someone will gain access to information they are not authorized to see. VLAN's can also be used to control broadcast domains, set up firewalls, restrict access, and inform the network manager of an intrusion
- **Broadcasts/Traffic flow** – Since a principle element of a VLAN is the fact that it does not pass broadcast traffic to nodes that are not part of the VLAN, it automatically reduces broadcasts. **Access lists** provide the network administrator with a way to control who sees what network traffic. An access list is a table the network administrator creates that lists what addresses have access to that network.
- **Departments/Specific job types** - Companies may want VLANs set up for departments that are heavy network users (such as Multimedia or Engineering), or a VLAN across departments that is dedicated to specific types of employees (such as managers or sales people).

8.7.1.4 VLAN Trunking

Trunk links are point-to-point, 100Mbps, or 1000Mbps links between two switches, between a switch and a router, or between a switch and a server. Trunk links carry the traffic of multiple VLANs, from 1 to 1005 at a time. You cannot run trunk links on 10Mbps links.

A trunk is a port that supports multiple VLANs, but before it became a trunk, it was the member of a single VLAN. The VLAN it is a member of when it becomes a trunk is called a native VLAN. If the port were to lose the trunking ability, it would revert to membership in its native VLAN.

VLANs can span across multiple switches and you can have more than one VLAN on each switch. For multiple VLANs on multiple switches to be able to communicate via a single link between the switches, you must use a process called **trunking**; trunking is the technology that allows information from multiple VLANs to be carried over just one link between switches.

The **VLAN Trunking Protocol (VTP)** is the protocol that switches use to communicate among themselves about VLAN configuration.

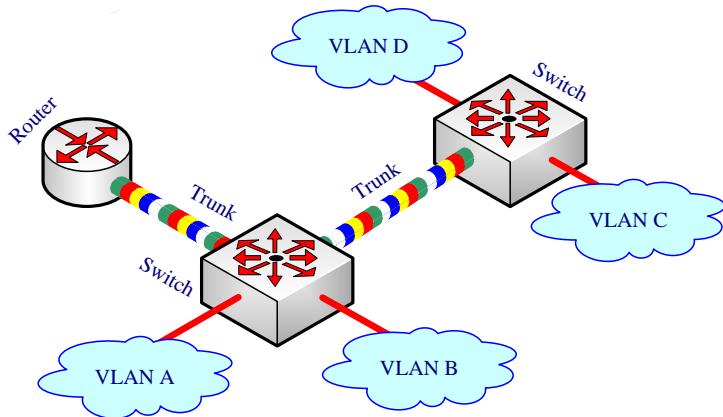


Figure 8.23: Virtual LAN Trunking

In the Figure 8.23 above, each switch has two VLANs. On the first switch, VLAN A and VLAN B are sent through a single port (trunked) to the router and through another port to the second switch. VLAN C and VLAN D are trunked from the second switch to the first switch and through the first switch to the router. This trunk can carry traffic from all four VLANs. The trunk link from the first switch to the router can also carry all four VLANs. In fact, this one connection to the router allows the router to appear on all four VLANs, as if it had four, different, physical ports connected to the switch.

The VLANs can communicate with each other via the trunking connection between the two switches using the router. For example, data from a computer on VLAN A that needs to get to a computer on VLAN B (or VLAN C or VLAN D) must travel from the switch to the router and back again to the switch. Because of the transparent bridging algorithm and trunking, both PCs and the router think that they are on the same physical segment!

8.7.2 Extending LAN Wirelessly

8.7.2.1 Wireless Access Points

An access point (AP) is a radio access transceiver (transmitter and receiver) that is used to enable wireless data devices (stations), such as laptop computers or PDAs, to communicate with a wired communication network. Access points convert and control the sending of data packets and can connect one or many wireless devices to a wired LAN (see Figure 8.24). This is typically an extension of your LAN, with the wireless connectivity adding to the already well-established wired connections.

APs come in all different shapes and sizes. Many are cheaper and designed strictly for home or small office use. Higher end APs used for commercial purposes enable extending the range that the wireless signal can travel. AP today can provide different services. Some AP might provide many ports that can be used to easily increase the size of the network. Many real-world applications exist where a single access point services from 15-50 stations. Access points hand the station off from one to another in a way that is invisible to the station, ensuring unbroken connectivity. Other APs provide firewall capabilities and dynamically allocate IP addresses to client machines using the

Dynamic Host Configuration Protocol, and then prevent Internet traffic from accessing client systems.

To solve particular problems of topology, the network designer might choose to use Extension Points (wireless repeater) to augment the network of access points as it is shown in Figure 8.24. Extension Points look and function like access points, but they are not tethered to the wired network as are APs. EPs function just as their name implies: they extend the range of the network by relaying signals from a client to an AP or another EP. EPs may be strung together in order to pass along messaging from an AP to far-flung clients. EP has become a recognized tool to help service providers expand coverage and fill in coverage in null areas without the expense of full Base station sites.

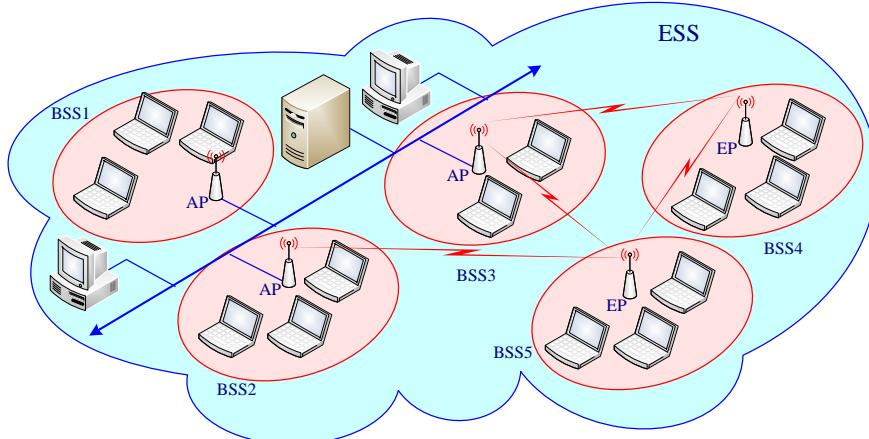


Figure 8.24: Illustration of AP, EP, BSS and ESS

APs are used to create a wireless LAN and to extend a wired network.
APs are used in the infrastructure wireless topology.

A collection of stations associated to a particular access point constitute a basic service set (BSS). When stations are participating in this BSS, they share certain common network parameters. For example, they all transmit and receive on the same channel, and they use a common basic service set identifier (BSSID).

The collection of BSSs connected to a single wired network forms an extended service set (ESS) (Figure 8.24). An ESS also has an identifier, the ESSID that is unique to that ESS but shared by the entire component BSSs. The ESS architecture provides a framework in which to deal with the problem of mobile stations roaming from one BSS to another in the same ESS. It would obviously be nice if a mobile station could be carried from the coverage area of one access point (i.e., one BSS) to that of another without having to go through a laborious process of reauthenticating, or worse, obtaining a new Internet protocol (IP) address; ideally, data transfers could continue seamlessly as the user moved.



AP can operate as a bridge connecting a standard wired network to wireless devices or as a router passing data transmissions from one access point to another.

8.7.2.2 wireless Bridge:

In essence, a wireless bridge provides connectivity between two wired LAN segments allowing buildings to connect wirelessly when wiring is too expensive or a second redundant connection is needed as a backup for a wired connection.

A wireless bridge is a half-duplex device, it is basically the same as a regular bridge but is equipped with a wireless transceiver; it offers an easy way to link LANs without using cable as shown in Figure 8.25. With variations that depend on atmospheric and geographic conditions, this distance can be up to 4.8 kilometers.

The translation wireless bridge can be with a longer range and provides both Ethernet and Token Ring bridging for a distance of up to 40 kilometers. A wireless bridge capable of Layer 2 wireless connectivity only.

Wireless bridges are generally at each end of a point-to-point link, such as those that interconnect two buildings. A bridge has a wired port that connects to the network and a wireless port that interfaces with a transceiver.

You can configure the wireless bridge as either point-to-point (P2P) or point-to-multipoint (P2MP). Point-to-point mode (also called master/slave or LAN-to-LAN) connects two LAN segments by using two bridge units. Point-to-multipoint mode lets you construct a network that has multiple bridges talking to each other wirelessly.

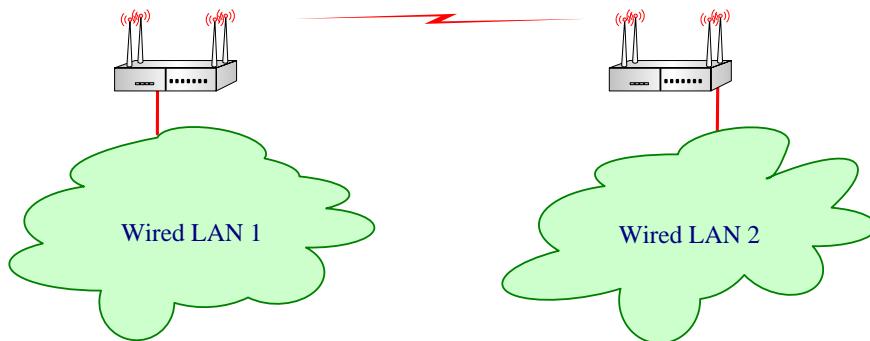


Figure 8.25: Wireless Bridge links LANs without using cable

When you have more than one bridge, one bridge must act as the root bridge. A root bridge can communicate only with non-root bridges and other data devices but cannot associate with another root bridge. Figure 8.22 shows a root bridge communicating with non-root bridges.



Some manufacturers give you the option to connect clients to bridges, which is actually the same as giving the bridge access point functionality. In some cases, the bridge has an access point mode that converts the bridge into an access point exclusively.

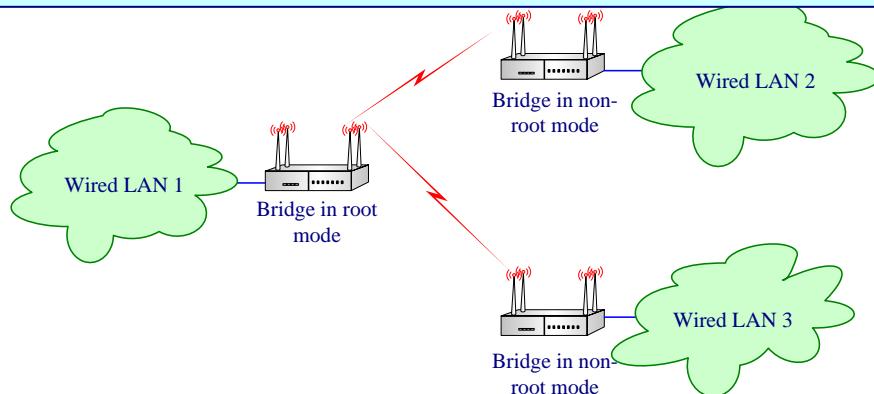


Figure 8.26: Root and non-root modes of wireless bridges

Bridges in non-root mode associate wirelessly with bridges in root mode (see Figure 8.26). Some wireless bridges support client connectivity to non-root mode bridges while the bridge is in access point mode. This mode is actually a special mode in which the bridge is acting as an access point and a bridge simultaneously. Client devices associate to access points (or bridges in access point mode), and bridges talk to other bridges. Some vendors call this offering a Wireless Distribution System (WDS). WDS is a bridging mode in which the access point can simultaneously bridge to another access point and act as an access point to clients. When using the Spanning Tree Protocol, all non-root bridges must have connectivity to the root bridge.

Wireless bridge can be used to repeat the signals in order to extend the length of the wireless bridged segment. In repeater configuration, you place a bridge between two other bridges. Repeater bridges are non-root bridges, and many times the wired port is disabled while the bridge is in repeater mode. Figure 8.27 shows a bridge in repeater mode.

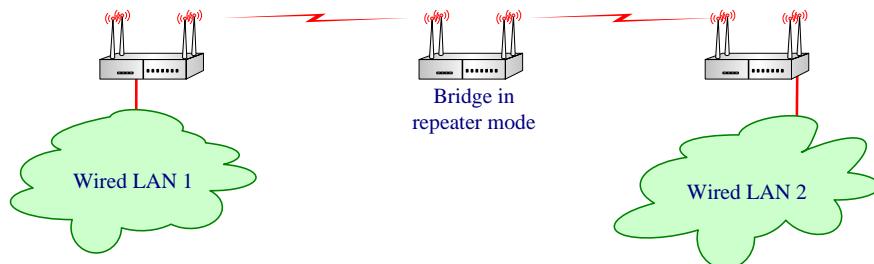


Figure 8.27: Repeater mode of wireless bridges



You can define wireless bridges as repeaters. In repeater configuration, you place a bridge between two other bridges for the purpose of extending the length of the wireless bridged segment. Repeater bridges are non-root bridges.

8.7.2.3 Wireless Switches

Wireless switches, or controllers, are not commonly used by home or small-office users. Rather, they would simply set up a small network by wirelessly connecting to an AP or broadband wireless router, which access the Internet by means of a DSL, cable or other types of modems.

Large wireless networks have numerous access points (AP) spread throughout a building or campus. The traditional model utilizes autonomous APs (fat clients) as independent devices working in conjunction with backend servers to authenticate network computers and users. This type of environment is acceptable but can become expensive and difficult to manage.

Wireless switches, or controllers, are used to reduce the total cost of administering wireless networks. Switches serve as the central nervous system for a group of access points often referred to as "thin clients." Switches can also control autonomous APs. The end result is cost savings through proactive network management and lower hardware expenses, especially if APs are deployed.

8.7.2.4 Wireless Router

A wireless router is a router configured for establishing a communication link between the mobile network and an attachment router of a wide area network, such as the Internet, providing connectivity for the mobile network to the wide area network. The wireless router thus serves as a gateway to route packets between the mobile network and the Internet.

A wireless router integrates a wireless access point with an IP router and an Ethernet switch. The integrated switch connects the integrated access point and the integrated Ethernet router internally, and allows for external wired Ethernet LAN devices to be connected as well as a (usually) single WAN device such as cable modem or DSL modem. A wireless router advantageously allows all three devices to be configured through one central configuration utility, usually through an integrated web server.

Mobile wireless routers eliminate the need for a host to be aware of mobility. The proximity of the routers permits the network to operate reliably at low power and at high data rates. Each wireless router can communicate with other nodes, i.e. other wireless routers in any direction. The wireless routers generally comprise three components, namely a TCP/IP protocol suite support, a wireless operating system that optimizes the wireless network performance and robustness, and a high-performance digital RF modem.



Most vendors that provide access points also manufacture products that act as routers and gateways. These products generally combine the functions of both the wireless access points and low-end cable/DSL routers. The wireless routers provide DHCP and NAT firewall features for the wireless clients.

8.7.3 Extending LANs over longer distances (Optical fiber Converter)

Using repeaters or bridges can extend a LAN within one building but these solutions are impractical between buildings. Optical fiber converter converts electrical signals into the corresponding light signals for Optical fibers cable. Fiber modems can be inserted into a thin wire or twisted pair Ethernet LAN either on a single machine connection or between a bridge and a second LAN segment in another building.

Due to the characteristics of optical fiber this link can be very long with little or no signal attenuation, no voltage to be lost in passing through copper.



Satellite links can be made to connect extremely far-flung parts of a LAN without requiring that wire be strung across someone else's property. Slow links such as satellites require bridges to buffer several frames since frames arrive faster than they can be sent.

8.9 Quick Review

- ❖ Connectivity devices that used to expand the size and range of a computer network are organized according to the layer at which they are connected in networks.
- ❖ Repeaters Amplifiers and hubs are physical layer devices that primarily extend the geographic distance spanned by a LAN protocol. A hub supports more ports than a repeater does and can be passive active or intelligent. Amplifiers are used in Broadband technology for analog signals while repeaters are used in Baseband technology for digital signals.
- ❖ A bridges and switches are data communication device. Bridge connects two or more segments of data communication networks by forwarding packets between them. Bridges can detect errors, do frame filtering and provide partial separation of a LAN into two or more collision domains.
- ❖ Switches are multi-input, multi-output device that allow different nodes or subnets to communicate directly with one another in a smooth and efficient manner. Unlike hub switch allows a device connected to it have the full bandwidth all to itself and allow a network to maintain full-duplex Ethernet.
- ❖ Routers are conceptually similar to bridge, except that they use IP address instead of MAC addresses and found in the Network layer. Routers link LANs and

connect them to the Internet and direct data from one path to another based on routing tables, and a variety routing algorithms. Routers also can have multiple interface types and can connect various network types (i.e. Ethernet, Token Ring, ATM, ISDN etc).

- ❖ Gateway repackages and converts data going from one environment to another so that each environment can understand the other environment's data.
- ❖ VLANs are becoming popular because of the flexibility they offer. With VLAN support network managers can define workgroups independent of underlying network topology. VLAN's allow a network manager to logically segment a LAN into different broadcast domains.
- ❖ An access point (AP) is a radio access transceiver (transmitter and receiver) that is used to enable wireless data devices to communicate with through a wired communication network. A collection of stations associated to a particular access point constitute a basic service set (BSS). The collection of BSSs connected to a single wired network forms an extended service set (ESS)
- ❖ A wireless bridge is the same as a regular bridge but is equipped with a wireless transceiver. When you have more than one bridge, one bridge must act as the root bridge. Bridges in non-root mode associate wirelessly with bridges in root mode. Wireless bridge can be used to repeat the signals in order to extend the length of the wireless bridged segment.
- ❖ Wireless switches, or controllers, are used to reduce the total cost of administering wireless networks. Switches serve as the central nervous system for a group of access points often referred to as "thin clients." Switches can also control autonomous APs.
- ❖ A wireless router is a router configured for establishing a communication link between the mobile network and an attachment router of a wide area network. A wireless router integrates a wireless access point with an IP router and an Ethernet switch.
- ❖ Optical fiber link can extend LANs to a very long distance with little or no signal attenuation.

8.10 Self Test Questions

A- Answer the following questions

1. Why do we extend LANs?
2. How do amplifiers, repeaters and hubs differ from each other?
3. What are the basic types of hubs and how do they differ from each other?
4. What are the basic types of bridges and how do they differ from each other?
5. Why are bridges considered to be adaptive or learning devices?
6. How does the cycles of bridges problem arise, and how can it be solved?
7. What are the differences between switches and bridges?
8. What are the differences between switches and hubs?
9. What is the role of switching address table?
10. What are the three methods used by packet-based switches for routing traffic?
11. Explain the structure of the switch.
12. List some features of the switch.

13. What are the differences between switches and routers?
14. What are the differences between bridges and routers?
15. Explain the physical structure of the router.
16. What are the differences between static and dynamic routing tables?
17. Where is the gateway applicable?
18. How does Virtual LAN differ from physical one?
19. What is the importance of the tagged frame?
20. Explain the structure of the tagged header.
21. List the main advantages of using VLANs.
22. What is the role of AP in WLANs?
23. What are the main configurations of the wireless bridges?
24. Where is the wireless switch applicable?
25. What is the role of the wireless router?
26. What is the role of the Optical fiber converter?

B- Identify the choice that best completes the statement or answers the question.

1. You must _____ to connect two Ethernet hubs together.
 - a. Purchase a special crossover cable
 - b. Connect the uplink ports on the two hubs together
 - c. Connect any standard port on one hub to a standard port on the other
 - d. Connect the uplink port in one hub to a standard port on the other
2. The bridge works at _____ layer of the OSI reference model.
 - a. Physical
 - b. Network
 - c. Data-link
 - d. Transport
3. When a bridge receives a packet that is destined for a system on the same network segment from which the packet arrived, it _____.
 - a. Discards it
 - b. Broadcasts it
 - c. Relays it
 - d. Unicasts it
4. Two network segments connected by a bridge share a _____ domain?
 - a. Collision
 - b. Source route
 - c. Broadcast
 - d. Unicast
5. _____ technique is used to prevent bridge loops.
 - a. Transparent bridging
 - b. Translation bridging
 - c. Packet filtering
 - d. The STA
6. _____ does not have buffers to store data during processing.
 - a. A repeating hub
 - b. A cut-through switch
 - c. A local bridge
 - d. All of the above
7. _____ is the term for a group of LANs in one building connected by routers?
 - a. A WAN
 - b. A collision domain
 - c. A broadcast domain
 - d. An internetwork
8. _____ is the device you most likely to use to connect a LAN to the Internet.

- b. Star

d. None of the above

20. When you add nodes to a collision domain:
a. More collisions may appear
c. The network performance is improved
b. The network bandwidth is increased
d. Nothing

21. ____ is a type of hub should you use when planning to have a high number of connections.
a. Standalone
b. Hubby
c. Stackable
d. Hublet

22. ____ is a connectivity device can extend an Ethernet network without further extending a collision domain, or segment.
a. Hub
b. Bridge
c. Repeater
d. Router

23. ____ is a kind of connectivity device that can be used to separate each single host on your network into its own collision domain.
a. Switch
b. Repeater
c. Hub
d. NIC

24. ____ is a kind of connectivity device can be used to ease traffic congestion in LAN workgroups.
a. Stackable hub
b. Hublet
c. Repeater
d. Switch

25. What connectivity device is appropriate for applications that transfer a large amount of traffic and are sensitive to time delays?
a. NIC
b. Router
c. Switch
d. Access point

26. Cut-through switches are recommended
a. When connecting a small workgroup where speed is not important
c. When connecting a large workgroup where speed is important
b. When connecting a large workgroup
d. When connecting a small workgroup where speed is important

27. Store and forward switches are appropriate
a. When connecting small networks where speed is important
c. When connecting large networks where data integrity is important
b. When connecting large networks where speed is important
d. When connecting small networks where data integrity is not important

28. To allow visitors access to minimal network functions—an Internet connection—without allowing the possibility of access to the company's data stored on servers you must
a. use a switch to create a VLAN
c. use a router to create a VLAN
b. use a smarthub to create a VLAN

- d. use repeaters instead of switches
29. One of the following is a disadvantage in creating VLANs.
- a. You can include nodes on groups
 - c. You can exclude nodes from groups
 - b. Nodes on a VLAN can listen to traffic from other VLANs
 - d. Nodes on a VLAN cannot listen to traffic from other VLANs
30. The important aspect to consider when troubleshooting a VLAN is
- a. That devices are using the right drivers
 - c. That the appropriate router is used to create it
 - b. VLAN configuration
 - d. None of the above
31. One of the following problems may be present in a network that uses static routing.
- a. Router's tables are always changing to reflect network changes
 - c. Router's tables may be invalid after a change in the network structure
 - b. Static routing is more insecure
 - d. They accept unroutable packets
32. One of the following problems may be present in a network that uses dynamic routing.
- a. It is not commonly used by other networks
 - c. They do not account for changes in the network
 - b. The tables contain fixed paths
 - d. In very unstable environments, router's tables can never reach a stable state
33. ____ is a kind of gateway you can use to allow dissimilar networks to communicate with each other.
- a. LAN gateway
 - b. Internet gateway
 - c. IBM gateway
 - d. E-mail gateway
34. ____ is a kind of gateway that can be used to connect a data network with a voice network.
- a. Application gateway
 - b. Phone gateway
 - c. Internet gateway
 - d. Voice/data gateway
35. ____ is a kind of problem is when a router is not properly connected to the backbone.
- a. Application layer problem
 - c. Network layer problem
 - b. Logical connectivity problem
 - d. Physical connectivity problem
36. ____ is a LAN switch method runs a CRC on every frame.
- a. Cut-through
 - b. Fragment-check
 - c. Store-and-forward
 - d. Fragment-free
37. ____ is a LAN switch type checks only the hardware address before forwarding a frame.
- a. Cut-through
 - b. Fragment-check
 - c. Store-and-forward
 - d. Fragment-free

38. One of the following is true about VLAN.
- It must be added and configured by the administrator.
 - It is automatically added by the switch, and the administrator cannot delete it.
 - It is automatically added by the switch, but the administrator can delete it.
 - It is optional on every switch.
39. One of the following describes a local VLAN.
- Local VLANs are configured on a switch by geographic location.
 - Local VLANs are configured by a VTP server.
 - End-to-end VLANs are configured by geographic location.
 - End-to-end VLANs are VLANs that span the switch fabric from end-to-end, and all switches understand about all configured VLANs.
40. One of the following describes an end-to-end VLAN.
- Local VLANs are configured by geographic location.
 - Local VLANs are configured by a VTP server.
 - End-to-end VLANs are configured by geographic location.
 - End-to-end VLANs are VLANs that span multiple switches.
41. Two network segments connected by a bridge share a _____ domain.
- | | |
|-----------------|--------------|
| a. Collision | c. Broadcast |
| b. Source route | d. Unicast |
42. The device that can segment a local area network into separate pieces and still operate efficiently during periods of high traffic is called a _____
- | | |
|------------|-------------|
| a. hub. | c. bridge. |
| b. switch. | d. gateway. |
43. Each node In a WAN is a _____ that accepts an input packet, examines the destination address of the packet, and forwards the packet onto a particular communications line.
- | | |
|-----------|------------|
| a. bridge | c. switch |
| b. router | d. station |
44. A _____ is a device required to move traffic between VLANs.
- | | |
|-----------|-----------------|
| a. Switch | c. Bridge |
| b. Router | d. VLAN-Gateway |
45. _____ is used in wireless LANs with an access point.
- | | |
|--------------|--------------------|
| a. CSMA/CA | c. polling |
| b. switching | d. demand priority |
46. The most common wireless NICs speed choices today are 11 Mbps or _____ Mbps.
- | | |
|-------|--------|
| a. 22 | c. 54 |
| b. 50 | d. 100 |
47. What is the IEEE standard standard for wireless networking for many different broadcast frequencies and techniques?
- | | |
|-----------|-----------|
| a. 802.3d | c. 802.15 |
| b. 802.11 | d. 802.16 |

48. Wireless networks typically use the ____ topology with communications directed by one or more access points, in the context of one or more offices within an organization,
- a. token ring
 - b. ESS
 - c. IBSS
 - d. star-bus
49. ____ is an area with public wireless access, which is simply a location that provides a public access point to users.
- a. hotspot
 - b. cell
 - c. nexus
 - d. hub
50. ____ technology is used for short distance wireless communications within an office, a building, or between buildings.
- a. infrared
 - b. microwave
 - c. ultraviolet
 - d. gamma ray
51. WiMAX is another name for the IEEE 802.16 standard for wireless ____.
- a. WANs
 - b. LANs
 - c. MANs
 - d. DANs
52. What is the wireless LAN, where user devices communicate with the nearest access point and may move from one cell to another?
- a. single-cell
 - b. multiple-cell
 - c. peer-to-peer
 - d. star-wired
53. What is the wireless LAN, where there is no access point at the center of a cell and each user device communicates to the other user devices.
- a. single-cell
 - b. multiple-cell
 - c. peer-to-peer
 - d. star-wired
54. What is the wireless LAN, where all user devices communicate with one access point, competing for the same set of frequencies?
- a. single-cell
 - b. multiple-cell
 - c. peer-to-peer
 - d. star-wired
55. ____ is another name for the 802.11b standard.
- a. HiperLAN/2.
 - b. Wi-Fi.
 - c. FDDI.
 - d. Hi-Fi.
56. In a wireless CSMA/CD, the user device waits for a small period of time called the ____ if it wishes to transmit, when the medium is idle.
- a. waiting period.
 - b. idle space.
 - c. interframe space.
 - d. medium wait period.
57. In a WLAN, ____ communicates with the wireless user device.
- a. interface card
 - b. access point
 - c. modem
 - d. controller
58. A wireless access point most likely functions as a ____.
- a. hub
 - b. switch
 - c. bridge
 - d. router

59. What is the IEEE standard that covers wireless technologies?

- a. 802.11
- b. 802.12
- c. 802.13
- d. 802.14

CHAPTER 9

WAN INTERNETWORKING TECHNOLOGY

9.1 About This Chapter

As we know WAN is a data communications network that covers a relatively broad geographic area. With WANs, you can't just run a cable, even if the WAN link is a mile long. In short, to build WANs, you must lease a physical network from someone who can run a cable between the buildings that you want to connect. So WAN often uses transmission facilities provided by common carriers, such as telephone companies. Different types of communication lines such as leased lines (dedicated connections), packet data systems, or fiber transmission lines can interconnect these networks. WANs may be interconnected to and/or through the public switched telephone network (PSTN) or public packet data networks (such as the Internet). WiMAX also provides a wireless alternative to cable and DSL for WAN access.

The network administrator should consider several advanced WAN environments that are becoming more popular as their technology matures. These include Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN), Fiber Distributed Data Interface (FDDI), and Synchronous Optical Network (SONET). In addition telephone companies have developed elaborate schemes for multiplexing many conversations over a single physical trunk.

Because WAN links, such as wide-area telephone connections, are too expensive and complex for most private companies to purchase, implement, and maintain on their own, they are usually leased from service providers.

WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

The vast majority of existing WAN connections work like what is described in this chapter. Here we will introduce the various transmission technologies used in wide-area network (WAN) environments.

9.2 Learning Outcome

After this chapter, you should be able to:

1. Understand the different types of WAN connections.
2. Become familiar with different types of WAN transmission technologies.
3. Become familiar with multiplexing aspects.
4. Understand the general aspects of carrier systems.
5. Describe how to create DSL by using part of your local phone line
6. Distinguish between the various xDSL types.
7. Explain the basic concepts of sending data over the multiplexing channel.
8. Describe the principles behind moving data quickly and economically across long distances.

9. Become familiar with Broadband Wireless Access Technology (BWA) aspects.
 10. Identify the primary features of each of the following: ATM, ISDN, FDDI, SONET, SDH and Broadband Wireless Access Technology (BWA).

9.3 Multiplexing

Multiplexing is the combining or interleaving of several data streams together to form one composite signal. This may also be done by allotting time segments to stations sharing the same circuit. Cost is the major benefit of using a multiplexer, since much redundant hardware is eliminated. Instead of each terminal having a direct link to its destination, there is one link shared by several terminals.

Multiplexing requires two multiplexers, one at each end of the circuit, since data sent must be demultiplexed. Another method is to have one multiplexer (MUX) and a communications processor that is capable of demultiplexing (DEMUX) the signal. Figure 9.1 shows multiplexing and demultiplexing link.

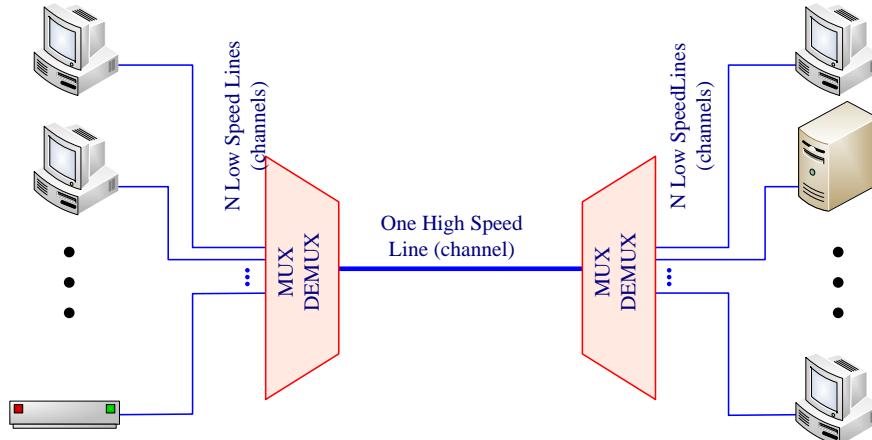


Figure 9.1: Multiplexing and Demultiplexing Interface

Multiplexers utilize the total bandwidth available on a communication circuit. They work by dividing the bandwidth into multiple frequency channels or time slots. This allows groups of terminals to communicate with a central computer over the same line. This is another source of cost savings as monthly fees for lines can be very expensive.

The fundamental purpose of the multiplexer is to interface many low speed devices into a single line that provides a high-speed channel to a host computer or central processor. Telephone companies use multiplexers to cope with their large traffic requirements. There are several types of multiplexers and they also often combine multiplexing with other functions such as porting, framing, and carrier interfacing.

Devices are connected to multiplexers via connections known as ports. Multiplexers are typically microprocessor controlled and configurable to perform various combinations of multiplexing. Multiplexers hold input from attached devices in memory buffers for periods of time in the microseconds, until they can be transmitted. On the receiving end the multiplexer separates the incoming data and routes it appropriately. Each port may be

configured to match parameters of terminals and transmission medium. Most multiplexers can be configured to support both synchronous and asynchronous terminals.

There are several different multiplexing methods which we will discuss in the following sections.



Multiplexing in networking, is the technique of combining separate communication channels from different sources into a single channel for transmission over a wide area network (WAN) link.

9.3.1 Frequency-Division Multiplexing (FDM)

Frequency division multiplexing is one of the original multiplexing techniques used in the data communications industry. FDM is an analog device and is mostly used in broadband local area networks where more than one channel is required. An FDM will divide the total available input and output bandwidths into the same number of channels on the circuit, depending on the number of ports and devices supported. The total bandwidth of input terminals or devices connected to the multiplexer cannot exceed the bandwidth of the output channel. Figure 9.2 shows Frequency-Division multiplexing for three multiple channels.

If a device that is attached to a FDM is removed from the circuit, turned off, no reallocation of the available frequency that was used by the device is made to enable the other devices that are still attached to take advantage of this bandwidth. What this means is that the multiplexer does not have the ability to dynamically reallocate its capabilities to make use of the available bandwidth. FDMs have built in digital to analog converters so they do not need modems attached to manage this conversion.

Each channel in the total bandwidth separated from the other channels by frequency bands called guard bands. These bands, or sub-channels, are intended to prevent the data channels from interfering with one another. This is necessary to prevent possible crosstalk (noise) and interference, though it reduces the amount of data that can be transmitted. The amount of frequency assigned to a channel depends upon the speed of the channel. Higher speed is required greater bandwidth. FDM is normally used for digitized voice applications.

Phone companies who wish to maximize their usage of a limited amount of cable may also utilize FDM. The phone companies typically allow about 4 MHz of bandwidth for calls after filtering.

Broadband networks use technology similar to that of cable TV companies in placing several channels of data on a cable at once. Broadband systems use the different frequencies to separate directional traffic and provide special services. Both analog devices and digital devices can use a broadband network, but only analog signals are carried on the wire.

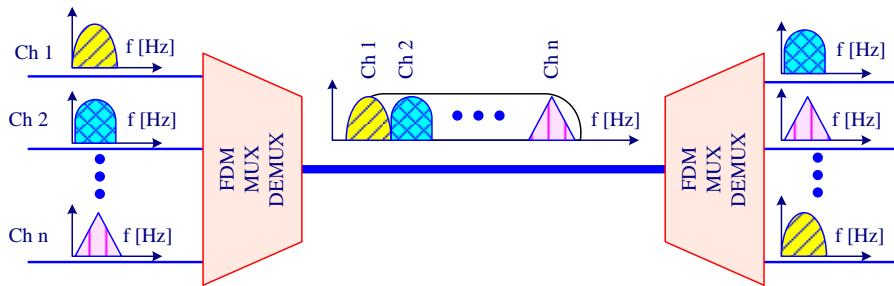


Figure 9.2: Frequency-Division Multiplexing



FDM is the simplest and oldest form of multiplexing in wireless networking technology. It can be used in both wired and wireless networking for transmitting large amounts of data at high speeds.

9.3.2 Time-Division Multiplexing (TDM)

Time division multiplexing is more efficient than frequency division multiplexing. TDMs are digital devices that combine several digital signals from computers or terminals into a single composite digital signal output.

TDMs work by allocating time slots to each terminal of device attached to a port. Typically, the total bit rate for all devices cannot exceed the output line bit per second rate. One way around this is by using data compression techniques. A binary algorithm in the multiplexer is used to reduce the total number of bits by some factor. The compression is reversed on the receiving end. If a port is inactive the time slot is not used, that is it is not available for use by other devices connected to the multiplexer. A more efficient version of TDM is Statistical Time Division Multiplexers or STDM. STDM make use of channels that are not busy by allocating their time slots to other devices that can use them.

Like frequency division multiplexers, some FDMs can support both synchronous and asynchronous modes. TDMs may or may not incorporate modems depending upon the design.

TDM is used both in networking and phone systems. It is a process whereby several slower speed signals are divided up and placed on a high-speed transmission channel. A multiplexer actually selects which source data will be sent at what amount and places that chunk of data on the wire. It then selects a different source, takes a portion of its data, and places it on the wire next. In this manner several "samplings" from several sources can be interleaved on the high-speed communications channel. This can be accomplished because the individual sources are sending their data at a relatively slow speed (i.e. 300 baud), while the outgoing channel has significant speed to accommodate a sampling from each source (i.e. 1200 baud). When the data reaches its destination, another multiplexer disassembles the combination data and places each chunk of data on an appropriate channel to its destination, once again at the slower speed at which it entered the original MUX. Figure 9.3 illustrates the concept of time-division multiplexing.

This same technology is used by phone service providers who must grapple with the task of getting a large number of conversations over limited numbers of wires contained in trunks. If the conversations are broken up and put back together fast enough, no one notices it. For this reason, high speed trunks use time-division multiplexing to carry several conversations at once - and no one is the wiser.

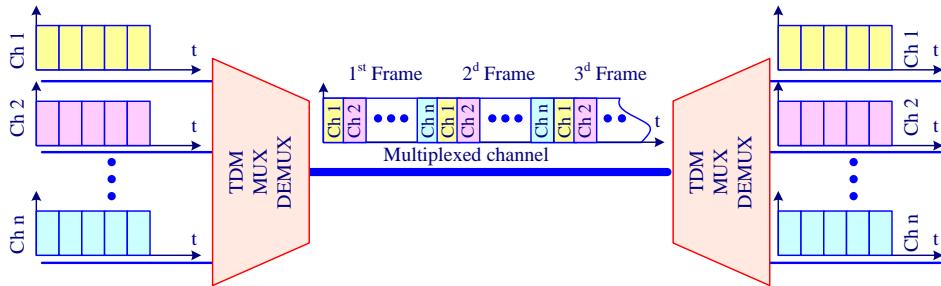


Figure 9.3: Concept of Time-Division Multiplexing

Sampling a conversation of data from several sources may take place on the bit, byte or block level. When only a bit from each source is placed on the wire, we call it "bit interleaving". When a byte is sampled and then placed on a wire with other sampled bytes from other sources, we call it "word interleaving". Figure 9.4 illustrates Basic Bit-Interleaved TDM; meanwhile, Figure 9.5 illustrates "word interleaving" TDM.

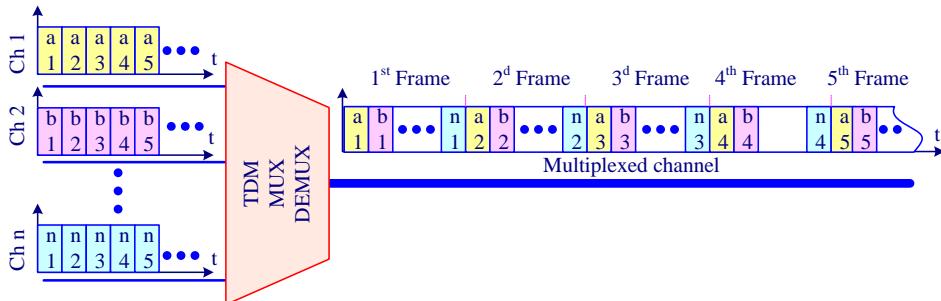


Figure 9.4: Basic Bit-Interleaved TDM

MUXs, at both ends of a high-speed link, must synchronize with one another so that the time required for each sampling matches. Otherwise, the demultiplexer would not be able to determine which source signal goes with what destination channel. Timing is obviously an extremely important element to a time-based methodology like TDM.

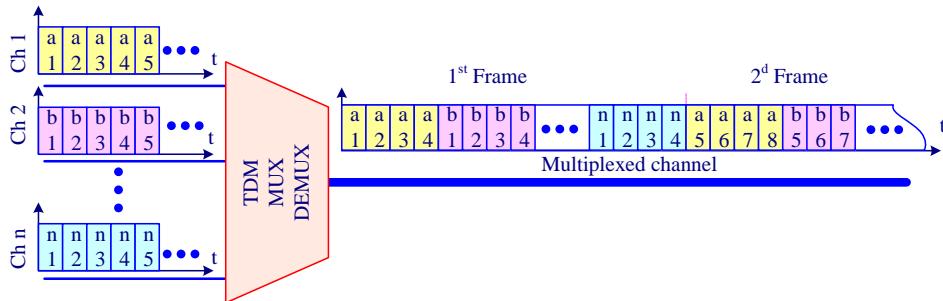


Figure 9.5: "word interleaving" TDM

TDM can be used on Baseband networks. If we recall, Baseband networks only carry digital data. Digital data is susceptible to attenuation and interferences. Fortunately, digital data can be used with repeaters that actually regenerate the digital signal and rebroadcast it at a higher level.

Since the various input channels are not all synchronized, we need some means of aligning this data in time, one method called pulse stuffing, is to use a link data rate which is higher than the sum of the incoming channels and framing data rate and increase the incoming channel rates by inserting dummy bits before input to the TDM and removing them after demultiplexing.

9.3.2.1 TDM Link Control

The transmitted data stream does not contain the headers and trailers that have come to associate with synchronous transmission. The reason is that the control mechanisms provided by a data link protocol are not needed. The data rate on the multiplexed line is fixed, and the multiplexer and demultiplexer are designed to operate at that rate. One refinement is needed. Both ends of the line need to be a combination multiplexer/demultiplexer with a full-duplex line in between. Then each channel consists of two sets of slots, one traveling in each direction. The individual devices attached at each end can, in pairs, use HDLC to control their own channel.

9.3.2.2 Framing

A link protocol is not needed to manage the overall TDM link. There is, however, a basic requirement for framing. The flag or SYNC characters to bracket TDM frames are not provided; some means is needed to assure frame synchronization. It is clearly important to maintain framing synchronization because, if the source and destination are out of step, data on all channels are lost. The most common mechanism for framing is known as added-digit framing. One control bit is added to each TDM frame. An identifiable pattern of bits, from frame to frame is used on this "control channel". To synchronize, a receiver compares the incoming bits of one frame to the expected pattern. If the pattern does not match, successive bit positions are searched until the pattern persists over multiple frames.

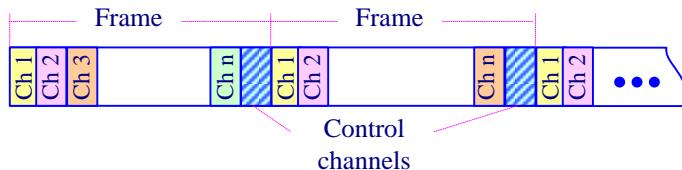


Figure 9.6: Multiplexed frame structure

Once framing synchronization is established, the receiver continues to monitor the framing bit channel. If the pattern breaks down, the receiver must again enter a framing search mode.

9.3.2.3 Pulse Stuffing

The most difficult problem in the design of a synchronous time-division multiplexer is that of synchronizing the various data sources. If each source has a separate clock, any variation among clock could cause loss of synchronization. In some cases, the data rates of the input data streams are not related by a simple rational number. For these problem, a technique known as pulse stuffing is an effective remedy. With this, the outgoing data rate of the multiplexer, excluding framing bits, is higher than the sum of the maximum instantaneous incoming rates. The extra capacity is used by stuffing extra dummy bits or pulses into each incoming signal until its rate is raised to that of a locally generated clock signal. The stuffed pulses are inserted at fixed locations in the demultiplexer frame format so that they may be identified and removed at the demultiplexer.



In TDM, the data from different input channels is combined in round-robin fashion into a single output data stream. If an input channel does not have anything important to carry for a time, empty segments are inserted into the output stream anyway.

9.3.3 Statistical TDM (STDM)

Statistical Time Division Multiplexing uses intelligent devices capable of identifying when a terminal is idle. They allocate time only to lines when required. This means that more lines can be connected to a transmission medium as this device statistically compensates for normal idle time in data communication lines. Newer STDM units provide additional capabilities such as data compression, line priority, mixed speed lines, host port sharing, network port control, automatic speed detection and much more.

As with a TDM, the statistical multiplexer has a number of I/O lines on one side and a higher-speed multiplexed line on the other. Each I/O line has a buffer associated with it. In the case of statistical multiplexer, there are n I/O input lines, but only k , where $k < n$, time slots available on the TDM frame. For input, the function of the multiplexer is to scan the input buffers, collecting data until a frame is filled, and then send the frame. On output, the multiplexer receives a frame and distributes the slots of data to the appropriate output buffers. As a result, there are more overheads per slot for statistical TDM as each slot carries an address as well as data.

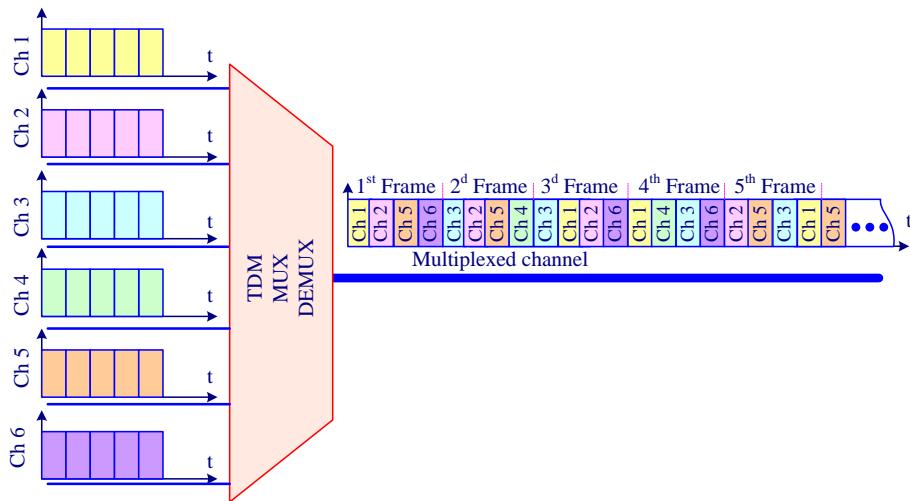


Figure 9.7: STDM with 6 I/O input lines, but only 4

Because statistical TDM takes advantage of the fact that the attached devices are not all transmitting all of the time, the data rate on the multiplexed line is less than the sum of the data rates of the attached devices. Thus, a statistical multiplexer can use a lower data rate to support as many devices as a synchronous multiplexer. Alternatively, if a statistical multiplexer and a synchronous multiplexer both use a link of the same data rate, the statistical multiplexer can support more devices.

The frame structure used by a statistical multiplexer has an impact on performance. It is desirable to minimize overhead bits to improve throughput. A statistical TDM will use a synchronous protocol such as HDLC. With this, the data frame must contain control bits for the multiplexing operation. A way to improve efficiency is to allow multiple data sources to be packaged in a single frame. Now, however, some means is needed to specify the length of data for each source. Thus, the statistical TDM subframe consists of a sequence of data fields, each labeled with an address and a length. Several techniques can be used to make this approach more efficient. Using relative addressing can reduce the address field. That is, each address specifies the number of the current source relative to the previous source, modulo the total number of source.

Another refinement is to use a two-bit label with the length field. A value of 00, 01, or 10 corresponds to a data field of one, two or three bytes; no length field is necessary. Value of 11 indicates that length fields are included.

9.3.3.1 STDM Performance

Data rate of the output of the statistical multiplexer is less than the sum of the data rates of the inputs. This is allowable because it is anticipated that the average amount of input is less than the capacity of the multiplexed line. The difficulty with this approach is that, while the average aggregate input may be less than the multiplexed line capacity, there may be peak periods when the input exceeds capacity.

The solution to this problem is to include a buffer in the multiplexer to hold temporary excess input. There is a trade-off between the size of the buffer used and the

data rate of the line. The use of the smallest possible data rate, but reduction in one requires an increase in the other. The trade-off is really one between system response time and the speed of the multiplexed line.



Wavelength Division Multiplexers (WDMs), allow multiple high speed channels to be supported over a single Optical fiber transmission system. This is accomplished through the transmission of multiple wave lengths of light.

9.4 Carrier Systems

The history of carrier systems really begins in the early years of the 20th century and progress in all areas has been rapid. Carrier modes of transmission increase the efficiency of utilization of transmission medium by multiplexing a large number transmission lines into a single line. A carrier system transit multiple channels of information by processing and converting them to a form suitable for the transmission medium used. Many information channels can be carried by one broadband carrier system. Broadband carrier systems are classified as either analog carrier systems or digital carrier systems.

9.4.1 Analog Carrier Systems

The long distance carrier system provided throughout the world is designed to transmit voice band signals over high capacity transmission links, such as coaxial cable and microwave systems.

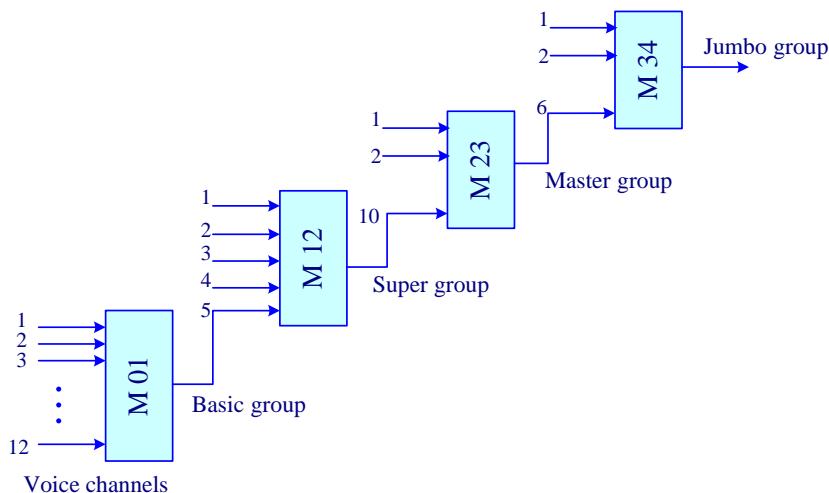


Figure 9.8: FDM standard system

Analog carrier systems can carry speech, data, video and supervisory signals, although they are best suited for speech signals. Analog carrier systems operating over coaxial cable and radio systems and are rapidly being replaced by digital facilities.

Figure 9.8 explain the principles of multiplexing voice channel using different level multiplexers. Each multiplexer uses several group channel of previous multiplexers to form a new higher multiplexed group.

L- Carrier system services as an example of FDM, it consists of four basic levels, three with an associated multiplexer function as shown in Figure 9.9.

In the L-Carrier system, a basic 4 KHz voice channel (0 - 4 KHz frequency range) is applied first to a channel modulator. The channel modulator would multiplex each of 12 channels with 12 different carrier frequencies in the range of 64 - 108 KHz as illustrated in Figure 9.9. The Lower Sideband (LSB) is used. The resulting aggregate multiplexed signal occupies a frequency range of 60 - 108 KHz (48 KHz of bandwidth).

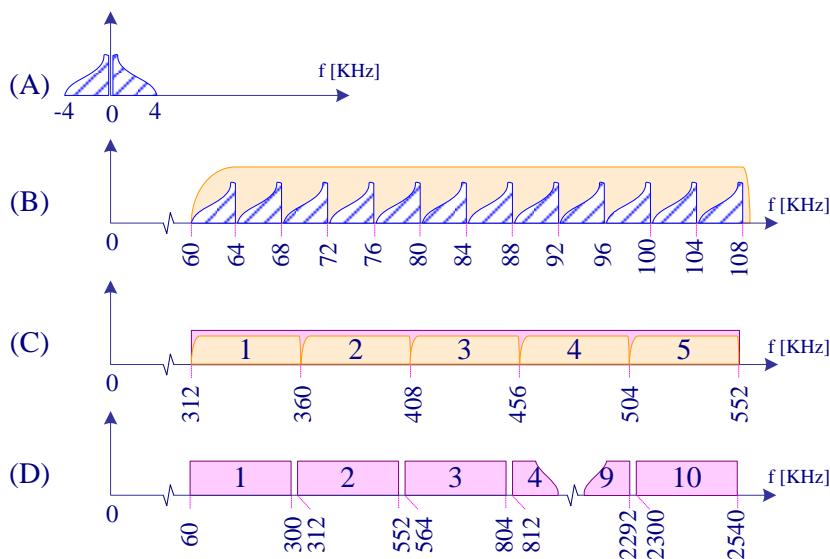


Figure 9.9: L- Carrier system, (A) voice channel, (B) basic group, (C) super group, and (D) master group

If more than 12 channels (1 group) are required, a Group multiplexer is required. This multiplexer takes the 60 - 108 KHz signals from up to 5 Group multiplexers to form a 60-channel Supergroup (Table 10.3).

The aggregate consists of a signal in the frequency range of 312 - 552 KHz (240 KHz of bandwidth).

A Super group multiplexer consolidates up to 10 Super group for the generation of a 600 voice channel aggregate (Figure 9.9). The aggregate consists of a signal in the frequency range of 60 - 2540 KHz (2480 KHz of bandwidth).

9.4.2 Digital Carrier System

Basic digital multiplexing in the united state is known as T1 carrier. It is also called the **Primary Rate Carrier** system, or simply “primary rate”. Using the T1 system, 24

digitized voice channels may be multiplexed together over a 4-wire cable (2 wires for transmit and 2 wires for receive).

9.4.2.1 Digital Carrier System Standards

The format used to frame transmitted data in the T1 system is called DS-1 and is shown in Figure 9.10 (A). DS-1 partitions data into frames of 193 bits. The first bit is always interpreted as a framing synchronization bit. The 192 remaining bits represent 8-bit interleaved words from 24 channels. Recall that the original analog voice signal is digitized using PCM at a rate of 8000 samples per second.

Each channel slot and hence, each frame must repeat 8000 times per second. At this rate, T1 must send or receive data at $8000 \times 193 = 1.544$ Mbps. For every sixth frame, each channel contains a 7-bit PCM word + a signaling bit. The signaling bits form a stream for each voice channel that contains network control information.

The same DS-1 format is used to provide digital data service. For compatibility with voice, the same 1.544 Mbps data rate is used. In this case, 23 channels of data are provided. The 24th channel position is reserved for a special sync byte, which allows faster and more reliable reframing following a framing error. Within each channel, 7 bits per frame are used for data, with 8 bit used to indicate whether the channel, for that frame, contain user data or system control data. With 7-bits per channel, and each frame is repeated 8000 times per second, a data rate of 56 Kbps can be provided per channel. Lower data rates are provided using a technique known as substrate multiplexing. For this technique, an additional bit is robbed from each channel to indicate which substrate multiplexing rate is being provided; this leaves a total capacity per channel of $6 \times 8000 = 48$ Kbps. This capacity is used to multiplex five 9.6 Kbps channels, ten 4.8 Kbps channels or twenty 2.4 Kbps channels.

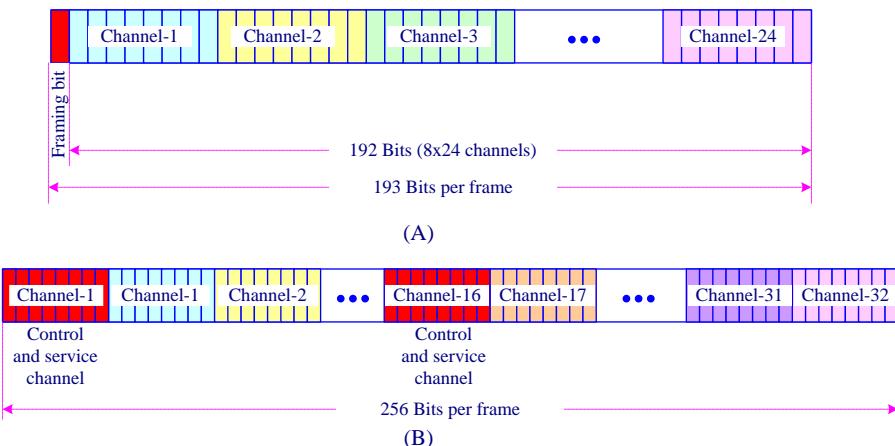


Figure 9.8: First level frame format, (A) T-1 carrier system and (B) E-1 System

Finally, the DS-1 format can be used to carry a mixture of voice and data channels. In this case, all 24 channels are utilized; no sync byte is provided. Multiple DS-1 frames are multiplexed to form DS-1c, DS-2 ... frames as shown in Figure 9.11.

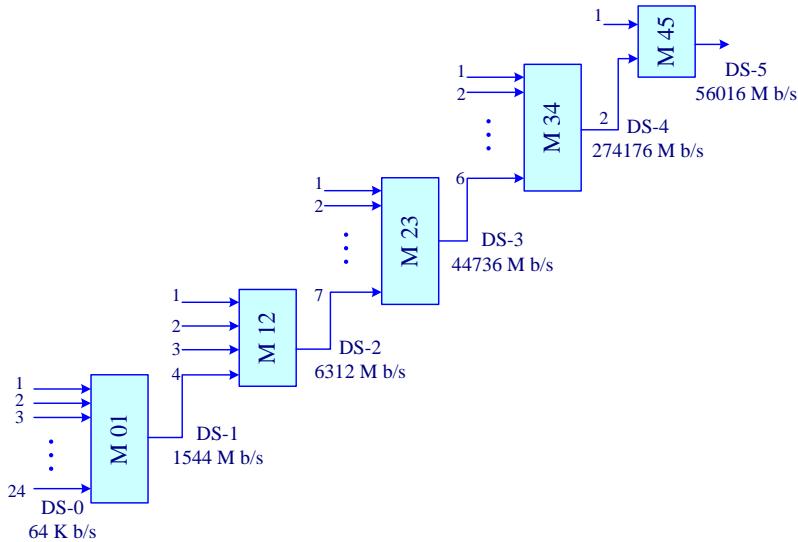


Figure 9.11: North American Digital Hierarchy (ANSI)

T1 has been specified first by AT&T and second, by ANSI (American National Standards Institute). This standard is the transmission standards in the United States, Canada, Korea, Taiwan, and Hong Kong (ANSI). The European (and the rest of the world) equivalent of T1 is called CEPT and is an ITU-T (formerly CCITT) standard. As a point of interest, the CEPT standard is at 2.048 Mbps. Multiple E-1 frames are multiplexed to form E-2, DS-2, Multiple E-2 frames are multiplexed to form E-3, and so on as shown in Figure 9.12.



T1 and E1 lines are among the most costly of all WAN links. Subscribers who do not need or cannot afford the bandwidth of an entire T1, or E1 line can subscribe to one or more T1 or E1 channels in 64 Kbps increments, known as Fractional T-1 (FT-1) or Fractional E-1 (FE-1).

Figure 9.10.(B) illustrates frame structure of E-1 in ITU-T Hierarchies

9.4.2.2 Channel Banks

The reference to the term "Channel Bank" is made quite often in the T-1 language. The type of Channel Bank is important since it defines the type of formatting that is required. For example, a D4 Channel Bank must have a DS-1 signal with data formatted in accordance with the D4 format.

The purpose of a Channel Bank in the telephone company is to form the foundation of multiplexing and demultiplexing the 24 voice channels (DS0). The D-type Channel Bank is used for digital signals. There are five kinds of Channel Banks that are used in the System: D1, D2, D3, D4, and DCT (Digital Carrier Trunk).

A transmitting portion of a Channel Bank digitally encodes the 24 analog channels, adds signaling information into each channel, and multiplexes the digital stream onto the

transmission medium. The receiving portion reverses the process. As these were designed as digitized voice circuits D1 banks (later called D1A) were first installed in 1962 and their success led to modifications of D1B and D1C. The original D1A, B, and C banks used 7 bits for each voice sample and one bit in each code word for carrying the signaling (off hook, ring, etc). When it became desirable to connect several T1 transmission spans together, the performance was not too good. In addition, it was realized that providing signaling information in every code word was wasteful since 8,000 bits per second was not required to provide the signaling information for a channel; the signaling information simply did not change that quickly.

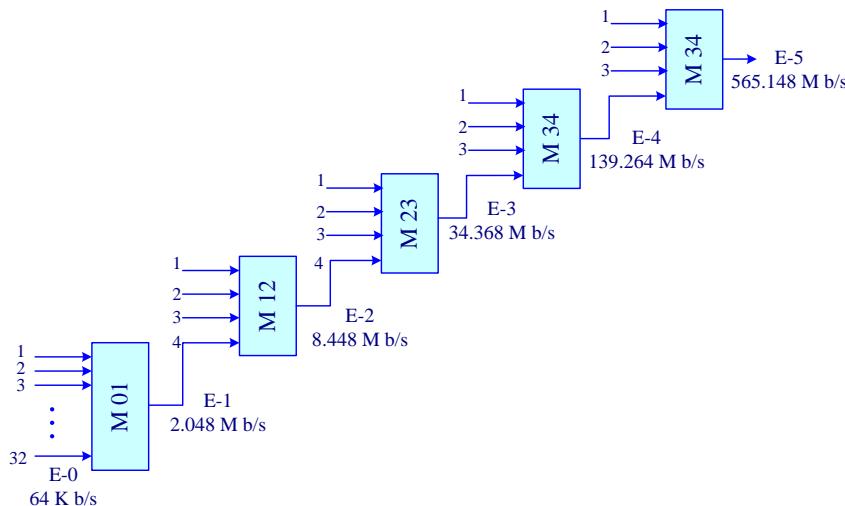


Figure 9.12: ITU-T Hierarchy

As a result of these conditions, another modification to the D1 series (D1D) and the new D2 channel bank were developed. The D2 bank uses all eight bits of every time slot to encode the analog signal except for selected frames. Supervisory and signaling information is sent by using the least significant bit from the code word in each channel every sixth frame. The companding characteristic also was changed to give better performance. The D2 bank increased the packing density to 96 channels in the same space as the 72 channels for a D1 bank.

D3 and D4 banks were motivated by advances in ICs, allowing packaging of 144 channels in a single bay. Following the D4 bank, advances in technology resulted in the development of the Digital Carrier Trunk unit, or DCT. It was developed by the Bell System to be smaller, lower cost, and easier to maintain than the D4 channel bank.

Intelligent multiplexers are the most important equipment in building the enterprise backbone network because they act dynamically to manage transmission resources. They allow you to make on-the-fly decisions about who is allocated the capacity, how much capacity needs to be allocated to each user, and whether individual users have rights to access the resource they want to access. In Figure 9.13, the intelligent muxes basically form a smart computer. An intelligent mux has a port side to which you interface the universe of information resources, which could be the videoconferencing systems, or the

voice systems, or the variety of data universe that you have. On the trunk side, you terminate the T-1s/E-1s or T-3s/E-3s.

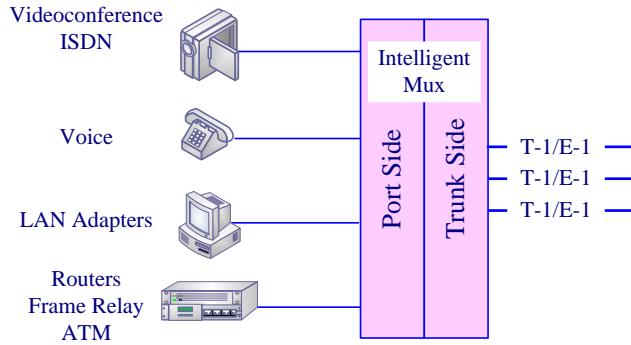


Figure 9.13: intelligent mux

 Channel bank is a type of telecommunications equipment that is located at the central office. It includes circuits for converting the analog signals to digital signals using pulse code modulation (PCM) techniques and supports the digital switching functions of the Public Switched Telephone Network (PSTN).

9.5 Synchronous Optical WAN Technology

9.5.1 Synchronous Optical Network (SONET)

Synchronous Optical Network (SONET) defines optical carrier (OC) levels and electrically equivalent synchronous transport signals (STSs) for the fiber-optic based transmission hierarchy. The standard SONET line rates and STS-equivalent formats are shown in table 9.1.

9.5.1.1 SONET Hierarchy and Multiplexing

SONET supports the multiplexing of multiple low-speed links in the following way. Various types of service adapters can accept any type of service, ranging from voice to high-speed data and video. A service adapter maps the signal into the payload envelope of the STS-1 or virtual tributary (VT). Adding new service adapters at the edge of the SONET network can transport new services and signals. All inputs are eventually converted to a Base format of a synchronous STS-1 signal (51.84 Mbps or higher). Lower speed inputs such as DS-1s are first bit or byte-multiplexed into virtual tributaries. Several synchronous STS-1s are then multiplexed together in either a single or two-stage process to form an electrical STS-n signal ($n = \text{one or more}$). A given SONET link runs at one of a finite set of possible rates, ranging from 51.84 Mbps (STS-1) to 2488.32 Mbps (STS-48) and beyond (See Table 9.1).

One of the benefits of SONET is that it can carry large payloads (above 50 Mbps). However, the existing digital hierarchy signals can be accommodated as well, thus protecting investments in current equipment.

To achieve this capability, the STS SPE can be sub-divided into smaller components or structures, known as VTs, for the purpose of transporting and switching payloads smaller than the STS-1 rate. All services below DS-3 rates are transported in the VT structure.

Figure 9.14 illustrates the basic multiplexing structure of SONET. Various types of service adapters can accept any type of service, ranging from voice to high-speed data and video. A service adapter maps the signal into the payload envelope of the STS-1 or VT. Adding new service adapters at the edge of the SONET network can transport new services and signals

Except for concatenated signals, all inputs are eventually converted to a Base format of a synchronous STS-1 signal (51.84 Mbps or higher). Lower-speed inputs such as DS-1s are first bit or byte-multiplexed into VTs. Several synchronous STS-1s are then multiplexed together in either a single- or two-stage process to form an electrical STS-N signal ($N \geq 1$).

STS multiplexing is performed at the byte interleave synchronous multiplexer. Basically, the bytes are interleaved together in a format such that the low-speed signals are visible. No additional signal processing occurs except a direct conversion from electrical to optical to form an OC-N signal.

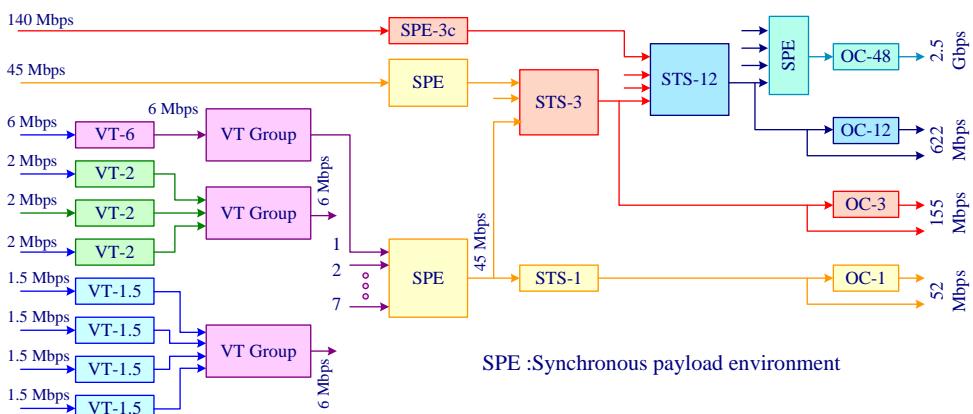


Figure 9.14: SONET Multiplexing Hierarchy

9.5.1.2 SONET Framing

The STS-1 frame is the basic building block of SONET transmission. The STS-1 frame consists of 810 bytes, or octets, and is transmitted every 125 microseconds, providing an overall data rate of 51.84 Mbps. The STS-1 frame can be logically viewed as a matrix of 9 rows, 90 bytes (or octets) per row. One row is transmitted at a time, from top left to bottom right. The first three columns (3 octets x 9 rows = 27 octets) are devoted to frame overhead. Nine octets are devoted to section-related overhead, and the remaining 18 octets are devoted to line overhead. The remainder of the frame is the payload. The frame

payload includes a column of path overhead, not necessarily in the beginning of the frame, as illustrated in Figure 9.15.

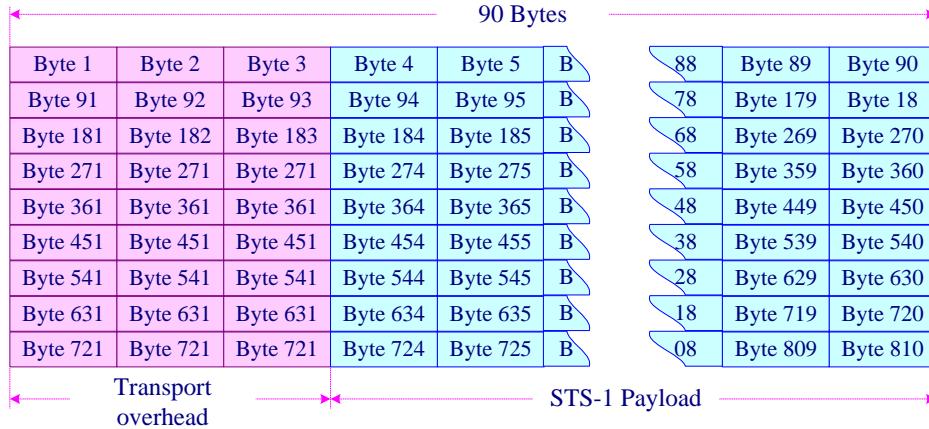


Figure 9.15: SONET STS-1 frame format

Intuitively, the STS- N frame can be thought of as consisting of N STS-1 frames, where the bytes from these frames are interleaved; that is, a byte from the first frame is transmitted, then a byte from the second frame is transmitted, and so on as it is illustrated in Figure 9.16. The reason for interleaving the bytes from each STS- N frame is to ensure that the bytes in each STS-1 frame are evenly paced; that is, bytes show up at the receiver at a smooth 51 Mbps, rather than all bunched up during one particular $1/N$ th of the 125- μ s interval.

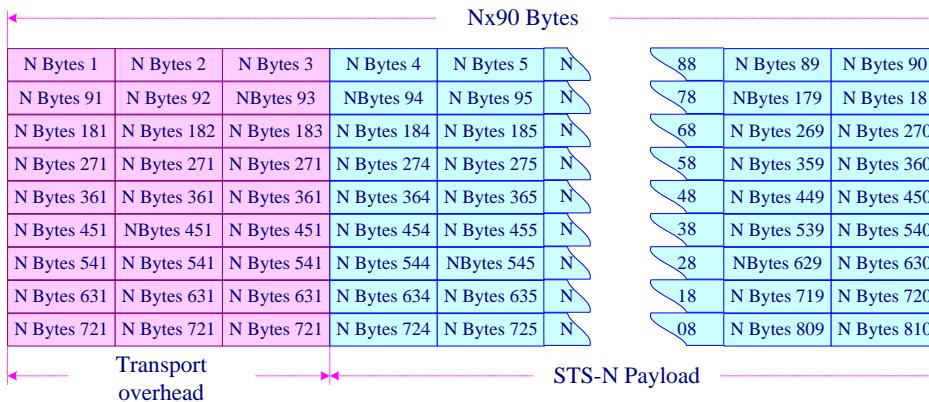


Figure 9.16: SONET STS- N frame format

 SONET can carry voice, video, and data simultaneously and provide the underlying transport mechanism for ATM networking. SONET can also be used as the underlying transport for FDDI, ISDN, and Switched Multimegabit Data Services.

9.5.2 Synchronous Digital Hierarchy (SDH)

Following development of the SONET standard by ANSI, the ITU undertook to define a synchronization standard that would address internetworking between the ITU and ANSI transmission hierarchies. That effort culminated in 1989 with CCITT's publication of the synchronous digital hierarchy (SDH) standards. SDH is a world standard, and, as such, SONET can be considered a subset of SDH.

9.5.2.1 SDH Hierarchy and Multiplexing

ITU TDM multiplexes thirty-two 64-kbps channels (E0s) into one 2.048-Mbps E1 signal. The issues between ITU-T and ANSI standards-makers involved how to accommodate both the 1.5-Mbps and the 2-Mbps nonsynchronous hierarchies efficiently in a single synchronization standard. The agreement reached specifies a basic transmission rate of 52 Mbps for SONET and a basic rate of 155 Mbps for SDH.

Synchronous and nonsynchronous line rates and the relationships between each are shown in Table 9.1

STS/STM Level	OC Level	Line Rate
STS-1	OC-1	51.840Mbps
STS-3/STM-1	OC-3/STM-1O	155.520Mbps
STS-9	OC-9	466.560Mbps
STS-12/STM-4	OC-12/STM-4O	622.080Mbps
STS-18	OC-18	933.120Mbps
STS-24	OC-24	1244.160Mbps
STS-36	OC-36	1866.230Mbps
STS-48/STM-16	OC-48/STM-16O	2488.32Mbps
STS-96	OC-96	4876.64Mbps
STS-192/STM-64	OC-192/STM-64O	9953.280Mbps
OC = Optical Carrier, which specifies the Optical fiber transport for SONET.		
STM-XO = Synchronous Transport Module (Digital Signal Level) Optical, which specifies the Optical fiber transport for SDH.		
Although STS-1 is the basic rate transport for SONET, STS-3 is the common implementation used for trunk and customer provisioning.		

Table 9.1: Synchronous and nonsynchronous line

SONET and SDH converge at SONET's 52-Mbps Base level, defined as synchronous transport module-0 (STM-0). The Base level for SDH is STM-1, which is equivalent to SONET's STS-3 (3×51.84 Mbps = 155.5 Mbps). Higher SDH rates are STM-4 (622 Mbps) and STM-16 (2.5 Gbps). STM-64 (10 Gbps) has also been defined.

Multiplexing is accomplished by combining or interleaving multiple lower-order signals (1.5 Mbps, 2 Mbps, etc.) into higher-speed circuits (52 Mbps, 155 Mbps, etc.). By changing the SONET standard from bit interleaving to byte interleaving, it became possible for SDH to accommodate both transmission hierarchies.

Asynchronous and Synchronous Tributaries

SDH does away with a number of the lower multiplexing levels, allowing nonsynchronous 2-Mbps tributaries to be multiplexed to the STM-1 level in a single step. SDH recommendations define methods of subdividing the payload area of an STM-1 frame in various ways so that it can carry combinations of synchronous and asynchronous tributaries. Using this method, synchronous transmission systems can accommodate signals generated by equipment operating from various levels of the nonsynchronous.



The equipments designed for SONET may not be used for SDH due to some cosmetic variations, but the concept is the same for both.

9.5.2.2 SDH Framing

The STM-1 frame is repeated 8,000 times a second, a rate equal to the sampling rate. This makes each 8-bit speech sample visible in a 155.52-Mbps data stream. The frame contains frame alignment information and other information such as management data channels and pointers that tell the location of tributaries in the frame.

If tributaries are not synchronous with the STM-1 frame, a pointer (a binary number) in a fixed location in the STM-1 frame tells the location of each tributary. By looking at the value of this pointer, we can easily find the desired tributary signal. The STM-1 frame structure is illustrated in Figure 9.17.

The transmission data streams of SDH are exact multiples of STM-1 at the 155.52-Mbps data rate, as we can see in Table 9.1. STM-1 data are simply byte interleaved with other STM-1 data streams to make up a higher transmission data rate; no additional framing information is added. Byte interleaving means that, for example, an STM-4 signal contains a byte (8 bits) from the first STM-1 tributary, then from the second, third, and fourth tributaries, and then again from the first one. The demultiplexer receives all STM-1 frames independently.

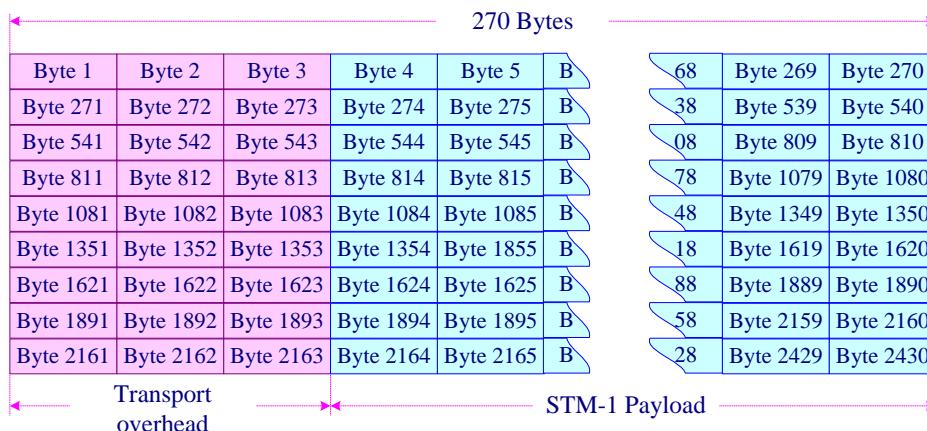


Figure 9.17: SDH frame format

9.6 Integrated Services Digital Network

Integrated Services Digital Network (ISDN) technology is standardized according to recommendations of the International Telecommunications Union (ITU), which describe the protocols and architecture to implement a worldwide digital communications network. All ISDN service providers and equipment vendors observe these recommendations to varying degrees.

9.6.1 ISDN Services

ISDN consists of two types of communications channels: bearer service B-channels, which carry data and services at 64 Kbps; and a single D-channel, which usually carries signaling and administrative information which is used to set up and tear down calls. The transmission speed of the D-channel depends on the type of ISDN service you've subscribed to. ISDN services available today can be divided into two categories: **Basic Rate Interface (BRI) service** and **Primary Rate Interface (PRI) service**

9.6.1.1 Basic Rate Interface (BRI)

ISDN BRI is the most basic ISDN interface. It provides the customer with two 64 Kbps B-channels and one 16 Kbps D-channel, all of which may be shared by numerous ISDN devices. It is the ideal service for homes and small offices, which, in the interest of controlling expenses, require a service that can integrate multiple communications needs. By bundling the 2 B-channels together and using 2:1 data compression, an ISDN BRI link can regularly achieve data throughput of over 250 Kbps.

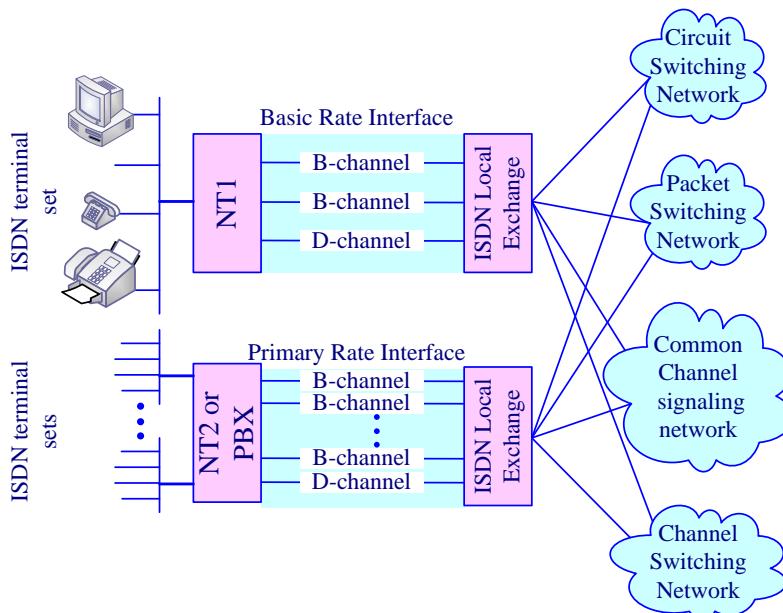


Figure 9.18: ISDN Basic and Primary Rate Interface

Up to eight ISDN devices can be connected on single bus, as signals on the D-channel automatically take care of contention issues, and route calls and services to the

appropriate ISDN device. Although only two B-channels are available to be used at any point in time, numerous other calls may be put "on hold" via D-channel signaling (a feature referred to as multiple call appearances). Figure 9.18 illustrates ISDN Basic Rate Interface

When more than one device is connected through a single ISDN BRI connection, individual devices are distinguished from one another through the use of multiple subscriber numbers, whereby a different ISDN number is assigned to each device served by the ISDN subscription. Alternatively, a separate sub address value can be used to differentiate between devices. BRI functionality is attainable without any modification to the existing telephony infrastructure. Telephone companies must simply change the signaling on the local loop to support ISDN, but no physical modifications are required (although some local lines which are 15,000 feet or longer may require adjustment).

9.6.1.2 Primary Rate Interface (PRI)

ISDN PRI includes one 64 Kbps D-channel and 23 B-channels in North America, and 30 B-channels in most other parts of the world. The number of B-channels is limited by the size of the standard trunk line used in the region; T1 in North America and Japan and E1 most everywhere else. Unlike BRI, PRI does not support a bus configuration, and only one device can be connected to a PRI line. Figure 9.18 illustrates ISDN Primary Rate Interface.

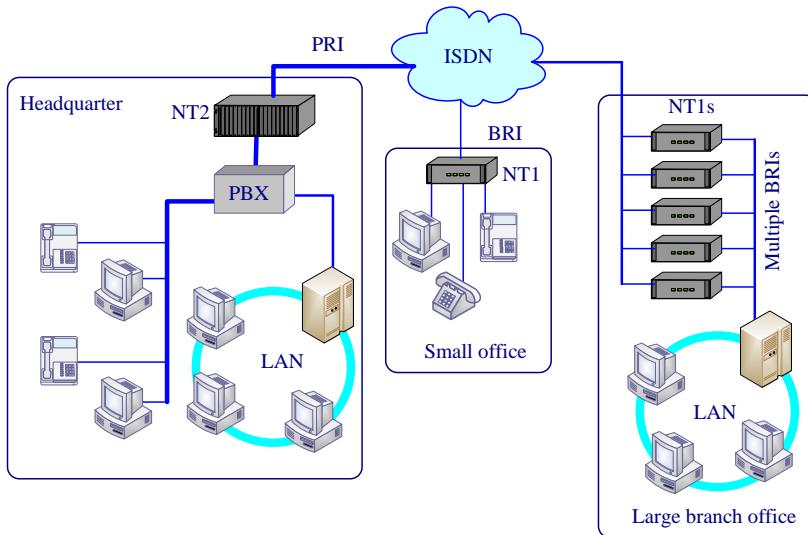


Figure 9.19: Common ISDN Configurations

A single PRI connection is usually much less expensive than obtaining the equivalent number of B-channels through multiple BRI connections. Aside from its higher bandwidth, the primary benefit of PRI is that its bandwidth can be dynamically allocated among applications as required. For instance, certain channels can be allocated for voice calls, but as those calls are terminated, the unused B-channels can be reallocated to a high-bandwidth application such as a videoconference. This is usually accomplished via powerful server, which is capable of distributing the T1/E1 bandwidth on a PRI link. With

its BRI and PRI services, ISDN has the flexibility to meet the needs of both individuals and corporations. Figure 9.19 demonstrates how BRI and PRI services can be used to meet bandwidth requirements of a home office, a branch office, or company headquarters.

In Figure 9.18, a small office is using ISDN BRI to meet all of its various voice and data communications requirements, a common solution when the expense of a Private Branch Exchange (PBX) cannot be justified. In the case of a large branch office ISDN BRI lines are being divided among all of the applications within the office. This can be accomplished using a server or a PBX. The configuration shown on the right is usually found in large offices where the entire ISDN PRI bandwidth is filled by a variety of applications.

9.6.2 ISDN Equipment Configurations

ISDN uses advanced digital equipment to provide its high-performance connections. Figure 9.20 illustrates a sample ISDN configuration and shows how devices can be attached to an ISDN switch at the central office using primary and basic rate accesses.

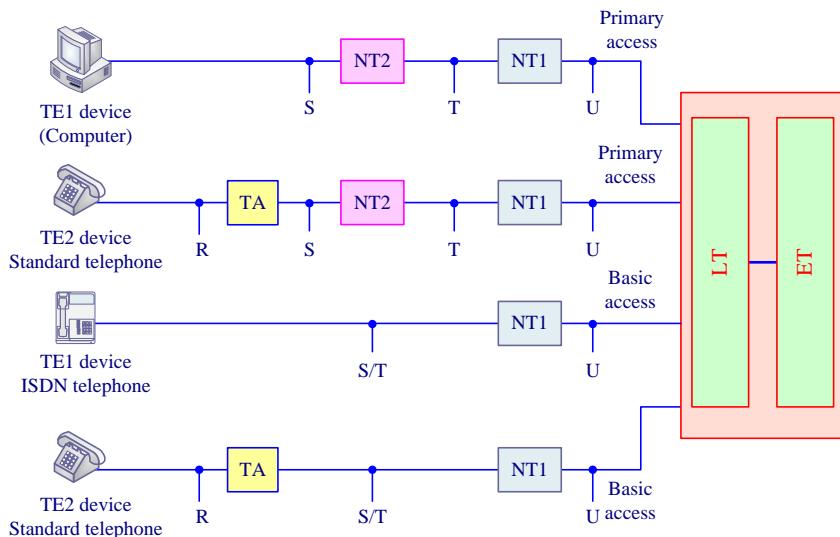


Figure 9.20: a sample ISDN configuration

ISDN devices and functional identifiers include the following:

➤ **ISDN terminals:** ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1).

- TE1s connect to the ISDN network through a four-wire, twisted-pair digital link.
- Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE2s connect to the ISDN network through terminal adapters (TA). The ISDN TA can be either a standalone device or a board inside the TE2. If the TE2 is implemented as a

standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

- **Terminal Adapter (TA):** A device that converts non-ISDN signals into ISDN compatible signals so that non-ISDN devices can connect to an ISDN network.
- **Network termination (NT):** there are 2 Network termination types NT1 and NT2 devices.
 - **NT1:** A device that connects 4-wire ISDN subscriber units to the conventional 2-wire local loop facility. In the U.S. the NT1 is part of the customer premises equipment CPE; in Europe and Japan, it is part of the local exchange facility. The NT1 converts between the signals/wiring from the ISDN device and the signaling/electrical standards adhered to by the local switch. Moreover, the NT1 takes care of ISDN line electrical requirements, powering the line and shielding ISDN equipment from any power surges. The ISDN equipment to which the NT1 is attached can be arranged in one of two configurations: a short-passive bus can be up to 200m in length and can support up to 8 ISDN devices, while an extended passive bus can be up to 1 Km long, but supports a maximum of 4 devices.
 - The **NT2** is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2.
- **Line Termination (LT):** A device that is located on the local exchange carrier (LEC) side of the subscriber line that functions as an NT1.
- **Exchange Termination (ET):** Subscriber cards in the ISDN exchange.

In Figure 9.20, different reference points are used to indicate connections into an ISDN network. ISDN reference points include the following:

- **U:** User reference point Located between the NT1 and LT. Corresponds to a subscriber line. The U reference point is relevant only in North America, where the NT1 function is not provided by the carrier network.
- **T:** Terminal reference point Located between the NT1 and NT2 or between the NT1 and TE1 or TA, if no NT2 device exists. Same characteristics as the S reference point.
- **S:** System reference point Located between the NT2 and TE1 or T1 connecting the terminal to the ISDN network. Same characteristics as the T reference point.
- **R:** Rate reference point Located between TA and TE2. The TE2 connects to the TA via a standard physical interface, such as EIA/TIA-232, V.24, X.21, and V.35.



It is worth pointing out that although NT1, NT2, and TAs may be offered as separate devices, in practice this is not always the case. Some manufacturers produce TAs that have NT1 and NT2 capabilities, as well as additional interfaces for other devices (e.g., analog telephones).

9.6.3 ISDN Applications

ISDN can be used in a number of different situations. The following are the main applications for ISDN:

- **Internet access:** ISDN can be used to increase the speeds otherwise supported by your analog voice-grade line when you do not have other broadband access options, such as DSL, cable modems, or broadband wireless.
- **Remote access:** ISDN is used to give teleworkers or telecommuters access to corporate resources.
- **LAN/WAN connections:** ISDN is a technique for LAN interconnection, by bridging multiple LANs across a WAN over ISDN connections.
- **High-capacity access:** ISDN can be used to increase the transmission capacity for application such as graphics, file transfer, video, and multimedia networking.
- **Private-line backup:** ISDN makes a good backup to the private-line services.
- **Dialup Frame Relay access:** ISDN provides measured-use dialup access to Frame Relay services in which the user dials in to a remote access port on the carrier's Frame Relay switch at either 64Kbps or 128Kbps.
- **Support low-speed data terminals:** BRI 0B+D for packet data One 16Kbps D-channel can be shared by up to eight devices. BRI 0B+D makes use of 9.6Kbps of D-channel capacity to support low-speed data terminals. This requires a terminal adapter that encapsulates the user data in D-channel frames. Applications for BRI 0B+D include credit card terminals and automatic teller machines.
- **Full-duplex, dedicated data services:** ISDN DSL (IDSL) IDSL delivers full-duplex, dedicated data services; it does not support voice services. It is provided either on a 1B or a 2B configuration (i.e., 64Kbps or 128Kbps).



ISDN has its own framing or encapsulation format called V.120, which is the international standard for synchronous ISDN data stream framing. ISDN frames are 48 bits long and are transmitted at 4000 frames per second.

9.7 Digital Subscriber Line (DSL)

9.7.1 DSL General Description

In the early 1990s, as the pressure started building on existing networks to support the increasing business needs for high-speed access, several varieties of symmetric Digital

Subscriber Line (DSL) technologies emerged in the market place as a solution to the “last mile” bottleneck. Using technology to increase the amount of information that can be transmitted on ordinary copper telephone wire, symmetric DSL provided a pragmatic and cost-effective alternative to expensive Optical fiber installation. However, as will be shown, each successive generation of symmetric DSL offered only incremental improvement over its predecessors without providing a comprehensive solution.

Digital Subscriber Line is fundamentally another name for an ISDN-BRI channel operating at the Basic Rate Interface. This circuit can carry both voice and data in both directions at the same time. However, DSL has come to refer to those various arrangements in which advanced modulating techniques are imposed onto the local channel in order to derive higher throughput in one or both directions. The various types of DSL are described in the following sections.

When you connect to the Internet, you might connect through a regular modem, through a local-area network connection in your office, through a cable modem or through a **digital subscriber line** (DSL) connection. DSL is a very high-speed connection that uses the same wires as a regular telephone line.



The last mile is that gap where a wired network ends and a business or home that wants access to the network resides. This gap is often too costly to fill or the terrain is too difficult to wire.

9.7.2 DSL Advantages and Disadvantages

Advantages

- You can leave your Internet connection open and still use the phone line for voice calls.
- The speed is much higher than a regular modem (1.5 Mbps vs. 56 Kbps)
- DSL doesn't necessarily require new wiring; it can use the phone line you already have.
- The company that offers DSL will usually provide the modem as part of the installation.

Disadvantages

- A DSL connection works better when you are closer to the provider's central office.
- The connection is faster for receiving data than it is for sending data over the Internet.
- The service is not available everywhere.

9.7.3 DSL Equipment

A DSL uses two pieces of equipment, one on the customer end and one at the Internet service provider, Telephone Company or other provider of DSL services. At the customer's location there is a DSL transceiver, which may also provide other services. The

DSL service provider has a DSL Access Multiplexer (DSLAM) to receive customer connections as shown in Figure 10.8.

9.7.3.1 DSL Transceiver

Most residential customers call their DSL transceiver a "DSL modem." The engineers at the Telephone Company or ISP call it an **ATU-R**. Regardless of what it's called, it's the point where data from the user's computer or network is connected to the DSL line. The transceiver can connect to a customer's equipment in several ways, though most residential installation uses USB or 10 Base-T Ethernet connections. While most of the ADSL transceivers sold by ISPs and telephone companies are simply transceivers, the devices used by businesses may combine network Routers, network Switches or other networking equipment in the same platform.

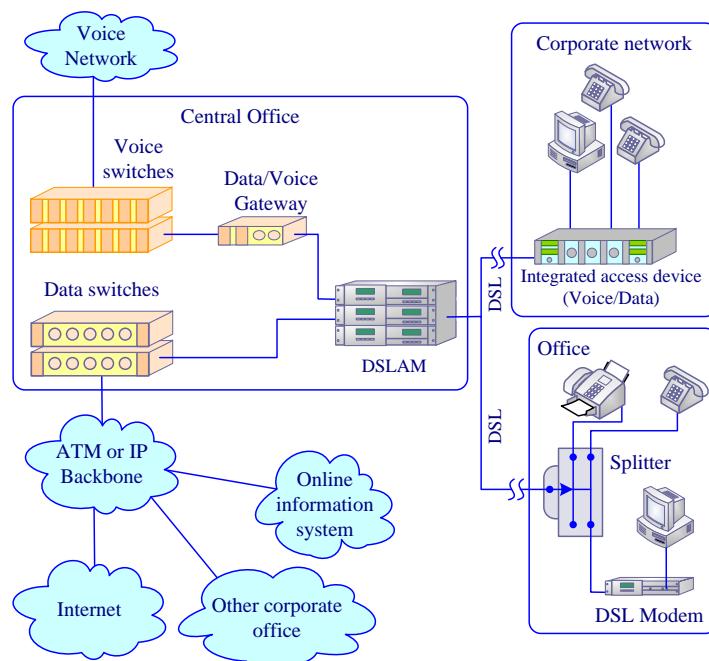


Figure 9.21: DSL Equipments

9.7.3.2 DSLAM

In Figure 9.21, DSL lines come in from residential and business premises. Their first point of termination is the DSLAM. The DSLAM is a network device, usually located at the telecommunication local exchange or within a neighborhood digital loop carrier configured to support DSL, although it can also reside at the customer premises in the case of a large enterprise. DSLAMs are designed to concentrate hundreds of DSL access lines onto ATM or IP trunks connecting to ATM switches, routers, or multiservice edge switches that then connect the DSLs to the ISPs. Each DSLAM has multiple DSLAM aggregation cards, and each card has multiple ports. DSLAMs typically contain power converters, DSLAM chassis, DSLAM cards, cabling, and upstream links. The DSLAM

splits the voice and data traffic, sending the voice traffic through traditional local exchanges onto the PSTN and sending the data traffic to the appropriate ISP or enterprise network.



Unlike cable modem the DSLAM provides a dedicated connection from each user back to the DSLAM, meaning that users won't see a performance decrease as new users are added until the total number of users begin to saturate the single, high-speed connection to the Internet.

9.7.4 DSL variations

There are several variations on DSL technology. In fact, there are so many that you will often see the term **xDSL**, where x is a variable, when the discussion is about DSL in general.

- **Asymmetric DSL (ADSL)** : It is called "asymmetric" because the download speed is greater than the upload speed. ADSL works this way because most Internet users look at, or download, much more information than they send, or upload.
- **High bit-rate DSL (HDSL)**: Providing transfer rates comparable to a T1 line (about 1.5 Mbps), HDSL receives and sends data at the same speed, but it requires two lines that are separate from your normal phone line.
- **ISDN DSL (ISDL)**: Geared primarily toward existing users of **Integrated Services Digital Network (ISDN)**, ISDL is slower than most other forms of DSL, operating at fixed rate of 144 Kbps in both directions. The advantage for ISDN customers is that they can use their existing equipment, but the actual speed gain is typically only 16 Kbps (ISDN runs at 128 Kbps).
- **Multirate Symmetric DSL (MSDSL)**: This is Symmetric DSL that is capable of more than one transfer rate. The transfer rate is set by the service provider, typically based on the service (price) level.
- **Rate Adaptive DSL (RADSL)**: This is a popular variation of ADSL that allows the modem to adjust the speed of the connection depending on the length and quality of the line.
- **Symmetric DSL (SDSL)**: Like HDSL, this version receives and sends data at the same speed. While SDSL also requires a separate line from your phone, it uses only a single line instead of the two used by HDSL.
- **Very high bit-rate DSL (VDSL)**: An extremely fast connection, VDSL is asymmetric, but only works over a short distance using standard copper phone wiring.
- **Voice-over DSL (VoDSL)**: A type of IP telephony, VoDSL allows multiple phone lines to be combined into a single phone line that also includes data-transmission capabilities.

Table 9.2 provides a comparison of the various DSL technologies:

DSL Type	Max. Send Speed	Max. Receive Speed	Max. Distance	Lines Required	Phone Support
ADSL	800 Kbps	8 Mbps	5,500 m	1	Yes
HDSL	1.54 Mbps	1.54 Mbps	3,650 m	2	No
IDSL	144 Kbps	144 Kbps	10,700 m	1	No
MSDSL	2 Mbps	2 Mbps	8,800 m	1	No
RADSL	1 Mbps	7 Mbps	5,500 m	1	Yes
SDSL	2.3 Mbps	2.3 Mbps	6,700 m	1	No
VDSL	16 Mbps	52 Mbps	1,200 m	1	Yes

Table 9.2: DSL Family

9.8 Asynchronous Transfer Mode (ATM)

9.8.1 ATM General Description

Asynchronous Transfer Mode (ATM) is the ITU standard for broadband ISDN. ATM has been accepted all over the world as the transfer mode used for B-ISDN (Broadband Integrated Services Digital Networks). B-ISDN is a result of the increasing demand for high-speed transfer of audio, video, high-speed LAN data. ATM can handle any kind of information i.e. voice, data, image, text and video in an integrated manner as shown in Figure 9.22. ATM provides good bandwidth flexibility and can be used efficiently from desktop computers to local area and wide area networks.

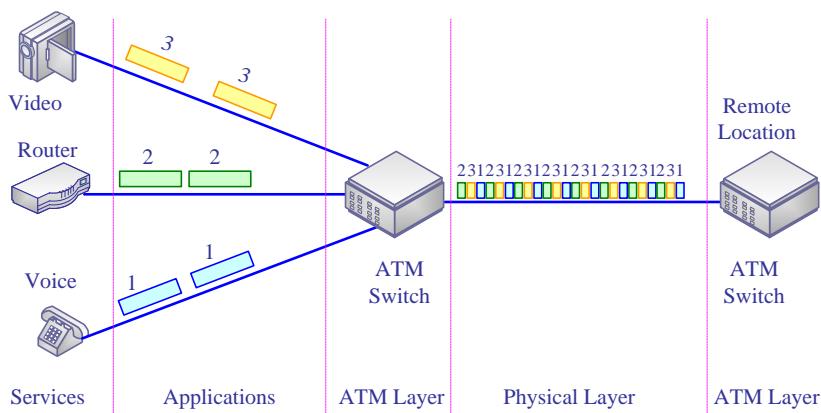


Figure 9.22: ATM multiplexes any kind of information

In ATM the information to be transmitted is divided into short 53 byte packets or cells, which have a 5-byte header. The reason for such a short cell length is that ATM must deliver real time service at low bit rates and thus it

minimizes packetization delay. ATM networks are connection oriented with virtual channels and virtual paths. The virtual channel carries one connection while a virtual path may carry a group of virtual channels. This ensures that cell sequence is maintained throughout the network. The virtual channel is identified by the Virtual Channel Identifier, (VCI), and the virtual path is identified by the Virtual Path Identifier, (VPI). Both the VCI and VPI may change within the network and they are stored in the header of the cell. As shown in Figure 9.23, the identity of a "physical" link is identified by two "logical" links: virtual channel (VC) and virtual path (VP). When a connection is set up, the values of these identifiers remain unchanged for the lifetime of the ATM connection.

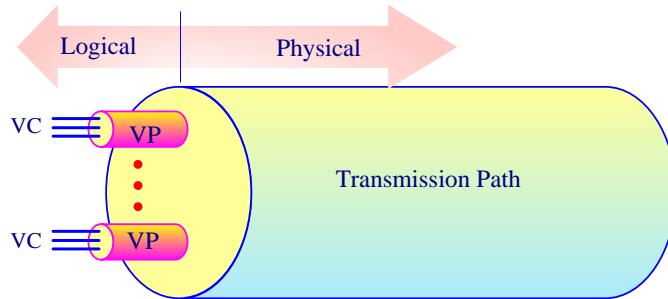


Figure 9.23: Overview of a typical ATM transmission medium

9.8.2 ATM Cell Format

The typical cell looks like that shown in Figure 9.24. The ATM header contains information about destination, type and priority of the cell.

- The Generic Flow Control (GFC) field allows a multiplexer to control the rate of an ATM terminal. The GFC field is only available at the User-to-Network Interface (UNI). At the Network-to-Network Interface (NNI) these bits belong to the Virtual Path Identifier (VPI).
- The Virtual Path Identifier (VPI) and the Virtual Channel Identifier (VCI) hold the locally valid relative address of the destination. These fields may be changed within an ATM switch.
- The Payload Type (PT) marks whether the cell carries user data, signaling data or maintenance information.
- The Cell Loss Priority (CLP) bit indicates which cells should be discarded first in the case of congestion.
- Finally, the Header Error Control (HEC) field is to perform a CRC check on the header data. Only the header is error checked in the ATM layer. Error check for the user data is left to higher layer protocols and is performed on an end-to-end Base.

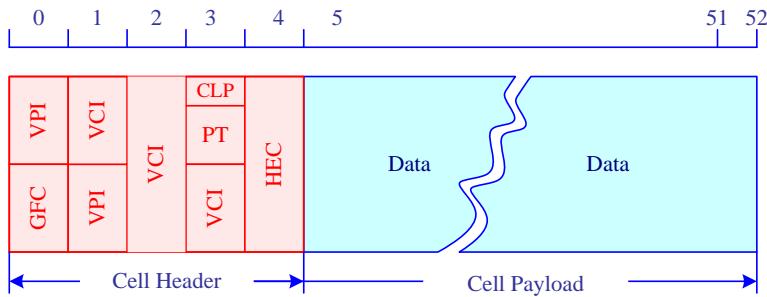


Figure 9.24: The ATM Cell Structure

9.8.3 ATM Switches

ATM protocol corresponds to layer 2 as defined in the open systems Interconnection OSI reference model. ATM is connection-oriented. That is, an end-to-end connection (or virtual *channel*) needs to be set up before routing ATM cells. Cells are routed based on two important values contained in the 5-byte cell header: the virtual *path identifier* (VPI) and virtual *channel identifier* (VCI), where a virtual path consists of a number of virtual channels. The number of bits allocated for a VPI depends on the type of interface.

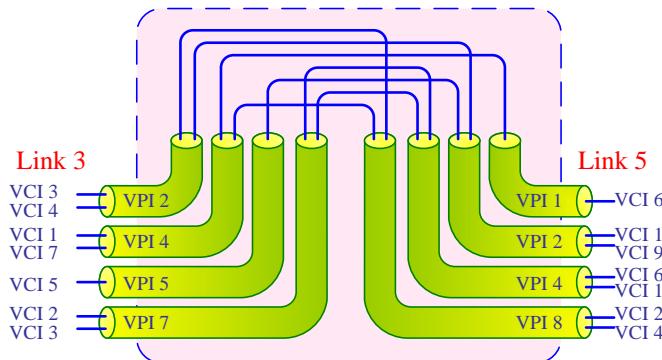


Figure 9.25: ATM switch

The combination of the VPI and the VCI determines a specific virtual connection between two ends. Instead of having the same VPI/VCI for the whole routing path, the VPI/VCI is determined on a per-link basis and changes at each ATM switch. Specifically, at each incoming link to a switch node, a VPI/VCI may be replaced with another VPI/VCI at the output link with reference to a table called a *routing information table* (RIT) in the ATM switch. This substantially increases the possible number of routing paths in the ATM network.

Figure 9.25 illustrate the structure of the ATM switch, while Figure 9.26 shows a routing table in an ATM switch, with routing information for all active connections passing through the switch. The routing information consists of the new VPI/VCI and new outgoing link for every incoming VC. Link 3, with VPIs 2, 4, 5, and 7, can be switched on link 5 with VPIs 1, 2, 4 and 8 through the ATM switch. A routing table provides the detail

of the switching function. For example, a cell with VPI 4 and VCI 7 on link 3 is set to be forwarded with VPI 8 and VCI 4 on link 5.

Routing table					
Incoming			Outgoing		
Link	VPI	VCI	Link	VPI	VCI
3	2	3	5	8	2
3	2	4	5	2	1
3	4	1	5	1	6
3	4	7	5	8	4
3	5	5	5	2	9
3	7	2	5	4	6
3	7	3	5	4	1

Figure 9.26: Routing table in a previous ATM switch example

💡 As ATM will be a broadband service the network will be a high speed one. So many functions will be carried out in the network such as error detection, correction, and flow control. They are done at the network edge rather than within the network.

At the start of a call to set up a connection in terms of a virtual channel, there is negotiation between the user and the network on the parameters. Once admission is achieved the call is then monitored to ensure that it is compliant with the call setup parameters. The network may drop low priority cells if congestion is about to or has occurred. High priority cells may only be dropped when there are no lower priority cells left to drop. Services not sensitive to cell loss may have some low priority cells and these cells may be dropped. Because of this it is possible to get much higher utilization than with previous networks.

9.8.4 ATM Cell Routing

The operation of routing cells is as follows. Each ATM switch has its own RIT containing at least the following fields: old VPI/VCI, new VPI/VCI, *output port address*, and *priority* field (optional).

💡 There are three modes of routing operations within the switch fabric: the *unicast mode* refers to the mode in which a cell is routed to a specific output port, the *multicast mode* refers to the mode in which a cell is routed to a number of output ports, and the *broadcast mode* refers to the mode in which a cell is routed to all output ports.

When an ATM cell arrives at an input line of the switch, it is split into the 5-byte header and the 48-byte payload. By using the VPI/VCI contained in the header as the old VPI/VCI value, the switch looks in the RIT for the arriving cell's new VPI/VCI. Once the match is found, the old VPI/VCI value is replaced with the new VPI/VCI value. Moreover, the corresponding output port address and priority field are attached to the 48-byte payload of the cell, before it is sent to the switch fabric. The output port address indicates to which output port the cell should be routed.

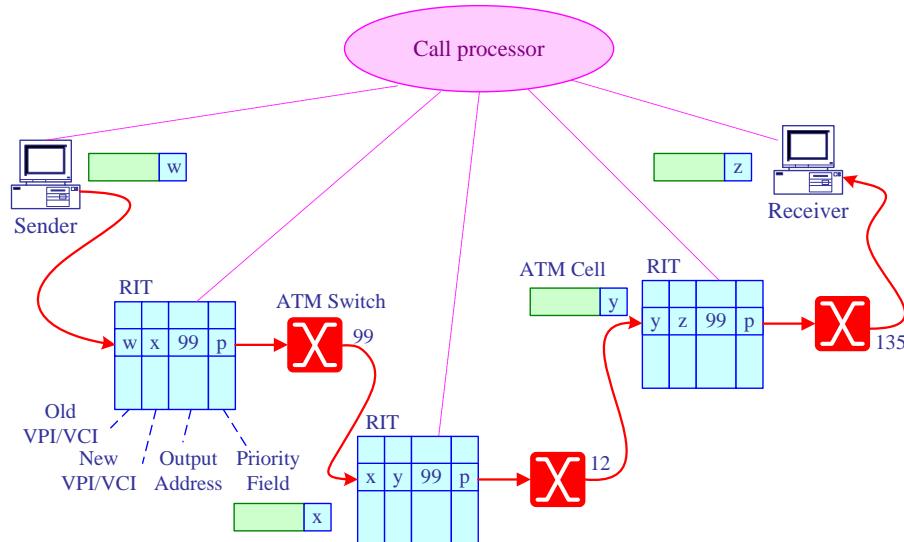


Figure 9.27: VPI/VCI translation along the path.

With respect to Figure 9.27, once a call setup is completed, the source starts to send a cell whose VPI/VCI is represented by W . As soon as this cell arrives at the first ATM switch, the entries of the table are searched. The matched entry is found with a new VPI/VCI X , which replaces the old VPI/VCI W . The corresponding output port address (whose value is 99) and the priority field are attached to the cell so that the cell can be routed to output port 99 of the first switch. At the second ATM switch, the VPI/VCI of the cell whose value is X is updated with a new value Y . Based on the output port address obtained from the table, the incoming cell is routed to output port 12 . This operation repeats in other switches along the path to the destination. Once the connection is terminated, the call processor deletes the associated entries of the routing tables along the path.



In the multicast case, a cell is replicated into multiple copies and each copy is routed to an output port.

9.8.5 Cell Switching versus Packet Switching

The ATM principle is very similar to the principle of a packet-switched network, but ATM differs in several ways:

- ATM provides cell sequence integrity, i.e. cells arrive at the destination in the same order as they left the source. This may not be the case with other packet-switched networks.
- Cells are much shorter than in standard packet-switched networks. This reduces the value of delay variance, making ATM acceptable for timing sensitive information like voice.
- The quality of transmission links has led to the omission of overheads, such as error correction, in order to maximize efficiency.
- Cells are transported at regular intervals. There is no space between cells. At times when the network is idle, unassigned cells are transported.



ATM does not restrict itself to any particular medium type. It can be used with existing medium designed for other communications systems. Some of ATM Forum recommendations are FDDI (100 Mbps), Fiber Channel (155 Mbps), OC3 SONET (155 Mbps), and T3 (45 Mbps).

9.9 Broadband Wireless Access Technology (BWA)

9.9.1 BWA Introduction

We explained how to get solutions to provide high-speed broadband access using wired access technologies, such as ISDN, digital subscriber line (DSL), Ethernet, ATM and Optical fiber. However, it is too difficult and expensive for carriers to build and maintain wired networks, especially in rural and remote areas. Broadband wireless access (BWA) technology is a flexible, efficient, and cost-effective solution to overcome the problems.

BWA is an access technology that can support a variety of wide area high-speed wireless data services. In addition to deployment as wireless backhaul links for fixed or mobile networks, the technology can also be used in customer access networks, such as direct access networks for mobile customers or broadband wireless local loops for fixed customers replacing the conventional copper wire.

Broadband Wireless Access (BWA) systems utilize Base stations to provide broadband voice, data, and video to businesses or homes, so it offers an alternative to the wired "last-mile" access links. Filling the gap between Wireless LANs and wide area networks, BWA systems will provide a cost-effective fixed wireless alternative to conventional wire-line DSL and cable in areas where those technologies are readily available. And more importantly the BWA technology can provide a cost-effective broadband access solution in areas beyond the reach of DSL and cable.

Consumers will have greater choice of innovative services, including mobile broadband networks, so they can access the Internet and multimedia services at affordable prices anytime, anywhere and while on the move.

There are a wide range of MAN and WAN BWA technologies developed and being developed the most recently popular of them are 802.16 family and 802.20 standards.

9.9.2 Wireless MAN (WMANs)

The air interface standard, IEEE 802.16, commonly referred to as WiMAX is a specification for broadband wireless communication standards developed for WMANs, is one of the most popular BWA technologies today, which aims to provide high-speed broadband wireless access for wireless metropolitan area networks. The IEEE 802.16 BWA technology family often referred to as worldwide interoperability for microwave access (WiMAX). It consists of “the last mile,” as it is sometimes referred to in industry supports fixed, nomadic, portable, and mobile broadband accesses and enables interoperability and coexistence of BWA systems from different manufacturers in a cost-effective way.

The Wireless MAN utilizes two ranges of frequency spectrum, the 10–66GHz range for the LoS access (IEEE 802.16) and 2–11GHz range for NLoS access (IEEE 802.16a). In both ranges the single-carrier is designed to accommodate either Time Division Duplexing (TDD) or Frequency Division Duplexing (FDD) deployments, allowing for both full and half-duplex terminals in the FDD case. In Time Division Duplex (TDD) allows the use of a single frequency to accommodate both transmits and receive duties at both ends of the link. This is accomplished by time slicing the channel fast enough so the transmitters and receivers see a continuous flow of information. The channel is temporally divided into transmit timeslots and receive timeslots with a small guard time between them. FDD requires two channels: one for transmission and one for reception while for TDD a single channel is shared by both the uplink and the downlink but separated by different time slots. FDD is designed only for symmetrical traffic with lower spectrum efficiency and higher cost but shorter delay.

The multiplexing technologies used in 802.16 are time division multiplexing (TDM)—for downlink channel and time division multiple access (TDMA) — for uplink channel. In TDM, subscribers share the same frequency band but are allocated by different time slots. TDMA is a flexible multiple access schemes in which time slots can be allocated to subscribers according to fixed or contention modes.

Three modulation schemes are supported: QPSK (quadrature phase shift keying), 16QAM (quadrature amplitude modulation), and 64QAM. The higher order of modulation allows more bits to be encoded per symbol to achieve higher data rate, but it is more prone to interferences.

WiMAX can provide broadband wireless access (BWA) up to 50 km for fixed stations, and 5 - 15 km for mobile stations.

Compared to the complicated wired network, a WiMAX system only consists of two parts: the WiMAX Base station (BS) and WiMAX subscriber station (SS) also referred to as customer premise equipments. Therefore, it can be built quickly at a low cost.

➤ **Base Station (BS):** The Base station controls and manages the connection. It sends data on the downlink in channels allocated to various subscribers. A Base

station can cover multiple cells (sectors) with the help of sectored antennas. In a point-to-multipoint (PMP) configuration, the downlink is multipoint. Each Base station is configured with a 48-bit MAC address. The first 24 bits of this address identify the operator.

➤ **Subscriber's Station (SS):** A subscriber's station is a terminal that communicates with the Base station (BS). It sends data on the uplink, which is point-to-point in a PMP network configuration and either point-to-point or point-to-multipoint in a mesh topology. All SSs within the same sector and frequency channel receive the same downlink information. The 48-bit IEEE 802 MAC address uniquely identifies a SS. An SS could be a packet data or multimedia terminal with a range of transmission rate capabilities.

802.16 defines two WiMAX network topologies:

➤ **Point-to-point (PTP):** It refers to a dedicated link that connects only two nodes, BS and subscriber terminal. It utilizes resources in an inefficient way and substantially causes high operation costs. It is usually only used to serve high-value customers who need extremely high bandwidth, such as business high-rises, video postproduction houses, or scientific research organizations. In these cases, a single connection contains all the available bandwidth to generate high throughput. A highly directional and high-gain antenna is also necessary to minimize interference and maximize security.

➤ **Point-to-multipoint (PMP):** The PMP topology, where a group of subscriber terminals are connected to a BS separately (shown in Figure 9.28), is a better choice for users who do not need to use the entire bandwidth. The available bandwidth now is shared between a group of users, and the cost for each subscriber is reduced.

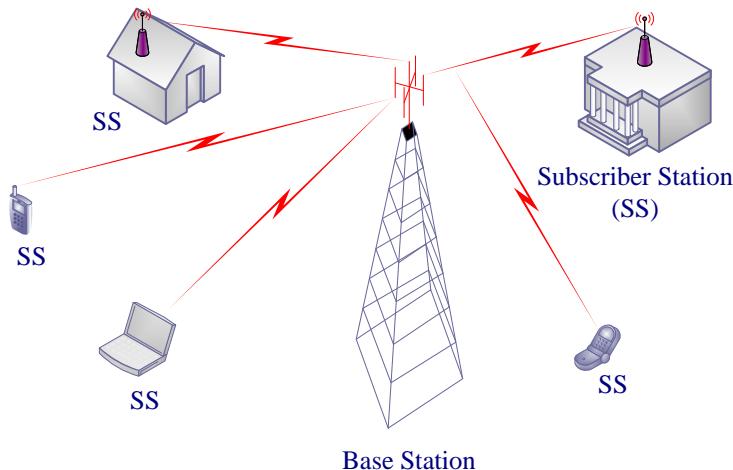


Figure 9.28: WiMax Point-to-Multipoint topology

Wireless mesh networks (WMN) are an exciting new topology for creating low-cost, high-reliability wireless networks in a building, across a campus, or in a metropolitan

area. In a mesh network, each wireless node serves as both an AP and wireless router, creating multiple pathways for the wireless signal. Mesh networks have no single point of failure and thus are self-healing. A mesh network can be designed to route around line-of-sight obstacles that can interfere with other wireless network topologies. However, using a wireless mesh currently requires the use of specialized client software that will provide the routing function and put the radio into ad-hoc or infrastructure mode as required.

In WMNs, two types of nodes perform the routing: mesh routers and mesh users. Figure 9.29 shows detailed connectivity of a backbone mesh network to WiFi, WiMAX, and wireless cellular networks. In this figure, a WiFi network, a cellular network, and a WiMAX network are connected through mesh routers with gateway bridges. A router with gateway bridge capability enables the integration of WMNs with other type networks, although traditional routers with regular network interface cards (NICs) can connect to mesh networks.

There are some important things to notice in Figure 9.29:

1. The resemblance to a map of the Internet is not entirely coincidental. Like the Internet and other router-based communication networks, a mesh network offers multiple redundant communication paths throughout the network.

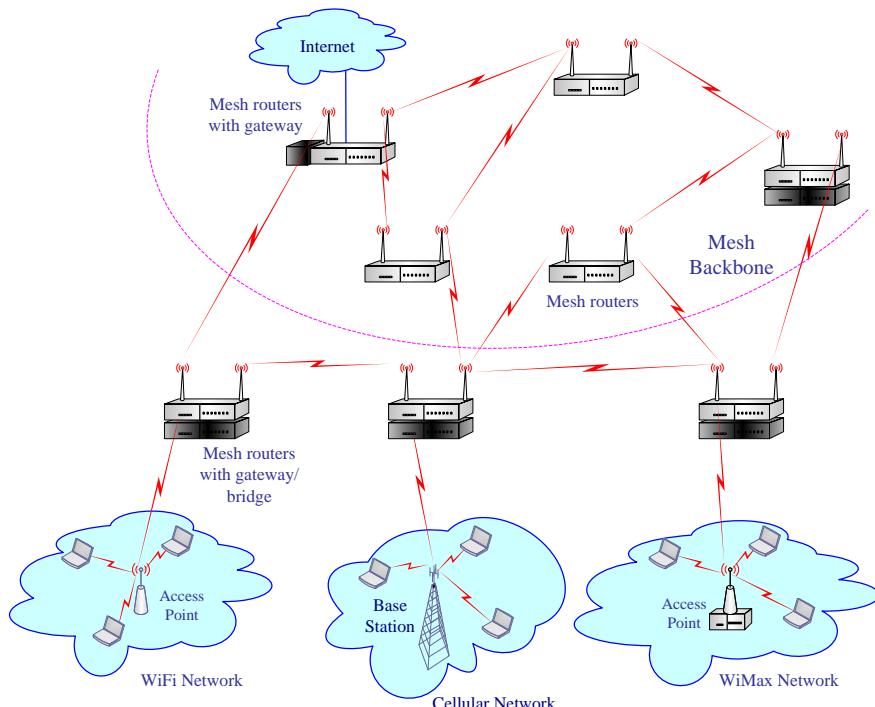


Figure 9.29: Overview of a backbone mesh network and connections to WiFi, WiMAX, and wireless cellular networks

2. If a single node fails for any reason (including the introduction of strong RF interference), messages will automatically be routed through alternate paths.

3. In a mesh network, the distance between wireless nodes is short, which dramatically increases the link quality between nodes. If you reduce distance by a factor of two, the resulting signal is at least four times more powerful at the receiver. This makes links more reliable without increasing transmitter power in the individual nodes.



A wireless mesh network (WMN) is a dynamically self-organized wireless network that maintains mesh connectivity and helps users stay online anywhere, anytime, for an unlimited time.

9.9.3 Mobile Broadband Wireless Access (MBWA)

Mobile Broadband Wireless Access (MBWA), nicknamed as Mobile-Fi, is an IEEE standard defined by the 802.20 group to define the interface that allows the creation of low-cost, always-on, and truly mobile broadband wireless networks.

The most complex network is one designed for true mobility. Like a voice-based cellular or PCS network, the high-speed mobile data network must provide ubiquitous coverage, and must support high velocity mobility. These requirements are not easily achieved or inexpensive. These systems will require many tens of megahertz of licensed spectrum, and will require technology that can deal with the hostile RF environment found in a truly mobile application. The 802.16e, 802.20 and CDMA2000 standards are several of the standards that may eventually bring true broadband mobile data solutions to large areas of the earth. Because of their cost, complexity, and need for interference managed dedicated spectrum, large telecom carriers, as opposed to the small businesses that offer nomadic network solutions, will be the most likely owner of these networks.

The 802.20 standard focuses on true high velocity mobile broadband systems. The 802.20 interface seeks to boost real-time data transmission rates in wireless metropolitan area networks to speeds that rival DSL and cable modem connections (1 Mbps or more). This will be accomplished with Base stations covering radii of up to 15 kilometers or more, and it plans to deliver those rates to mobile users even when they are traveling at speeds up to 250 kilometers per hour. This would make 802.20 an option for deployment in high-speed trains.

The main objective of the 802.20 standard is to have specifications for the PHY and MAC for mobile broadband wireless access systems for packet exchange between the 802.20-enabled mobile terminal and external networks (e.g., IP network) or another 802.20-enabled terminal.

- The target frequency spectrum is below 3.5GHz.
- It should be optimized for IP data transport.
- Peak data rates per user in excess of 1Mbps.
- Vehicular speeds up to 250 kmph supported.
- Spectral efficiency, sustained user data rate and number of active users to be higher than any current mobile system.

9.10 Quick Review

- ❖ WANs may be interconnected to and/or through the existing public networks. So to build WANs, you must lease a physical network.
- ❖ Using multiplexing eliminate much redundant hardware by one link shared by several terminals. Multiplexer interfaces many low speed devices into a single high-speed line.
- ❖ Frequency division multiplexing FDM which is the simplest and oldest form of multiplexing. While time division multiplexing is more efficient.
- ❖ Statistical Time Division Multiplexing allocates time only to lines when required. Newer STDM units provide additional capabilities such as data compression, line priority, mixed speed lines, host port sharing, network port control, automatic speed detection and much more.
- ❖ Broadband carrier systems are classified as either analog carrier systems or digital carrier systems. They can carry speech, data, video and supervisory signals. Analog carrier systems are best suited for speech signals while digital carrier systems are best suited for data signals. T1 and E1 lines are among the most costly of all WAN links.
- ❖ Synchronous Optical Network (SONET) defines optical carrier (OC) levels and electrically equivalent synchronous transport signals (STSs) for the fiber-optic based transmission hierarchy. SONET supports the multiplexing of multiple low-speed links in the following way. SONET can carry voice, video, and data simultaneously with a speed above 50 Mbps. SONET can also be used as the underlying transport for ATM, FDDI, ISDN, and Switched Multimegabit Data Services.
- ❖ SDH is a world standard, and, as such, SONET can be considered a subset of SDH.
- ❖ ISDN consists of two types of communications channels: bearer service B-channels, and D-channel. ISDN can be divided into two categories: Basic Rate Interface (BRI) service and Primary Rate Interface (PRI) service. It provides the customer with two 64 Kbps B-channels and one 16 Kbps D-channel. ISDN PRI includes one 64 Kbps D-channel and 23 B-channels in North America, and 30 B-channels in most other parts of the world. ISDN can be used in a number of different situations such as Internet access Remote access, LAN/WAN connections and others.
- ❖ Digital Subscriber Line is fundamentally another name for an ISDN-BRI channel operating at the Basic Rate Interface. This circuit can carry both voice and data in both directions at the same time. There are several variations on DSL technology such as ADSL, HDSL, ISDL, MSDSL, RADSL, SDSL, VDSL and VoDSL.
- ❖ Asynchronous Transfer Mode (ATM) is the ITU standard for broadband ISDN. In ATM the information to be transmitted is divided into short 53 byte packets or cells. Cells are routed based on two important values contained in the 5-byte cell

header. The combination of the VPI and the VCI determines a specific virtual connection between two ends. ATM does not restrict itself to any particular medium type.

- ❖ BWA is an access technology that can support a variety of wide area high-speed wireless data services. Broadband Wireless Access (BWA) systems utilize Base stations to provide broadband voice, data, and video to businesses or homes, so it offers an alternative to the wired "last-mile" access links.
- ❖ Consumers will have greater choice of innovative services, including mobile broadband networks, so they can access the Internet and multimedia services at affordable prices anytime, anywhere and while on the move.
- ❖ There are a wide range of MAN and WAN BWA technologies developed and being developed the most recently popular of them are 802.16 family (WiMAX) and 802.20 (MBWA), nicknamed as Mobile-Fi.

9.11 Self Test Questions

A- Answer the following questions

1. What is the aim of multiplexing?
2. What is the multiplexer?
3. What is the main feature of Frequency-division multiplexing?
4. What is the main feature of Time-division multiplexing?
5. What is the main feature of Statistical time division multiplexing?
6. What is the main feature of Wavelength-division multiplexing?
7. What are the differences between bit interleaving and byte interleaving technologies?
8. Explain the framing process.
9. Why do we need to use the stuffing bits?
10. What is the main feature of analog carrier systems?
11. What is the relation between basic group and super group?
12. What is the relation between super group and master group?
13. What is the primary rate carrier?
14. Describe the frame format used by T-1 carrier.
15. Compare North American digital hierarchy with ITU-T digital hierarchy.
16. What is the intelligent multiplexer?
17. Illustrate the basic multiplexing structure of SONET.
18. What is the STS-1?
19. Explain the SONET frame structure.
20. What is the difference between SONET and SDH Hierarchies?
21. What do the ISDN communication channels types consist of?
22. What are the categories of ISDN services?
23. What are the common ISDN configurations?
24. List the main ISDN devices and functional identifiers.
25. Where is ISDN applicable?
26. List the advantages of DSL?
27. What are the main equipments of DSL?

28. List the variations of x-DSL?
 29. What kind of information can be handled by ATM?
 30. What is the ATM logical connection an ATM physical connection?
 31. Explain the ATM cell format?
 32. How does the ATM switch work?
 33. Explain the VPI/VCI translation along the path.
 34. What is the BWA?
 35. What is WiMax?
 36. What are the multiplexing technologies and modulation schemes that are supported by WiMax?
 37. What are the WiMax network topologies?
 38. What is the MBWA?

B- Identify the choice that best completes the statement or answers the question.

- _____ is not the name of an ISDN service.
 - BRI
 - PRI
 - 2B+D
 - IDSL
 - _____ enables you to use a computer with an ISDN connection.
 - A terminal adapter
 - Terminal equipment
 - An NT-1
 - A U interface
 - A SONET network uses _____ type of cable at the physical layer.
 - UTP
 - Coaxial
 - Shielded twisted pair
 - Optical fiber
 - Digital subscriber line (DSL) refers to
 - a specific gauge of wire used in modem communications
 - a modem enabling high-speed communications
 - a connection created by a modem pair enabling high-speed communications
 - a specific length of wire
 - Which of the following statement is correct?
 - T1 and HDSL are essentially equivalent technologies.
 - ADSL cannot handle Internet or LAN access.
 - E1 and HDSL are essentially equivalent technologies.
 - All of them
 - Non of them
 - IV
 - I&III
 - V
 - III
 - _____ is better suited to handle bursty traffic.
 - Circuit switching
 - Virtual Circuit Packet switching
 - ATM
 - Packet switching
 - _____ is the basic connection unit in an ATM network
 - virtual channel connection
 - virtual path connection

- c. virtual loop connection
 - d. Virtual Circuit Packet switching
8. _____ is the preferred mode of operation in an ATM network.
- a. permanent virtual circuits
 - b. switched virtual circuits
 - c. a&b
 - d. non
9. Asynchronous transfer mode (ATM) is _____
- a. a cell-based data transmission protocol
 - b. an opto-electronic component
 - c. a circuit-switched access systems
 - d. non of them
10. In order to provide a communications link between two existing LAN systems, all of the native protocols must be _____ before transmission over the ATM portion of the network.
- a. formatted
 - b. encapsulated
 - c. placed in packets
 - d. placed in cells
11. The _____ is a particular set of a standard that allows the interworking of products from different vendors. It usually embodies a Optical fiber ring that will permit transmission in both directions.
- a. local-area network (LAN)
 - b. wide-area network (WAN)
 - c. synchronous optical network (SONET)
 - d. common channel signaling network
12. Packet switching is used for _____
- a. credit-card verification
 - b. automated teller machines
 - c. the Internet and the World Wide Web
 - d. all of the above
13. _____ is a high-performance switching and multiplexing technology that utilizes fixed-length packets to carry different types of traffic.
- a. asynchronous transfer mode (ATM)
 - b. asymmetric digital subscriber line (ADSL)
 - c. synchronous optical network (SONET)
 - d. none of the above
14. _____ is a standards-based multiplexing and switching technology used to deliver multimedia services over broadband networks.
- a. ATM
 - b. PTT
 - c. TCP
 - d. none of the above
15. _____ is there to generate the fastest bit stream possible or economical in a part of the network.
- a. TDM
 - c. WDM

- FDM d. non

16. Which is (are) true statement(s)?
a. Synchronous optical network offers cost-effective transport in the access area but not the core of the network.
b. With SONET, the traffic flowing in and out of a node is exactly equal.
c. SONET is a simple replacement for asynchronous digital hierarchy.
d. all

17. Choose the statement that you think is true?
a. ADSL is an Internet-only technology.
At present, service providers are able to deliver all three basic service types or communications classifications (voice, data, and video).
c. ADSL is able to deliver full Internet access service, including video.
d. All

18. The combination of VDSL and _____ delivers the Internet services of today in an architecture that is capable of supporting tomorrow's applications.
a. X.25 packet switching
b. frame relay
c. Internet protocol
d. ATM

19. _____ is the channel configuration of a BRI.
a. 1 B, 2 D channels c. B. 2 B, 1 D channel
b. 23 B, 1 D channel d. 30 B, 1 D channel

20. _____ is the data transfer rate for an ISDN bearer channel.
a. 16Kbps c. 56Kbps
b. 64Kbps d. 128Kbps

21. _____ is the data transfer rate for a BRI ISDN delta channel.
a. 16Kbps c. 56Kbps
b. 64Kbps d. 128Kbps

22. _____ bearer channel(s) (is) are provided in BRI.
a. 1 c. 2
b. 16 d. 23

23. _____ bearer channel(s) (is) are provided in PRI for North America.
a. 1 c. 2
b. 16 d. 23

24. _____ is the data transfer rate for a PRI ISDN delta channel.
a. 16Kbps c. 56Kbps
b. 64Kbps d. 128Kbps

25. _____ bearer channels are provided in PRI for Europe?
a. 16 c. 24
b. 30 d. 32

26. _____ provides setup, signaling, and termination in ISDN.

38. Which of the following is a digital telephone service that provides voice and data transfer services over standard twisted pair wire into a home or small business?

 - a. T-1
 - b. DSL
 - c. SONET
 - d. ISDN

39. How many separate channels ISDN basic rate interface (BRI) multiplexes?

 - a. two
 - b. three
 - c. four
 - d. five

40. A(n) ____ is a network device that can receive multiple inputs and transmit them to a single shared network medium.

 - a. multiplexer
 - b. decoder
 - c. adder
 - d. shifter

41. What is the fiber-optic technology that can transmit data faster than one gigabit per second?

 - a. ADSL
 - b. ISDN
 - c. SONET
 - d. X.25

42. What is the spread spectrum technique that broadcasts the signal over a seemingly random series of radio frequencies?

 - a. direct sequence
 - b. frequency hopping
 - c. time-hopped
 - d. chirp

43. Which of the following can provide data transmission at speeds of hundreds of thousands up to millions of bits per second?

 - a. T-1 lines
 - b. Cable television networks
 - c. ISDN
 - d. DSL

44. A few companies use frequency division multiplexing with _____ to deliver multiple audio and video channels to computer workstations.

 - a. shielded twisted pair wire
 - b. Baseband coaxial cable
 - c. broadband coaxial cable
 - d. unshielded twisted pair wire

45. _____ is/are inserted between two signals to provide a form of insulation and to keep one signal from interfering with another signal.

 - a. Guard bands
 - b. Shielding
 - c. Insulation
 - d. Padding

46. To maintain synchronization between sending multiplexor and receiving demultiplexor, the data from the input sources are often packed into a simple frame with synchronization _____ added somewhere with the frame.

 - a. controls
 - b. data
 - c. bits
 - d. bytes

47. The T-1 multiplexed output stream is a continuous repetition of

 - a. frames.
 - b. bits.
 - c. bytes.
 - d. channels.

48. By whom SONET was developed?
a. ISO.
b. IEEE.
c. ANSI.
d. ITU-T.

49. By whom SDH was developed?
a. ISO.
b. IEEE.
c. ANSI.
d. ITU-T.

50. _____ carrier is physical specification that each synchronous transport signal level of SONET is supported by.
a. data
b. synchronization
c. optical
d. logical

51. In a SONET network, you can multiplex three STS-1 signals easily into one _____.
a. STS-1
b. STS-3
c. STS-12
d. STS-18

52. How many frames per second does the STS-1 signaling level of a SONET network supports?
a. 1000
b. 5000
c. 8000
d. 10000

53. What is the field of a statistical multiplexor packet that provides information that the receiving multiplexor can use to detect transmission errors within the frame?
a. frame check sequence
b. address
c. control
d. flag

54. Which multiplexing technology has very high capacities over fiber?
a. Synchronous time division
b. Wavelength division
c. Code division
d. Frequency division

55. Basic Rate Interface connections offer three channels: two at 64 Kbps and one at _____ Kbps.
a. 8
b. 16
c. 24
d. 32

56. Primary Rate Interface connections offer one _____ -Kbps D-channel.
a. 16
b. 32
c. 48
d. 64

57. ISDN standards use function groups and _____ to describe the various components that can be utilized in making an ISDN connection.
a. equipment lists
b. schematics
c. reference points
d. schemas

58. What is the converter device that allows non-ISDN devices to operate on an ISDN network?
a. Terminal Adapter
b. Terminal Equipment 1
c. Terminal Equipment 2

- d. Network Termination 1
59. What is the device that supports ISDN standards and can be connected directly to an ISDN network connection?
- Terminal Adapter
 - Terminal Equipment 1
 - Terminal Equipment 2
 - Network Termination 1
60. What is the device that multiplexes and switches signals between various network devices at the customer site?
- Network Termination 2
 - Terminal Equipment 1
 - Terminal Equipment 2
 - Network Termination 1
61. What is the small connection box that is attached to ISDN BRI lines?
- Network Termination 2
 - Terminal Equipment 1
 - Terminal Equipment 2
 - Network Termination 1
62. What is the non-ISDN device, such as an analog phone or modem, which requires a TA in order to connect to an ISDN network?
- Terminal Adapter
 - Terminal Equipment 1
 - Terminal Equipment 2
 - Network Termination 1
63. A T1 line is a North American 24-channel digital supports data transmission of up to _____ Mbps.
- | | |
|----------|----------|
| a. 1.128 | c. 1.544 |
| b. 1.256 | d. 1.643 |
64. A T2 line is a North American, 96-channel digital line supports data transmission of up to _____ Mbps.
- | | |
|----------|----------|
| a. 2.986 | c. 3.304 |
| b. 3.152 | d. 6.312 |
65. A T3 line is a North American, 672-channel digital line supports data transmission of up to _____ Mbps.
- | | |
|-----------|-----------|
| a. 22.986 | c. 38.304 |
| b. 33.152 | d. 44.376 |
66. A T4 line is a North American, 4032-channel digital line supports data transmission of up to _____ Mbps.
- | | |
|------------|------------|
| a. 222.986 | c. 318.304 |
| b. 274.176 | d. 424.376 |
67. _____ is a pieces of equipment required to connect an ISDN router with an S/T interface to the telecommunications provider?

- a. PRI
- b. BRI
- c. TA
- d. NT1

CHAPTER 10

IP PROTOCOLS

10.1 About This Chapter

The Internet Protocol (IP) is the centre piece of the Internet and IP-suite of protocols. It established itself as the most widely-used data networking protocol. It provides an interface function on which the Internet is based. IP is used not only in end devices which access the Internet but also between the nodes of wide area data networks.

A good understanding of IP is necessary to continue on to TCP and UDP, because the IP is the component that handles the movement of datagrams across a network. Knowing how a datagram must be assembled and how it is moved through the networks helps you understand how the higher-level layers work with IP. For almost all protocols in the TCP/IP family, IP is the essential element that packages data and ensures that it is sent to its destination.

Although the IP version 4 was robust at the time of its publication in 1981, it did not anticipate several Internet advances. These advances are taken in consideration by IP version 6 which made many improvements on internet protocol to accommodate the development of the Internet. IP version 6 was referred to as IP the Next Generation (IPng).

Other protocols are necessary to handle error reporting, Multicasting and group managements. ICMP is an error-reporting system. It is an integral part of IP and must be included in every IP implementation. This provides for consistent, understandable error messages and signals across the different versions of IP and different operating systems.

Group membership on a single network is communicated between systems by the IGMP protocol. Multicast routers propagate group membership information using multicast routing protocols a standard IP router may support multicast routing, or multicast routing may be handled by a router dedicated to that purpose.

There are a lot of experimental applications on the Internet that take advantage of multicasting include audio and video conferencing applications, resource discovery tools, and shared whiteboards.

The Address Resolution Protocol (ARP) is designed to convert IP addresses to MAC addresses, while the Reverses Address Resolution Protocol (RARP) works in the opposite direction. Suppose that a user wants to transmit a packet to its destination.

This chapter describes how wide area networks can use the Internet Protocol. We will discuss in detail the two most important variations of the Internet protocol—version 4 (IPv4) and version 6 (IPv6). We shall cover the functions and describe the structure of an IP packet and the basic IP processing including input, forwarding, and output. Option processing and fragmentation and reassembly will be discussed. The construction of the IP header is important to many TCP/IP family protocol members, so you can use this knowledge in later chapters.

This chapter will also cover the basics of ICMP, IGMP, ARP, and RARP protocols, their fundamental operations and functions, their characteristics, and how their data units are built and transferred.

10.2 Learning Outcome

After this chapter, you should be able to:

1. Be familiar with the TCP/IP suite protocols.
2. Understand the necessity of using the Internet Protocol
3. Provide an overview of IPv4.
4. Provide an overview of IPv6.
5. Distinguish between IPv4 and IPv6 operations and capabilities.
6. Understand the basics of Internet Control Management Protocol (ICMP).
7. Understand the basics of Internet Group Management Protocol (IGMP).
8. Understand the importance and the basics of logical to physical address translation and vice versa.

10.3 TCP/IP Suite Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is one of today's most widely used networking protocols. A TCP/IP network is generally a heterogeneous network, this means that there are many different types of network computing devices attached.

The Internet Protocol (IP) had its roots in early military networks of the 1970s, but it's been within the past decade that IP has made its unstoppable conquest of the world's networks. Today, IP has established itself as the primary vehicle for our global system of electronic commerce, enabling a vast array of client/server and peer-to-peer computing applications. TCP/IP allowed for open communications to exist, LAN to LAN and LAN to WAN connectivity between multiple operating environments.

The TCP/IP became the main protocol in communication for many reasons such as:

1. The capability of the protocol to allow dissimilar systems to communicate through the network.
2. TCP could be layered on top of any datagram protocol, even the ones that are part of other protocol suites.
3. The protocol is an "open" protocol and anyone who wishes to implement it may do so freely.
4. Perhaps no other protocol designed to work above the Data Link and Physical OSI layers is as popular as TCP/IP. That's primarily because this global protocol suite has been used by and continually promulgated thousands of government and educational institutions worldwide.
5. The TCP/IP protocol combination offers a "connection-oriented reliable byte stream", sometimes called a "virtual circuit." TCP deals with datagram loss as well as potential datagram reordering and duplication to provide a degree of "reliability."
6. TCP/IP protocol runs independently of the data link and physical layer. At these layers the TCP/IP protocol can run on Ethernet, Token Ring, FDDI, serial line, X.25, etc. It

has been adapted to run over these protocols. TCP/IP was first used to interconnect computer systems through synchronous lines and high-speed local area networks. Today, it is used on any type of medium. This includes serial (asynchronous and synchronous) and high-speed networks such as FDDI, Ethernet, and token Ring.

Let's start with understanding the functions and protocols by studying their placement in the OSI model. In looking at Figure 10.1, we can see that there are distinct protocols that run at each layer of the OSI model, starting from the network layer to the application layer. The heart of the TCP/IP network protocol is at layers 3 and 4. The applications for this protocol (file transfer, mail, and terminal emulation) run at the application layer.



Protocol suite is a collection of protocols that work together as a group. Examples of protocol suites include the Internetwork Packet Exchange (IPX) and Sequenced Packet Exchange (SPX), the Internet's TCP/IP protocol suite and the AppleTalk and its related protocols.

TCP/IP is actually a family of protocols working together to provide a path that allows internet data communication. These protocols can be classified into three categories:

- Network Layer protocols
- Transport Layer protocols
- Applications protocols

We will discuss the network layer protocols in the following section, while the other protocols will be discussed in the other coming chapters.

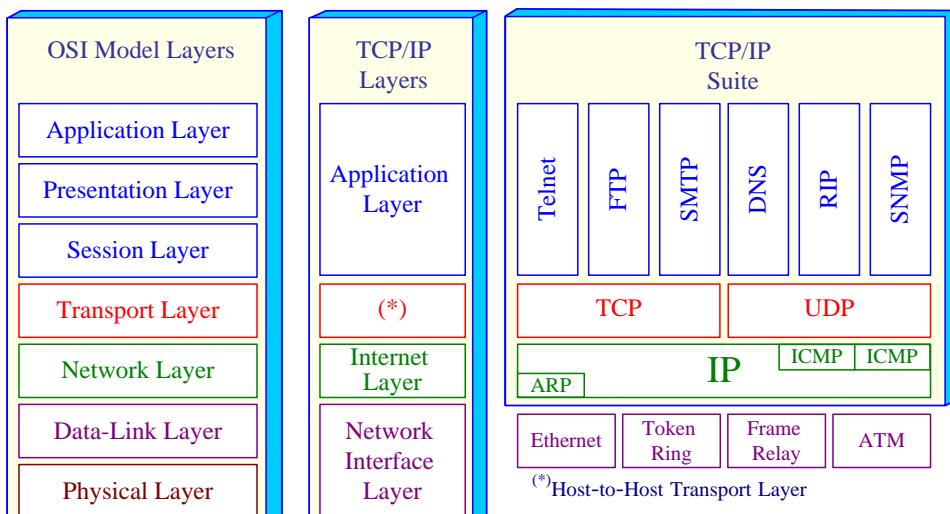


Figure 10.1: OSI and TCP/IP architectural Model

10.4 The Network layer Protocols

IP protocol is designed to transport data between any two arbitrary computers within the Internet, i.e., through many LANs.

A number of routers can appear between the sender and the recipient. The data is thereby transferred from one router to another. Each router resolves routing to the next router (next hop) independently. A hop means the next router or destination machine to which the data is being transferred.

The IP is a protocol enables the connection of individual networks into a worldwide Internet. It consists of several individual protocols:

- **The actual IP.**
- **Internet Control Message Protocol (ICMP)** that serves specifically to signal abnormal states.
- **Internet Group Management Protocol (IGMP)** that serves for local transportation of multicasts.
- **Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)** that serve as a translator from IP addresses to MAC addresses and vice versa. These protocols are often seen as independent protocols because their packets are not encapsulated in IP datagrams.

Whereas in the link protocol, each network interface has its MAC address, which for LANs consists of 6 bytes, in the IP protocol, each network interface has at least one IP address, which for IP version 4 is 4 bytes and for IP version 6 is 16 bytes.

The basic element used to build a **Wide Area Network (WAN)** is a router with which serves to transfer data packets between two network interfaces.

10.5 Internet Protocol (IP)

The ability to transfer data packets between the network interfaces of a router is called **forwarding**. The basic question is "*Why are two protocols needed? Why is one link protocol not enough?*" A link protocol only serves for transporting data within a LAN (i.e., for transporting to the nearest router, which *unpacks* the data from the link framework and *repacks* the data into a different link frame).

IP transports data between two remote computers on a WAN, while the link protocol only transports data frames to the next router. While each router throws away the envelope in which the data is wrapped on a link layer and creates a new one, an IP datagram (IP packet) is not changed by the router. The router must not change the IP datagram content. The exception are the **Time To Live (TTL)** entry in the IP v4 datagram header, hop limit entry in the IP v6 datagram header fragmentation, source routing, and so on, which we will talk about later.

While for link protocols, the basic unit of transferred data is called a **link frame**, in the IP the basic unit of transferred data is called an **IP datagram**.

Let's look at the situation illustrated in Figure 10.2 in which a sender from the **LAN 1** network sends an IP datagram to a recipient on the **LAN 2** network.

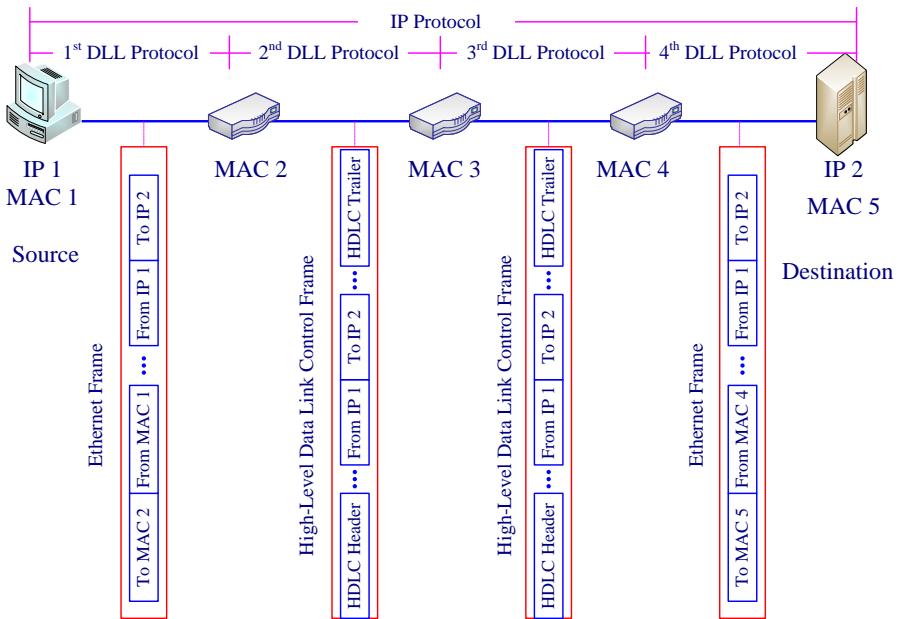


Figure 10.2: Sender sending IP datagram encapsulated into data link layer frame

The sender wants to send an IP datagram to the recipient with the IP address IP2. It creates an IP datagram, but to insert it into a local network, the sender must insert it into a data link frame which has the sender's MAC 4 address and the recipient's MAC 5 address. The data can only travel through the link protocol to router 1, which unpacks the IP datagram from the Ethernet frame and looks at the recipient's IP address. Depending on the recipient's IP address, it decides to which of its routers the IP datagram should be sent, i.e., on which link protocol the IP datagram should be encapsulated based on its routing table. In our example the routers have decided on the HDLC line. So the IP datagram is encapsulated into an HDLC frames.

Our IP datagram is transported via the HDLC protocol through the routers to the final router, which again unpacks the IP datagram from the HDLC envelope and, after wrapping it in a data link layer envelope, inserts it into the destination LAN. The IP datagram is again encapsulated into a data link layer frame which has the sender's MAC 4 address and the recipient's MAC 5 address.



High-level Data Link Control (HDLC) is a standard synchronous communication protocol at the data-link layer that is used for WAN synchronous serial connections over leased lines.

The main goal of IP is to provide interconnection of sub-networks to form an internet in order to pass data. IP is the primary layer 3 protocol (network layer) in the Internet suite. The IP protocol provides four main functions:

- Basic unit for data transfer
- Addressing

- Routing.
- Fragmentation of datagrams.

10.5.1 IP v4 Data Unit

The primary goals for IP are to provide the basic algorithm for transfer of data to and from a network. It provides a connectionless delivery service for the upper layer protocols. IP submits a formatted data packet to the destination station and does not expect a status responds. IP will add its control information, specific to the IP layer only, to the data received by the upper layer (transport layer). Once this is accomplished, it will inform the data-link layer that it has a message to send to the network. The unit of information that IP transfers is known as *datagram*. The IP protocol does not care what kind of data is in the packet. All it knows is that it must apply some control information, called an IP header, to the data received from the upper layer protocol and try to deliver it to some station on the network or internet. To understand the IP functionality, a brief look at the control information it adds (the IP header) to the packet as shown in Figure 10.3.

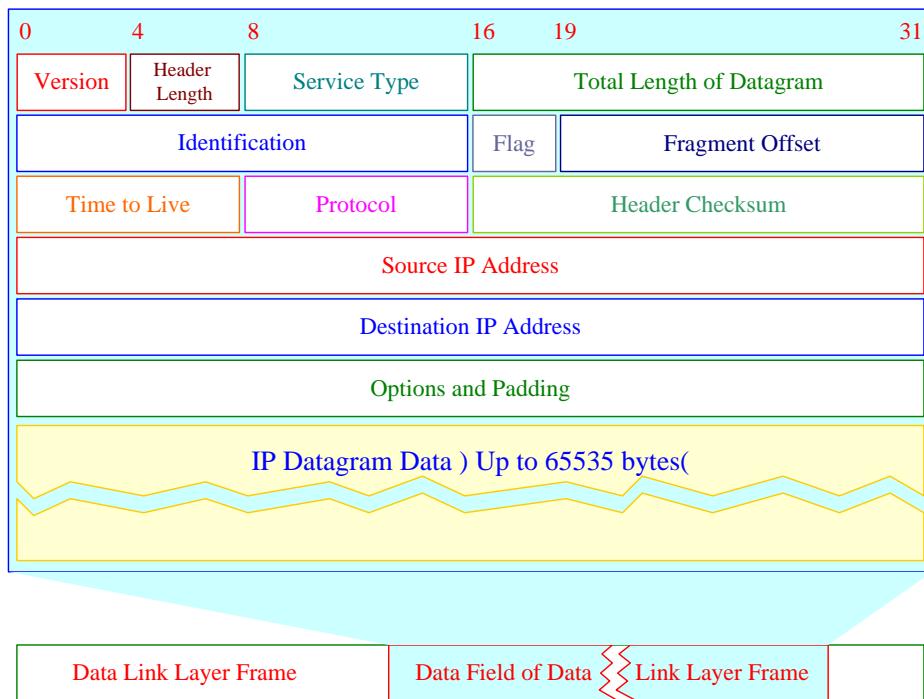


Figure 10.3: The IP v4 data unit encapsulated in data link layer frame

The IP packet is composed of several fields as shown in Figure 10.2. Instead of referring to the length of IP packets according to bits and bytes, the IP frame uses a length measurement of 32 bits referring to that grouping as a word. Consequently, any diagrams used to illustrate IP frame construction will divide the frame into 32-bit words.

- The first field is four bits in length and is called the version field. It contains the version number of the IP software used to create the datagram so that any device along the way that looks at the datagram will know what format it is in.

Decimal	Keyword	Version
0	Reserved	
1–3	Unassigned	
4	IP	Internet Protocol
5	ST	ST Datagram Mode
6	IPv6	
7	TP/IX	TP/IX: The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TCP and UDP over Bigger Addresses
10–14	Unassigned	
15	Reserved	

- A 4-bits IP header length follows (HLEN) gives the total length of the datagram header. The type of service field is 8-bits. It is divided into five distinct sections. The total length field appearing next as a 16-bits field contains the total length of the entire datagram in bytes. The IP datagram is virtually unlimited in size. It can be as large as 65,535 bytes, a size that few applications can even begin to approach. However, in the future, higher speed networks may suffer from this limitation.
- The next 16-bits field is the identification field containing a combination of an integer and the Internet source address. Together these create a unique ID for the datagram. This same information is used to keep the fragments of a datagram together.
- Once a datagram has been fragmented, the datagrams created from the original have virtually the same header. The only difference lies in the next field, the flags 4-bits field. Only the last two of the three bits in this field control fragmentation. The first of the two is called the "do not fragment" (DF) field. If this bit is on, then a datagram does not get fragmented. The next bit is the "more fragments" bit specifying whether or not the current fragment is the last fragment.
- The next eight bits comprise what is known as the "time to live" field. This field is a safety preventative to keep data packets from swarming around an Internet forever. Each datagram is given a lifetime length when first transmitted. This value is in seconds and gets decremented whenever the packet reaches a routing device. These devices must decrement the field by at least a value of one. Most record the amount of time that a packet has been held by the device and then decrement the field accordingly before transmitting the packet on out along a pathway.
- Next we have the protocol field that contains eight bits specifying what higher layer functions are being used. These higher layer protocols might be TCP/IP protocols or some other protocol type. Since the higher layer protocol is specified by this field we may have several protocols active at the receiver and this data would ensure the correct one used that packet.
- The header checksum follows. This 16-bit field assures the integrity of the IP header itself. Every time the datagram gets routed, the time to live field gets decremented. Consequently the checksum must be recalculated at each hop. The

source and destination fields are next. Each address is 32 bits in size and contains a unique IP address. The next to last 32-bits field is a variable length field known as the options field. It is used to allow additions to the header information such as strict source route, loose source route, record route, time stamps, security, or padding. Finally there is the data itself.

10.5.2 IP v6 Data Unit

IP version 4 did not anticipate several Internet advances including:

- The recent exponential growth of the Internet while the IP version 4 address space is limited to maximum 2^{32} addresses.
- The need for simpler configuration
- The requirement for security at the IP level
- The need for better support for real-time delivery of data, also called quality of service

IP version 6 has not only enlarged the IP address size from 4 to 16 bytes, but also offers a revamped view of the IP datagram. The IP version 6 datagram consists of a 40 byte-long Base header followed by various extensions.

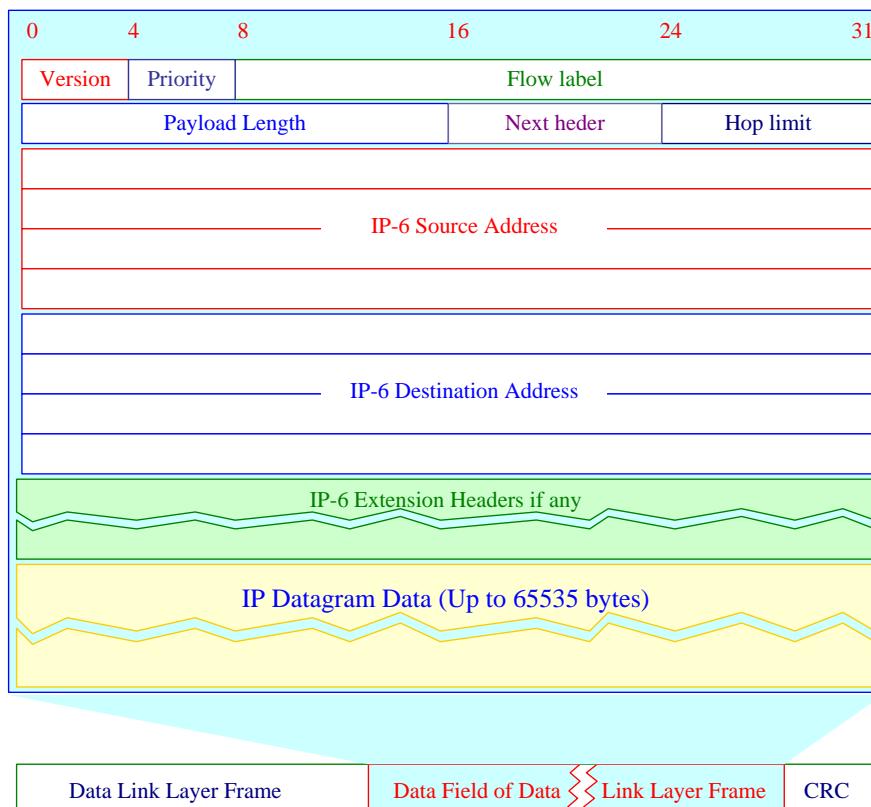


Figure 10.4: The IP data unit encapsulated in data link layer frame

- **Version:** The IP version field has the value 6 rather than the value 4 found in IP version 4.
- **Priority:** The priority field contains four bits describing the traffic class. This field prioritizes which datagrams are less important and can be discarded when the router is forced to discard certain IP datagrams.
- **Flow label:** This field along with the source address identifies individual data flows on the Internet. When datagrams reach the router, they are stored in the queue. The router simply searches its cache. If it finds no matches, it solves the routing task for that particular datagram as well. But the datagrams of the same flow are automatically sent to the interface selected for the first one. In the result the router dose not solve the same task for thousands of datagrams with the same result.
- **Payload length:** This field specifies the total length of the IP datagram excluding the Base header. The maximum length of the datagram transferred might be 65,535 bytes. It is also possible, however, to use a larger datagram from the next header of the router information that enables sending even larger datagrams (jumbograms).
- **Next header:** It specifies the next header type.
- **Hop limit:** TTL field in IP v4 is replaced with the hop limit. The hop limit is decreased every time the IP datagram passes through a router. When it reaches 0, the datagram is considered lost and, subsequently, discarded.



The hop is a logical distance between networks based on the number of routers that must be traversed by packets sent between them. For example, in TCP/IP internetworking, the number of hops between two hosts would be the number of routers that an Internet Protocol (IP) packet would have to pass through in order to reach its destination.

10.5.3 IP v 6 Extension Header Types

One of the more interesting changes to IP with version 6 is the concept of concatenated headers. This is accomplished using the next header field on the IPv6 header. Extension headers form chains. The chain contains only those headers that are necessary. The Next header field is followed by the header length field as it is shown in Figure 10.5. This field specifies the shift that is necessary in order to reach the next header. The Base header does not have a header length field since it is always 40 bytes long. The length is not used with Base and fragment headers since these headers are with known length (40 bytes for Base and 8bytes for fragment).



Figure 10.5: Extension header general structure

The types of extension headers are:

- **Hop-by-Hop Extension Header Options:** It is used to carry optional information that must be examined by every node along a packet's delivery path such as:
 - inform the router what it is expected to do with the datagram if the option is not recognized
 - indicate whether the router is allowed to change the option or not
 - indicate Jumbograms option, 4 bytes of the Jumbogram option provide for a maximum length of up to 4 GB.
- **Destination Extension Header Options:** This header is used to carry optional information that needs be examined only by a packet's destination node(s).
- **Routing Extension Header (Type 0) :** The Routing header is used by an IPv6 source to list one or more intermediate nodes to be “visited” on the way to a packet's destination. The lower part of the header contains the IP addresses of routers that the source wants to use for routing the datagram.
- **Fragment Extension Header:** The Fragment header is used by an IPv6 source to send packets larger than would fit in the path MTU to their destinations. Unlike IP version 4 only the operating system source is capable of fragmenting IP datagrams in IP version 6. Identification of the IP datagram is necessary for fragmenting so that the destination user knows which fragment is part of the same datagram. In IP version 6, the datagram identification is only contained in the next header; therefore, it is not a part of each IP datagram.
- **Authentication Extension Header:** It is used for ensuring data integrity and also enables the source user to authenticate data in order to verify that they have been sent. The datagram is protected against any potential modifications in the IP datagram along its delivery path such as by a hacker.
- **Encapsulating Security Payload Extension Header:** This header enables encryption of the transferred data. It must be the final Next header in the IP datagram if the subsequent data is encrypted, otherwise following headers will be unavailable for processing by the routers transmitting the IP datagram.

From end-to-end communication, these fields should be ignored by all stations that may receive them. These fields are generally built and consumed by the source and destination stations only. The exception is the hop-by-hop options field, which may be reviewed by routers in the path to the destination.



IPv6 and IPv4 nodes can peacefully coexist on a network using tunneling. This is a technology for sending data units from one network to another. Data unit from the source network are encapsulated in the Data unit format of a different protocol and then sent over the link, called a tunnel. Frames are Decapsulated at the destination network and forwarded to their destination node.

10.5.4 Fragmentation of Datagrams

In addition to internetwork routing, IP provides error reporting and fragmentation and reassembly of datagrams for transmission over networks with different maximum data unit sizes.

If a router receives an IP packet that is too large for the network to which the packet is being forwarded, IP fragments the original packet into smaller packets that fit on the downstream network. When the packets arrive at their final destination, IP on the destination host reassembles the fragments into the original payload. This process is referred to as *fragmentation and reassembly*.

Fragmentation can occur in environments that have a mix of networking technologies, such as Ethernet or Token Ring.

The fragmentation and reassembly work as follows:

- When an IP packet is sent by the source, it places a unique value in the Identification field.
- The IP packet is received at the router. The IP router notes that the size of data unit of the network onto which the packet is to be forwarded is smaller than the size of the IP packet.
- IP divides the original IP payload into fragments that fit on the next network. Each fragment is sent with its own IP header that contains:
 - The original Identification field identifying all fragments that belong together.
 - The More Fragments Flag indicating that other fragments follow. The More Fragments Flag is not set on the last fragment, because no other fragments follow it.
 - The Fragment Offset field indicating the position of the fragment relative to the original IP payload.

When the fragments are received by IP at the remote host, they are identified by the Identification field as belonging together. The Fragment Offset field is then used to reassemble the fragments into the original IP payload.

10.5.5 Mobile IP

Today's computers are smaller and more mobile than they used to be. They can now be easily carried around and be used anywhere. A lot of people generally want to read their e-mail and access their normal file systems wherever in the world they may be using their portable computers. A user may now disconnect his computer in the office and reconnect from another site within the same office or elsewhere.

In wireless connectivity the point of attachment may change even while the user is connected since the user may travel between Base stations of a wireless LAN or a mobile phone system.

Mobile IP allows a node to change its point of attachment to the Internet without needing to change its IP address. This is not simply a configuration simplification, but can facilitate continuous application-level connectivity as the node moves from point to point.

In most mobile IP cases, TCP cannot be used, as the congestion-control scheme would greatly reduce the throughput and the inherent delays and error bursts may result in a large number of retransmissions. Mobile IP faces many challenges such like mobility, registration, interoperability, connection reliability and security. We will cover the mobile IP issues in chapter 12.



A mobile node must be able to communicate with other nodes after changing its link-layer point of attachment to the Internet, yet without changing its IP address.

10.6 Internet Control Message Protocol

ICMP is a service protocol that is part of IP. It is used to signal abnormal events in networks built on the IP protocol. ICMP packets are wrapped into an IP datagram.

This protocol offers flow control and error-detection to the unreliable delivery method of IP. It provides a facility for routers and gateways on the net to communicate with a source if there is a problem. It also provides a mechanism for determining if a destination can not be reached.

Since IP is a connectionless, unreliable delivery service, allowing routers and hosts on an internet to operate independently, there are certain instances when errors will occur on the internet. Some of these errors could be: a packet is not routed to the destination network, the router is too congested to handle any more packets, or a host may not be found on the internet. There is no provision in IP to generate error messages or control messages. ICMP is the protocol that handles these instances for IP.

One of the most common uses for ICMP is the PING program. PING is an ICMP message that tries to locate other station on the internet to see if they are active or to see if a path is up. It can also be used to test intermediate networks along the way to the destination.



Ping stands for Packet Internet Groper, a TCP/IP utility that verifies the integrity of a network connection with a host on a TCP/IP network. The ping command is one of the first commands to use to troubleshoot communication problems on a TCP/IP network.

10.6.1 ICMP Data Unit

Figure 10.6 shows the packet format for ICMP. An ICMP packet header is always 8-bytes long. The first four bytes always have the same meaning, and the contents of the remaining four depend on the ICMP packet type.

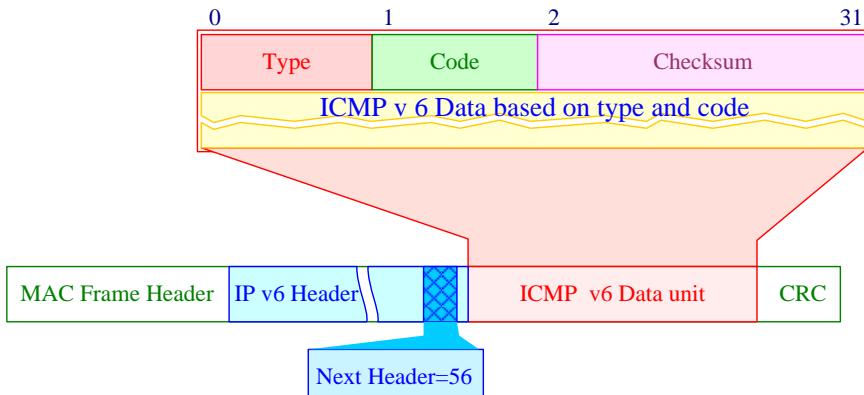


Figure 10.6: ICMP v4 Packet format and how it is encapsulated in the MAC frame



ICMP is a TCP/IP network layer protocol used by routers and TCP/IP hosts for building and maintaining routing tables, adjusting data flow rates, and reporting errors and control messages for TCP/IP network communication.

The first four bytes of the header always contain the message type, message code, and a 16-bit checksum. The message format depends on the value of the type field. The Message Type indicates which ICMP message is present, and the Message Code qualifies this for meaning specific to the type of message. Table 10.3 lists the ICMP message types.

Type	Message	Description
0	Echo Reply	Sent in direct response to an ICMP Echo Request message.
3	Destination Unreachable	An error message sent when a node cannot forward any IP datagram toward its destination.
4	Source Quench	Sent by a destination node to slow down the rate at which a source node sends IP datagrams.
5	Redirect	Used to tell a source node that there is a better first hop for it to use when trying to send IP datagrams to a given destination.
8	Echo	Sent by a node to probe the network for reachability to a particular destination.
9	Router Advertisement	Used by a router to tell hosts in its network that it exists and is ready for service.
10	Router Solicitation	Used by a host to discover which routers are available for use.

11	Time Exceeded	An error message generated by a router when it cannot forward an IP datagram because the TTL has expired.
12	Parameter Problem	An error sent by any node that discovers a problem with an IP datagram it has received.
13	Timestamp Request	Used to probe the network for the transmission and processing latency of messages to a given destination.
14	Timestamp Reply	Used in direct response to a Timestamp Request message.
15	Information Request	Used by a host to discover the subnet to which it is attached.
16	Information Reply	Used in direct response to an Information Request message.
17	Address Mask Request	Used by a host to discover the subnet mask for the network to which it is attached.
18	Address Mask Reply	Used in direct response to an Address Mask Request message.

Table 10.3: Summary of ICMP Message Types

10.6.2 ICMP Version 6 Protocol

IP v 6 uses an ICMP v 6 protocol. It offers different functionality than the previous version of ICMP. For example, while the IP v4 protocol uses ARP and RARP to translate IP addresses into link addresses and vice versa, ICMP v 6 deals with the translation of IP addresses into link addresses.

With regard to packet structure, the ICMP packet has a higher-layer protocol; thus, the Base header of the IP protocol as well as Next headers, if necessary.

The **ICMP type** field contains the message type (approximate classification of the message) and the **ICMP code** field specifies the detailed classification of the message.

ICMP message types are divided in two intervals:

- The 0 to 127 interval for error messages
- The 128 to 255 interval for informational messages

The function of the ICMP messages shown in Table 10.4 within the 0–129 interval is similar to the ICMP messages in the IP version 4 protocol. Therefore, it is worth taking a look at the remaining message types.

Type	Code	Description
1		Destination unreachable
	0	No route to destination
	1	Communication with destination administratively prohibited

	3	Address unreachable
	4	Port unreachable
2	0	Packet too big
3		Time exceeded
	0	Hop limit exceeded in transit
	1	Fragment reassembly time exceeded
4		Parameter Problem
	0	Erroneous header field encountered
	1	Unrecognized Next header
	2	Unrecognized IP version 6 option encountered
128	0	Echo request
129	0	Echo reply
133	0	Router solicitation
134	0	Router advertisement
135	0	Neighbor solicitation
136	0	Neighbor advertisement
137	0	Redirect message

Table 10.4: The function of the ICMP v6 messages

All control messages that were not used such as timestamp, timestamp reply, source quench, information request and reply are moved and most of these functions are incorporated into other protocols.

The format of the ICMPv6 header is the same format as ICMPv4. The type field indicates the type of the message. Its value determines the format of the remaining data. Error messages are identified as such by 0 or 0 in the high-order bit of their message Type field values. Thus, error messages have message Types from 0 to 127; informational messages have message Types from 128 to 255. The code field depends on the message type and further identifies the ICMP message.

ICMPv6 is not backwards compatible with ICMPv4. It uses the next-header function of IP and the next-header type of 56.



ICMP redirects can modify a router's routing table, so sometimes hackers try to subvert routers by issuing forged ICMP redirects in order to perform a denial of service attack.

10.7 Internet Group Management Protocol (IGMP)

IGMP is a TCP/IP network layer protocol used to exchange information on the status of membership in multicast groups between routers on the network. In other words, once a router becomes aware that there are hosts on a locally attached network that are members of a particular multicast group, it advertises this information to other routers on the internetwork so that multicast messages are forwarded to the appropriate routers.

Internet Group Management Protocol solves many problems associated with multicast addressing including:

- Starting and terminating groups.
- Choosing the group address.
- Adding new sender or receiver hosts to the group.
- Controlling how anyone join a group and send to, or receive from, that group.
- Controlling the group membership restriction and defining the responsibility for this.
- Do group members know the identities of the other group members as part of the network layer protocol?
- The manner the network routers interoperate with each other to deliver a multicast datagram to all group members.

As a result the simple host membership reporting protocol (IGMP) is the basic building block for multicasting. But what does multicasting and multicast group mean?

10.7.1 Multicasting and Multicast Group

Multicasting is a way to send a message to multiple recipients. Multicasting imposes less overhead in comparison with broadcasting on hosts that are not participating in the communication, so in many applications it is preferred to be used.

A number of emerging network applications requires the delivery of packets from one or more senders to a *group of receivers*. These applications include bulk data transfer, streaming continuous media, shared data applications, data feeds, and interactive gaming. For each of these applications, an extremely useful abstraction is the notion of a **multicast**: the sending of a packet from one sender to multiple receivers with a single "transmit" operation.

With multicast communication, we face two problems that are much more complicated than in the case of unicast:

- How to identify the receivers of a multicast datagram?
- How to address a datagram sent to these receivers?

If datagram will carry the IP addresses of all of the multiple recipients, the amount of addressing information in the datagram would swamp the amount of data actually carried in the datagram's payload field and requires that the sender knows the identities and addresses of all of the receivers.

Instead of carrying all addresses, a single "identifier" is used for the group of receivers and a copy of the datagram that is addressed to the group using this single "identifier" is delivered to all of the multicast receivers associated with that group. The multicast address is the single "identifier" that represents a group of receivers. In this case the **multicast group** is the group of receivers associated with this address. The multicast group abstraction is illustrated in Figure 10.7. Here, all hosts, labeled as members, are associated with the multicast group address of MCG address and will receive all datagrams addressed to that multicast address. The difficulty that we must still address is

the fact that each host has a unique IP unicast address that is completely independent of the address of the multicast group in which it is participating.

An *IP multicast group*, also known as a *host group*, is a set of hosts with an assigned multicast IP address. Members of the group still retain their own IP addresses, but also have the ability to absorb data that has been sent to the multicast address. Any system may belong to zero or more multicast groups. IP multicast traffic is sent to a single MAC address but processed by multiple IP hosts. A specific host listens on a specific IP multicast address and receives all packets to that IP address. The following are some of the additional aspects of IP multicasting:

- Host group membership is dynamic; hosts can join and leave the group at any time.
- A host group can be of any size.
- Members of a host group can span IP routers across multiple networks. This situation requires IP multicast support on the IP routers and the ability for hosts to register their group membership with local routers. Host registration is accomplished using IGMP.

A host can send traffic to an IP multicast address without belonging to the corresponding host group.

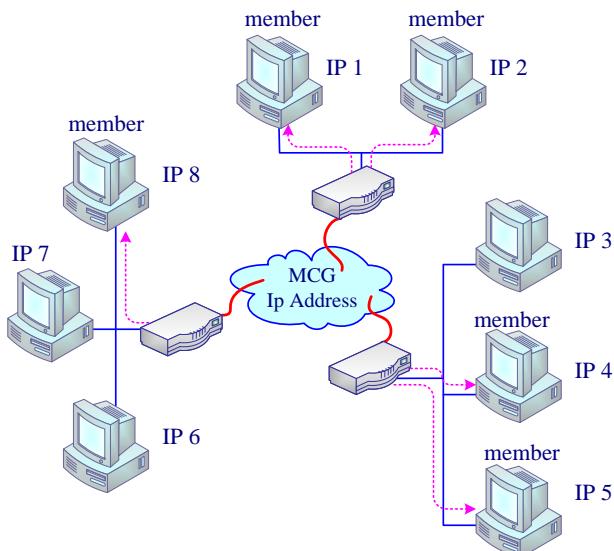


Figure 10.7: Illustration of the multicast group



Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the Internet.

10.7.2 IGMP Function

Like ICMP, IGMP is a service protocol for IP. IGMP packets are wrapped into IP datagrams as shown in Figure 10.8. It is used for forwarding multicasts. Hosts use the IGMP to report their group memberships to neighboring routers that support multicast routing. The reports are sent to the IP multicast address that belongs to the group that the host is joining.

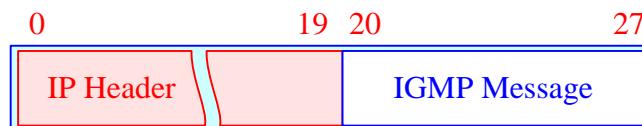


Figure 10.8: Encapsulation of an IGMP message within an IP datagram.

To ensure that their membership information is complete, the IGMP enables routers to poll hosts periodically, asking for reports of their current membership. The polls are sent to the all-hosts multicast IP address.

For a host to receive IP multicasts, an application must inform IP that it will receive multicasts at a specified IP multicast address. If the network technology supports hardware-based multicasting, the network interface is told to pass up packets for a specific IP multicast address. In the case of Ethernet, the network adapter is programmed to respond to a multicast MAC address corresponding to the specified IP multicast address.



Membership in a multicast group on a given interface is dynamic—it changes over time as processes join and leave the group.

Implied here is that a host identifies a group by the group address *and* the interface. A host must keep a table of all the groups that at least one process belongs to, and a reference count of the number of processes belonging to the group.

The Internet Group Management Protocol (IGMP) provides a dynamic service to registered individual hosts in a multicast group on a particular network. It is used for TCP/IP between a receiver and its immediate multicast-enabled routers reporting multicast group information. This protocol has several versions and is required on all machines that receive IP multicast.

10.7.3 IGMP Message

When a host wants to join a group, the group's multicast address receives an IGMP message stating the group membership. The local multicast router receives this message and constructs all routes by propagating the group membership information to other multicast routers throughout the network.

The IGMP packet format has several versions; Figure 10.9 shows three versions of this protocol.

- **Version:** 8 bits Field indicate the message type, which may be one of the following:

- 0x11: IP Membership query ("Are there any members on the LAN?")
- 0x12: IGMPv1 Membership Report
- 0x16: IGMPv2 Membership Report
- 0x17: IGMPv2 Leave Group

Hosts send IGMP membership reports corresponding to a particular multicast group, expressing an interest in joining that group.

- **Maximum Response Time (MRT):** 8 bits field is used only in router requests and specifies (in tenths of a second) the time that members of the group have to repeat their requests for membership in the group. In all other cases, the MTR field has a value of 0.
- **Checksum:** 16 bits field is calculated to control the errors that may have occurred in the header.
- **IP group address:** field is zero for a general request, and in all other cases, specifies the particular IP address of a multicast.

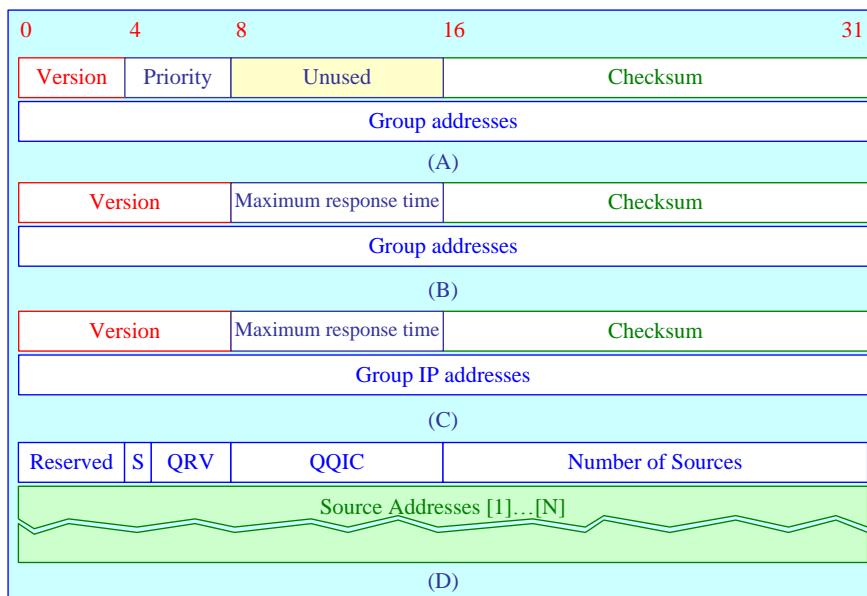


Figure 10.9: IGMP Data Unit, Version 1 (A), Version 2 (B), Version 3 (C), and the other common part included in all version's data unit

IGMP version 3 supports two modes:

- **Include mode:** In this mode a receiver announces the membership to a host group and provides a list of source addresses from which it wants to receive traffic.
- **Exclude mode:** With this mode, a receiver expresses the membership to a multicast group and provides a list of source addresses from which it does not want to receive traffic.

With the leave group message, hosts can report to the local multicast router that they intend to leave the group. If any remaining hosts are interested in receiving the traffic, the

router transmits a group-specific query. In this case, if the router receives no response, the router times out the group and stops forwarding the traffic.

Every IGMP data unit contains the following common fields:

- **Resv:** The Resv field is set to 0 and is reserved for future development.
- **S flag:** This is one bit field to suppress router-side processing.
- **QRV:** three bits field indicates the querier's robustness variable.
- **QQIC:** 8 bits field indicates the querier's query interval code.
- **N:** 16 bits field shows the number of sources
- **Source Address [i]:** provides a vector of N individual IP addresses.

10.7.4 IGMP Reports and Queries

IGMP messages are used by multicast routers to keep track of group membership on each of the router's physically attached networks. The following rules apply.

1. A host sends an IGMP report when the first process joins a group. If multiple processes on a given host join the same group, only one report is sent, the first time a process joins that group. This report is sent out the same interface on which the process joined the group.
2. A host does not send a report when processes leave a group, even when the last process leaves a group. The host knows that there are no members in a given group, so when it receives the next query (next step), it won't report the group.
3. A multicast router sends an IGMP query at regular intervals to see if any hosts still have processes belonging to any groups. The router must send one query out each interface. The group address in the query is 0 since the router expects one response from a host for every group that contains one or more members on that host.
4. A host responds to an IGMP query by sending one IGMP report for each group that still contains at least one process.

Using these queries and reports, a multicast router keeps a table of which of its interfaces have one or more hosts in a multicast group.



Due to the dynamic nature of the IPv6 and its Neighbor Discovery protocols (routers and hosts), IGMP functions were moved into the ICMP protocol suite. When a node initializes in an IPv6 environment, it must immediately join the all-nodes multicast address on that interface, as well as the solicited-node multicast address corresponding to each of the IP addresses assigned to the interface.

10.8 Address Resolution Protocol

Address resolution provides a mapping between the two different forms of addresses: 32-bit IP addresses and whatever type of address the data link uses.

ARP provides a dynamic mapping from an IP address to the corresponding hardware address. We use the term *dynamic* since it happens automatically and is normally not a concern of either the application user or the system administrator.

Address Resolution Protocol (ARP) functions as a translator between IP addresses and Physical addresses. Every Internet host and router on a LAN has an ARP module. To motivate ARP, consider the network shown in Figure 10.10. In this figure each node has an IP address and each node's adapter has a Physical address (MAC address). Now suppose that the node A with IP address (IP a) wants to send an IP datagram to node C with IP address (IP c). To accomplish this task, the sending node must give its adapter not only the IP datagram but also the Physical address for node c (MAC c).

 ARP is plug-and-play, that is, a node's ARP table gets built automatically, and it doesn't have to be configured by a systems administrator. And if a node is disconnected from the LAN, its entry is eventually deleted from the table.

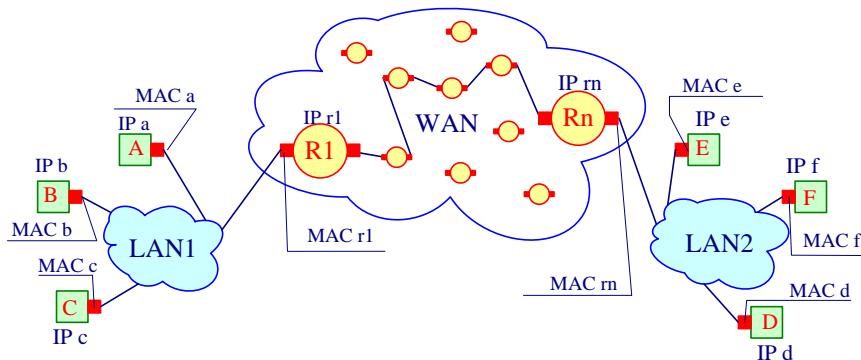


Figure 10.10: Each node on a LAN has an IP address, and each node's adapter has a Physical address.

When passed the IP datagram and the Physical address, the sending node's adapter can construct a data link layer frame and broadcast the frame into the LAN. The ARP module in each node has a table in its RAM called an ARP table. This table contains the mappings of IP addresses to Physical addresses.

Sending node needs to obtain the Physical address of the destination node, given the IP address of that node. This task is easy if the destination node has an entry in the sending node's ARP table.

IP address	Physical address	TTL
IP b	MAC b	13:45:00
IP c	MAC c	13:52:00

Table 10.5: A possible ARP table in node A

 Each host has exactly one IP address and one adapter, while each router has an IP address for *each* of its interfaces. Each router interface also has its own ARP module (in the router) and its own adapter. Of course, each adapter in the network has its own Physical address.

But what if the destination node does not currently have an entry in the ARP table? In particular, suppose node A wants to send a datagram to node D. In this case, the sending node uses the ARP protocol to resolve the address.

- First, the sending node constructs a special packet called an **ARP packet**. An ARP packet has several fields, including the sending and receiving IP and Physical addresses. The purpose of the ARP query packet is to query all the other nodes on the LAN to determine the Physical address corresponding to the IP address that is being resolved.
- Returning to the example, node A passes an ARP query packet to the adapter along with an indication that the adapter should send the packet to the LAN broadcast address, namely, FF-FF-FFFF-FF-FF. The adapter encapsulates the ARP packet in a data link frame, uses the broadcast address for the frame's destination address, and transmits the frame into the LAN.
- The frame containing the ARP query is received by all the other adapters on the LAN, and each adapter passes the ARP packet within the frame up to its parent node.
- Each node that receives the ARP packet checks to see if its IP address matches the destination IP address in the ARP packet. The one node with a match sends back to the querying node a response ARP packet with the desired mapping.
- The querying node A can then update its ARP table and send its IP datagram.

But now let's look at the more complicated situation when a destination node is *off the LAN* for example from A to D.

- The sending host passes the datagram to its adapter, as usual.
- In order for a datagram to go from A to D on LAN 2, the datagram must first be sent to the router R1 interface (IP r1). Thus, the appropriate Physical address for the frame is the address of the adapter for router interface (IP r1), namely, (MAC r1).
- A acquire the Physical address of (IP r1) by using ARP, of course. Once the sending adapter has this Physical address, it creates a frame and sends the frame into LAN 1.
- The router adapter on LAN 1 sees that the data link frame is addressed to it, and therefore passes the frame to the network layer of the router.
- The router now has to determine the correct interface on which the datagram is to be forwarded. The routing table tells the router that the datagram is to be forwarded router interface Rn with IP address (IP rn).
- This interface then passes the datagram to its adapter, which encapsulates the datagram in a new frame and sends the frame into LAN 2.
- This time, the destination Physical address of the frame is indeed the Physical address of the ultimate destination.
- Rn obtain the required destination Physical address (MAC d) using ARP in the same way as discussed in the situation of sending a packet to a node in the same LAN.
- Rn then responds to R1 with a packet containing (MAC d).
- R1 in turn responds to A with (MAC d).

 The query ARP message is sent within a broadcast frame whereas the response ARP message is sent within a standard frame.

10.8.1 ARP Packet Format

The ARP packet format is shown in Figure 10.11. ARP packets are wrapped directly into the MAC frame, i.e., they are not preceded by an IP header. The ARP protocol is in fact independent of the IP protocol. That is why even other protocols that have nothing in common with the TCP/IP protocol family can use it.

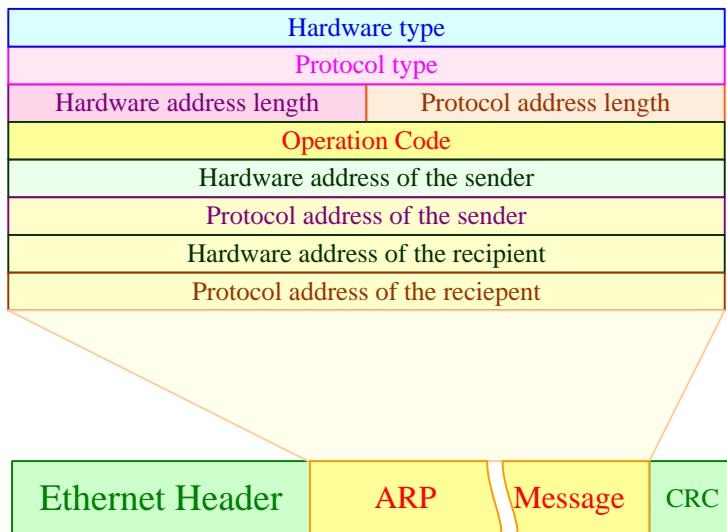


Figure 10.11: ARP packet format

- **Hardware type:** This field specifies the link protocol used on the LAN.
- **Protocol type:** specifies the network's protocol type.
- **Hardware address of the sender:** field sets the length of a link address and the sender. By default, HS=6.
- **Protocol address of the sender:** field sets the length of a network address. By default PS=4.
- **Operation code field:** specifies which operation is running. The ARP request has a value of 1 and the ARP reply has a value of 2. This field is also defined for the reverse translation (RARP protocol), where the RARP request uses a value of 3 and the RARP reply has a value of 4.
- **Hardware Address Length:** Hardware address length is the length of each hardware address in the datagram, given in bytes.
- **Protocol Address Length:** Protocol address length is the length of the protocol address in the datagram, given in bytes.
- **Recipient Hardware Address:** The recipient hardware address is the hardware address of the recipient device.

- **Recipient IP Address:** The recipient IP address is the IP address of the recipient device.

 Neighbor discovery (ND) is introduced; it uses ICMPv6 messages in order to determine link-layer addresses for neighbors attached to the same link, to find routers, to keep track of which neighbors are reachable, and to detect changed link-layer addresses.

10.9 Reverse Address Resolution Protocol (RARP)

This protocol can be used to obtain an IP address from the host's hardware address, when a network station knows its MAC address but does not know its IP address. Obviously a RARP server is required for this technique to be used.

RARP is suited to diskless hosts on a small network and fails to provide a useful service with larger networks due to its use of broadcasting to communicate with the server, as routers do not forward these packets.

RARP uses the ARP packet format and does not involve IP; therefore, this packet cannot be routed. This protocol has been in use for some time, but there are other protocols that do a better job.

 There are other protocols for address assignment that do a better translation such as BOOTP and DHCP because they can be forwarded over a router with a little assistance from the router.

The packet format for a RARP packet is the same as for ARP. The only difference is that the field that will be filled in will be the sender's physical address. The IP address fields will be empty. A RARP server will receive this packet, fill in the IP address fields, and reply to the sender—the opposite of the ARP process.

RARP suffers from the same problems as static addressing. As a RARP server maintains a data base relating hardware addresses to IP addresses, any change in the IP addressing scheme requires a manual update of the data base. Thus, maintenance of a large RARP data base can be expensive.

10.10 Quick Review

- ❖ TCP/IP became the main suite protocol in communication. It is a family of protocols working together to provide a path that allows internet data communication.
- ❖ The main goal of IP is to provide interconnection of sub-networks to form an internet in order to pass data. It provides a connectionless delivery service for the upper layer protocols.

- ❖ IP is a best-effort datagram service that provides the delivery mechanism for all other Internet protocols. The standard IP header is 20 bytes long, but may be followed by up to 40 bytes of options. IP can split large datagrams into fragments to be transmitted and reassembles the fragments at the final destination.
- ❖ In addition to internetwork routing, IP provides error reporting and fragmentation and reassembly of datagrams for transmission over networks with different maximum data unit sizes.
- ❖ IP version 6 has not only enlarged the IP address size from 4 to 16 bytes, but also offers a revamped view of the IP datagram. One of the more interesting changes to IP with version 6 is the concept of concatenated headers. Extension headers form chains. The chain contains only those headers that are necessary. IPv6 and IPv4 nodes can peacefully coexist on a network using tunneling.
- ❖ Today's computers can now be easily carried around and used anywhere. In wireless connectivity the point of attachment may change, Mobile IP allows a node to change its point of attachment to the Internet without needing to change its IP address.
- ❖ ICMP is a service protocol that is part of IP. It is used to signal abnormal events in networks built on the IP protocol. ICMP packets are wrapped into an IP datagram. This protocol offers flow control and error-detection to the unreliable delivery method of IP. One of the most common uses for ICMP is the PING program. ICMPv6 is not backwards compatible with ICMPv4.
- ❖ IP v 6 uses an ICMP v 6 protocol. It offers different functionality than the previous version of ICMP. For example, ICMP v 6 deals with the translation of IP addresses into link addresses.
- ❖ Internet Group Management Protocol solves many problems associated with multicast addressing
- ❖ IGMP communicates IP multicast membership information between hosts and routers on a single network. IGMP membership reports are generated when an interface joins a group, and on demand when multicast routers issue an IGMP report query message.
- ❖ Multicast routers share the IGMP information they collect with each other to route multicast datagrams toward remote members of the multicast destination group.
- ❖ ARP provides the dynamic mapping between IP addresses and hardware addresses. It functions as a translator between IP addresses and Physical addresses.
- ❖ RARP can be used to obtain an IP address from the host's hardware address, when a network station knows its MAC address but does not know its IP address. It is suited to diskless hosts on a small network.

10.11 Self Test Questions

A- Answer the following questions

1. Why has TCP/IP become the main protocol in communication?
2. What does forwarding mean?
3. What are the main goal and the main functions of IP?

4. Explain the structure of IP v4 data unit.
5. Explain the structure of IP v6 data unit.
6. Why is fragmentation process sometimes necessary?
7. What is the importance of TTL field?
8. What are the differences between IP v4 and IP v6 data units?
9. What is the role of Next header field?
10. What are the types of extension headers?
11. What are the most common uses of ICMP?
12. Explain how ICMP data unit can be encapsulated in the MAC frame.
13. How does the ICMP used by IP v4 differ from ICMP used by IP v6?
14. What is the IP multicast group?
15. List some problems that can be solved by IGMP.
16. How does the IGMP used by IP v4 differ from IGMP used by IP v6?
17. What is the purpose of using the ARP?
18. How does ARP work?
19. Explain the ARP packet format.
20. Where is RARP applicable?

B- Identify the choice that best completes the statement or answers the question.

1. _____ of the IP header elements is never modified during the IP fragmentation process.
 - a. The Identification field
 - b. The More Fragments bit
 - c. The Fragment Offset field
 - d. The TimeTo Live field
2. A IP address identify_____
 - a. A network
 - b. A computer
 - c. A network interface adapter
 - d. A network and a network interface adapter
3. _____ makes the trace route utility possible.

a. Version	c. Type of Service
b. Identification	d. Time to Live
4. _____ is responsible for responding to a ping request.

a. ICMP	c. TCP
b. ARP	d. UDP
5. _____ resolves IP addresses to MAC addresses.

a. DNS	c. ARP
b. NetBIOS	d. TCP
6. _____ is the process when a Network layer protocol subdivides the segments it receives from the Transport layer into smaller packets.

a. segmentation	c. sequencing
b. fragmentation	d. reassembly
7. Which of the following is TRUE statement about TCP/IP?
 - a. TCP/IP comprises several subprotocols

- b. TCP/IP comprises only one protocol
 - c. TCP/IP has been replaced by ARP
 - d. TCP/IP has been replaced by IPX/SPX
8. TCP/IP has grown extremely popular because of _____
- a. It is expensive
 - b. It cannot be routable
 - c. Its private nature made its programming code secure
 - d. Its open nature
9. Internet Protocol (IP) belongs to _____ layer of the OSI Model.
- a. Network
 - b. Data Link
 - c. Transport
 - d. Application
10. _____ allows TCP/IP to internetwork.
- a. TCP
 - b. UDP
 - c. IP
 - d. ARP
11. A packet is also known as _____ in the context of TCP/IP.
- a. TCP/IP flow
 - b. IP segment
 - c. IP packet stream
 - d. IP datagram
12. What can be said about IP? (Choose 2)
- a. IP is a reliable protocol
 - b. IP is an unreliable protocol
 - c. IP is a connection-oriented protocol
 - d. IP is a connectionless protocol
13. What can be said about IP?
- a. IP is a reliable protocol
 - b. IP operates at the Data Link layer of the OSI Model
 - c. IP contains a header checksum field
 - d. IP checksum also verifies the integrity of the message
14. _____ field of the IP datagram identifies the number of 4-byte (or 32-bit) blocks in the IP header.
- a. Flags
 - b. Internet Header Length
 - c. Total length
 - d. Version
15. _____ field of the IP datagram informs routers what level of precedence they should apply when processing the incoming packet.
- a. Differentiated Services
 - b. Options
 - c. Total Length
 - d. Flags
16. _____ field of the IP datagram identifies the message to which a datagram belongs and enables the receiving node to reassemble fragmented messages.
- a. Fragment Offset
 - b. Internet Header Length
 - c. Identification
 - d. Flags
17. _____ field of the IP datagram indicates the maximum time that a datagram can remain on the network before it is discarded.
- a. Flags
 - b. TTL
 - c. Total Length
 - d. Options
18. What is the network layer protocol that reports on the success or failure of data delivery?
- a. IP
 - b. TCP

31. What is the layer in the TCP/IP model that handles software, or logical, addressing?
 - a. Internetwork
 - b. Application
 - c. Transport
 - d. Network Interface
 32. What is the protocol that resolves IP addresses to MAC addresses for source hosts that knows the IP addresses of the destination host but not the MAC address?
 - a. ICMP
 - b. ARP
 - c. RARP
 - d. CARP
 33. How many different groups of IP addresses exist on the Internet?
 - a. Three
 - b. Four
 - c. Five
 - d. Six
 34. What is the name of tables of the MAC and IP addresses of other devices on the network that many network devices maintain?
 - a. reference
 - b. destination
 - c. ARP
 - d. APR
 35. The device that discovers its own IP address in the IP header of the ARP request packet reads the rest of the packet and returns an ARP _____.
 - a. confirm
 - b. ACK
 - c. answer
 - d. reply
 36. _____ can route between autonomous systems.
 - a. IGRP
 - b. RIP
 - c. BGP
 - d. IGP

CHAPTER 11

NETWORK LAYER ADDRESSING

11.1 About This Chapter

Fundamental to the operation of IP are the addresses that are used to identify the senders and receivers of individual messages. There is information on how the address space is subdivided for ease of management and routing.

Networks that are directly connected to the Internet must have their IP addresses assigned by the Internet Network Information Center (InterNIC) or some other authority. Businesses usually obtain these addresses through their local Internet service provider (ISP). However, firewall and proxy server combinations, which are popular on today's networks, hide a network's IP addresses from other hosts on the Internet.

An IPv4 address has 32 bits and is familiar. An IPv6 address has 128 bits and looks wild. Extending the address space was one of the driving reasons to develop IPv6, along with optimization of routing tables, especially on the Internet.

The ability to manipulate IP addresses is affected not only on customer sites but within the global Internet as well. Class-oriented IP addresses are still used in the customer environment, whereas Classless IP addressing is used in the Internet itself. Customers are free to use whichever mechanism efficiently uses the address that is assigned to them. These routing update protocols distribute the subnet mask for each entry in its table.

Subnetting is the process of partitioning a single TCP/IP network into a number of separate networks called subnets. These subnets are then joined using routers. Advantages of subnetting a network include the reducing network congestion by limiting the range of broadcasts using routers, enabling different networking architectures to be joined and sufficiently use the IP addressing space.

If a network using one of the private address ranges is connected to the Internet, Network Address Translation (NAT) must be applied to map local addresses into publicly visible addresses. This process provides a useful security barrier since no information about the internal addressing or routing structure will leak out into the wider Internet. Further, the private network can exist with only a small number of public addresses because only a few of the hosts in the private network will be attached to the Internet at any time.

This chapter will help you become familiar with the old IPv4 addresses and addressing scheme and will also explain how IPv4 and how IPv6 addressing works and why they have been designed the way they are. We will also cover the necessity, the principles and the methods of subnetting. Then we will provide the concepts of Network Address Translation (NAT).

11.2 Learning Outcome

After this chapter, you should be able to:

1. Understand the necessity of IP Addressing.
2. Be familiar with IPv4 classes.
3. Distinguish between public and private IP addresses and their applications.
4. Be familiar with the types of addresses that are used by the IPv4 and IP v6 protocols.
5. Describe the IPv4 and IP v6 addressing format.
6. Make a comparison between IPv4 and IP v6 addressing schemes capabilities.
7. Understand the necessity, the principles and the methods of subnetting.
8. Be familiar with the concepts of Network Address Translation (NAT).
9. Understand how the address space is managed.

11.3 IP Addressing

Addressing allows IP to communicate between hosts on a network or on an internet. Every device that exchanges information using the TCP/IP protocol suite needs a unique IP address.

Internet Protocol (IP) handles networking aspects and establishes routes for packets. The network layer, in fact, handles the method of assigning addresses to packets and determines how they should be forwarded from one end point to another.

The Internet Protocol produces a header for packets. An IP header contains the IP addresses of a source node and a destination node, respectively. There are two IP addressing schemes. The first is the current 32-bit IPv4 addressing scheme used on TCP/IP networks worldwide. Because the number of hosts connecting to the Internet has skyrocketed in recent years, unique IP addresses are gradually running out. A new scheme called IPv6 has been proposed. However, with most corporate networks now hiding their networks behind firewalls, the pressure to move to IPv6 has lessened because companies can choose any network ID they want for their private network. The only assigned IP addresses they require from their Internet service provider (ISP) are for the public interfaces on their firewall machines. At this point, IPv4 seems to be firmly entrenched in the networking world for at least the next few years. Before going far, it is important to distinguish between the types of addresses in general.



Note that always a unique IP address must always be assigned to each host as client or server or router interface (input port or output port).

11.3.1 Types of Addresses

While existing network is functioning it may use one of the following types of addresses:

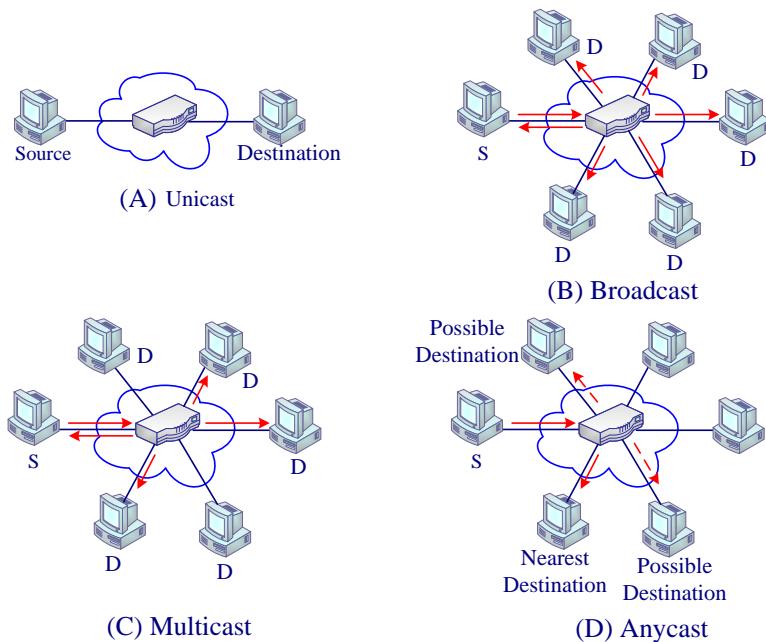


Figure 11.1: There are four types of communication supported by the Internet protocol

- **Unicast address:** An identifier for a single interface. A unique address delivered to a single destination. Unicasting take place when a certain source sends packets over the network containing a special address that instructs a certain destination on the network to accept and process the packet (see Figure 11.1 (A)).
- **Broadcast address:** A broadcast address is exactly an address that is received by every host on the subnet. Broadcasts take place when broadcast packets are sent over the network. These packets contain a special address that instructs every station on the network to accept and process the packet (see Figure 11.1 (B)). Broadcasts are typically used for announcements by network services, for resolving names into addresses, and for other similar functions. Broadcasts are usually not an efficient use of network bandwidth, since only one or a few network stations might actually be interested in the information being broadcast. For this reason, directed packets are used for most network communication, which involves targeting a packet directly for the intended station. All other stations ignore the directed packet. Broad casting in a certain network conditions can cause broadcast storms that can bring down a network. Because of that in most networks, with IPv6, the broadcast address is not used anymore; IPv6 uses multicast addresses instead.
- **Anycast:** an address assigned from unicasts address space referring to a group of network interfaces typically belonging to different nodes. An IP datagram containing the anycast type of address will be delivered to one of the interfaces listed (the “nearest” one, according to the routing protocols’ measure of distance) (see Figure 11.1 (D)).
- **Multicast:** A group addresses for a set of interfaces, typically belonging to different nodes. A packet sent to a multicast address is delivered to all interfaces

identified by that address. Multicasting is an alternative to broadcasting, which involves a form of limited broadcast to a select group of hosts (see Figure 11.1 (C)).

11.3.1 IPv4 Addressing Scheme

The addressing scheme used to identify hosts is called the 32-bit IP address. This is also known as a protocol address. There are two types of network addressing schemes used with IP:

Classless: The full address range can be used without regard to bit reservation for classes. This type of addressing scheme is primarily not used in direct host assignment. The scheme is directly applied to the routing tables of the Internet and ISPs.

Classful: The original segmentation of the 32-bit address into specific classes denoting networks and hosts.

Most of us will never have to worry about the classless range of IP addressing, for it is used on the Internet itself and not on customer networks. It provides an easy method with which to reduce the routing tables and allow large address ranges to be provided to the ISPs. The first part of this section will deal with classful, since it started first and is continuing to be used on many networks. It is confusing, but keeps reading.

In order to provide the flexibility required to support different size networks, the IP address space divided into five different address classes, Class A, Class B, Class C, Class D, and Class E. This is often referred to as "classful" addressing because the address space is split into five predefined classes, groupings, or categories. Each class fixes the boundary between the network-prefix and the host-number at a different point within the 32-bit address. The formats of the fundamental address classes are illustrated in Figure 11.2.

11.3.2 IP Classes

One of the fundamental features of classful IP addressing is that each address contains a self-encoding key that identifies the dividing point between the network-prefix and the host-number. For example, if the first two bits of an IP address are 1-0, the dividing point falls between the 15th and 16th bits. This simplified the routing system during the early years of the Internet because the original routing protocols did not supply a "deciphering key" or "mask" with each route to identify the length of the network-prefix.

11.3.3.1 Class A Networks

Each Class A network address has an 8-bit network-prefix with the highest order bit set to 0 and a seven-bit network number, followed by a 24-bit host-number. A maximum of 126 ($2^7 - 2$) networks can be defined. The calculation requires that the 2 is subtracted because the network 0.0.0.0 is reserved for use as the default route and the network **127.0.0.0** has been reserved for the "**loopback**" function. Each of class A networks supports a maximum of 16,777,214 ($2^{24} - 2$) hosts per network. The host calculation requires that 2 is subtracted because the all-0s ("this network") and all-1s ("broadcast") host-numbers may not be assigned to individual hosts.

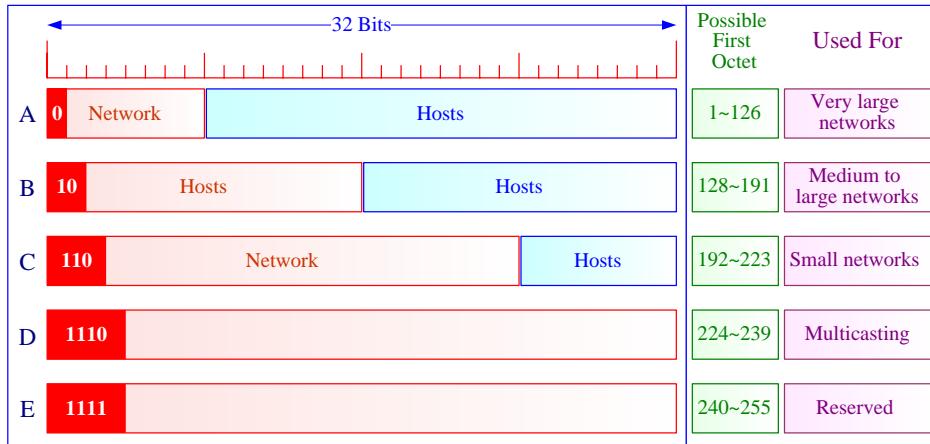


Figure 11.2: Principle Classful IP Address Formats

Since the address block contains 2^{31} (2,147,483,648) individual addresses and the IPv4 address space contains a maximum of 2^{32} (4,294,967,296) addresses, the address space is 50% of the total IPv4 unicast address space.

Today, Class A addresses are being handed out through a different method involving Internet Service Providers that uses the Classless InterDomain Routing Protocol (CIDR). When you get a Class A address, you will be told to subnet it appropriately (you will be told what the subnet address is). You will not get the whole Class A address.

11.3.3.2 Class B Networks

Class B addresses is the most requested and is the easiest to assign subnets to. Each Class B network address has a 16-bit network-prefix with the two highest order bits set to 1-0 and a 14-bit network number, followed by a 16-bit host-number. Class B networks are now referred to as "/16s" since they have a 16-bit network-prefix.

A maximum of 16,384 (2^{14}) networks can be defined with up to 65,534 ($2^{16} - 2$) hosts per network. Since the entire address block contains 2^{30} (1,073,741,824) addresses, it represents 25% of the total IPv4 unicast address space.

Because of this class provides the largest range of addressing possibilities it is exhausted and its addresses are no longer given out unless companies have handed in their Class B addresses.

11.3.3.3 Class C Networks

Class C addresses are the most commonly assigned by the NIC. Class B addresses have been exhausted. Each Class C network address has a 24-bit network-prefix with the

three highest order bits set to 1-1-0 and a 21-bit network number, followed by an 8-bit host-number. Class C networks are now referred to as "/24s" since they have a 24-bit network-prefix.

A maximum of 2,097,152 (2^{21}) networks can be defined with up to 254 ($2^8 - 2$) hosts per network. Since the entire address block contains 2^{29} (536,870,912) addresses, it represents 12.5% (or 1/8th) of the total IPv4 unicast address space.

This class allows lots of networks with a fewer hosts per network. A Class C address is identified by the first 3 bits of the first field. If the first and second bits are 1s and the third bit is a 0, this will identify a Class C address. This allows 2,097,152 network numbers, each capable of supporting 254 hosts (all 0s and all 1s are still reserved no matter what type of routing and addressing you are using).

11.3.3.4 Class D

The value of the four highest bits of the first byte is 1110. The class D addresses are not divided into a network and a computer addresses, because they are multicast addresses themselves.

Class D addresses are special addresses and are known as multicast addresses. This address type is assigned to a group of network work-stations and is not assigned to represent a unique address. They are used to send IP datagrams to a group, but not all of the hosts on a network. These addresses have many uses, including being used for addressing router update messages as well as delivering data, video, and voice over IP. D space address consist 6.25 percent of total IPv4 addressing space.

11.3.3.5 Class E

Class E always starts with 1111; it consists of the rest of the addressing space and is reserved for future use and network experiments. Most networking equipment will reject addresses from the Class E space.



Using a multicast address is a more efficient way of “broadcasting” rather than using a broadcast address, for the upper-layer software will not always be interrupted every time a broadcast packet arrives. Multicasting is different than broadcasting. With broadcasting, every station that receives the broadcast packet will automatically pass it to the upper-layer software without regard to the address. Every station that receives a broadcast packet must process it.

11.3.4 Dotted-Decimal Notation

To make Internet addresses easier for human users to read and write, IP addresses are often expressed as four decimal numbers, each separated by a dot. This format is called "dotted-decimal notation."

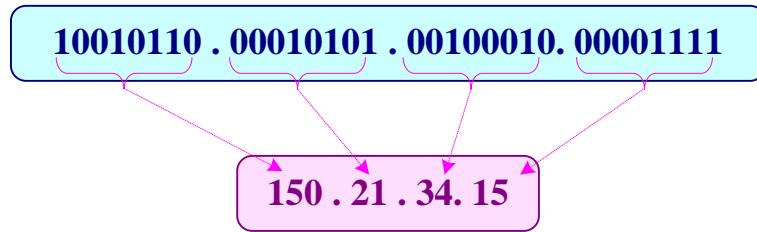


Figure 11.3: Dotted-Decimal Notation

Dotted-decimal notation divides the 32-bit Internet address into four 8-bit (byte) fields and specifies the value of each field independently as a decimal number with the fields separated by dots. Figure 11.3 shows how a typical /16 (Class B) Internet address can be expressed in dotted decimal notation.

Figure 11.2 displays the range of dotted-decimal values that can be assigned to the first octet for each of the three principle address classes. The other octets can be represented by any positive decimal number less than 256.

11.4 Subnet and Subnet Mask

The Internet Address Classes A, B, and C, were designed to accommodate three different scales of IP internetwork, where the 32 bits of the IP address are apportioned between network IDs and host IDs depending on how many networks and hosts per network are needed. However, consider the class A network ID, which has the possibility of over 16 million hosts on the same network. All the hosts on the same physical network bounded by IP routers share the same broadcast traffic; they are in the same broadcast domain. It is not practical to have 16 million nodes in the same broadcast domain. The result is that most of the 16 million host addresses are not assignable and are wasted. Even a class B network with 65 thousand hosts is impractical.

In an effort to create smaller broadcast domains and to better utilize the bits in the host ID, an IP network can be subdivided into smaller networks, each bounded by an IP router and assigned a new *subnetted network ID*, which is a subset of the original class-based network ID.

This creates *subnets*, subdivisions of an IP network, each with its own unique subnetted network ID. Subnetted network IDs are created by using bits from the host ID portion of the original class-based network ID.

Consider the example in Figure 11.4. The class B network of 174.38.0.0 can have up to 65,534 nodes. This is far too many nodes and, in fact, the current network is becoming saturated with broadcast traffic. The subnetting of network 174.38.0.0 should be done in such a way so that it does not impact or require the reconfiguration of the rest of the IP internetwork.

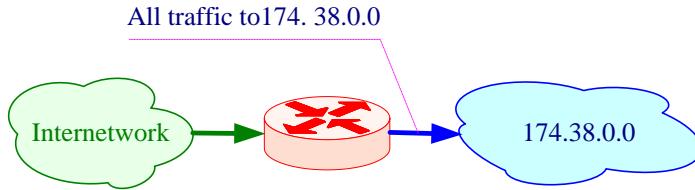


Figure 11.4: Network 174.38.0.0 before subnetting

Network 174.38.0.0 is subnetted by utilizing the first 8 host bits (the third octet) for the new subnetted network ID. When 174.38.0.0 is subnetted, as shown in Figure 11.5, separate networks with their own subnetted network IDs (174.38.1.0, 174.38.2.0, 174.38.3.0) are created. The router is aware of the separate subnetted network IDs and will route IP packets to the appropriate subnet.

Note that the rest of the IP internetwork still regards all the nodes on the three subnets as being on network 174.38.0.0. The other routers in the IP internetwork are unaware of the subnetting being done on network 174.38.0.0, and therefore require no reconfiguration.

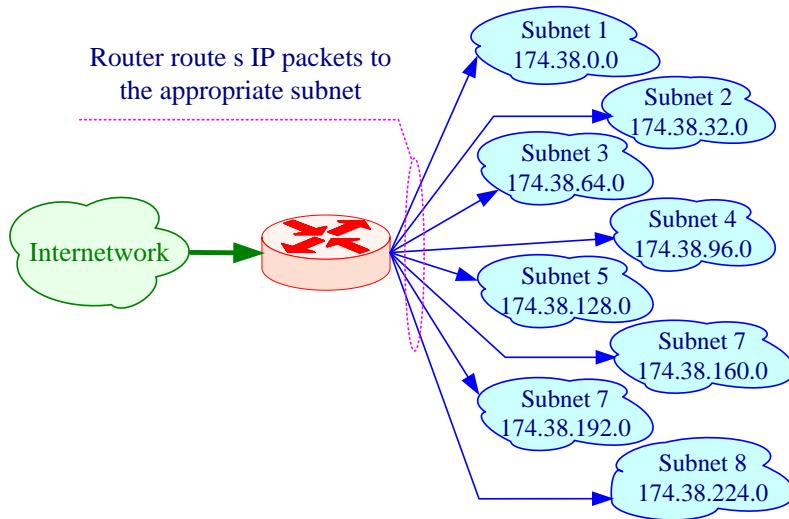


Figure 11.5: Network 174.38.0.0 after subnetting

A key element of subnetting is still missing. How does the router that is subdividing network 174.38.0.0 know how the network is being subdivided and which subnets are available on which router interfaces? To give the IP nodes this new level of awareness, the router must be told exactly how to discern the new subnetted network ID regardless of Internet Address Classes. To tell an IP node exactly how to extract a network ID, either class-based or subnetted, a *subnet mask* is used.



The subnetting is the process of partitioning a single TCP/IP network into a number of separate networks called subnets. These subnets are then joined using routers.

11.4.1 Subnet Masks

The computer has no way of knowing what kind of IP address you have, this means that there has to be some way of letting your software extract the network ID from the IP address. To do this, you can use subnet masks. Typically a subnet mask will look like this: 255.255.255.0. This tells us quickly that we are using a Class C IP address as the first three 255's tell us that these individual numbers cannot change. The zero tells us that this is the only digit that we can use, so it has to be a Class C IP address.

If we had an IP address of 128.10.11.23 and a subnet mask of 255.255.0.0 then we can quickly see that we have a Class B IP address. The whole point of a subnet mask is to tell the computer which is the Network ID and which is the host ID.

The bits of the subnet mask are defined as:

- All bits that correspond to the network ID are set to 1.
- All bits that correspond to the host ID are set to 0.

A default subnet mask is based on the IP address classes and is used on TCP/IP networks that are not divided into subnets. Table 11.1 lists the default subnet masks using the dotted decimal notation for the subnet mask.

IP Class	Bits for Subnet Mask	Subnet Mask	Net .Prefix
Class A	1111111.0000000.0000000.0000000	255.0.0.0	/8
Class B	1111111.1111111.0000000.0000000	255.255.0.0	/16
Class C	1111111.1111111.1111111.0000000	255.255.255.0	/24

Table 11.1: Default subnet masks

Since the network ID bits must be always chosen in a contiguous fashion from the high-order bits, a shorthand way of expressing a subnet mask is to denote the number of bits that define the network ID as a network prefix using the network prefix notation: /<# of bits>. Table 11.1 lists the default subnet masks using the network prefix notation for the subnet mask.

Custom subnet masks are those that differ from the above default subnet masks when doing subnetting. For example, 138.96.58.0 is an 8-bit subnetted class B network ID. Eight bits of the class-based host ID are being used to express subnetted network IDs. The subnet mask uses a total of 24 bits (255.255.255.0) to define the subnetted network ID.

Subnet masks can be expressed using prefix notation. For example, the class B network ID 187.96.0.0 with the subnet mask of 255.255.255.0 would be expressed in network prefix notation as 187.96.0.0/26.

And for an 8-bit subnetted class B network ID 138.96.58.0 the subnet mask uses a total of 24 bits to define the subnetted network ID. The subnetted network ID and its corresponding subnet mask are then expressed in network prefix notation as: 138.96.58.0/24

Since all hosts on the same network must use the same network ID, the ID must be defined by the same subnet mask. For example, 138.23.0.0/16 is not the same network ID as 138.23.0.0/24. The network ID 138.23.0.0/16 implies a range of valid host IP addresses from 138.23.0.1 to 138.23.255.254. The network ID 138.23.0.0/24 implies a range of valid host IP addresses from 138.23.0.1 to 138.23.0.254. Clearly, these network IDs do not represent the same range of IP addresses.

11.4.2 Determining the network ID

To extract the network ID from an arbitrary IP address using an arbitrary subnet mask, IP uses a mathematical operation called a logical AND comparison. In an AND comparison, the result of two items being compared is true only when both items being compared are true, otherwise, the result is false. Applying this principle to bits, the result is 1 when both bits being compared are 1; otherwise, the result is 0.

IP takes the 32-bit IP address and logically *ANDs* it with the 32-bit subnet mask. This operation is known as a ***bit-wise logical AND***. The result of the bit-wise logical AND comparison of the IP address and the subnet mask is the network ID.

To find the network ID of the IP node 172.61.16.119 with a subnet mask of 255.255.240.0, as given in Table 13.5.

Host IP	172.61.16.119	10101100 00111101 00010000 01110111
Mask	255.255.240.0	11111111 11111111 11110000 00000000
bit-wise logical <i>AND</i> operation		
Network ID	172.61.16.0	11001111 00111101 00010000 00000000

Figure 11.6: Bit-wise logical AND to obtain network ID

To obtain the result, turn both numbers into their binary equivalents and line them up. Then perform the AND operation on each bit and write down the result as in Figure 11.6.

Host IP	172.61.16.119	11001111 00111101 00010000 01110111
NOT Mask	0.0.0.255	00000000 00000000 00001111 11111111
bit-wise logical <i>AND</i> operation		
Host ID	0.0.0.119	00000000 00000000 00000000 01110111

Figure 11.7: Bit-wise logical AND to obtain host ID

The result of the bit-wise logical AND of the 32 bits of the IP address and the subnet mask is the network ID 172.61.16.0.

To obtain the host ID we can perform the NOT operation on the mask then perform the bit-wise logical AND operation of the 32 bits of the IP address and the NOT subnet mask and write down the result as in Figure 11.7.

11.4.3 Subnetting

While the conceptual notion of subnetting by utilizing host bits is straightforward, the actual mechanics of subnetting are a bit more complicated. Subnetting is a three-step procedure:

1. Determine the number of host bits to be used for the subnetting.
2. Enumerate the new subnetted network IDs.
3. Enumerate the IP addresses for each new subnetted network ID.

11.4.3.1 Determining the Number of Host Bits

The number of host bits being used for subnetting determines the possible number of subnets and hosts per subnet. Before you choose how many host bits, you should have a good idea of the number of subnets and hosts you will have in the future. Using more bits for the subnet mask than required will save you the time of reassigning IP addresses in the future.

Follow these guidelines to determine the number of host bits to use for subnetting:

1. Determine how many subnets you need now and will need in the future. Each physical network is a subnet. WAN connections may also count as subnets depending on whether your routers support unnumbered connections.
2. Use additional bits for the subnet mask if:
 - You will never require as many hosts per subnet as allowed by the remaining bits.
 - The number of subnets will increase in the future, requiring additional host bits.

To determine the desired subnetting scheme, you will start with an existing network ID to be subnetted. The network ID to be subnetted can be a class-based network ID, a subnetted network ID, or a supernet. The existing network ID will contain a series of network ID bits, which are fixed, and a series of host ID bits, which are variable. Based on your requirements for the number of subnets and the number of hosts per subnet, you will choose a specific number of host bits to be used for the subnetting. The following formula used to calculate number of host per subnet:

$$H = 2^n - 2$$

Where,

H = number of host per subnet

n = number of bits reserve for hosts per subnet

Host address 0's reserved for subnet address, and when all 1's it reserved for broadcasting.

Example 11.1:

class	A
-------	---

number of subnets	9-16
Number of host bits to be masked	4
subnet mask (binary)	11111111 . <u>1111</u> 0000 . 00000000 . 00000000
subnet mask (decimal)	255.240.0.0
Number of hosts per subnet	$2^{20} - 2 = 1,048,574$

Example 11.2:

class	A
number of subnets	131,073-262,144
Number of host bits to be masked	18
subnet mask (binary)	11111111 . <u>11111111</u> . <u>11111111</u> . <u>11</u> 000000
subnet mask (decimal)	255.255.255.192
Number of hosts per subnet	$2^6 - 2 = 62$

Example 11.3:

class	B
number of subnets	17-32
Number of host bits to be masked	5
subnet mask (binary)	11111111 . 11111111 . <u>11111</u> 000 . 00000000
subnet mask (decimal)	255.255.248.0
Number of hosts per subnet	$2^{11} - 2 = 2046$

Example 11.4:

class	C
number of subnets	5-8
Number of host bits to be masked	3
subnet mask (binary)	11111111 . 11111111 . 1111 <u>111</u> . <u>111</u> 00000
subnet mask (decimal)	255.255.255.224
Number of hosts per subnet	$2^5 - 2 = 30$

11.4.3.2 Enumerating Subnetted Network IDs

Based on the number of host bits you use for your subnetting, you must list the new subnetted network IDs.

1. Based on n , the number of host bits chosen for subnetting, create a 3-column table with 2^n entries. The first column is the subnet number (starting with 1), the second column is the binary representation of the subnetted network ID, and the third column is the dotted decimal representation of the subnetted network ID.

2. For each binary representation, the bits of the network ID being subnetted are fixed to their appropriate values and the remaining host bits are set to all 0s. The host bits chosen for subnetting will vary.
3. In the first table entry, set the subnet bits to all 0s and convert to dotted decimal notation. The original network ID is subnetted with its new subnet mask.
4. In the next table entry, increase the value within the subnet bits.
5. Convert the binary result to dotted decimal notation.
6. Repeat steps 3 and 4 until the table is complete.

Example 11.5:

Construct a table for available subnetted network ID if the network ID is 192.168.0.0 and the Subnet Mask is 255.255.224.0

- Binary representation for 224 = 11100000
- Based on $n = 3$, construct a table with $8 (= 2^3)$ entries. The entry for subnet 1 is the all-0s subnet. Additional entries in the table are successive increments of the subnet bits, as shown in Table 11.2. The host bits used for subnetting are underlined. The “/ #” where # indicates number of masked bits used to calculate subnet mask.

Subnet	Binary Representation	Subnetted Network ID
1	11000000.10101000. <u>00000000</u> .00000000	192.168.0.0/19
2	11000000.10101000. <u>00100000</u> .00000000	192.168.32.0/19
3	11000000.10101000. <u>01000000</u> .00000000	192.168.64.0/19
4	11000000.10101000. <u>01100000</u> .00000000	192.168.96.0/19
5	11000000.10101000. <u>10000000</u> .00000000	192.168.128.0/19
6	11000000.10101000. <u>10100000</u> .00000000	192.168.160.0/19
7	11000000.10101000. <u>11000000</u> .00000000	192.168.192.0/19
8	11000000.10101000. <u>11100000</u> .00000000	192.168.224.0/19

Table 11.2: Subnetting technique for network ID 192.168.0.0

11.4.3.2 IP Addresses for Each Subnetted Network ID

Based on the enumeration of the subnetted network IDs, we must now list the valid IP addresses for new subnetted network IDs. To list each IP address individually would be too tedious. Instead, we will enumerate the IP addresses for each subnetted network ID by defining the range of IP addresses (the first and the last) for each subnetted network ID.

1. Based on n , the number of host bits chosen for subnetting, create a 3-column table with 2^n entries. Alternately, add two columns to the previous table used for enumerating the subnetted network IDs. The first column is the subnet number (starting with 1), the second column is the binary representation of the first and last IP address for the subnetted network ID, and the third column is the dotted decimal representation of the first and last IP address of the subnetted network ID.
2. For each binary representation, the first IP address is the address where all the host bits are set to 0 except for the last host bit. The last IP address is the address where all the host bits are set to 1 except for the last host bit.
3. Convert the binary representation to dotted decimal notation.

4. Repeat steps 2 and 3 until the table is complete.

Example 11.6:

Construct a range of IP addresses table for the 3-bit subnetting of 192.168.0.0
The range of IP addresses is shown in Table 11.3. The bits used for subnetting are underlined.

Subnet	Binary Representation	Range of IP Addresses
1	11000000.10101000. <u>000</u> 00000.00000001 – 11000000.10101000. <u>000</u> 11111.11111110	192.168.0.1 - 192.168.31.254
2	11000000.10101000. <u>001</u> 00000.00000001 – 11000000.10101000. <u>001</u> 11111.11111110	192.168.32.1 - 192.168.63.254
3	11000000.10101000. <u>010</u> 00000.00000001 – 11000000.10101000. <u>010</u> 11111.11111110	- 192.168.64.1 - 192.168.95.254
4	11000000.10101000. <u>011</u> 00000.00000001 – 11000000.10101000. <u>011</u> 11111.11111110	- 192.168.96.1 - 192.168.127.254
5	11000000.10101000. <u>100</u> 00000.00000001 – 11000000.10101000. <u>100</u> 11111.11111110	- 192.168.128.1 - 192.168.159.254
6	11000000.10101000. <u>101</u> 00000.00000001 – 11000000.10101000. <u>101</u> 11111.11111110	- 192.168.160.1 - 192.168.191.254
7	11000000.10101000. <u>110</u> 00000.00000001 – 11000000.10101000. <u>110</u> 11111.11111110	- 192.168.192.1 - 192.168.223.254
8	11000000.10101000. <u>111</u> 00000.00000001 – 11000000.10101000. <u>111</u> 11111.11111110	- 192.168.224.1 - 192.168.255.254

Table 11.3: Binary enumeration of IP addresses

Combining the above two Tables (11.2 and 11.3) we construct the following general Table 11.4 which represented in dotted decimal format. Note that IP address with 1's usually used for broadcasting.

Subnet	Subnetted Network ID	Subnet Mask	Range of IP Addresses	Broadcasting
1	192.168.0.0	255.255.224.0	192.168.0.1 - 192.168.31.254	192.168.31.255
2	192.168.32.0	255.255.224.0	192.168.32.1 - 192.168.63.254	192.168.63.255
3	192.168.64.0	255.255.224.0	192.168.64.1 - 192.168.95.254	192.168.95.255
4	192.168.96.0	255.255.224.0	192.168.96.1 - 192.168.127.254	192.168.127.255
5	192.168.128.0	255.255.224.0	192.168.128.1 - 192.168.159.254	192.168.159.255
6	192.168.160.0	255.255.224.0	192.168.160.1 - 192.168.191.254	192.168.191.255

7	192.168.192.0	255.255.224.0	192.168.192.1 - 192.168.223.254	192.168.223.255
8	192.168.224.0	255.255.224.0	192.168.224.1 - 192.168.255.254	192.168.255.255

Table 11.4: General IP addresses

Example 11.7

Design an IP addresses for fifteen subnets with up to 2,000 hosts of the network ID 135.41.0.0

To achieve a requirement of 15 subnets with approximately 2,000 hosts, a 4-bit subnetting of the subnetted network ID of produces 16 subnets. To produce 2000 hosts, 11-bits are needed. The first bit in the in the third octane is masked. This setup will be as the following:

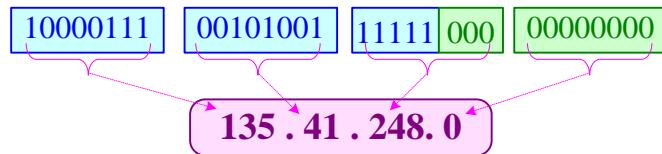


Table 11.5 illustrates Subnets with up to 2,046 hosts

Subnet	Subnetted Network ID	Subnet Mask	Range of IP Addresses	Broadcasting
1	135.41.128.0	255.255.248.0	135.41.128.1 - 135.41.135.254	135.41.135.255
2	135.41.136.0	255.255.248.0	135.41.136.1 - 135.41.143.254	135.41.143.255
3	135.41.144.0	255.255.248.0	135.41.144.1 - 135.41.151.254	135.41.151.255
4	135.41.152.0	255.255.248.0	135.41.152.1 - 135.41.159.254	135.41.159.255
5	135.41.160.0	255.255.248.0	135.41.160.1 - 135.41.167.254	192.168.167.255
6	135.41.168.0	255.255.248.0	135.41.168.1 - 135.41.175.254	192.168.175.255
7	135.41.176.0	255.255.248.0	135.41.176.1 - 135.41.183.254	192.168.183.255

8	135.41.184.0	255.255.248.0	135.41.184.1 - 135.41.191.25 4	192.168.191.255
9	135.41.192.0	255.255.248.0	135.41.192.1 - 135.41.199.25 4	135.41.199.255
10	135.41.200.0	255.255.248.0	135.41.200.1 - 135.41.207.25 4	135.41.207.255
11	135.41.208.0	255.255.248.0	135.41.208.1 - 135.41.215.25 4	135.41.215.255
12	135.41.216.0	255.255.248.0	135.41.216.1 - 135.41.223.25 4	135.41.223.255
13	135.41.224.0	255.255.248.0	135.41.224.1 - 135.41.231.25 4	192.168.231.255
14	135.41.232.0	255.255.248.0	135.41.232.1 - 135.41.239.25 4	192.168.239.255
15	135.41.240.0	255.255.248.0	135.41.240.1 - 135.41.247.25 4	192.168.247.255

Table 11.5: Subnets with up to 2,046 hosts

Example 11.8

Design an IP addresses for 8 subnets with up to 250 hosts of the network ID 135.41.0.0

To achieve a requirement of 8 subnets with up to 250 hosts, a 3-bit subnetting of subnetted network ID of 135.41.248.0/21 is done, producing 8 subnets and allowing up to 254 hosts per subnet. All 8 subnetted network IDs (135.41.248.0/24 to 135.41.255.0/24) are chosen as the network IDs, which fulfills the requirement. Table 11.6 illustrates 8 subnets with 254 hosts.

Subnet	Subnetted Network ID	Subnet Mask	Range of IP Addresses	Broadcasting
1	135.41.248.0	255.255.255.0	135.41.248.1 - 135.41.248.254	135.41.248.255
2	135.41.249.0	255.255.255.0	135.41.249.1 - 135.41.249.254	135.41.249.255
3	135.41.250.0	255.255.255.0	135.41.250.1 - 135.41.250.254	135.41.250.255
4	135.41.251.0	255.255.255.0	135.41.251.1 - 135.41.251.254	135.41.251.255
5	135.41.252.0	255.255.255.0	135.41.252.1 - 135.41.252.254	192.168.252.255

6	135.41.253.0	255.255.255.0	135.41.253.1 - 135.41.253.254	192.168.253.255
7	135.41.254.0	255.255.255.0	135.41.254.1 - 135.41.254.254	192.168.254.255
8	135.41.255.0	255.255.255.0	135.41.255.1 - 135.41.255.254	192.168.255.255

Table 11.6: Subnets with up to 254 hosts



Advantages of subnetting a network include the following:

- ❖ Reducing network congestion by limiting the range of broadcasts using routers
- ❖ Enabling different networking architectures to be joined.

11.5 Public and Private Addresses

If your intranet is not connected to the Internet, any IP addressing can be deployed. If direct (routed) or indirect (proxy or translator) connectivity to the Internet is desired, then there are two types of addresses employed on the Internet, public addresses and private addresses.

11.5.1 Public Addresses

Public addresses are assigned by Internet Assigned Numbers Authority (IANA) and consist of class-based network IDs that are guaranteed to be globally unique to the Internet.

When the public addresses are assigned, routes are programmed into the routers of the Internet so that traffic to the assigned public addresses can reach their locations. Traffic to destination public addresses is reachable on the Internet.

For example, when an organization is assigned a network ID and subnet mask, that {network ID, subnet mask} pair also exists as a route in the routers of the Internet. IP packets are routed to the proper destination.

11.5.2 Private Addresses

Each IP node requires an IP address that is globally unique to the IP internetwork. In the case of the Internet, each IP node on a network connected to the Internet requires an IP address that is globally unique to the Internet. As the Internet grew, organizations connecting to the Internet required a public address for each node on their intranets. This requirement placed a huge demand on the pool of available public addresses.

When analyzing the addressing needs of organizations, the designers of the Internet noted that, for many organizations, most of the hosts on the organization's intranet did not require direct connectivity to Internet hosts. Those hosts that did require a specific set of Internet services, such as the World Wide Web access and e-mail, typically access the

Internet services through application layer gateways, such as proxy servers and e-mail servers. The result is that most organizations only required a small amount of public addresses for those nodes (such as proxies, routers, firewalls, and translators) that were directly connected to the Internet.

For the hosts within the organization that do not require direct access to the Internet, IP addresses that do not duplicate already-assigned public addresses are required. To solve this addressing problem, the Internet designers reserved a portion of the IP address space and named this space the *private address space*. An IP address in the private address space is never assigned as a public address. IP addresses within the private address space are known as *private addresses*. Because the public and private address spaces do not overlap, private addresses never duplicate public addresses.

The private address space is defined by the following three address blocks:

- **10.0.0.0/8:** The 10.0.0.0/8 private network is a class A network ID that allows the following range of valid IP addresses: 10.0.0.1 to 10.255.255.254. The 10.0.0.0/8 private network has 24 host bits which can be used for any subnetting scheme within the private organization.
- **172.16.0.0/12:** The 172.16.0.0/12 private network can be interpreted either as a block of 16 class B network IDs or as a 20-bit assignable address space (20 host bits) which can be used for any subnetting scheme within the private organization. The 172.16.0.0/12 private network allows the following range of valid IP addresses: 172.16.0.1 to 172.31.255.254.
- **192.168.0.0/16:** The 192.168.0.0/16 private network can be interpreted either as a block of 256 class C network IDs or as a 16-bit assignable address space (16 host bits), which can be used for any subnetting scheme within the private organization. The 192.168.0.0/16 private network allows the following range of valid IP addresses: 192.168.0.1 to 192.168.255.254.

Address Range	Subnet
10.0.0.0 to 10.255.255.255	10.0.0.0/8
172.16.0.0 to 172.31.255.255	172.16.0.0/12
192.168.0.0 to 192.168.255.255	192.168.0.0/16

Table 11.7: Addresses Reserved for Use on Private Networks

Some groups of addresses are reserved for use in private networks and are never exposed to the wider Internet. The ranges appear to be random and have historic reasons for their values, but note that there is one address range chosen from each of Class A, B, and C. They are shown in Table 11.7. Of course, in a genuinely private network any addresses could be used, but it is a good exercise in self-discipline to use the allocated ranges.

11.6 Network Address Translation (NAT)

In many organizations using private addresses the private address space is reused, helping to prevent the depletion of public addresses.

Since the IP addresses in the private address space will never be assigned by the IANA as public addresses, there will never exist routes in the Internet routers for private

addresses. Traffic to destination private addresses is not reachable on the Internet. Therefore, Internet traffic from a host that has a private address must either send its requests to an application layer gateway (such as a proxy server), which has a valid public address, or have its private address translated into a valid public address by a *network address translator* (NAT) before it is sent on the Internet.

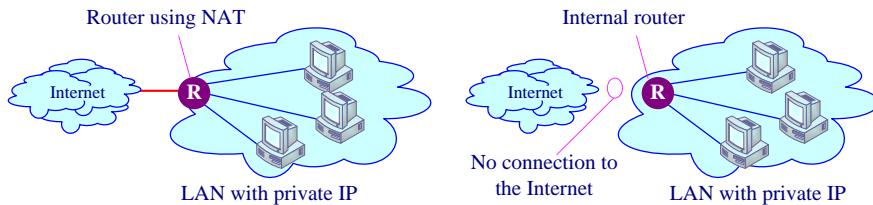


Figure 11.8: LANs with and without intent to connect to the Internet

 The proxy server is a computer that can act on the behalf of other computers to request content from the Internet or an intranet. It acts as secure gateway to the Internet for client computers.

Private LANs may have or don't have intent to connect to the Internet as in figure 11.8. Private LANs with no intent to connect to the Internet can choose any addresses they want, even public addresses that have been assigned by the IANA. If an organization later decides to connect to the Internet, its current address scheme may include addresses already assigned by the IANA to other organizations. These addresses would be duplicate or conflicting addresses and are known as *illegal addresses*. Connectivity from illegal addresses to Internet locations is not possible and it must be changed.

Further, if the private network does become attached to the public Internet at some point, it is much easier to see whether internal addresses are leaking into the Internet and simple for the ISP to configure routers to filter out any packets to or from the private address ranges.

If a network using one of the private address ranges is connected to the Internet, Network Address Translation (NAT) must be applied to map local addresses into publicly visible addresses. This process provides a useful security barrier since no information about the internal addressing or routing structure will leak out into the wider Internet. Further, the private network can exist with only a small number of public addresses because only a few of the hosts in the private network will be attached to the Internet at any time.

 NAT is a form of packet filtering used in firewall products that protects a network from outside intrusion by hackers. NAT also eliminates the need for an organization to have a set of globally unique IP addresses.

NAT replaces the internal network IP address for each Internet Protocol (IP) packet passing through the firewall with a dummy one from a fixed pool of addresses. The actual IP addresses of computers on the private network are thus hidden from users outside the firewall. All requests that pass through the firewall have their addresses translated on the way to the private network, and all responses returned to the unsecure public network have their addresses translated back on the way out of the private network.

Implementing NAT on a router or firewall essentially involves creating and configuring a NAT table containing the private/public IP address mappings. These mappings can be statically created or dynamically generated from a specified pool of IP addresses (either randomly or, more often, on a round-robin basis). A static NAT table essentially consists of a series of NAT rules that specify how IP addresses will be translated.

In addition to securing your private corporate network, NAT also reduces the need to get a block of unique IP addresses from your Internet service provider (ISP). Only the far side of your router or firewall server needs a unique IP address from your ISP—you can use any IP addresses within your network because your private network is securely hidden from the outside world behind your firewall. This reduces costs and helps extend the viability of the current IPv4 system by reducing the number of unique IP addresses required on the Internet.



In fact, the original impetus for the development of NAT technologies was the fact that the available pool of unique IPv4 addresses was steadily running out.

11.6.1 Automatic IP Address Allocation

We'll never get a device to work on a TCP/IP network unless it has an IP address. There are three automatic ways of getting an IP address into a network device. DHCP is found in Windows NT and Novell Netware. BOOTP and RARP are typically used in UNIX systems. If we do not use one of these automatic procedures, you must manually allocate an IP address to the device.

11.6.1.1 Dynamic Host Configuration Protocol (DHCP)

DHCP is a way of getting your server to allocate an IP address to the device that you wish to connect to the network. Basically a piece of software on the server is programmed with a list of IP addresses that it can give to a device upon request. This means that if a product supports DHCP, and you have enabled that protocol and the DHCP server is running on our network, then our device will be given an IP address by the server.

DHCP is sometimes called a plug-and-play protocol, whereby hosts can join or leave a network without requiring configuration by network managers.

The convenience of this method of address assignment gives DHCP multiple uses of IP addresses. If any ISP manager does not have a sufficient number of IP addresses,

DHCP is used to assign each of its connecting hosts a temporary IP address. When a host joins or leaves, the management server must update its list of available IP addresses. If a host joins the network, the server assigns an available IP address; each time a host leaves, its address is included in the pool of available addresses. DHCP is especially useful in mobile IP, with mobile hosts joining and leaving an ISP frequently.

One way to configure DHCP is to use a router employing DHCP. The router acts as a gateway between a private IP network and the public Internet. In this configuration, the IP address is only temporarily assigned to the communicating host within the private IP network as it is illustrated in Figure 11.10. By such means it is possible to share the public IP address space given that the number of hosts requiring addresses at any one time does not exceed the total number of public addresses available to the DHCP for dynamic address assignment.

DHCP servers can be employed for the allocation of IP addresses in private LANs and private IP networks since this makes for much easier administration of the numbering range.

DHCP clients obtain a DHCP lease for an IP address, a subnet mask, and various DHCP options from DHCP servers in a four-step process as it are illustrated in Figure 11.9:

1. **DHCPDISCOVER:** The client broadcasts a Discover message for a DHCP server when it is attached to an Ethernet and boots up.
2. **DHCPOFFER:** DHCP servers on the network respond with offer messages offering an address to the client.
3. **DCHPREQUEST:** The client broadcasts a request to lease an address from one of the offering DHCP servers. It asks the selected server for configuration information
4. **DHCPPACK:** The selected DHCP server responds with an Ack message carrying the requested information. It assigns client any configured DHCP options, and updates its DHCP DataBase. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.

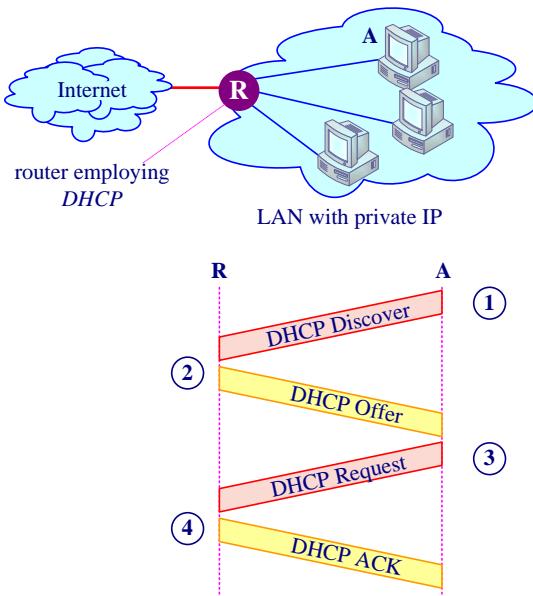


Figure 11.9: Steps of DHCP client-server configuration

DHCP has a further use in dial-up networking for discovering the IP address and network configuration parameters a computer should use when it is attached to the Internet. The same technique is used more generally for any dynamic assignment of IP addresses such as in DSL or cable modem connectivity.

At its most basic level, the IP address is taken from a pool of free IP addresses, this means that the IP address could change from one day to another. This can cause problems in some situations. For example, if a printer is configured on the network queue to work with a particular IP address and the DHCP server allocates a different IP address to the one that the queue is expecting to use, the printer will not be able to print as the IP address is different.

11.6.1.2 Bootstrap Protocol (BOOTP)

BOOTP is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a bootstrap protocol (BOOTP) server. The network interface card (NIC) on these diskless workstations contains a programmable read-only memory (PROM) chip containing code necessary to initialize the client.

BOOTP is used on many UNIX systems and is a more controllable way of allocating IP addresses. Basically, there is a BOOTP server, which contains a list of all available network resources. There are two pieces of information that the BOOTP server needs:

- MAC Address
- IP address that the supervisor would like to use.

When a BOOTP compatible device is switched on, it communicates with the BOOTP server. The server retrieves the MAC address and then looks in a look up table to

see if it can find the device MAC address, if it finds the MAC address the server then looks at what IP address it should allocate to the server. The device is then programmed with that address.

This is better than DHCP as you always know what IP address you will have in the device. The drawback to it is that you have to add an entry to the BOOTP server every time you buy a new network device.

11.6.2 Prioritization of Automatic IP Addresses

We'll often find the devices that support these three protocols have some kind of prioritization that allows us to specify which protocol should be used first. Imagine that you had a DHCP server; a BOOTP server and a RARP server. As the network card supports all three IP address allocation methods, there may be some confusion as to what IP address the card might get. To get around this, a card should be able to specify which IP address method it will use first, so it might use DHCP first, then fall back to BOOTP, etc...

It is also possible to specify an IP address using the ARP command from a TCP/IP system.

11.7 IP v6 Addresses

An IPv6 address has 128 bits and looks wild. Extending the address space was one of the driving reasons to develop IPv6, along with optimization of routing tables, especially on the Internet.

While it is true that the addressing was changed to 128 bits, there are many more features about the address space and its allocation that were carefully crafted. IPv6 addresses provide the same function as IPv4: identifiers for interfaces and sets of interfaces.

11.7.1 Types of Address Inscription

An IPv6 address is written in hexadecimal and consists of groupings of 8 containing 4 hexadecimal digits or 8 groups of 16 bits each. This takes the form:

XXXX : XXXX

There are principal types of address inscription:

- An IPv6 address is normally written as eight blocks of four hexadecimal digits separated by colons. For example 2001:0250:02FF:0210:0250:8BFF:FEDE:67C8 is an IP v6 address.
- Leading zeros do not need to be written. So we can write the previous address as follows 2001:250:2FF:210:250:8BFF: FEDE:67C8.
- A double colon, at most one of which may appear in any address, indicates multiple zero blocks. So the following IP v6 address:

FEDC: 0000:0000:0000:00DC:0000:7076:0010

could be written more compactly as

FEDC:: DC:0:7076:10).

- In mixed networks of IPv6 and IPv4, the last four bytes of the IPv6 address are sometimes written as an IPv4 dotted quad address. For example

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

could be written as:

FEDC:BA98:7654:3210:FEDC:BA98:118.84.50.16.

As in IPv4, nodes don't assigned IPv6 addresses. Only interfaces can be assigned IP addresses. Nodes can therefore be identified by the address of any of its interfaces, so each interface of a node needs at least one unicast address. A single interface can also be assigned multiple IPv6 addresses of any type (unicast, multicast, anycast).

It is also possible to assign one unicast address to multiple interfaces for load-sharing reasons, but if you do this, you need to make sure that the hardware and the drivers support it. Unlike IPv4 with IPv6, all zeros and ones are legal values for any field in an address.

A typical IPv6 address consists of three parts as shown in Figure 11.10.



Figure 11.10: IPv6 general address format

- **Global routing prefix:** It is used to identify a special address, such as multicast, or an address range assigned to a site.
- **Subnet ID:** This part is used to identify a link within a site. The subnet ID may also be referred to as subnet prefix or simply "subnet". A subnet ID is associated with one link. Multiple subnet IDs may be assigned to one link.
- **Interface ID:** An interface ID is used to identify an interface on a link and needs to be unique on that link.

The first few bits of the IPv6 address don't specify the class, but they tell something about the address. For example where the address has been assigned an address type and is known as the format prefix.

The amount of space used for these prefixes are specified by the formula $1 / 2^x$, where x is the number of bits used. For example, if the first 8 bits are 0000 0000, then this is $1 / 2^8$, or 1/256.

Prefixes are also used in this environment just like in the CIDR environment. A /30 indicates the first 30 bits are used for routing. Also notice that fields in certain types of addresses are given names to further identify the subaddress portions.

There are three address types that are assigned out of the 0000 0000 format prefix space. These are the “unspecified address,” the loopback address, and the IPv6 addresses with embedded IPv4 addresses. This allocation supports the direct allocation of provider addresses, local use addresses, and multicast addresses. Space is reserved for NSAP addresses, IPX addresses, and geographic addresses. The remainder of the address space is unassigned for future use. This can be used for expansion of existing use (e.g., additional provider addresses, etc.) or new uses (e.g., separate locators and identifiers).

A value of FF (11111111) identifies an address as a multicast address; any other value identifies an address as a unicast address. Multicast addresses are used extensively throughout auto configuration of addresses and neighbor discovery. Anycast addresses are taken from the unicast address space, and are not syntactically distinguishable from unicast addresses.

A 128-bit address obviously allows scope for 2^{128} distinct addresses.

IPv6 addresses are represented for human manipulation using hexadecimal encoding with a colon placed between each 16-bit word.

The first bits of an IPv6 address, called the *Format Prefix* (FP), indicate the use to which the address is put and the format of its contents. They are now managed by the Internet Assigned Numbers Authority (IANA). The number of FP bits varies from usage to usage, but can always be determined by the pattern of the early bits. Table 11.8 lists the currently defined FP bit settings.

FP Bits	Usage	Number of Addresses
0000 0000	Reserved	2^{120}
0000 0001	Unassigned	2^{120}
0000 001	NSAPs	2^{121}
0000 01	Unassigned	2^{122}
0000 1	Unassigned	2^{123}
0001	Unassigned	2^{124}
001	Global unicast addresses	2^{125}
01	Unassigned	2^{126}
10	Unassigned	2^{126}
110	Unassigned	2^{125}
1110	Unassigned	2^{124}
1111 0	Unassigned	2^{123}
1111 10	Unassigned	2^{122}
1111 110	Unassigned	2^{121}
1111 1110 0	Unassigned	2^{119}
1111 1110 10	Link local unicast addresses	2^{118}
1111 1110 11	Site local unicast addresses	2^{118}
1111 1111	Multicast addresses	2^{120}

Table 11.8: The IPv6 address space is divided according to the format prefix



NAT was viewed as a temporary solution until IPv6 could be standardized and implemented, but the security advantages of using NAT in firewalls has revitalized IPv4 and made migration to IPv6 less urgent.

11.7.2 IPv6 Address Formats

There are five address types identified by the Format Prefix bits shown in Table 11.8.

1. **Global unicast addresses** are formatted as shown in Figure 11.11. The address is broken into three topology-related segments.

➤ **Public Topology** contains four fields:

- Format Prefix (FP): 3 bits information field identifies the address type.
- Top Level Aggregation ID (TLA ID): 13-bits used by the naming authorities to identify up to 8192 major ISPs or carriers.
- Next Level Aggregation ID (NLA ID): 24-bits is used by an individual major ISP to subdivide its address space for administrative purposes or for assignment to small ISPs or customer networks that get their IPv6 Internet attachment through the larger ISP.
- Reserved: 8 bits between the TLA ID and NLA ID make it possible to extend the range of either of these fields in the future if necessary.

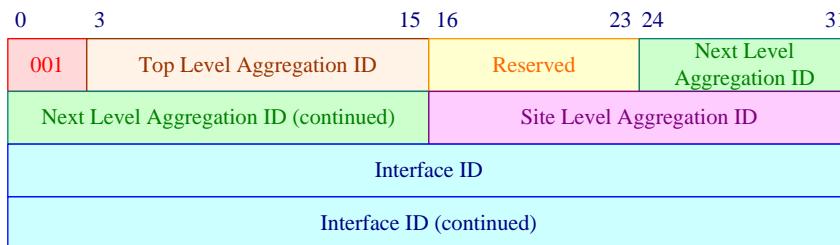


Figure 11.11: The format of a global unicast IPv6 address.

- **Site Topology:** 16 bit field contains Site Level Aggregation ID (SLA ID), which is used by an ISP or organization to break their network up into as many as 65,536 smaller administrative chunks.
- **Interface Topology:** 64 bits of the address used for the Interface ID to identify an individual router, host, or interface.
2. **Link Local Unicast Addresses:** (see Figure 11.12) are used between neighbors on the same link. Their scope is limited to the link and they are not distributed more widely. This is useful for dial-up devices or for hosts on a local network.

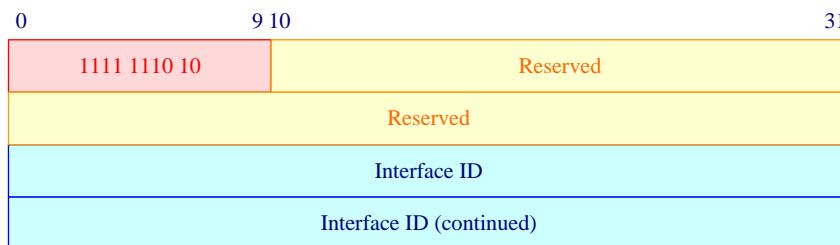


Figure 11.12: The format of a link local unicast IPv6 address.

3. **Site Local Unicast Addresses:** As shown in Figure 11.13, the site local address includes a subnetwork ID which can be used in a hierarchical manner within the organization's network in the same way as the SLA ID in the global address. They are equivalent to the three reserved address ranges 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 in IPv4. They are addresses that are allocated within an organization

but are not distributed more widely. Hosts using site local addresses rely on Network Address Translation to access the wider Internet.

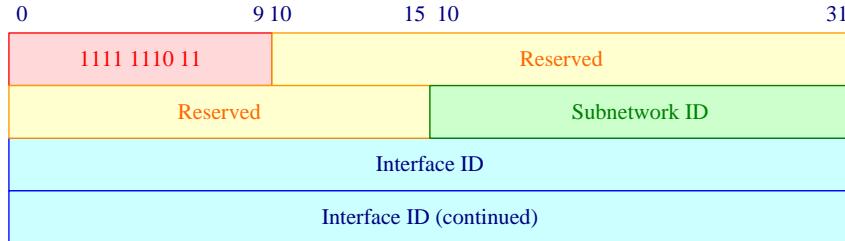


Figure 11.13 The format of a site local unicast IPv6 address.

4. **Multicast addresses:** The multicast address format is shown in Figure 11.14. It contains in addition to FT and reserved fields the following other fields:

- **T-bit flag:** It is used to indicate that the address is transient (1) or is permanently assigned (0).
- **Scope:** 4 bits indicates how the group ID should be interpreted and how widely it applies only a few values have been defined so far, as shown in Table 11.9. The rest of the address carries the group identifier which is otherwise unstructured.

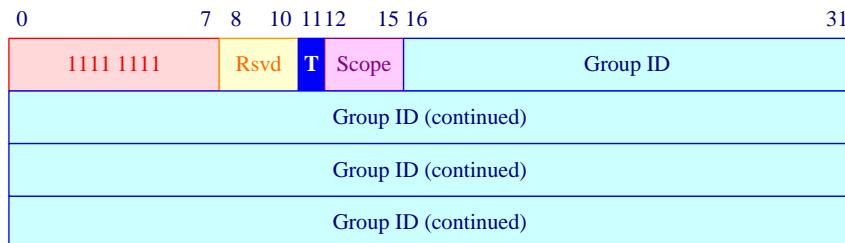


Figure 11.14 The format of an IPv6 multicast address.

Scope	Value Meaning
0	Reserved
1	Node-local scope
2	Link-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved

5. **Network Service Access Point (NSAP) addresses:** NSAP address is encoded into 121 bits within the IPv6 address, as shown in Figure 11.15. The NSAP address is a 40-digit hexadecimal string

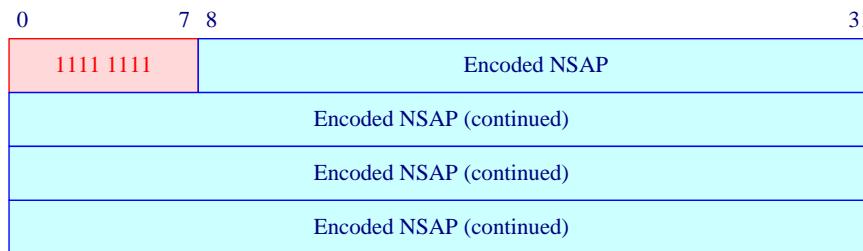


Figure 11.15: The format of an IPv6 NSAP address.

11.8 Managing the Address Space

The Internet's stability is directly dependent on the uniqueness of publicly used network addresses. Thus, some mechanism was needed to ensure that addresses were, in fact, unique. This responsibility originally rested within an organization known as the Internet Network Information Center (InterNIC). This organization is now defunct and was succeeded by the Internet Assigned Numbers Authority (IANA).

One important goal is to ensure that duplication of publicly used addresses does not occur. Such duplication would cause instability on the Internet, and compromise its ability to deliver datagrams to networks using the duplicated addresses.

The Internet Registry (IR) hierarchy was established in order to achieve address uniqueness, distribution of hierarchical distribution of global Internet addresses, and, most of all, produce a conservation of IPv4 Internet addressees. It consists of IANA, Regional IRs, and Local IRs.

The IANA is the Internet Assigned Numbers Authority, and it has overall authority for the number space used in the Internet. This number space includes port number, address, IP version numbers, and many other significant number assignments.

The Regional IRs operate under the authority of IANA. They operate in large geographical areas such as continents. Currently, there are three defined:

- The American Registry for Internet Numbers (ARIN), which manages North America, South America, and sub-Saharan Africa
- Réseaux IP Européens (RIPE), which manages Europe and North Africa
- The Asia Pacific Network Information Center (APNIC), which manages Asia and Australia

These IRs do not cover all areas. It is expected that each IR covers any area not specifically specified, but within its immediate area. Local IRs are established under the authority of the regional IR and IANA. They cover national dimensions.

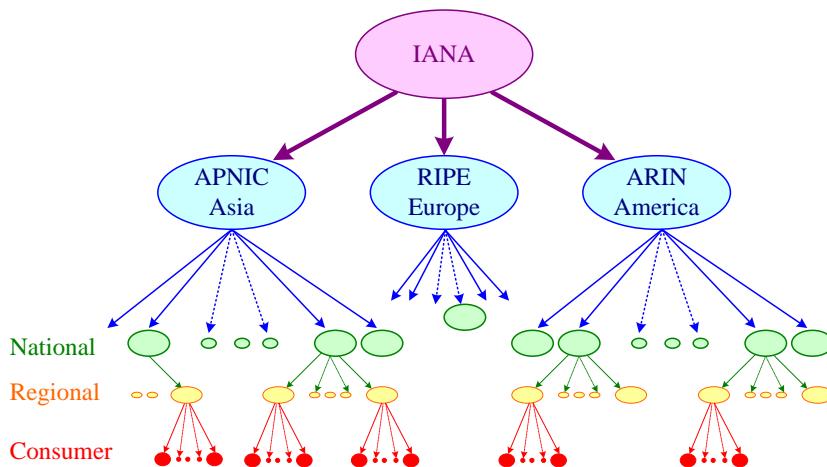


Figure 11.16: IANA bodies and divisions

Addresses are allocated to ISPs by regional registries, which in turn assign them to their customer base. ISPs that exchange routing information directly with other ISPs get their address allocation from their geographic IR. Other ISPs are referred to these ISPs for address assignment. In other words, if your address block has a reasonable chance of being propagated through the global Internet routing tables, then your address allocation will come from the IR. Otherwise, you will get your address assignment from your upstream ISP. Customers (commercial corporations) need not worry about this. They will get their address assignments from the ISP they sign up with. This is just a basic introduction to the IP addressing scheme.

IANA, too, has been dismantled, and the new caretaker of the Internet's names and address numbers is the Internet Corporation for the Assignment of Names and Numbers (ICANN). ICANN is currently creating a competitive registry structure that will enable commercial entities to compete with each other in the registration of IP names and numbers.



An ISP can request a block of addresses from ICANN. Then, an organization can also request a block of addresses from its ISP. A block of addresses obtained from an ISP can be assigned over hosts, servers, and router interfaces by a network manager.

11.9 Quick Review

- ❖ Addressing allows IP to communicate between hosts on a network or on an internet. The network layer handles the method of assigning addresses to packets and determines how they should be forwarded from one end point to another.
- ❖ There are two IP addressing schemes. The first is the current 32-bit IPv4 addressing scheme used on TCP/IP networks worldwide, the second is IPv6. Networks may use Unicast, Broadcast, Anycast, or Multicast address

- ❖ There are two types of network addressing schemes Classless and Classful. The IP address space of classful addressing scheme is divided into five different address classes, Class A, Class B, Class C, Class D, and Class E.
- ❖ Classes A, B, and C, were designed to accommodate three different scales of IP internetwork. The class D addresses are not divided into a network and a computer addresses, because they are multicast addresses themselves. Class E is reserved for future use and network experiments.
- ❖ IP addresses are often expressed as four decimal numbers, each separated by a dot.
- ❖ IP network can be subdivided into smaller networks to create smaller broadcast domains and to better utilize the IP addressing space.
- ❖ Subnet mask tells us quickly what the Class we are using is. A default subnet mask is based on the IP address classes and is used on TCP/IP networks that are not divided into subnets.
- ❖ Custom subnet masks are those that differ from the default subnet masks when doing subnetting. Subnet masks can be expressed using prefix notation.
- ❖ Subnet masks are used to extract the network ID and the host ID from an arbitrary IP address
- ❖ Two types of addresses are employed on the Internet, public addresses and private addresses. Public addresses are assigned by Internet Assigned Numbers Authority (IANA) and consist of class-based network IDs that are guaranteed to be globally unique to the Internet.
- ❖ The Internet designers reserved a portion of the IP address space and named this space the *private address space* which is never assigned as a public address.
- ❖ Internet traffic from a host that has a private address must either send its requests to an application layer gateway or use a *network address translator* (NAT).
- ❖ There are three protocols DHCP, BOOTP and RARP to get an IP address into a network device. If we do not use one of these protocols, you must manually allocate an IP address to the device.
- ❖ An IPv6 address has 128 bits and looks wild. IPv6 addresses provide the same function as IPv4. An IPv6 address is normally written as eight blocks of four hexadecimal digits separated by colons.
- ❖ IANA, too, has been dismantled; ICANN is currently creating a competitive registry structure that will enable commercial entities to compete with each other in the registration of IP names and numbers.

11.10 Self Test Questions

A- Answer the following questions

1. List the IP address types.
2. What is the difference between Classless and Classful IP addresses?
3. Why are IP addresses often expressed as four decimal numbers, each separated by a dot?
4. List the IP address classes.
5. What is the reason behind subnetting
6. How can the subnet mask be useful in determining the host id and net id?

7. How can we determine the number of host bits in order to use for subnetting?
8. How can private addresses be distinguished from public addresses?
9. What are the three private address blocks?
10. Why does some network need to use the NAT?
11. How dose the NAT work?
12. How dose the DHCP work?
13. What are the differences between DHCP and BOOTP?
14. What are the five IPv6 addresses types?
15. Explain the role of the IANA in managing the address space.

B- Identify the choice that best completes the statement or answers the question.

1. ____ provides for the largest number of hosts.
 - a. Class A
 - b. Class C
 - c. Class B
 - d. All three classes provide the same number of hosts.
2. A system must have a ____ address to be visible from the Internet?

a. Subnetted	c. Registered
b. Class A	d. Binary
3. One of the following statements about subnet masks is NOT true.
 - a. Subnet masks can have the same range of values as IP addresses.
 - b. The subnet mask specifies which bits of an IP address are the network identifier and which bits are the host identifier.
 - c. The dividing line between network bits and host bits can fall anywhere in a subnet mask.
 - d. Subnet masks are assigned by the IANA, but can be modified by network administrators.
4. What type of route does a packet in which the Destination IP Address and the data-link layer Destination Address values refer to different computers use?

a. The default gateway	c. A direct route
b. The default route	d. An indirect route
5. ____ is the column that contains the address of the router that should be used to reach a particular network or host in a Windows routing table.

a. Network Destination	c. Netmask
b. Gateway	d. Interface
6. In a Windows routing table, what is the Network Destination value for the default gateway entry?
 - a. 0.0.0.0
 - b. The address of the network to which the router is connected
 - c. 255.255.255.255
 - d. The address of the router's network interface
7. The first word in a full DNS name identifies
 - a. The top-level domain
 - b. The second-level domain
 - c. The DNS server

- b. IP operates at the Data Link layer of the OSI Model
 - c. IP contains a header checksum field
 - d. IP checksum also verifies the integrity of the message
21. ____ is the field of the IP datagram that identifies the number of 4-byte (or 32-bit) blocks in the IP header.
- a. Flags
 - b. Total length
 - c. Version
 - d. Internet Header Length
22. ____ is the core protocol responsible for logical addressing for TCP/IP.
- a. MAC
 - b. TCP
 - c. ARP
 - d. IP
23. ____ is a valid IP address example.
- a. 144.92.43.178
 - b. 144-92-43-178
 - c. 144.92.43.1780
 - d. 144,92,43,178
24. ____ octets are in a valid IP address.
- a. 3
 - b. 4
 - c. 6
 - d. 8
25. To identify networks and hosts in an IP address you can use only numbers between:
- a. 0 and 255
 - b. 1 and 254
 - c. 2 and 256
 - d. 125 and 256
26. ____ is the IP address that is used to send a message to all devices connected to your network segment.
- a. 0.0.0.0
 - b. 255.1.1.1
 - c. 255.0.0.0
 - d. 255.255.255.255
27. ____ is network class that an IP address whose first octet is in the range of 1-126 belongs.
- a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
28. What is the network ID in this example: 23.78.110.109?
- a. 23
 - b. 78
 - c. 109
 - d. 110
29. ____ is network class that an IP address whose first octet is in the range of 128-191 belongs.
- a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
30. In 168.34.88.28, which of the following is the network ID?
- a. 34.88
 - b. 34.88.28
 - c. 88.28
 - d. 168.34
31. ____ is a network class that an IP address whose first octet is in the range of 192-223 belongs.
- a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
32. In 204.139.118.12, which is the network ID?
- a. 12
 - b. 118.12
 - c. 139.118.12
 - d. 204.139.118
33. Which of the following is a reason why IPv6 was originally developed?
- a. So that IP can operate at the Transport layer of the OSI Model

- b. To create a protocol that is not based on TCP
 - c. To respond to an exponentially growing demand for IP addresses
 - d. So that a network Class F can be used
34. To what network class does the IP address 127.0.0.1 belong?
- a. Class A
 - b. Class B
 - c. Class C
 - d. None of the above
35. The IP address 127.0.0.1 is also known as:
- a. Loopback address
 - b. Broadcast address
 - c. Multicast address
 - d. Class B broadcast address
36. What kind of IP address notation is address 133.66.12.19 using?
- a. Hexadecimal notation
 - b. Dotted decimal notation
 - c. Binary notation
 - d. Octal notation
37. What kind of IP address notation is address 10010011 01010001 00101010 00110100 using?
- a. Hexadecimal notation
 - b. Dotted decimal notation
 - c. Binary notation
 - d. Octal notation
38. A special 32-bit number that, when combined with a device's IP address, informs the rest of the network about the segment or network to which the device is attached:
- a. Subnet mask
 - b. ARP address
 - c. MAC address
 - d. DNS mask
39. What is true about subnet masks?
- a. They can be expressed using hexadecimal notation
 - b. They are composed of four octets
 - c. They are composed of three octets
 - d. They can be expressed using octal notation
40. _____ is the name of the process of subdividing a single class of network into multiple, smaller logical networks, or segments.
- a. Masking
 - b. Segmentation
 - c. Fragmentation
 - d. Subnetting
41. Which of the following is TRUE statement?
- a. Subnet masks are assigned only to devices from a Class A network
 - b. Devices are assigned a subnet mask only if they belong to a subnetted network
 - c. Devices are always assigned a subnet mask
 - d. Subnet masks are assigned only to devices from a Class A or B network
42. The mask 255.0.0.0 is the default subnet mask for _____ network.
- a. Class A
 - b. Class B
 - c. Class C
 - d. Class E
43. The mask 255.255.0.0 is the default subnet mask for for _____ network.
- a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
44. The mask 255.255.255.0 is the default subnet mask for for _____ network.
- a. Class B
 - b. Class C
 - c. Class D
 - d. Class E
45. Which of the following is TRUE statement about IP addresses within a LAN?
- a. Two devices can share the same IP address
 - b. Exactly two devices can share an IP address at a time

- c. Exactly one device can use an IP address at a time
 - d. Several devices can share the same IP address
46. When you add a node to a network and its IP address is already in use by another node on the same subnet:
- a. Both hosts will stop working
 - b. The new node will work, but the existing host will stop working
 - c. They both will receive a message alert and stop working
 - d. The existing host will continue working
47. What is the name of manually assigned IP addresses?
- a. Static IP addresses
 - b. Dynamic IP addresses
 - c. Variable IP addresses
 - d. Changing IP addresses
48. ____ is the type of IP address more easily results in the duplication of address assignments.
- a. Static IP addresses
 - b. Dynamic IP addresses
 - c. Variable IP addresses
 - d. Changing IP addresses
49. ____ is one benefit for implementing DHCP.
- a. Keep users from moving their workstations without changing their TCP/IP configuration
 - b. Prevent mobile users from using your network
 - c. Reduce the time and planning spent on IP address management
 - d. None of the above
50. ____ is the next step a client will take upon receiving responses from all DHCP servers on the client's subnet.
- a. The client accepts all IP addresses it receives
 - b. The client accepts only one IP address
 - c. The client accepts two IP address
 - d. The client accepts the last IP address it receives
51. ____ is a name that describes the device on a network.
- a. Host name
 - b. IP name
 - c. IP address
 - d. Socket
52. Packets that are used for network testing begin with ____ in the first octet.
- a. 1
 - b. 126
 - c. 127
 - d. 128
53. An IP address is divided into two distinct parts: one part designates the logical network the computer is a part of, while the remainder of the address represents the ____.
- a. NIC's MAC address
 - b. domain name
 - c. host ID
 - d. subnet mask
54. ____ is the first field in an IPv6 header.
- a. Priority
 - b. Version
 - c. Payload Length
 - d. Destination Address
55. ____ is the field in IPv4 that is no longer present in the IPv6 header.
- a. Destination Address
 - b. Hop Limit
 - c. Flow Label
 - d. Header Length

CHAPTER 12

ROUTING

12.1 About This Chapter

This chapter on routing and routing protocols covers a large amount of material, from the basics of routing and the techniques used to distribute routing information, to the protocols that realize these techniques.

Routing and forwarding is what the Internet is all about: How can an IP packet from one host be delivered to the destination host? Within an individual router, the answer lies in a routing table which is accessed through a look-up function. This function maps the destination address carried in a datagram to the address of the next hop along the path (the *next hop address*) and the interface on the router through which the datagram should be forwarded (the *outgoing interface*).

In simple networks, routing tables can be manually configured or learned from the configuration of interfaces on the router. In more complex networks in which there are many routers arranged in a mesh with lots of links between routers, each link having different capabilities, manual configuration becomes onerous.

We rely on *routing protocols* to collate and distribute information about network connectivity. As with all complex problems, there are a multitude of solutions. Each solution has its advantages and disadvantages, each has its advocates and disparagers, and each a specific applicability. Some knowledge of the best path is implicit in the way the information is gathered and distributed, but there are also sophisticated *routing algorithms* that can be run against the view of the network to determine the best path along which to forward a datagram. These algorithms are discussed in this chapter.

There are two classes of routing protocols: intradomain routing protocol or intranetwork routing protocol or intranet, and interdomain routing protocol or internetwork routing protocol or extranet. These two concepts are briefly covered in this chapter.

The actual protocols (*routing protocols*) used to distribute the connectivity information make up the core of the chapter. The Routing Information Protocol (RIP) is simple and ubiquitous. The Open Shortest Path First (OSPF) protocol is very popular and has a close rival, The Border Gateway Protocol (BGP) is important for hooking together the many Service Provider networks into a single Internet. This chapter summarizes the basic capabilities and features associated with these three protocols.

The chapter then outlines some of the issues of routing for mobile IP traffic. Combining the best of both wireless and IP technologies has brought us into the era of wireless IP. Wireless IP will enable cost-effective, high-quality IP-based wireless multimedia services, including voice over IP, in large volumes.

12.2 Learning Outcome

After this chapter, you will be able to:

1. Understand the basics of routing protocols.
2. Distinguish between routing and forwarding.
3. Make a comparison between link-state and distance vector routing algorithm.
4. Be familiar with the metrics used by routing protocols to determine path selection.
5. Understand the basics of how data travels from end stations through intermediate stations and on to the destination end station.
6. Understand the difference between routed protocols and routing protocols.
7. Classify and explain the most popular routing protocols.
8. Distinguish between interdomain and interdomain routing protocols.
9. Understand the basics of mobile routing.

12.3 Routing Principles

In order to transfer packets from a sending host to the destination host, whether the network layer provides a datagram service or a virtual circuit service, the network layer must determine the path or route that the packets are to follow.

How can an IP packet from one host be delivered to the destination host? Router uses a look-up function. This function maps the destination address carried in a datagram to the address of the next hop along the path, the next hop address, and the interface on the router through which the datagram should be forwarded, the outgoing interface.

So packets are routed based on the address that is in the packet. The datagram may be routed locally in this case the destination is on the same subnet as the originator, which is known as direct routing, or it may invoke the use of a forwarding device such as a router if the destination is remote i.e. on a different subnet than the originator which is known as indirect routing. In general a datagram that is sent may invoke both direct and indirect routing.

12.3.1 Building and Using a Routing Table

The routing table is a look-up table containing all available destination addresses and the corresponding switch output port. An external algorithm fills this routing lookup table. Thus, the purpose of the routing table is to look up an entry corresponding to the destination address of the incoming packet and to provide the output network port. As soon as a routing decision is made, all the information should be saved on the routing table. When a packet enters the router, the destination port should be chosen based on the destination address of the incoming packet. This destination port needs to be appended to the incoming packet as part of the header.

When a packet carrying a destination address arrives from a given link, its destination address is used to identify the corresponding output port. The table makes the routing decision, based on the estimated cost of the link, which is also stated in the corresponding entry.

The router calculates the link cost between a pair of source and destination nodes, which refers to the number of packets currently waiting ahead in the destination node. The goal is to choose a routing based on the least-cost path. The least-cost path between each pair of nodes is the minimum cost of the routing between the two nodes, taking into

account all possible links between the two nodes. The cost may reflect the level of congestion on that link (e.g., the current average delay for a packet across that link) or the physical distance traversed by that link (e.g., a transoceanic link might have a higher cost than a terrestrial link). For our current purposes, we will simply take the link costs as a given and won't worry about how they are determined.

A router only has to answer a very simple question: given an IP datagram carrying a specific destination host address, out of which interface should the datagram be sent, and to which next hop?

A routing table, therefore, is some form of look-up algorithm that takes an IP address and derives an interface identifier and a next hop IP address. The implementation of routing tables varies significantly from one router manufacturer to another, and the conflicting requirements of performance and data occupancy drive the competitive advantages they claim. There are, nevertheless, some common abstract themes that run through all implementations and that can be seen when a routing table is examined at a user interface.

An entry in an IP routing table contains the following information as it is shown in Figure 2.1:

- **Network Destination:** The network ID corresponding to the route. The network destination can be class-based, subnet, or super-net, or an IP address for a host route.
- **Net-mask:** The mask used to match a destination IP address to the network destination.
- **Forwarding address or Gateway:** The forwarding or next-hop IP address for the network destination.
- **Interface:** The IP address corresponding to the network interface that is used to forward the IP datagram. This is a port number or other type of logical identifier.
- **Metric:** A number used to indicate the cost of the route so the best route among possible multiple routes to the same destination can be selected. Routing metrics can include the following:
 - **Hops:** The number of intermediate routers between a given network and the local router
 - **Latency:** The time delay in processing a packet through the router or over a given route
 - **Congestion:** The length of the packet queue at the incoming port of the router
 - **Load:** The processor use at the router or the number of packets per second that it is currently processing
 - **Bandwidth:** The available capacity of a route to support network traffic; decreases as network traffic increases
 - **Reliability:** The relative amount of downtime that a particular router might experience because of malfunctions
 - **Maximum Transmission Unit (MTU):** The largest packet size that the router can forward without needing to fragment the packet
- **Lifetime:** The Lifetime field indicates the lifetime that the route is considered valid. When routes are learned through the exchange of information with other

routers, this is an additional field that is used. Learned routes have a finite lifetime. To keep a learned route in the routing table, the route must be refreshed through a periodic process. If a learned route's lifetime expires, it is removed from the routing table.

Network ID	Forwarding address	Interface	Metric	Net Mask	Life time

Figure 12.1: Routing table entries

Routing table entries can be used to store the following types of routes:

- **Directly Attached Network ID Routes:** These routes are for network IDs that are directly attached. For directly attached networks, the Gateway IP address is the IP address of the interface on that network.
- **Remote Network ID Routes:** These are for network IDs that are not directly attached but are available across other routers. For remote networks, the Gateway IP address is the IP address of a local router in between the forwarding node and the remote network.
- **Host Routes:** A route to a specific IP address. Host routes allow routing to occur on a per-IP address basis. For host routes, the Network Destination is the IP address of the specified host and the subnet mask is 255.255.255.255.
- **Default Route:** The default route is designed to be used when a more specific network ID or host route is not found. The default route Network Destination is 0.0.0.0 with the subnet mask of 0.0.0.0.

In its most basic form, a routing table comprises a list of all possible destinations, identified by their IP addresses, in one column and the next hop for each destination in a second column as it shown in Figure 12.2.

The creation, updating and maintenance of the routing table are critical to the operation of a router. This may be undertaken manually by human network administrators, in which case the router is said to perform **static routing**, but this is impractical in most networks. Alternatively, routing table creation and maintenance may be undertaken automatically by the routers, in which case the routers perform **dynamic routing**.

Most routers even allow for a mix of the two methods allowing some routing table entries to be maintained statically, e.g. the default route and local route preferences, while leaving the rest to be dynamically maintained.

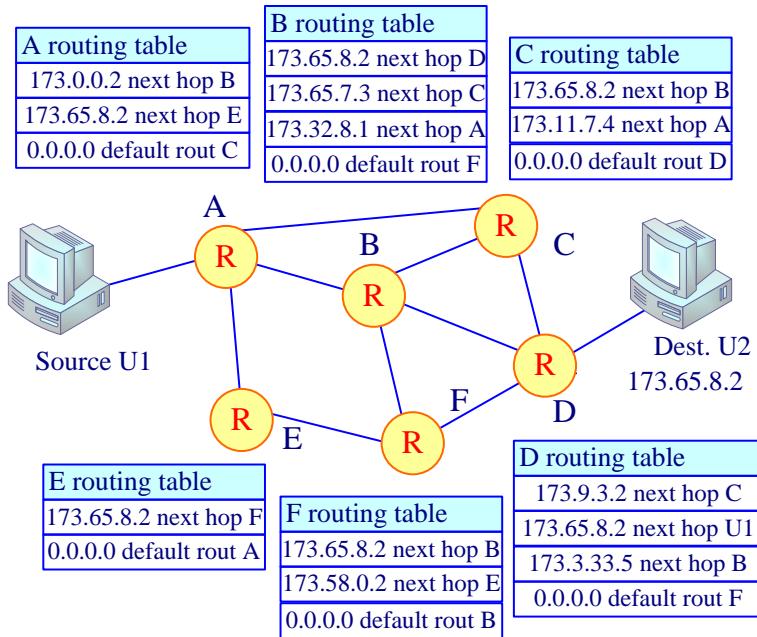


Figure 12.2: Example of simple routing tables

12.3.2 Static Routing versus Dynamic Routing

Static routing, as its name implies, is configuring the routing tables in the routers within a network prior to operation. It is mainly used in small networks, with two or three routers and a few IP subnets. The benefits of using static routing are as follows:

- **It is simple:** Since static routing is configured by network managers before operations of the router.
- **It has lower overheads:** Since every route is configured statically, no run-time updates are necessary.
- **It is easy to troubleshoot:** Since routing is configured before implementation, it is possible to troubleshoot the network "on paper" first. Checking can be made offline and rectified before effecting any changes.



Static routing can be used only in a small network, with minimal configuration required. It is always recommended when a remote network is connected to a central network with only one link. Since there is only one link, a default route can be put into the remote router to forward all traffic to the central site router.

The problem associated with a static routing network is:

- As network grows, more effort is required to implement the static definitions. These definitions have to be introduced in every router for new networks, and any changes means having to configure most, if not all, routers.

- Because routing instructions are constructed before deployment, static routing lacks the ability to adapt to any changes in the operating environment.
- Traffic is not diverted if there is a link failure. This poses a serious problem for networks that need intelligence to overcome link failures.

Using the dynamic routing, routers build their own routing table through information exchanged with each other during run time. No static definition is required. Since the routers learn the routes on their own, they can react to link failure by re-learning the way the new network is connected.

The advantage of dynamic routing is that the network adjusts its routing to all reachable destination addresses on an up-to-the-minute basis. Dynamic routing reacting dynamically to:

- addition of new devices or addresses to the network;
- removal of devices or addresses from the network;
- moving of devices or address from one location in the network to another; and even for
- re-adjustment of routes when links between routers fail.

The three greatest challenges faced when creating routing tables are:

- determining the full list of reachable addresses and keeping this permanently up-to-date;
- creating a routing algorithm (calculation procedure) for ensuring the most efficient overall use of the network when working out the best routes to each individual destination; and
- avoiding network instability, which might occur if different nodes chose routes uncoordinated with their neighbors.

12.4 Routing Algorithms and Routing Protocols

We rely on routing protocols to collate and distribute information about network connectivity. The job of the network layer **routing protocol** is to determine the path or route that the packets are to follow when transferring packets from a sending host to the destination host. Routing algorithm that determines the **best** path for a packet is the heart of any routing protocol. Typically, the best path is one which has the least cost.

Some knowledge of the best path is implicit in the way the information is gathered and distributed, but there are also sophisticated routing algorithms that can be run against the view of the network to determine the best path along which to forward a datagram. The Route Determination Process:

To determine a single route to use to forward an IP datagram, IP uses the following process:

- For each route in the routing table, IP performs a bit-wise logical AND between the Destination IP address and the net-mask. IP compares the result with the network destination for a match. If they match, IP marks the route as one that matches the Destination IP address.

- From the list of matching routes, IP determines the route that has the most bits in the net-mask. This is the route that matched the most bits to the Destination IP address and is therefore the most specific route for the IP datagram. This is known as finding the longest or closest matching route.
- If multiple closest matching routes are found, IP uses the route with the lowest metric. If multiple closest matching routes with the lowest metric are found, IP randomly chooses the route to use.

When determining the forwarding or next-hop IP address from the chosen route, IP uses the following procedure:

- If the Gateway address is the same as the Interface address, the forwarding IP address is set to the destination IP address of the IP packet.
- If the Gateway address is not the same as the Interface address, the forwarding IP address is set to the Gateway address.
- The end result of the route determination process is the choice of a single route in the routing table. The route chosen yields a forwarding IP address (the Gateway IP address or the Destination IP address of the IP datagram) and an interface (identified through the Interface IP address). If the route determination process fails to find a route, IP declares a routing error. For a sending host, an IP routing error is internally indicated to the upper layer protocol such as TCP or UDP. For a router, the IP datagram is discarded and an ICMP "Destination Unreachable-Host Unreachable" message is sent to the source host.

Routing algorithms can be differentiated on several key characteristics used to determine how efficiently a route is selected including:

- Accuracy: An algorithm must operate correctly so that it can find the destination in an appropriate amount of time.
- Simplicity: Low complexity of algorithms is particularly important where routers with limited physical resources involve software.
- Optimality: This refers to the ability of the routing algorithm to select the best route.
- Stability: Routing algorithms must perform correctly in the face of unforeseen circumstances, such as node failure and routing table corruptions.
- Adaptability: When a failure happens in a network, an algorithm should be able to adapt load increases or decreases.
- Convergence: Routing algorithms must converge rapidly when a network distributes routing update messages.
- Load balancing: A good routing algorithm balances over eligible links to avoid having a heavily and temporarily congested link.



In simple networks, routing tables can be manually configured or learned from the configuration of interfaces on the router. In more complex networks in which there are many routers arranged in a mesh with lots of links between routers, with each link having different capabilities, manual configuration becomes onerous.

12.4.1 Choosing the Least Cost Path

We will use the graph abstraction to formulate routing algorithms as shown in Figure 12.3; where, nodes in the graph represent routers and the lines connecting these nodes represent the physical links between these routers. Every link has a value representing the "cost" of sending a packet across the link.

The router gathers routing information about the ever-changing topology of the network. It then calculates the shortest routing distance or route cost to each reachable destination.

The routing policy might include particular preferences when choosing between alternative routes to a given destination (e.g. 'use the cheapest route rather than the one with the least hops', 'use the route with the most bandwidth', 'ignore routing information received from party X').

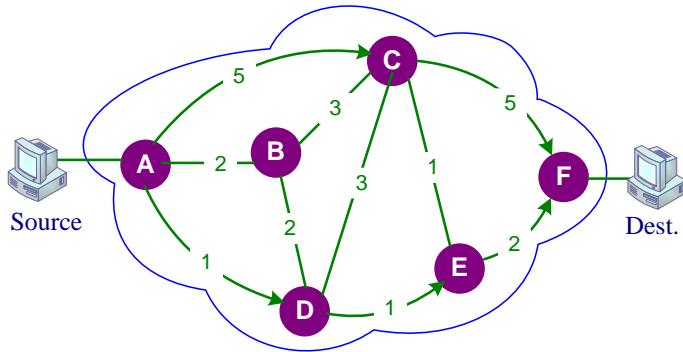


Figure 12.3: Abstract model of a network

The determination of the best route to a particular destination is normally based upon the shortest routing distance (or path cost) from the router in question. First, the individual link distances (link costs) for all possible paths to the destination are added together. These are the alternative path distances (or path costs). The path with the lowest overall path distance (or path cost) is chosen to be the shortest path. The first hop of this path is inserted into the router's routing table as the next hop for purpose of forwarding packets.



Distances and costs are usually integer values. When the distance or cost assigned manually by the human during the configuration of the router, the value is known as the *administrative distance* or *administrative cost*. When calculated automatically by the router, the distance or cost value can be changed over time to reflect the link bit rate, current transmission delay, link loading, link reliability or some other *metric*.

Each router will either be configured to 'know', or will calculate, the distances or costs of the links to which it is directly connected. Thus taken together, the routers have enough information to calculate the shortest paths to all destinations. But before any single

router can determine its routing table, the routers must ‘pool’ their information—sharing what they know with all the other routers in order that they can all create a ‘map’ of the network.

In Figure 12.2, for example, the least cost path between source and destination is along the path ADEF.

Several least-cost-path algorithms have been developed for packet-switched networks. In particular, Dijkstra's algorithm is the most popular and widely used algorithm. This algorithm determines least-cost paths from a source node to a destination node by optimizing the cost in multiple iterations. It works as follows:

For a given graph abstraction, we must identify a series of links in order to find the best path such that:

- the first link in the path is connected to the source
- the last link in the path is connected to the destination
- always the link i , and $i-1$ in the path are connected to the same node
- the **least cost path** is the minimum sum of the links costs over all possible paths between the source and destination.

Using the graph abstraction in Figure 12.3 we will compute the shortest path from A to all possible destinations. The result of the algorithm's computation is shown too, where each line in the table gives the values of the algorithms variables at the end of every iteration. Let us define the following notation:

- $c(i,j)$: link cost from node i to node j . If nodes i and j are not directly connected, then $c(i,j) = \text{infinity}$.
- $S(d)$: the cost of path from the source node to destination d that has currently the least cost.
- $p(d)$: previous node (neighbor of d) along current least cost path from source to d
- N : set of nodes whose shortest path from the source is definitively known

Step	N	$S(B), p(B)$	$S(C), p(C)$	$S(D), p(D)$	$S(E), p(E)$	$S(F), p(F)$
0	A	2, A	5, A	1, A	infinity	infinity
1	AD	2, A	4, D		2, D	infinity
2	ADE	2, A	3, E			4, E
3	ADEB		3, E			4, E
4	ADEBC					4, E
5	ADEBCF					

Figure 12.4: calculating the least cost rout from A to F

- **Initial step:** the currently known least path costs from A to its directly attached neighbors, B, C and D are initialized to 2, 5 and 1 respectively. Note in particular

that the cost to C is set to 5 (even though we will soon see that a lesser cost path does indeed exist) since this is cost of the direct (one hop) link from A to C. The costs to unreachable nodes E and F (not directly connected to A) are set to infinity.

Adding nodes one by one and calculate the least cost to every node in the set N.

- **First iteration:** we look among those nodes not yet added to the set N and find that node with the least cost as of the end of the previous iteration. That node is D, with a cost of 1, and thus D is added to the set N. The calculation is then performed to update S(d) for all nodes d, yielding the results shown in the second line (step 1) in Figure 12.4.
- **Second iteration:** nodes B and E are found to have the shortest path costs (2), and we break the tie arbitrarily and add E to the set N so that N now contains A, D, and E. The cost to the remaining nodes not yet in N, i.e., nodes B, C and F, are updated, yielding the results shown in the third row in the above table.
- **and so on ...**

12.4.2 Classification of Routing Algorithms

Routing algorithms can be classified in several ways. One way is to classify them as either least-cost path, whereby the lowest-cost path must be determined for routing, or non-least-cost path, whereby the determination of a route is not based on the cost of a path.

Another way is based on whether an algorithm is distributed or centralized. In distributed routing, all nodes contribute in making the routing decision for each packet. In other words, an algorithm in distributed routing allows a node to gain information from all the nodes, but the least-cost path is determined locally. In centralized routing, only a designated node can make a decision. This central node uses the information gained from all nodes, but if the central node fails, the routing function in the network may be interrupted. A special case of centralized routing is source routing, whereby the routing decision is made only by the source server rather than by a network node. The outcome is then communicated to other nodes.

From a mathematical point of view, routing algorithms come in two common types: distance vector routing algorithms and link state routing algorithms.

12.4.2.1 Distance Vector Algorithm (DVA)

The distance vector algorithm was designed mainly for small network topologies. It is the simplest and most intuitive way to distribute network connectivity information also makes the construction of routing tables particularly easy. Protocols that work in this way are called distance vector protocols. The idea behind the DVA is that each router on the network routing domain or process compiles a list of the networks it can reach and sends the list to their directly connected neighbors. The routers then create routing tables based on what they can reach directly and indirectly, using their neighbor routers as gateways. If multiple paths exist, the router only keeps the best one. This route is chosen based on the protocol's particular metric for determining the best route.

The term distance vector derives from the fact that the protocol includes its routing updates with a vector of distances, or hop counts from each possible source router to each possible destination.

Once the distance and vector have been determined, they can be advertised as routing information to other neighboring routers within the network, which in turn can then calculate their routing tables.

In order to illustrate how this works the given example in Figure 12.3 comprises a network of 6 routers in which the source is connected to router A and the destination is connected to router F. We shall assume that router A's neighbors, routers B, C and D have already calculated their routing tables for the shortest path to reach the destination and each is advertising this information to router A as well as to all their other directly-connected neighbors by means of the routing protocol. Each node's distance table has a row for each destination in the network and a column for each of its directly attached neighbors.

In our example, router A will conclude that its next hop to the destination should be via router D, and that the hop count from router A to the destination will be $1 + 1 + 2 = 4$ hops. A simple process of deduction reaches this conclusion: the route advertised to the destination by router.

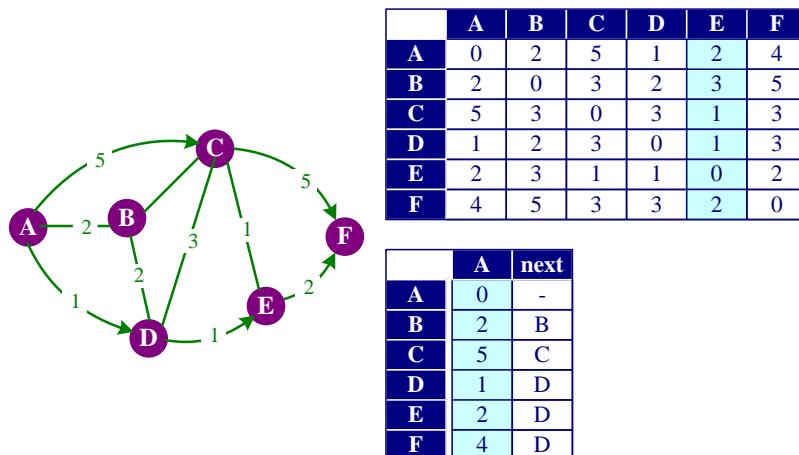


Figure 12.5: Building the routing table of A according to the gathered information from its neighbors

Assuming that least cost is used as a metric and that the router knows the least cost to each of its neighbors, each router sends to each neighbor a list of its estimated least cost to each destination once every T msec.

So if any changes take place in the routing table of node E, this node will send a packet containing these changes to all its neighbors C, D and F. C and D in turn will update their tables and send its updated contents to their neighbors including A. Finally A will update its table according to these changes. The updating process is illustrated in Figure 12.6.

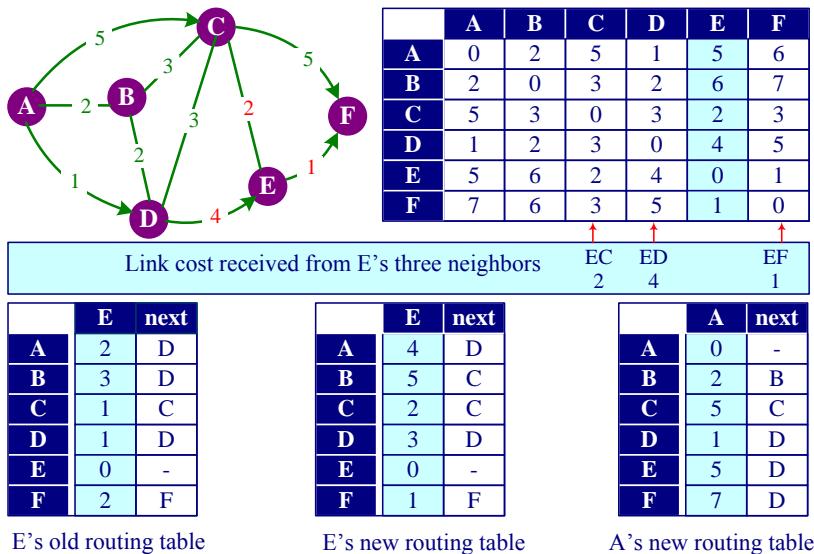


Figure 12.6: Modification of A's routing table according to the changes taking place in E's links

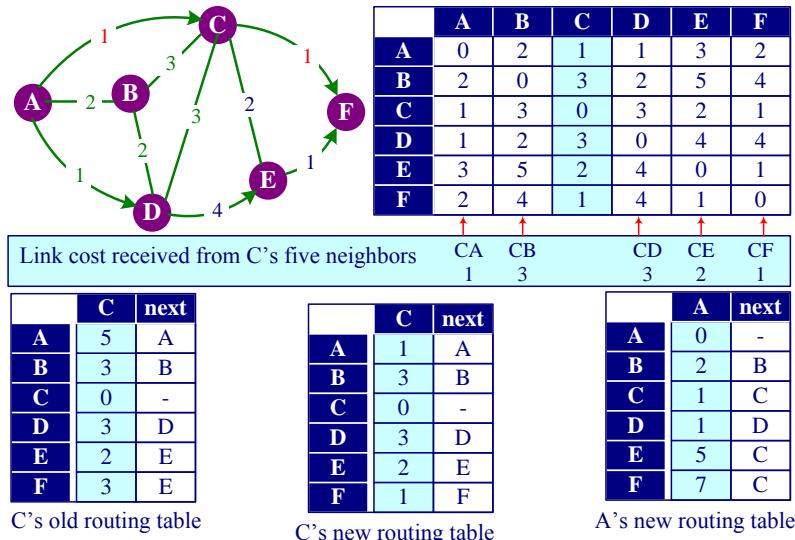


Figure 12.7: Modification of A's routing table according to the changes taking place in C's links

Another example is when some changes happen in C's routing table; these changes will be passed to the neighboring nodes. The neighboring nodes including A in turns will modify their tables and pass its content to the neighboring node and so on. The modified table of the node A will be as it is shown in Figure 12.7.

When this algorithm is used by a routing protocol, each router advertises its routing table to its adjacent neighbors. Each advertisement contains the following information about each route in that routing table:

- The hop count for the route (the distance)
- The direction in which the route is located (the vector)

Routers select the route with the lowest cost to each possible destination and add this to their own routing tables. The main disadvantage of the distance vector routing algorithm is that changes are propagated very slowly throughout a large internetwork because all routing tables must be recalculated. This is called the Slow Convergence Problem. Other disadvantages are that routing tables can become extremely large, making distance vector routing protocols unsuitable for large internetworks, and that route advertising generates a large amount of traffic overhead

12.4.2.2 Link-State Routing Algorithm

Link state protocols (LSPs) are based on a different algorithm than DVAs. In the link-state routing, routers collaborate by exchanging packets carrying status information about their adjacent links. A router collects all the packets and determines the network topology, thereby executing its own shortest-route algorithm.

Link state routing does not distribute any routes, but exchanges topology information that describes the network. Each node is responsible for advertising the details of the links it supports, and for passing on similar information that it receives from other routers. In this way each router in the network builds up a complete data base of the available links and which nodes they interconnect.

Each router using link state routing must do the following simple steps:

A. Learning about the Neighbors: This is the first step and is achieved through a Hello protocol in which each router sends a Hello message on each link to introduce itself to its neighbors. The format and precise content of the Hello message is, of course, dependent on the link state routing protocol in use, but it must uniquely identify the link on which the message was sent using an IP address and the router that sent the message using a network-unique router ID. The receiver of a Hello message responds with its own Hello so that the routers both know about each other. The Hello message is periodically retransmitted by both routers, and if a router does not hear from its neighbor for a number of retransmission periods it declares the link to have failed.

B. Measuring Line Cost: In order to have a reasonable estimate of the delay to each of its neighbors, the router sends over the line a special ECHO packet that the other side is required to send back immediately. By measuring the round-trip time and dividing it by two, the sending router can get a reasonable estimate of the delay.

Arguments can be made both ways. Including traffic-induced delays in the measurements means that when a router has a choice between two lines with the same bandwidth, one of which is heavily loaded all the time and one of which is not, the router will regard the route over the unloaded line as a shorter path. This choice will result in better performance.

C. Building Link State Packets: Once the information needed for the exchange has been collected, the next step is for each router to build a packet containing all the data. The routers exchange and negotiate the parameters they will use to manage their association, such as timer values, and then they declare themselves to be peers. The first thing that peers do is synchronize their link state dataBases by exchanging messages that report on each link that they know about. The information about each link is sent as a link state advertisement (LSA) or link state packet (LSP) which is formatted and built into a message according to the rules of the specific routing protocol.

The packet starts with the identity of the sender, followed by a sequence number and age (to be described later), and a list of neighbors. For each neighbor, the delay to that neighbor is given.

The link state packets can be built periodically, that is, at regular intervals. Or they can be built when some significant event occurs, such as a line or neighbor going down or coming back up again or changing its properties appreciably.

D. Distributing the Link State Packets: The fundamental idea to distribute the link state packets reliably is to use flooding. The flooding process is simple. The router receives an LSA and searches its link state data base to determine whether it already knows about the link; if it does it discards the new LSA, but if it does not it adds the link to its data base and sends the new LSA out of each of its interfaces except the interface on which the LSA was originally received. To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent. Routers keep track of all the (source router, sequence) pairs they see. When a new link state packet comes in, it is checked against the list of packets already seen. If it is new, it is forwarded on all lines except the one it arrived on. If it is a duplicate, it is discarded. If a packet with a sequence number lower than the highest one seen so far ever arrives, it is rejected as being obsolete since the router has more recent data.

Adding an age field for each packet will guarantee the solution of the problem, which may arise in the some situations:

- if the sequence numbers wrap around
- when a router ever crashes it will start again at 0, the next packet will be rejected as a duplicate.
- if a sequence number is ever corrupted it may be rejected as duplicate.

The age is decreased by one per second every hope. When the age hits zero, the information from that router is discarded. Normally, a new packet comes in, say, every 10 sec, so router information only times out when a router is down.

E. Computing the New Routes: Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Every link is, in fact, represented twice, once for each direction.

Now the shortest path to all possible destinations can be calculated, and the results can be installed in the routing tables.

Link state routing is widely used in actual networks, so a few words about some example protocols using it are in order. The OSPF protocol, which is widely used in the Internet, uses a link state algorithm. Another link state protocol is IS-IS

(Intermediate System-Intermediate System), which is adopted by ISO for use with its connectionless network layer protocol, CLNP.

Figure 12.8 illustrates the content of the packet of every node.

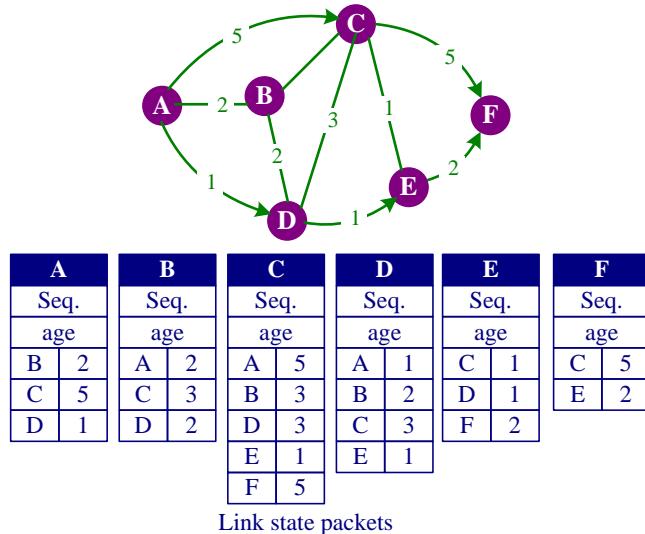


Figure 12.8: Building Link State Packets



An AS or routing domain is a group of networks that use the same routing protocol and are under common administration. All routers in an AS have identical link state databases, which contain information about each router's local state.

12.4.2.3 Distance Vector versus Link State

The link state routing algorithm offers the following advantages over the distance vector routing algorithm:

- DVA based routers exchange their entire routing table on a periodic basis, adding to overall network traffic, while LSA Based routers exchange only routing table updates.
- DVA based routers use only the single metric hop count to create their routing tables, while LSA based routers can also use link speeds and traffic patterns to establish cost values for routing traffic.
- On the other hand, LSA based requires considerably more processing on the part of the router, making it more expensive to implement. LSA based is also more complex to configure than RIP.

12.5 Routing protocols

Routing protocols are application protocols used not by users, but by routers to fill their routing tables automatically by mutual communication.

Routing protocols provide a basis for routers to share routing information and to calculate routing tables. Each routing protocol defines the data elements of a network topology data base (routing DataBase, or equivalent otherwise-named DataBase) which can be communicated by means of the routing protocol and will provide the basis of the routing table calculation. The routing protocol specification also defines the routing algorithm which is mathematical procedures for determining the cost of various paths or routes through an internetwork so that traffic can be routed most efficiently.



There is a difference between a routing protocol and a routable protocol. A routable protocol is one that allows for routing such IP. Routing protocols enable the routing functions to work properly. *Routable protocol* needs a *routing protocol* to enable it to route between networks.

There are more routing protocols than you can shake a stick at. Some are historic, most are experimental, and a few were mistakes. Here we will explain the basic Intradomain and Interdomain Routing Protocols

12.5.1 Intradomain and Interdomain Routing

There are two classes of routing protocols: intradomain routing protocol or intranetwork routing protocol or intranet, and interdomain routing protocol or internetwork routing protocol or extranet. An intradomain routing protocol routes packets within a defined domain, such as for routing e-mail or Web browsing within an institutional network. By contrast, an interdomain routing protocol is a procedure for routing packets on networks of domains.

When large enterprise and regional networks use centralized routing protocols to manage their routers, an intradomain routing policy is followed. In instances where multiple routing protocols are being used to cross-pollinate routing information, an interdomain routing policy is followed because more than one routing domain is being used to manage the route discovery across the entire network.

The distinctions between intradomain and interdomain make more sense when you examine how large and extremely large IP networks are structured. Intradomain routing is generally used in intranets. Most company-wide networks can be considered intranets. Most intranets pursue an intradomain routing policy.



When large enterprise and regional networks use centralized routing protocols to manage their routers, an *intradomain* routing policy is followed. In instances where multiple routing protocols are being used to cross-pollinate routing information, an *interdomain* routing policy is followed.

12.5.2 Intradomain Routing Protocols

The most widely used intranetworking routing protocols are the two unicast routing protocols RIP and OSPF.

12.5.2.1 Routing Information Protocol (RIP)

RIP is based on the distance vector routing algorithm and used in small to medium-sized internetworks. RIP is an intradomain routing protocol that can function only within a given routing domain. Microsoft Windows NT Server and Microsoft Windows 2000 Server support RIP; a multihomed machine running Windows NT or Windows 2000 can be used as a RIP router.

Routing Information Protocol (RIP) is a distance vector routing protocol used widely in simple IP networks to dynamically calculate the cost or metric of each possible path through an internetwork. RIP is designed for intradomain routing. Its Routing tables are calculated on the basis of the number of hops to the destination network and do not use other routing metrics such as load, bandwidth, latency, or Maximum Transmission Unit (MTU) in calculating routing costs. The routing table of a RIP router contains the cost in hops of every path to every destination network in the internetwork.

12.5.2.1.1 RIP Data Unit Format

RIP messages are carried within UDP datagrams .UDP offers basic delivery and checksum protection for its payload. RIP uses a single message format, as shown in Figure 12.9. Each message consists of a single 4-byte header and between 1 and 25 route entries. The header identifies the RIP command using a single-byte command code value selected to indicate what purpose the message serves. There is also a protocol version indicator that carries the value. For example 2 is used to show that it is RIPv2.

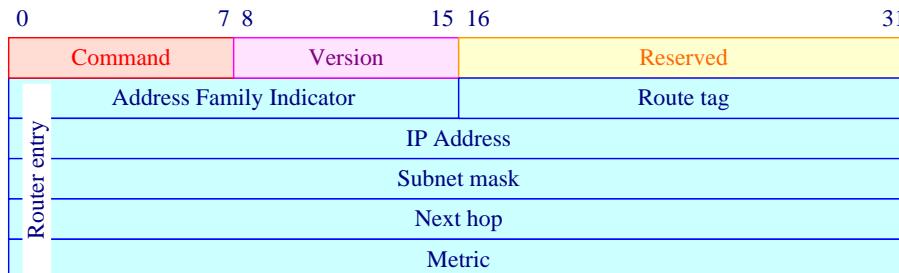


Figure 12.9: RIP message consists of a 4-byte header followed by route entries.

The body of the message is made up of route entries. The number of route entries can be determined from the length of the UDP datagram and there is no other length indicator. Each route entry carries information about one route that can be reached through the reporting node, so to report a full routing table may require more than one message. The Address Family Indicator (AFI) indicates the type of addressing information that is being exchanged and is set to 2 to indicate IPv4—the interface address being reported is carried in the IP Address field in network byte order (note that unnumbered links are not supported by RIP). The Metric is the cost of reaching the destination through the reporting router—the distance.

The other fields build more information into the basic distance vector distribution. The Route Tag allows a 16-bit attribute or identity to be associated with each route and must accompany the route if it is advertised further by the receiving router. The intention here is to allow all routes advertised from one domain or autonomous system to be easily recognized. Route tagging is not special to RIP, and other routing protocols use it equally; there is good scope for using route tags to integrate RIP with other routing protocols.

The Subnet Mask identifies the network address for the route being advertised when applied to the IP address carried in the route entry. A zero value means that the address is a host address (that is, no subnet mask has been supplied).

The Next Hop field announces the next hop router that should be used to satisfy this route. That is, the route advertisement may advertise a route on behalf of another node on the directly connected network. This may be particularly useful if RIP is not being run on all of the routers on a network, as indicated in Figure 12.10. A value of 0.0.0.0 indicates that routing should be via the originator of the RIP advertisement.

RIP-enabled routers broadcast their complete routing tables every 30 seconds over (UDP) port 520. This information is propagated only throughout the local network and received only by routers that have a routing interface to the local network as it is broadcast information. RIP does not support multipath routing. If a routing table has multiple routes for a single network ID, RIP stores the route with the lowest metric (number of hops to destination).

When a RIP router is first turned on, it announces its presence using a General RIP Request message so that neighboring RIP routers can send it advertisements of their routing tables. These RIP advertisements from neighboring RIP routers allow the router to build its own routing tables. In addition, the new RIP router announces to its neighbors all network IDs of locally attached networks so that they can update their routing tables with this information.

RIP supports a maximum metric of 15; networks that are more than 15 hops away are unreachable using RIP. After that a RIP router returns an Internet Control Message Protocol (ICMP) Destination Unreachable message.

RIP is a well-supported industry standard routing protocol. Its main disadvantage is that the routing table of a RIP-enabled router can be quite large because it contains all possible routes to all possible networks. RIP advertisement packets are only 512 bytes in length and can contain a maximum of 25 different routing table entries, so a large routing table with hundreds of entries means that dozens of RIP packets are broadcast every 30 seconds. This can result in a lot of extra broadcast traffic on the local subnet. RIP is therefore not suitable for large internetworks or for networks with many slow wide area network (WAN) links.

In addition, routing entries in a RIP routing table time out 3 minutes after the last RIP announcement is received. If neighboring routers do not hear from a RIP router within 3 minutes, networks that are locally attached to the missing router are assigned a hop count of 16, making them unreachable.

 A RIP-enabled router that can receive RIP broadcasts but cannot send them is called a Silent RIP Router.

12.5.2.2 Open shortest path first

OSPF was developed by the Internet Engineering Task Force (IETF) in 1988 as a more scalable solution than RIP. It is a link-state routing protocol. Every router using OSPF is aware of its local link-cost status and periodically sends updates to all routers. After receiving update packets, each router is responsible for informing its sending router of receipt of the update.

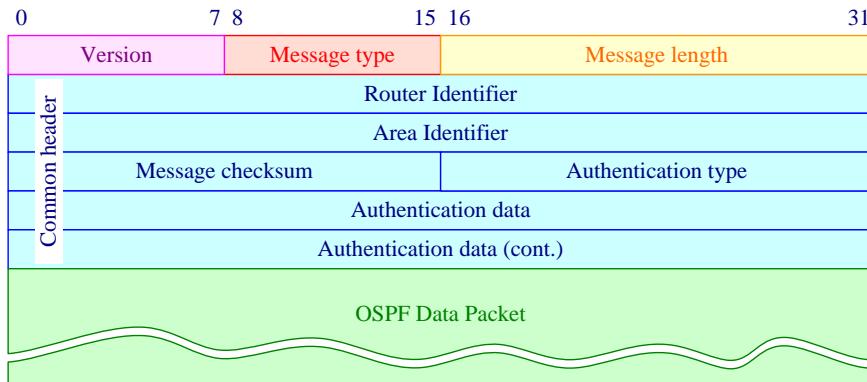


Figure 12.10: OSPF General Packet format

 When you design an OSPF-Based internetwork, you should work from the top down—that is, you should first plan your autonomous system and how it will interact with other autonomous systems, and then you should subdivide the autonomous system into areas and then into individual networks.

12.5.2.2.1 OSPF Packet Format

An IP packet that contains OSPF has a standard broadcast IP address of 224.0.0.5 for flood routing. All OSPF packets use a 24-byte header as follows:

- Version number: indicates the version of OSPF.
- Message Type: It takes one of the values from 1 to 5 according to the type of packet. The types of packets are:
 - Hello packet (message type =1): It is used to discover its active neighboring routers, each router periodically sends out hello packets to its neighbors. Each packet contains the identity of the neighboring router interface taken from the hello packet already received from it.
 - Data base description packet (message type =2): It is used for data base structure exchange between two adjacent routers to synchronize their knowledge of network topology.

- Link state request packet (message type =3): It is transmitted to request a specific portion of link-state data base from a neighboring router.
 - Link state update packet (message type =4): It transfers the link-state information to all neighboring routers.
 - Link state acknowledgment packet (message type =5): It acknowledges the update of a link-state packet.
- Packet length: specifies the length of the OSPF packet.
- Router ID: specifies the packet's source router ID.
- Area ID: refers to the area that the source router belongs to.
- Checksum: specifies the standard IP checksum of the packet contents.
- Authentication type: identifies which authentication method to choose.
- 0: Null authentication
 - 1: Simple password
 - 2: Cryptographic authentication
 - 3- 65 535: Reserved values
- Authentication specifies the authentication codeword and algorithm.

The entire OSPF packet is carried directly by the Internet protocol, with the IP packet header protocol field value set to protocol number 89.

When a router is turned on, it transmits hello packets to all neighboring routers and then establishes routing connections by synchronizing dataBases. Periodically, each router sends a link-state update message describing its routing data base to all other routers. Therefore, all routers have the same description of the topology of the local network. Every router calculates a shortest-path tree that describes the shortest path to each destination address, thereby indicating the closest router for communications.



Interior Gateway Protocols (IGPs) is the general name of intradomain protocol specifies how routers within an autonomous system (AS) exchange routing information with other routers within the same autonomous system. Examples of IGPs for TCP/IP internetworks include RIP and OSPF Protocols.

12.5.3 Interdomain Routing Protocols

Interdomain routing protocols route packets outside of a defined domain. Each domain consists of several networks and routers that can be accessed publicly. They are used to create a network of networks, or an internetwork.

The networks managed by the ISPs are designated as autonomous systems (ASs) as in Figure 12.11, and routing is achieved within each AS by running an Interior Gateway Protocol (IGP). The IGPs are unaware of the topology of the Internet outside of the AS, but do know how to route traffic to any node in the AS and to the nodes that lie on the edge of the AS: the autonomous system border routers (ASBRs).



Autonomous systems are part of the routing infrastructure of a large internetwork and can be subdivided into routing domains. They can be defined by the uniform use of a particular routing protocol such as Open Shortest Path First (OSPF).

The ASBRs provide connectivity to ASs under separate management. The issue arises of how to route traffic between ASs. In effect, out of which ASBR should an AS route traffic for a target host that lies in some other AS? It is feasible to configure this information manually and to inject it into the IGP running in the AS, but the number of ASs in the Internet has grown quite large, the interconnections between ASs are numerous, and such manual configuration would be very hard to maintain accurately. The answer is to run a routing protocol between the ASs. Such a protocol is described as an Exterior Gateway Protocol (EGP). The Border Gateway Protocol is an EGP.

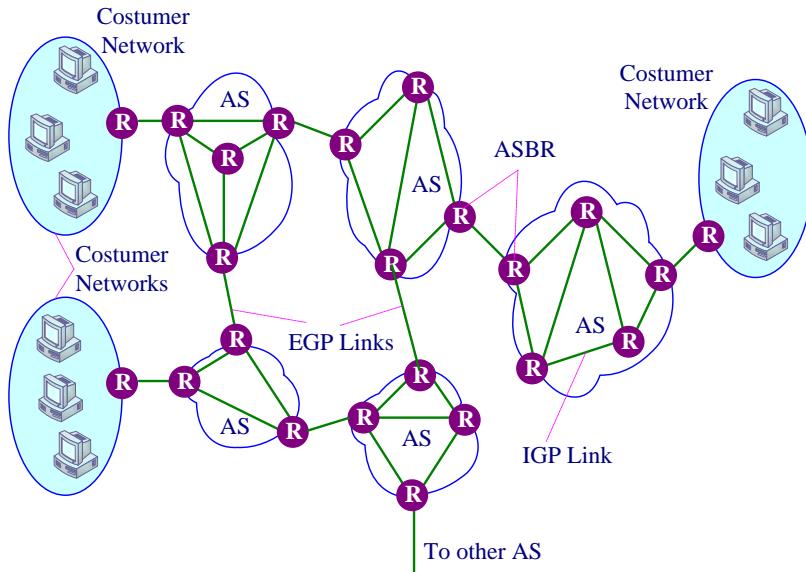


Figure 12.11: Autonomous systems within the Internet



An autonomous system (AS) is an administrative domain, it is a portion of a large internetwork that is under a given administrative authority. In order for the routing between two different *autonomous systems* (ASs) to be controlled by BGP, at least one router in each system must be configured to speak BGP.

12.5.3.1 Border Gateway Protocol

In order for the routing between two different autonomous systems (ASs) to be controlled by BGP, at least one router in each system must be configured to speak BGP. BGP speakers exchange reachability information by means of the border gateway protocol

(BGP)—in the case of speakers in different autonomous systems, the BGP is termed exterior border gateway protocol (EBGP). All reachable destinations are identified by means of their AS number, the IP address-ranges associated with the destination AS and the complete path to the destination AS from the BGP router advertising the route. The path is described as a list of networks (i.e. autonomous systems) which must be transited along the way. In addition, a list of path attributes is also provided. This identifies the types of services which can be carried and any limitations on the use of the path.

With BGP, routers exchange more comprehensive information about routes to a certain destination instead of simply costs and the best link. In BGP, two contributing routers can exchange routing information even if they are located in two different autonomous systems. When an external destination is chosen, a router sends the information to all internal neighbors. Then, all routers decide whether the new route is possible, and if so, the new route is added to the router's DataBase. Thus, the new update message is propagated. One of the most important techniques in BGP is path-vector routing.

BGP works well for making a connection when a long-haul TCP session must be established. BGP has three functional components:

1. Neighbor relationship: The neighbor relationship refers to an agreement between two routers in two different autonomous systems to exchange routing information on a regular basis. A router may reject its participation in establishing a neighbor relationship for several reasons, such as the rule of the domain, overload, or a temporary malfunctioning of external links.
2. Neighbor maintenance: Neighbor maintenance is a process of maintaining the neighbor relationship already established. Normally, each corresponding router needs to find out whether the relationship with the other router is still available. For this reason, two routers send keep-alive messages to each other.
3. Network maintenance: The last BGP process is network maintenance. Each router keeps the data base of the subnetworks that it can reach and tries to get the best route for that subnetwork.

12.5.3.1.1 BGP Data Unit

BGP Data Unit consists of header and message as it is shown in Figure 12.12. The header in its turn consists of three fields:

- **Marker field:** It is either set with all bits of value ‘1’ or alternatively contains authentication information.
- **Length field:** It indicates the length of the BGP-packet in octets (including header). Allowed values are 19–4096.
- **Type field:** This value indicates the type of BGP message and therefore the format of the remainder of the message following the BGP common header.
- **BGP Message:** Data unit may contain any of the following five different BGP messages:
 - **Open Message (Message type=1):** This packet is used to negotiate the mutual configuration of BGP peer routers after establishment of the TCP connection.

- **Update Message (Message type=2):** This packet conveys update information about routes. Once a BGP peer relationship has been opened, the BGP peers exchange their complete routing tables by means of BGP update messages.
- **Notification Message (Message type=3):** This packet is used to notify protocol errors which may occur during a BGP connection. Should such an error occur, then the connection is cleared immediately after sending the notification message.
- **Keep-alive Message (Message type=4):** This packet has a similar function to the hello packet of OSPF. The keepalive message informs the peer BGP router, that despite not having sent a routing update message, the router is still ‘alive’ and fully operational, and that all previously advertised reachable destinations are still available. This prevents routing information from being aged and therefore deleted and removed from routing table calculations.
- **Route-Refresh message:** A specific request to a BGP router for it to re-advertise all of the routes in its routing table using Update messages.

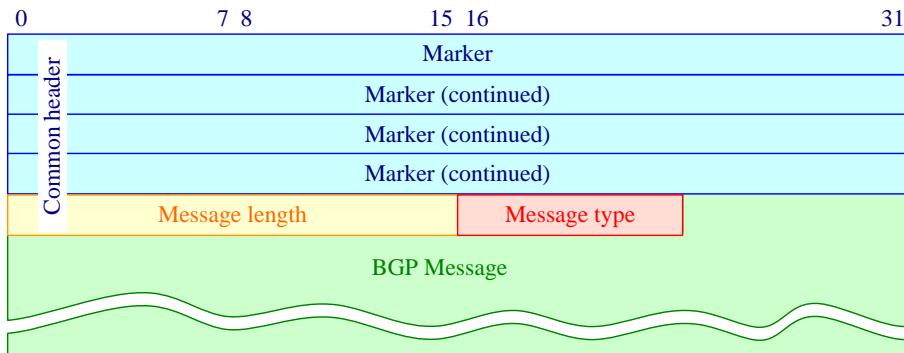


Figure 12.12: The common BGP data unit format

BGP is carried by the Transmission Control Protocol (TCP), which is a reliable transport protocol. Using this protocol means that BGP is able to concentrate on routing and leave issues of reliable delivery, retransmission, and detection of connection failure to the underlying transport protocols. On the other hand, a consequence of using TCP is that each BGP router must be configured with the address details of its peers so that it can initiate connectivity.



Exterior Gateway Protocol (EGP) can also be used as an Interior Gateway Protocol for route exchange between routers within an autonomous system or for transporting exterior routes across an AS to advertise them into the next AS.

12.6 Mobile Routing

12.6.1 Addresses and Agents

In a mobile IP network, a mobile host (Roaming host) actually computes on the run and wants to maintain its connections as he moves around. Mobile host is allowed to hold two addresses simultaneously. One of the two addresses is permanent, which is the conventional IP address in its home network called the home address and is assigned to a mobile host for an extended period of time. The other address is temporary. Any host needs to be registered by the home mobile switching center (MSC) called the home agent.

When a mobile host leaves its home network and enters a foreign network, the host must also be registered by the new network and obtain a temporary address. It is assigned to the mobile host when he leaves its home network for a foreign network; this address is called a foreign address reflecting the mobile host's current point of attachment when away from its home network. Host's messages from the Internet corresponding servers are still sent to the mobile's home address. Similarly, a foreign agent is a router in the mobile host's foreign network that informs a host's home agent of its current foreign address. The home agent always forwards messages to the mobile host's current location as it is shown in Figure 12.13.

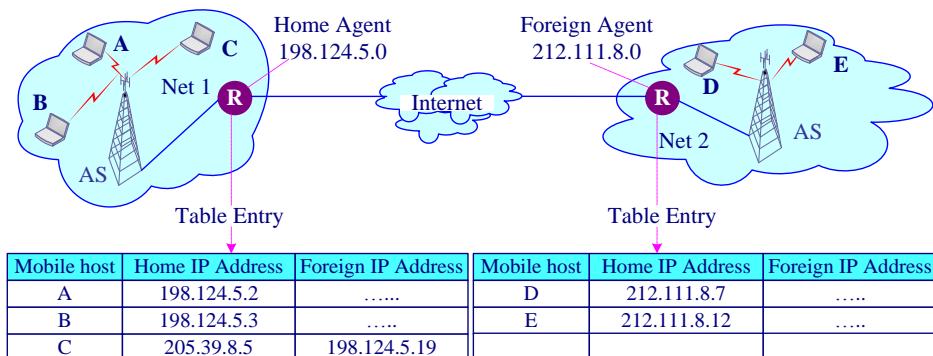


Figure 12.13: Two wireless networks connected to the Internet.

The routing goal in systems with mobile hosts is to make it possible to send packets to mobile hosts using their home addresses and have the packets efficiently reach them wherever they may be. The trick, of course, is to find them.

A home agent maintains a data base containing the mobile host's home address. When a mobile host moves to a foreign network, its home and foreign agents establish an association for updating registration with its home agent through the foreign agent using agent advertisement messages. The message type defined whether the mobile host is located in its home network or in a foreign network.

Advertisement messages are propagated periodically in a broadcast manner by all agents. If the mobile host does not receive the advertisement for any reason it sends a request message to the agent which it is attached to. If the host is attached to a home agent,

the registration process is the same as traditional host in a fixed place. But, if the agent is a foreign one, the agent replies with a message containing a foreign address for the agent.

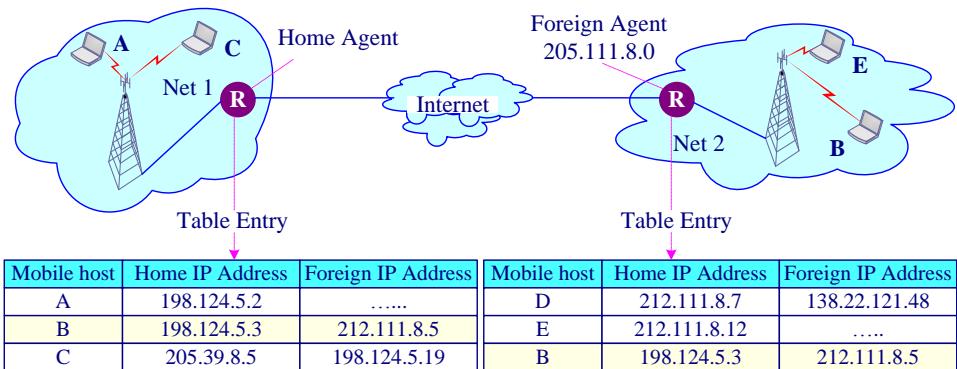


Figure 12.14: The previous two wireless networks connected to the Internet after sometime.

For example consider the Figure 12.13 which shows two wireless networks connected to the Internet. Network 1 has a net ID 198.124.5.0 and it has three active mobile hosts A, B, and C. Suppose that this network is the home network for hosts A and B and but not for host C as it appears from the home IP addresses of the agent routing entry. Consider a situation in a different time as shown in Figure 12.14 in which host A stays in this network, thus there is no foreign address for it, and host B moves out of this network, thus it obtains a foreign address. Particularly, host B has moved to network 2. Network 2 has Net ID 212.111.8.0, and it has three active mobile hosts D, E, and B. Network 2 is now considered a foreign network for B and is therefore assigned a foreign address of 212.111.8.5. This address appears in its both associated home and foreign agents as seen in the figure.

Mobile IP acts as an interface between the mobile's home network and the foreign network where the mobile currently resides. Mobile IP keeps track of the mobile's locations, and maps a home address into a current foreign address. The mobile IP interface delivers messages from the mobile's home network to the mobile host in its current foreign location in a seamless fashion after a registration process with the foreign agent is completed.

12.6.2 IP Routing in Mobile Network

In mobile IP systems, datagrams are encapsulated by a mobile IP header. Figures 12.15 and 12.16 show the message format of mobile IP registration.

- **Type field:** determines whether the registration is a request or a reply.
- **Flags/code field:** is used in the reply-message to specify forwarding details.
- **Lifetime field:** gives the permitted time (in seconds) a registration is valid.
- **Node address field:**

- **Care-of address (Temporary address) field:** are the two addresses explained.
- **Home agent field** specifies the home-agent address of the host.
- **Identification field:** helps a mobile host prevent repeated messages.
- **Extensions** to the Request and Reply messages exist to convey authentication details. The extensions are defined for use in communication between the different components of the mobile IP network. Thus, there are extensions for Mobile-Home Authentication, Mobile-Foreign Authentication, and Foreign-Home Authentication.

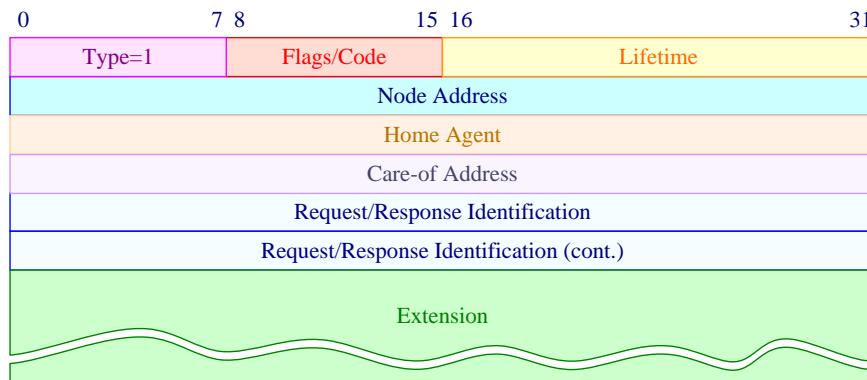


Figure 12.15: The Mobile Node Registration Request message.

Figure 12.17 shows the basic operation of Mobile IP. A mobile node is normally attached to its home network using a static home address. When the mobile node moves to a foreign network, it makes its presence known by registering with a foreign agent (FA) as follows:

- Use UDP datagram to register with an agent on the new network
- Register with home agent to request call forwarding
- Renew any registration when it is about to expire
- Cancel the registration with the new network when returning to the home network,

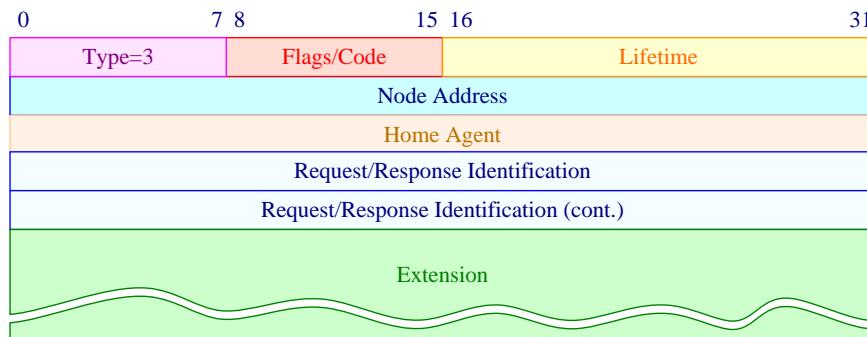


Figure 12.16 The Mobile Node Registration Reply messages.

A registration phase involves an exchange of two messages between the mobile host and its home agent: registration request and registration response. Once a mobile host

enters a foreign network, it listens for agent advertisements and then obtains a foreign address from the foreign network it has moved to. The mobile node then communicates with a home agent (HA) in its home network, giving it the care-of address (COA), which identifies the foreign agent's location. Typically, routers in a network will implement the roles of home and foreign agents. The host's home-network agent then adds the foreign network address agent to its home-location DataBase. This is done after the agent authenticates the host through the host's home-network agent. The host's home-network agent now forwards all calls to the host in the foreign network. On the Internet, the location management and routing are done through mobile IP.

When IP datagrams are exchanged over a connection between the mobile node B and a correspondent host F, the following operations occur:

1. Host F transmits an IP datagram destined for mobile node B, with B's home address in the IP header. The IP datagram is routed to B's home network.
2. The incoming IP datagram is intercepted by the home agent, which encapsulates the entire datagram inside a new IP datagram, which has B's care-of address (foreign address) in the header, and retransmits the datagram. The use of an outer IP datagram with a different destination IP address is known as tunneling.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a MAC-level PDU and delivers the original datagram to B across the foreign network.
4. When B sends IP traffic to F, it uses F's IP address. In our example, this is a fixed address; i.e., F is not a mobile node. Each IP datagram is sent by B to a router on the foreign network for routing to F.
5. The IP datagram from B to F travels directly across the Internet to F, using F's IP address.

Each datagram forwarded to the mobile host's home address is received by its home agent, and then it is forwarded to the mobile host's foreign address. In this case, mobile host's foreign agent receives the datagram and forwards it to the mobile host. If a mobile host residing in a foreign network wants to send a message to host outside of its new network, the message is not required to be passed through its home agent. In such a case, the message is handled by the foreign agent.

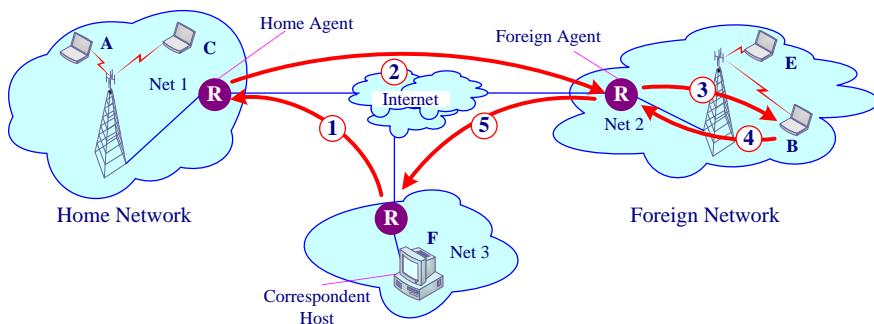


Figure 12.17: The basic operation of Mobile IP.



With mobile IPv4:

- ▶ Multicast packets had to be tunneled to the Home Agent in order to use the home address as source address of the multicast packet.
- ▶ all packets sent to the home address while the mobile node is connected to a foreign network must be encapsulated.
- ▶ a mobile node detects a Home Agent by sending out a broadcast request and therefore receives separate answers from all Home Agents on its segment.

12.6.3 Mobile Routing with IPv6

IPv6 has so many addresses available that the mobile node can make up its own by combining the visited network's prefix with an identifier unique to the device, such as its MAC address. This eliminates the need for a mobility agent, speeds up the process, and ensures that a care-of address is always available. Mobile IPv6 offers a simpler mobile routing scheme. With IPv6, no foreign agent is required. A mobile host should use the address autoconfiguration procedure embedded in IPv6 to obtain a foreign address on a foreign network. The procedure to route with mobile IPv6 is summarized as follows:

12.6.3.1 Mobile IPv6 Routing Steps

1. A host informs its home agent and also corresponding machines about its foreign address.
2. If a corresponding machine knows the mobile's current foreign address, it can send packets directly to the mobile host by using the IPv6 routing header; otherwise the corresponding machine sends packets without the IPv6 routing header.
3. Packets are routed to the mobile host's home agent
4. Packets are forwarded to the mobile host's foreign address
5. If the mobile host moves back to its home network, the host notifies its home agent.



In IPv6:

- ▶ multicast packets are included in the Destination Options header and can be processed by every receiving node.
- ▶ packets sent to the mobile nodes home address must still be encapsulated, but packets exchanged directly once the binding update has happened can be sent using a Routing header, which is more efficient and creates less overhead.
- ▶ the request is sent using an anycast address, which results in one reply only.

12.7 Quick Review

- ❖ The datagram may be routed locally (direct routing), using of a forwarding device (indirect routing), or in general invoke both of them.
- ❖ The routing table looks up an entry (network destination, net-mask, forwarding address or gateway, interface, metric and lifetime) corresponding to the destination address of the incoming packet and provides the output network port.
- ❖ The router calculates the link cost between a pair of source and destination nodes and chooses the least-cost path.
- ❖ The creation, updating and maintenance of the routing table may be undertaken manually (static routing), or automatically by the routers (dynamic routing).
- ❖ Routing algorithms can be differentiated on several key characteristics such as accuracy, simplicity, optimality, stability, adaptability, convergence and load balancing.
- ❖ Dijkstra's is the most popular and widely used least-cost-path algorithm. This algorithm determines least-cost paths from a source node to a destination node by optimizing the cost in multiple iterations.
- ❖ Routing algorithms can be classified as either least-cost path, or non-least-cost path. They can be classified based on whether an algorithm is distributed or centralized. Mathematically they come in two common types: distance vector routing algorithms and link state routing algorithms.
- ❖ DVA based protocol includes its routing updates with a vector of distances, or hop counts from each possible source router to each possible destination. In the link-state routing, routers collaborate by exchanging packets carrying status information about their adjacent links.
- ❖ Routing protocols provide a basis for routers to share routing information and to calculate routing tables.
- ❖ The most widely used intranetworking routing protocols are the two unicast routing protocols RIP, which is based on the distance vector routing algorithm and used in small to medium-sized internetworks, and OSPF which is a link-state routing protocol.
- ❖ In BGP, two contributing routers can exchange routing information even if they are located in two different autonomous systems. Exterior Gateway Protocol (EGP) can also be used as an Interior Gateway Protocol for route exchange between routers within an autonomous system or for transporting exterior routes across an AS to advertise them into the next AS.
- ❖ Mobile host is allowed to hold two addresses simultaneously. One is permanent and called the home address, while the other is temporary and called foreign address.
- ❖ Any host needs to be registered by the home mobile switching center (MSC) called the home agent.
- ❖ When a mobile host enters a foreign network, the host must also be registered by the new network and obtain a temporary address.
- ❖ The routing goal in systems with mobile hosts is to make it possible to send packets to mobile hosts using their home addresses and have the packets efficiently reach them wherever they may be.

- ❖ Mobile IP acts as an interface between the mobile's home network and the foreign network where the mobile currently resides. Mobile IP keeps track of the mobile's locations, and maps a home address into a current foreign address.
- ❖ With IPv6, a mobile host should use the address auto configuration procedure embedded in IPv6 to obtain a foreign address on a foreign network.

12.8 Self Test Questions

A- Answer the following questions

1. What is the difference between direct and indirect routing?
2. What is the purpose of the routing table and what are the entries that it can contain?
3. What may the cost path reflect? List some routing metrics.
4. What are the types of routes that can be used to store the routing table entries?
5. Compare between static and dynamic routing.
6. What are the differences between routing and routable protocols?
7. List some key characteristics that can be used to evaluate routing algorithms.
8. Explain how to choose the least cost path.
9. How does the distance vector algorithm work?
10. What is the difference between distributed and centralized algorithms?
11. Can you make a comparison between Distance Vector versus Link State routing algorithms.
12. What are the differences between intradomain and interdomain routing?
13. Explain the RIP Data Unit Format.
14. What are the relations between autonomous systems (ASs) and Interior Gateway Protocol (IGP)?
15. What are the relations between autonomous systems (ASs) and autonomous system border routers (ASBRs)?
16. How does BGP work?
17. How does Exterior Gateway Protocol differ from Interior Gateway Protocol (IGP)?
18. Why mobile host is allowed to hold two addresses simultaneously?
19. What is the routing goal in systems with mobile hosts?
20. What is the role of foreign host in mobile routing?
21. How does the mobile node register when it moves to a foreign network?
22. Make a comparison between mobile IPv4 and mobile IPv6.

B- Identify the choice that best completes the statement or answers the question.

1. Which routing algorithm chooses a route that minimizes the sum of the costs of all the communications paths along the route?

a. best-cost	c. shortest-path
b. least-cost	d. best-path
2. Which type of routing algorithm dictates that the routing information generated from the least cost algorithm is stored at a central location within the network?

a. Distributed	c. Centralized
b. Adaptive	d. Static

3. Which routing technique allows each node to maintain its own routing table?
 - a. Distributed
 - b. Adaptive
 - c. Centralized
 - d. Static
4. Which of the following technique is a dynamic system in which routing tables react to network fluctuations.
 - a. Static
 - b. Adaptive
 - c. Centralized
 - d. Distributed
5. In which routing technique routing tables remain the same when network changes?
 - a. centralized
 - b. isolated
 - c. static
 - d. adaptive
6. In which routing technique each node takes the incoming packet and retransmits it onto every outgoing link?
 - a. distributed
 - b. saturating
 - c. flooding
 - d. adaptive
7. What is the name of the classic algorithm that calculates a least-cost path through a network?
 - a. Donagel
 - b. Dagmet
 - c. Dilbert
 - d. Dijkstra
8. _____ must be checked to determine what addresses to names are mapped on the router.
 - a. router names
 - b. name table
 - c. address table
 - d. location table
9. What is the routing protocol that depends on broadcasting the entire routing table to each neighbor router at predetermined intervals?
 - a. Link-state
 - b. Router-state
 - c. Distance-vector
 - d. Cross-vector
10. RIP is a member of a _____ routing protocol.
 - a. Distance-link
 - b. Link-distance
 - c. Distance-vector
 - d. Link-vector
11. One of the following problems may be present in a network that uses static routing.
 - a. Router's tables are always changing to reflect network changes
 - b. Router's tables may be invalid after a change in the network structure
 - c. Static routing is more insecure
 - d. They accept unroutable packets
12. One of the following problems may be present in a network that uses dynamic routing.
 - a. It is not commonly used by other networks
 - b. They do not account for changes in the network
 - c. The tables contain fixed paths
 - d. In very unstable environments, router's tables can never reach a stable state
13. The routers communicate with one another and create and maintain routing tables automatically when using _____ routing.

- a. Distance-vector
b. Link-state

c. Distance-link
d. Link-vector

25. Which of the following algorithms does not transmit the subnet mask in the routing updates?
a. IGRP
b. OSPF
c. EIGRP
d. RIP

26. _____ supports classless routing, variable length subnet masks, and authentication.
a. OSPF
b. RIPv1
c. IGRP
d. DUAL

27. _____ is a classful routing protocols.
a. GRP
b. SPF
c. RIPv2
d. EIGRP

28. _____ is aclassless routing protocols.
a. OSPF
b. RIPv2
c. EIGRP
d. all of the above

29. _____ summarizes networks to their major network boundaries.
a. Classful
b. Classless
c. Interclass
d. Exclusive

30. _____ is required for two routers to share routing table information.
a. Identical networks configuration
b. Identical next hop routers
c. Identical autonomous system numbers
d. Identical protocol configurations

31. _____ can route between autonomous systems.
a. IGRP
b. RIP
c. BGP
d. IGP

32. One of the following is an advantages provided by NAT.
a. It conserves public IP addresses.
b. It hides your internal IP addressing scheme from the outside world.
c. It allows for easy renumbering of your IP addresses.
d. all of the above

33. _____ is a type of NAT is the simplest form.
a. Dynamic with overload
b. Port address translation
c. Static
d. Dynamic

34. In _____ type of NAT the router automatically maps a group of valid local IP addresses to a group of Internet IP addresses as needed.
a. Port address translation
b. Dynamic
c. Reverse
d. Static

35. The home agent always forwards messages to the _____ current location.
a. mobile host's
b. Base station
c. central office
d. access point

36. In mobile routing _____ are propagated periodically in a broadcast manner by all agents.
- a. addressing messages
 - b. request messages
 - c. advertisement messages
 - d. management messages
37. Mobile IP acts as an interface between _____ network and the foreign network where the mobile currently resides.
- a. any wireless home
 - b. any
 - c. the fixed home
 - d. the mobile's home
38. Which of the following helps a mobile host prevent repeated messages?
- a. Identification field
 - b. Care-of address field
 - c. Home agent field
 - d. Type field
39. Which of the following determines whether the registration is a request or a reply?
- a. Identification field
 - b. Care-of address field
 - c. Extensions field
 - d. Type field
40. A registration phase involves an exchange of _____ between the mobile host and its home agent
- a. identification request and identification response.
 - b. registration request and registration response.
 - c. identification request and registration response.
 - d. registration request and identification response.
41. Routing protocols provide a basis for routers to _____
- a. share routing information only.
 - b. share routing information and to calculate routing tables.
 - c. calculate routing tables only.
 - d. do none of the above
42. Which of the following algorithms allows two contributing routers to exchange routing information even if they are located in two different autonomous systems.
- a. BGP
 - b. NAT
 - c. DNS
 - d. OSPF

CHAPTER 13

THE TRANSPORT LAYER PROTOCOLS

13.1 About This Chapter

The Internet Protocol family includes the User Datagram Protocol (UDP), and the Transmission Control Protocol (TCP). Transport protocols play an important role in the IP suite, where they provide data delivery services for most application protocols and for a large number of control protocols. This chapter introduces some of the concepts of transport before describing each of the three transport protocols.

A transport layer allows communication to exist between network stations. Data is handed down to this layer from an upper-level application. The transport layer then envelopes the data with its headers and gives it to the IP layer for transmission onto the network. There are two transport-layer protocols in TCP/IP: UDP and TCP.

The Internet protocol (IP) provides for end-to-end carriage of data through the routers and across the hops of an internetwork, but it is the role of a transport protocol to control and manage the end-to-end communication (between the hosts). The transport protocol provides a transport service to the software application running in the host—ensuring that data is delivered to the right application in the destination device, that individual packets are in the right order and that none have gone missing en route.

This chapter will begin by studying the services that a transport layer protocol can provide to network applications, including multiplexing/demultiplexing function for communicating processes. We will see that a transport layer protocol can provide reliable data transfer even if the underlying network layer is unreliable.

We will then go on to describe in detail the UDP provides for connectionless service and TCP provides for connection-oriented service. .

Flow control and congestion control algorithms will be examined in this chapter. Without flow and congestion control, a network can easily become gridlocked, with little or no data being transported end-to-end.

Reliable data transfer will be covered in this chapter while we take a close look at TCP. We will learn that TCP is complex, involving connection management, flow control, roundtrip time estimation, as well as reliable data transfer.

Mobile systems require using a modified TCP and UDP protocols. We include a short description of these protocols and how to be modified to accommodate the requirement of mobility.

If a client on one host wants to reliably send data to a server on another host, it simply opens a TCP socket to the server and then pumps data into that socket. The client-server application is oblivious to all of TCP's complexity. In the final section of this chapter we will briefly cover the principles of communication between processes using client and server sockets.

13.2 Learning Outcome

After this chapter, you should be able to:

1. Be familiar with the services provided by the transport layer protocols.
2. Understand the TCP structure, services and functions.
3. Understand the UDP structure, services and functions.
4. Explain the flow control mechanism and be familiar with its algorithms.
5. Explain the principles of congestion control and be familiar with its algorithms.
6. Make a right decision about where to use TCP and where to use UDP.
7. Understand the transport protocol for mobility.
8. Be familiar with the socket concepts.

13.3 The Transport Layer services

While the function of the network protocol is to provide for the actual carriage of the data across the network, the function of a transport protocol is to manage the end-to-end communication between applications in the two end devices (hosts) which are interconnected by means of a data network. The transport protocol ensures that all the individual packets of information making up the application's message to its peer arrive at the destination and are presented in the right order.

- A transport layer protocol provides for **logical communication** between application processes running on different hosts. Application processes use the logical communication provided by the transport layer to send messages to each other, free for the worry of the details of the physical infrastructure used to carry these messages.
- As the router is a network layer device, transport layer protocols are implemented in the end systems but not in network routers.
- Data is handled down to this layer from an upper-level application. The transport layer then envelopes the data with its headers and passes the resulting data unit down to the network layer. At the receiving side, the transport layer receives these data units, reassembles and passes them to a receiving application process.
- A computer network can make more than one transport layer protocol available to network applications. For example, the Internet has two protocols TCP and UDP. Each of these protocols provides a different set of transport layer services to the invoking application.
- As it is mentioned, the network layer provides only one communication path between the source network interface and the destination network interface, while all transport layer protocols provide an application multiplexing/demultiplexing service. The transport protocol, as Figure 13.1 illustrates, allows multiple communication sessions to be in progress at the same time, all using different protocols for email, network management, and network file system (NFS), Worldwide Web (www) or other applications.

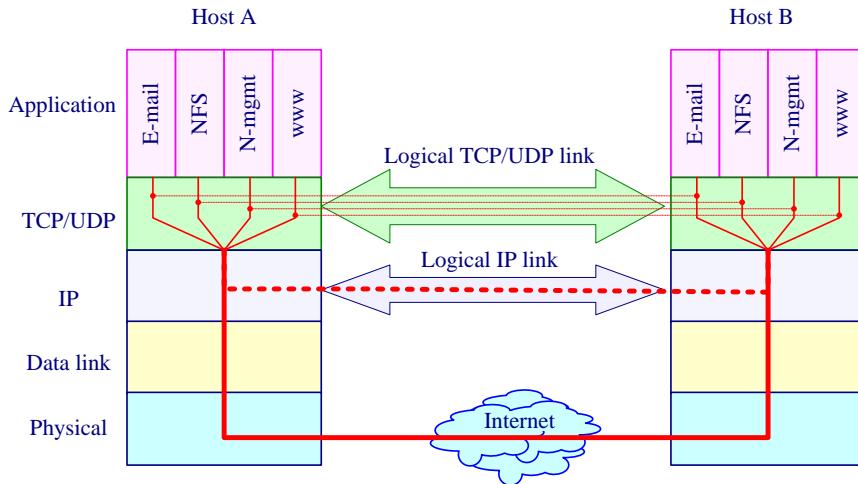


Figure 13.1: Multiplexing function of TCP and UDP transport protocols.

Whereas a transport layer protocol provides logical communication between processes running on different hosts, a network layer protocol provides logical communication between hosts.

13.4 Application multiplexing and demultiplexing

The job of the transport layer's application multiplexing and demultiplexing service is to make a process-to-process delivery.

At the destination host, the transport layer receives segments from the network layer just below. The transport layer has the responsibility of delivering the data in these segments to the appropriate application process running in the host. When you are downloading Web pages and running one FTP session and two Telnet sessions, you therefore have four network application processes running. The question is: how the transport layer in your computer will direct the received data to one of these four processes?

Each transport-layer segment has a field that contains information that is used to determine the process to which the segment's data is to be delivered.

At the sending end, the transport layer protocol gathers data at the source host from different application processes, enveloping the data with header information including the value of the mentioned field. This value indicates a certain application. The process of creation segments and passing the segments to the network layer is called multiplexing.

At the receiving end, the transport layer can then examine this field to determine the receiving process, and then direct the segment to that process. This job of delivering the data in a transport-layer segment to the correct application process is called demultiplexing.

UDP and TCP perform the demultiplexing and multiplexing jobs by including two special fields in the segment headers: the source port number field and the destination port

number field. When taken together, the fields uniquely identify an application process running on the destination host.

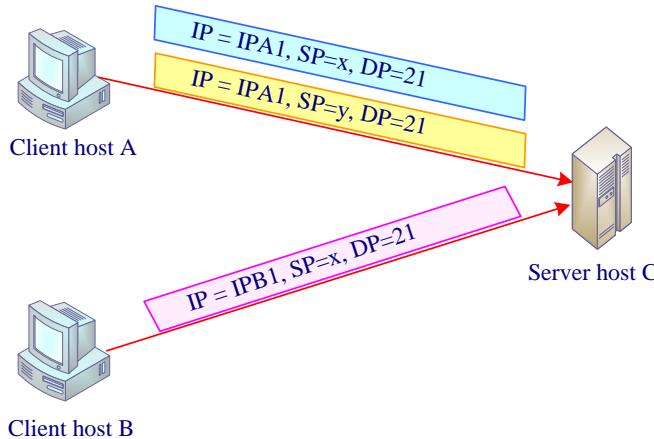


Figure 13.2: Multiplexing of two client applications, using the same port numbers

In order to be able to demultiplex the application when the two sessions have exactly the same port number pair segments the server also uses the IP addresses in the IP datagrams carrying these segments. The situation is illustrated in Figure 13.2, in which host A initiates two FTP sessions to host C, and host B initiates one FTP session to host C. Hosts A, B and C each has its own unique IP address. Host A assigns two different source port (SP) numbers (x and y) to the two FTP connections emanating from host A. But because host B is choosing source port numbers independently from A, it can also assign $SP=x$ to its FTP connection. Nevertheless, host C is still able to demultiplex the two connections since the two connections have different source IP addresses.



When a destination host receives data from the network layer, the triplet (source IP address, source port number, destination port number) is used to forward the data to the appropriate process.

13.5 The Transport Control Protocol (TCP)

TCP is a connection-oriented transport protocol that sends data as an unstructured stream of bytes. By using sequence numbers and acknowledgment messages, TCP can provide a sending node with delivery information about packets transmitted to a destination node. Where data has been lost in transit from source to destination, TCP can retransmit the data until either a timeout condition is reached or until successful delivery has been achieved. TCP can also recognize duplicate messages and will discard them appropriately. If the sending computer is transmitting too fast for the receiving computer, TCP can employ flow control mechanisms to slow data transfer. TCP can also communicate delivery information to the upper-layer protocols and applications it supports.

The main services provided by TCP are:

1. Establishing, maintaining, and terminating connections between two processes.
2. Reliable packet delivery, through an acknowledgment process.
3. Sequencing of packets, reliable transfer of data.
4. TCP congestion control
5. Mechanism for correcting errors.
6. The ability to allow multiple connections with different processes inside a particular source or destination host through the use of ports.
7. Data exchange using full-duplex operations.

13.5.1 TCP Segment

As defined earlier, a TCP segment is a TCP session packet containing part of a TCP byte stream in transit. The fields of the TCP header segment are shown in Figure 13.3. The TCP segment contains a minimum of 20 bytes of fixed fields and a variable-length options field. The details of the fields are as follows:

- **The source port field:** specifies the application software in the transmitting host. It takes one of possible values in the range of 0–65 535.
- **The destination port field:** specifies the intended destination application software in the receiving host. It takes one of possible values in the range of 0–65 535. Table 10.3 lists some of the most popular port numbers

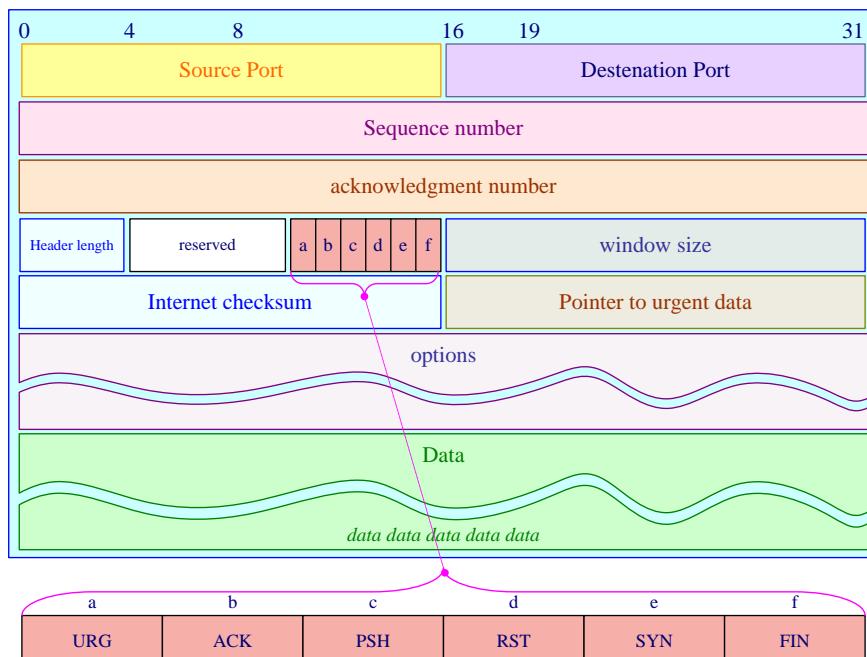


Figure 13.3: TCP Data Unit structure

- **Sequence number:** is a 32-bit field that TCP assigns to each first data byte in the segment. The sequence number commences at the initial sequence number (ISN)

number, which is chosen randomly by the transmitter, and each subsequent data segment has a sequence number accordingly greater than the previous segment. The increment in the sequence number depends upon the number of octets in the previous segment. The sequence number thus counts octets, but its value also uniquely identifies a particular segment. The sequence number restarts from 0 after the number reaches $2^{32} - 1$.

Suppose that a process in host A wants to send a stream of data to a process in host B over a TCP connection. The TCP in host A will implicitly number each byte in the data stream. Suppose that the data stream consists of a file consisting of 100,000 bytes, that the MSS is 500 bytes, and that the first byte of the data stream is numbered 100. As shown in Figure 13.4, TCP constructs 200 segments out of the data stream. The first segment gets assigned sequence number 100, the second segment gets assigned sequence number 600, the third segment gets assigned sequence number 1100, and so on.. Each sequence number is inserted in the sequence number field in the header of the appropriate TCP segment.

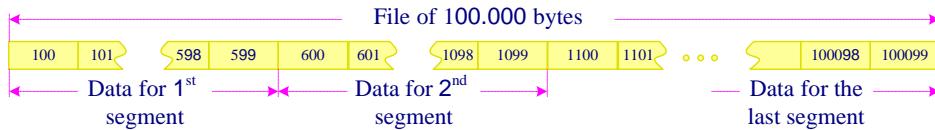


Figure 13.4: TCP constructs segments out of the data stream

- **Acknowledgment number:** specifies the sequence number of the next byte that a receiver waits for and acknowledges receipt of bytes up to this sequence number. If the SYN field is set, the acknowledgment number refers to the initial sequence number (ISN).
- **Header length (HL):** is a 4-bit field indicating the length of the header in 32-bit words.
- **Control Bits:** 6 flag bits that identify the functions of the message.
 - **Urgent (URG):** is a 1-bit field implying that the urgent-pointer field is applicable.
 - **Acknowledgment (ACK):** shows the validity of an acknowledgment.
 - **Push (PSH):** if set, directs the receiver to immediately forward the data to the destination application.
 - **Reset (RST):** if set, directs the receiver to abort the connection.
 - **Synchronize (SYN):** is a 1-bit field used as a connection request to synchronize the sequence numbers.
 - **Finished (FIN):** is a 1-bit field indicating that the sender has finished sending the data.
- **Window size:** specifies the advertised window size.
- **Checksum:** is used to check the validity of the received packet.
- **Urgent pointer (URG):** if set, directs the receiver to add up the values in the urgent-pointer field and the sequence number field to specify the last byte number of the data to be delivered urgently to the destination application.

- **Options:** is a variable-length field that specifies the functions that are not available as part of the basic header. A receiver can use this option to specify the maximum segment size it can receive. It can use this field also to scaling the advertised beyond the specified $2^{16} - 1$ in the header. The advertised window can be scaled to a maximum of 2^{14} .
- **Data (variable):** This field may contain one segment of an information sequence generated by an application layer protocol.



Both the sequence number and the acknowledgement number can be incremented up to the value $2^{32} - 1$, before the value is *wrapped* (i.e., reset to zero) and counting starts from '0' again.



The reuse of sequence numbers can cause a problem, if there is any chance that two segments might be in existence at the same time with the same segment number.

13.5.2 TCP Connection Setup

As a connection-oriented protocol, TCP requires an explicit connection set-up phase. Connection is set up using a three-step mechanism, as shown in Figure 13.5. Assume that host A is a sender and host B a destination.

Step1: The sender sends a TCP connection request to the destination. This special segment contains no application-layer data. It comprises the initial sequence number indicated by $\text{seq}(Ai)$, with the SYN bit set to 1.

Step2: The destination receipts the connection request extracts the TCP segment from the datagram, allocates the TCP buffers and variables to the connection, and sends a connection-granted segment to sender. This connection-granted segment also contains no application-layer data. The destination sends an acknowledgment, $\text{ack}(Ai + 1)$, back to the source, indicating that the destination is waiting for the next byte. The destination also sends a request packet comprising the sequence number, $\text{seq}(Bj)$, and the SYN bit set to 1.

Step3: Upon receiving the connection-granted segment, the sender also allocates buffers and variables to the connection and returns an acknowledgment segment, $\text{ack}(Bj + 1)$, specifying that it is waiting for the next byte. The sequence number of this next segment is $\text{seq}(Ai + 1)$. This process establishes a connection between the sender and the receiver. The SYN bit is set to 0, since the connection is established.

Once these three steps have been completed, hosts A and B can send segments containing data to each other. In each of these future segments, the SYN bit will be set to zero. TCP connection establishment procedure is often referred to as a because of in order to establish the connection, three packets are sent between the two hosts.

When one of the hosts wants to end the connection, it sends a segment with the RST bit set to 1. If the application has no data to transmit, the sender sends a segment with the FIN bit set to 1. The receiver acknowledges receipt of this segment by responding with an ACK and notifies the application that the connection is terminated. Now, the flow from the sender to the receiver is terminated. However, in such cases, the flow from the receiver to the sender is still open. The receiver then sends a segment with the FIN bit is set to 1. Once the sender acknowledges this by responding with an ACK, the connection is terminated at both ends.

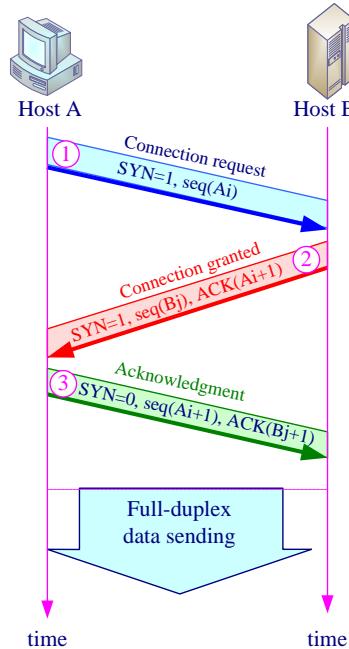


Figure 13.5: TCP connection establishment

13.5.3 TCP Flow Control

Each peer machine in a TCP session has the capability to control the flow of data that is streaming into its physical input (receive) buffers. The sending host stops sending data when it becomes suspicious that the receiver might not have received one of the segments, but it need not do this. It could continue sending data, but that might lead to the receiving buffer becoming swamped with data that it cannot deliver to its application and must store. The receiver could choose to throw away excess data and force the sender to retransmit, but ideally it needs a way to apply back-pressure on the sender to slow the sender down.

When the TCP connection receives bytes that are correct and in sequence, it places the data in the receive buffer. In some situations when the application is relatively slow at reading data from the receive buffer, the sender can overflow the connection's receive buffer by sending data which the receiving application can't read. In such case TCP provides a **flow control service** (speed matching service). You are familiar with wait and stop algorithms and sliding window algorithms used to provide flow control for frames of data

link layer. The same algorithms can be used here to handle the problem of segments flow control in transport layer.

13.5.3.1 Sliding Window TCP Flow Control

TCP provides flow control by having the sender maintain a variable called the **receive window** (to give the sender an idea about how much free buffer space is available at the receiver). The receiver uses **the receive window** field to control the amount of data beyond the last acknowledged byte that the sender may transmit. The **receive window** effectively grants the sender permission to send a certain number more bytes. Figure 13.6 illustrates the use of the Window Size.

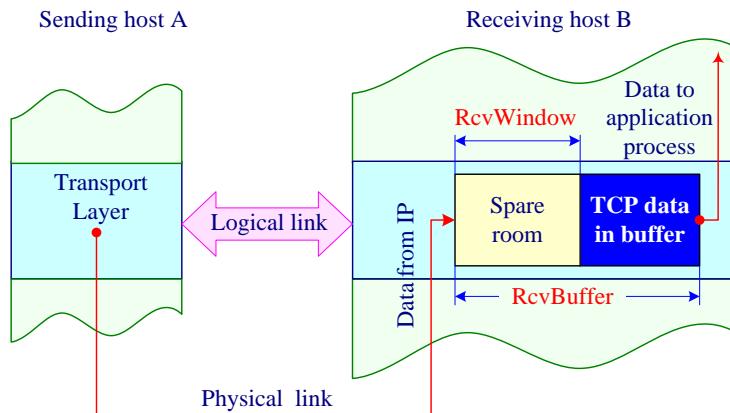


Figure 13.6: Illustration of the flow control algorithm.

Send and receive applications are shown with a send and receive buffer, respectively. The send application places data in the send buffer for the sending TCP application to transmit to the receiving TCP application. The receiving TCP application places the data in the receive buffer from where the receiving application can retrieve it. The receive window is dynamic, i.e., it changes throughout a connection's lifetime.

A window size is communicated between a source and destination machine via the TCP header. Host B informs host A of how much spare room it has in the connection buffer by placing its current value of `RcvWindow` in the window field of every segment it sends to A. When host B is becoming backlogged with incoming data and have no more spare room it may throttle back the rate at which the transmitting machine can transmit, simply by informing that machine of its new window size. If a machine's buffers fill up completely, it will send an acknowledgment of the last received data segment with a new window size of 0. This effectively halts transmission until that host B can clear its buffers. Each segment that it processes must be acknowledged and, with this acknowledgment, comes another opportunity to restart transmissions by re-establishing a window size greater than 0.

As the application process at B empties the buffer, TCP does not send new segments with new RcvWindows to host A. Therefore host A is never informed that some space has opened up in host B's receive buffer. In this case host A is blocked and can transmit no more data!

To solve this problem TCP specification requires host A to continue to send segments with one data byte when B's receive window is zero. These segments will be acknowledged by the receiver. Eventually the buffer will begin to empty and the acknowledgements will contain non-zero RcvWindow.

13.5.3.2 Round Trip Time and Timeout

TCP uses timing mechanisms for several critical functions. Each time a segment is transmitted, a timer is set. If that timer expires (that is, decrements to 0) before an acknowledgment is received, the segment is assumed to be lost. Consequently, it is retransmitted. In theory, transmission of segments is throttled back until timeouts cease occurring (this is the time from when the timer is started until when it expires). The timeout should be larger than the connection's round-trip time. But the timeout should not be much larger than the round-trip time to insure quick retransmission the segment, thereby introducing significant data transfer delays into the application.

13.5.4 TCP Congestion Control

Congestion is the situation when too many packets are present in a part of the subnet, causing the performance to degrade. In the case of sending packets in a rate which doesn't exceed the path capacity, they are all delivered, except for a few that are afflicted with transmission errors. However, as traffic increases too far, the routers are no longer able to cope and they begin losing packets.

Congestion can be brought on by several factors. If all of a sudden, streams of packets begin arriving on three or four input lines and all need the same output line, a queue will build up. If there is insufficient memory to hold all of them, packets will be lost. Waiting in the memory increase the problem because of the sender will mark these packets as timed out and will send duplicates of them increasing the load all the way to the destination.

One reason to cause congestion is the inability of the node to process the incoming packets as fast as needed. Similarly, low-bandwidth lines can also cause congestion.



Congestion control has to do with making sure the subnet is able to carry the offered traffic. It is a global issue, involving the behavior of all the hosts, all the routers, the store-and-forwarding processing within the routers, and all the other factors that tend to diminish the carrying capacity of the subnet.

 Flow control, in contrast, relates to the point-to-point traffic between a given sender and a given receiver. Its job is to make sure that a fast sender cannot continually transmit data faster than the receiver is able to absorb it. Flow control frequently involves some direct feedback from the receiver to the sender to tell the sender how things are doing at the other end.

TCP attempts to achieve this goal by dynamically manipulating the window size.

When a connection is established, a suitable window size has to be chosen (Based on the buffer size of receiver). But even if the sender sticks to this window size:

- congestion will occur due to buffer overflow at the receiving end (Figure 13.7 (a)).
- congestion may still occur due to internal congestion within the network (Figure 13.7 (b)).

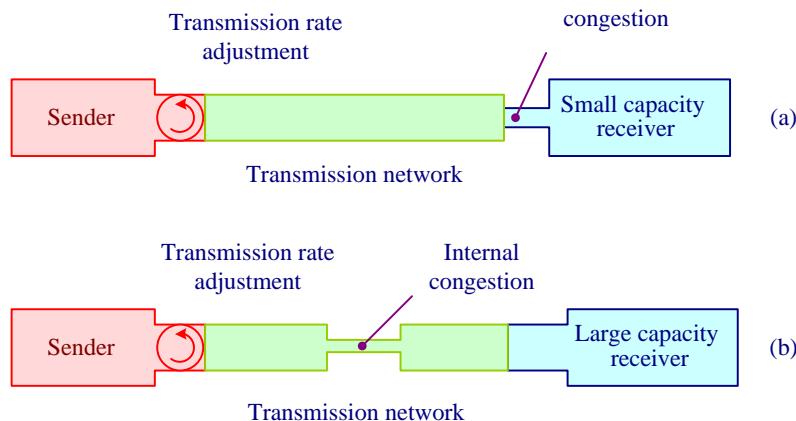


Figure 13.7: Illustration of congestion
 (a) A fast network feeding a low-capacity receiver.
 (b) A slow network feeding a high-capacity receiver.

The Internet solution is to realize that two potential problems exist

- network capacity
- receiver capacity

Each sender maintains two windows each reflects the number of bytes the sender may transmit:

- 1.the window the receiver has granted
- 2.the congestion window

The number of bytes that may be sent is the minimum of the two windows. Thus, the effective window is the minimum of what the sender thinks is all right and what the receiver thinks is all right.

13.5.4.1 Slow Start Congestion Control Algorithm:

When a connection is established

- the sender initializes the congestion window to the size of the maximum segment in use on the connection
- sends one maximum segment
- If this segment is acknowledged before the timer goes off, it doubles the congestion window to make it two maximum size segments and sends two segments
- As each of these segments is acknowledged, the congestion window is doubled. In effect each burst acknowledged doubles the congestion window.
- The congestion window keeps growing exponentially until either a timeout occurs or the receiver's window is reached.

The idea is that if bursts of size, say, n , $2n$, and $4n$ bytes work fine but a burst of $8n$ bytes gives a timeout, the congestion window should be set to $4n$ to avoid congestion. As long as the congestion window remains at $4n$, no bursts longer than that will be sent, no matter how much window space the receiver grants.

13.5.4.2 Internet Congestion Control Algorithm

This algorithm is slightly different from the previous one in the manner that it is used to accommodate data flow. It uses a third parameter, the threshold, initially 64 KB, in addition to the receiver and congestion windows, and works as follows (see Figure 13.8):

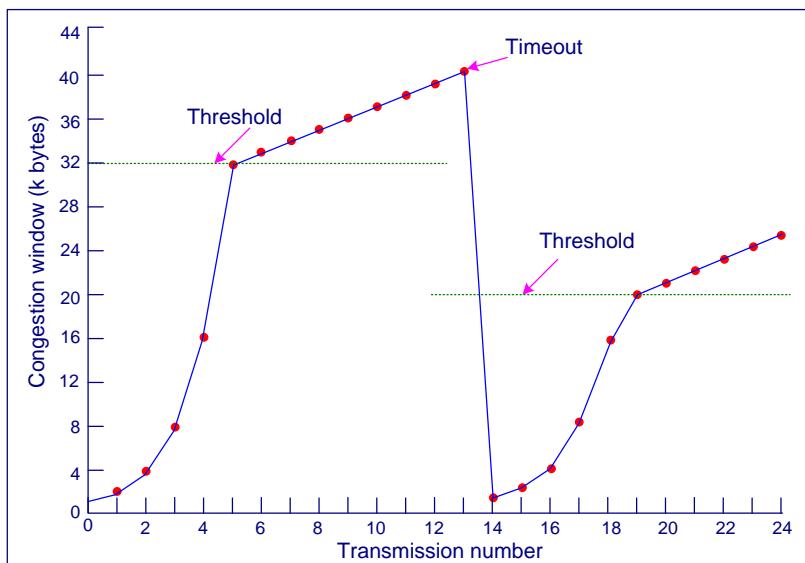


Figure 13.8: Illustration of the Internet congestion control algorithm

- When a timeout occurs, the threshold is set to half of the current congestion window, and the congestion window is reset to one maximum segment.
- Slow start is then used to determine what the network can handle, except that exponential growth stops when the threshold is hit.
- From that point on, successful transmissions grow the congestion window linearly (by one maximum segment for each burst) instead of one per segment.

- In effect, this algorithm is guessing that it is probably acceptable to cut the congestion window in half, and then it gradually works its way up from there.
- If no more timeouts occur, the congestion window will continue to grow up to the size of the receiver's window.
- At that point, it will stop growing and remain constant as long as there are no more timeouts and the receiver's window does not change size.



Other transport protocols are sometimes used in a misguided attempt to handle some of the security issues. TCP is occasionally chosen when a management application does not handle lost messages.

13.6 User Datagram Protocol

The user datagram protocol (UDP) is another transport-layer protocol that is placed on top of the network layer. UDP is a connectionless protocol, as no handshaking between sending and receiving points occurs before sending a segment. UDP does not provide a reliable service. The UDP/IP protocol combination is simply a means of delivering a datagram from one program to another with a simple one-to-one correspondence between IP datagrams and UDP datagrams. That is, each UDP datagram is carried by a single IP datagram. Hence, UDP shares all of the unreliability of the IP protocol. It is up to higher layers of software to deal with this unreliability as needed. As shown in Figure 12.6, an application data is encapsulated in a UDP header.

The enhancement provided by UDP over IP is its ability to check the integrity of flowing packets. IP is capable of delivering a packet to its destination but stops delivering them to an application. UDP fills this gap by providing a mechanism to differentiate among multiple applications and deliver a packet to the desired application. UDP can perform error detection to a certain extent but not to the level that TCP can.

UDP has the following characteristics:

1. UDP is a connectionless, unreliable transport protocol. Unlike TCP, which is connection oriented, UDP operates in the datagram mode. UDP makes no attempt to create a connection. Data is sent by encapsulating it in a UDP header and passing the data to the IP Layer. The IP Layer sends the UDP packet in a single IP datagram unless fragmentation is required.
2. Does not provide acknowledgment to the sender upon the receipt of data.
3. UDP does not attempt to provide sequencing of data; therefore, it is possible for data to arrive in a different order from which it was sent. Applications that need sequencing services must either build their own sequencing mechanism as part of the application or use TCP instead of UDP. In many LAN environments, the chance of data being received out of sequence is small because of small predictable delays and simple network topology.
4. May lose packets or duplicate them without issuing an error message to the sender.
5. UDP tends to run faster than TCP, less overhead. UDP is useful in applications that are command/response oriented and in which the commands and responses can be sent

in a single datagram. There is no overhead involved in opening and then closing a connection just to send a small amount of data.

13.6.1 UDP Segment

The format of the UDP segment is shown in Figure 13.9. The segment starts with the source port, followed by the destination port. These port numbers are used to identify the ports of applications at the source or the destination, respectively. The source port identifies the application that is sending the data. The destination port helps UDP to demultiplex the packet and directs it to the right application. The UDP length field indicates the length of the UDP segment, including both the header and the data. UDP checksum specifies the computed checksum when transmitting the packet from the host. If no checksum is computed, this field contains all zeroes. When this segment is received at the destination, the checksum is computed; if there is an error, the packet is discarded.

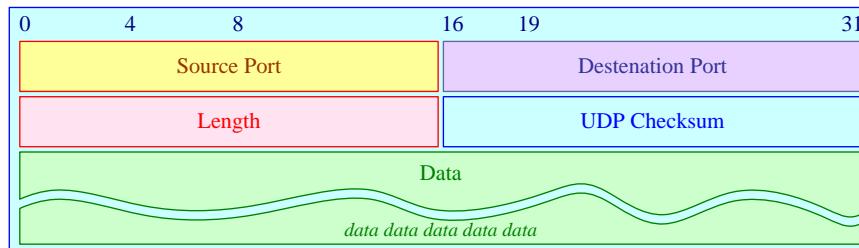


Figure 13.9: UDP segment structure

13.7 Choosing Between UDP and TCP

TCP is designed for reliable transmission of data. If data is lost or damaged in transmission, TCP ensures that the data is resent; if packets of data arrive out of order, TCP puts them back in the correct order; if the data is coming too fast for the connection, TCP throttles the speed back so that packets won't be lost. A program never needs to worry about receiving data that is out of order or incorrect. However, this reliability comes at a price. That price is speed. Establishing and tearing down TCP connections can take a fair amount of time.

The User Datagram Protocol (UDP) is an alternative protocol for sending data over IP that is very quick, but not reliable. That is, when you send UDP data, you have no way of knowing whether it arrived, much less whether different pieces of data arrived in the order in which you sent them. However, the pieces that do arrive generally arrive quickly.

Surely, if you have data worth sending, you care about whether the data arrives correctly? Clearly, UDP isn't a good match for applications like FTP that require reliable transmission of data over potentially unreliable networks. However, there are many kinds of applications in which raw speed is more important than getting every bit right. For example, in real-time audio or video, lost or swapped packets of data simply appear as static. Static is tolerable, but awkward pauses in the audio stream, when TCP requests a retransmission or waits for a wayward packet to arrive, are unacceptable. In other applications, reliability tests can be implemented in the application layer. For example, if a

client sends a short UDP request to a server, it may assume that the packet is lost if no response is returned within an established period of time; this is one way the Domain Name System (DNS) works. (DNS can also operate over TCP.) In fact, you could implement a reliable file transfer protocol using UDP, and many people have: Network File System (NFS), Trivial FTP (TFTP), and FSP, a more distant relative of FTP, all use UDP. (The latest version of NFS can use either UDP or TCP.) In these protocols, the application is responsible for reliability; UDP doesn't take care of it. That is, the application must handle missing or out-of-order packets. This is a lot of work, but there's no reason it can't be done—although if you find yourself writing this code, think carefully about whether you might be better off with TCP. Table 10.4 lists popular Internet applications and the transport protocols that they use.



The correct amount of data to stuff into one packet depends on the situation. If the network is highly unreliable, such as a packet radio network, smaller packets are preferable since they're less likely to be corrupted in transit. On the other hand, very fast and reliable LANs should use the largest packet size possible.

Application	Transport Protocol
electronic mail (SMTP)	TCP
remote terminal access (Telnet)	TCP
Web (HTTP)	TCP
file transfer (FTP)	TCP
remote file server (NFS)	typically UDP
streaming multimedia	typically UDP
Internet telephony	typically UDP
Network Management (SNMP)	typically UDP
Routing Protocol (RIP)	typically UDP
Name Translation (DNS)	typically UDP

Table 13.1: Some of popular Internet applications and their transport protocols.

13.8 Transport Protocols for Mobility

The Internet was born in an era when no mobile networking equipment was available. Therefore, all the basic protocols were designed under the tacit assumption that the end points of a communication would stay fixed all along a session. With the arrival of modern communications equipment that allows these end-points to change their position, new protocols for handling mobility have been proposed.

In order to retain transport layer connections, a mobile host's address must be preserved regardless of its point of attachment to the network. The problem with a transport layer protocol such as TCP is that a TCP connection is identified by source IP address, source TCP port, destination IP address and destination TCP port. So, if neither

host moves, all of elements remain fixed and the TCP connection can be preserved. However, if either ends of the connection moves, the following problem will take place:

- If the mobile host acquires a new IP address, then its associated TCP connection identifier also changes. This causes all TCP connections involving the mobile host to break.
- If the mobile retains its address, then the routing system cannot forward packets to its new location.

In wireless mobile networks, both UDP and TCP have their own applications. However, some modifications are needed in these protocols to become appropriate for wireless networks.

13.8.1 TCP for Mobility

Mobile computing systems are characterized by a poor link quality typically causing to lose TCP data segments which lead to a possible timeout. While TCP provides a reliable data delivery owing to the feature of its connection-oriented nature, the most challenging aspect of providing its services to a mobile host is the prevention of disruption caused by poor wireless link quality and thereby preventing the loss of packets due to congestion.

Disallowing a sender to shrink its congestion window when packets are lost for any reason, serves as an option to solve this problem. If a wireless channel soon recovers from disconnection, the mobile host begins to receive data immediately.

The Indirect Transmission Control Protocol (I-TCP), and the fast transmit will be the focus of our discussion are two other protocols used to solve this problem.

13.8.1.1 Indirect TCP

If two hosts, A is a mobile host and B fixed, are trying to establish an I-TCP connection as shown in Figure 13.10. The protocol first splits the connection into two separate connections. One wireless link is established between the mobile host and the mobile switching center (MSC), and the other fixed link between the MSC and the fixed host.

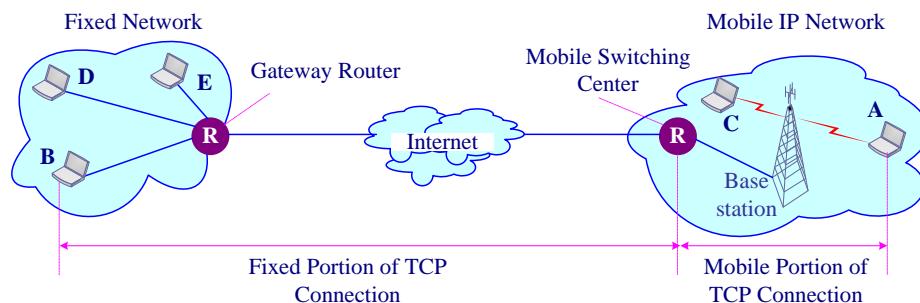


Figure 13.10: Indirect TCP for mobile hosts

This resembles two different TCP connections linked together. Note that, if for any reason the mobile host disconnects the communication on the wireless portion, the sender

may not become aware of the disconnection as the wired portion is still in tact, and the Base station still delivers the TCP segments to the mobile host. Consequently, the sender of segments may not know of segments being delivered to the mobile host. A TCP connection on the wireless link can separately support disconnections, and user mobility in addition to wired TCP features such as notification to higher layers on changes in the available bandwidth. Also, the flow control and congestion control mechanisms on the wireless link remain separated from those on the wired link. In the I-TCP scheme, the TCP acknowledgments are separate for the wireless and the wired links of the connection.

13.8.1.2 Fast Retransmit Mobile TCP

This scheme does not split the TCP connection to wireless and wired connections. Fast Retransmit improves the connection throughput especially during a cell handoff. Once two wireless cell MSCs hand off the switching function for a mobile host, the mobile host stops receiving TCP segments. The sender may interpret this as a situation of congestion leading to implement a congestion control such as window size reduction or retransmitting. This may also result in a long timeout causing the mobile host to wait a long period of time. With the fast retransmit TCP, the last old acknowledgment is triplicated and retransmitted by the mobile host as soon as it finishes a handoff. This results in significant reduction of the congestion window.

13.8.2 UDP for Mobility

UDP is used in wireless mobile IP networks because of a mobile host needs to register with a foreign agent. This process starts with a foreign agent propagating advertisements using UDP connection. Since the traditional UDP does not use acknowledgments and does not perform flow control, it is not a preferred choice of transport protocol. One way of handling this situation is to stop sending datagrams to a mobile host once it reports fading. But this method cannot be practical due to its poor quality of connection.

13.9 Communicating Processes Using Sockets

Any network application involves at least two processes in two different hosts communicating with each other over the network. These processes use sockets to send and receive messages while they communicate with each. A process's socket can be thought of as a gate for the process to send and receive messages through the network. The process assumes that there is a transportation infrastructure on the other side of the gate that will transport the message to the gate of the destination process. Figure 13.11 illustrates socket communication between two processes that communicate over the network.



Sockets provide a mechanism for building distributed network applications such as client/server applications. Two sockets form a complete bidirectional communication path between processes on two different TCP/IP hosts. Network-aware applications and services can create and destroy sockets as needed.

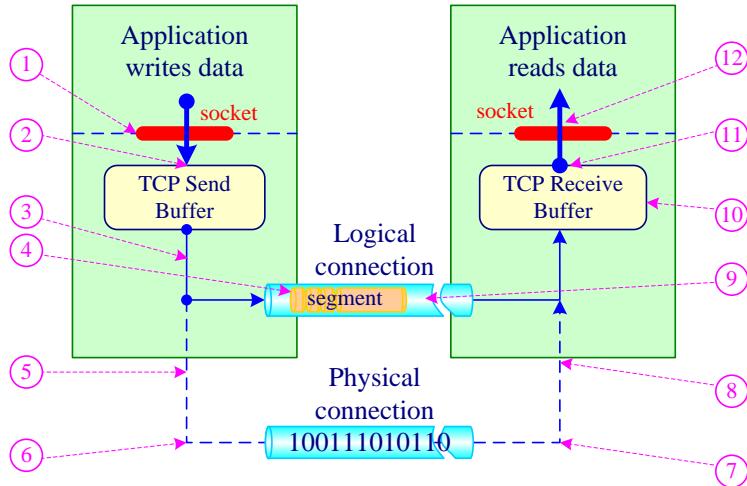


Figure 13.11: Socket communication between two processes over the network using TCP.

The **socket serves as** an interface between the application layer and the transport layer within a host. It is a logical endpoint for communication between two hosts on a TCP/IP network. A socket is an application programming interface (API) for establishing, maintaining, and tearing down communication between TCP/IP hosts. Sockets were first developed as a way of providing support for creating virtual connections between different processes.

The socket is uniquely identified by three attributes:

- The host's IP address
- The type of service needed and consequently the transport layer protocol to use. If applications need to guarantee the delivery of data, the socket chooses the connection-oriented service (TCP). If the applications do not need to guarantee data delivery, the socket chooses the connectionless service (UDP). Once the application developer chooses a transport protocol, the application is built using the transport layer services offered by that protocol.
- The application or service that will use this socket. The application is defined by a port number used by this application or service running on the host.

So the socket can perform the following basic operations:

- Connect to a remote machine
- Send data
- Receive data
- Close a connection
- Bind to a port
- Listen for incoming data
- Accept connections from remote machines on the bound port

We can refer to the previous Figure to illustrate how the sockets work:

1. The client process passes a stream of data through the socket
2. TCP directs this data to the connection's send buffer

3. From time to time, TCP will "grab" chunks of data (Maximum Segment Size MSS) from the send buffer.
4. TCP encapsulates each MSS of client data with TCP header, thereby forming TCP segments.
5. The segments are passed down to the network layer, where they are separately encapsulated within network-layer IP datagrams.
6. The IP datagrams are then sent into the network.
7. The IP datagrams are received from the network.
8. The datagrams are passed up to the network layer, where they are decapsulated to a separate TCP segments
9. TCP decapsulates each TCP segments, thereby forming MSS.
10. The MSS is placed in the TCP connection's receive buffer
11. The MSSs in the TCP connection's receive buffer perform a stream of data
12. The application reads the stream of data from this buffer

The application developer has control of everything on the application-layer side of the socket but has little control of the transport-layer side of the socket. The only control that the application developer has on the transport-layer side is

- the choice of transport protocol
- the ability to fix a few transport-layer parameters such as maximum buffer and maximum segment sizes.

Sockets are a nearly standard programming interface to IP and IP transport protocols that allow applications to be written in a portable way and run on different systems, getting the same level of access to the IP transport. Sockets implementations themselves provide a level of queuing of messages and buffering of data that is of great help to an application implementer.



Note that sockets implementations exist to provide access to UDP and TCP. Direct access to IP (without the use of a transport protocol) is often provided through *raw sockets*.

Although sockets are a roughly standardized solution, it should be noted that they are not part of the specification of IP or the IP transport protocols but are only a means of access to them. Many application implementations choose to use sockets because of their convenience or because they provide the only access to the IP or IP transport support in the systems in which they will run.

The sockets API deviates slightly from one implementation to another, with the result that unless an application is to be run on a single well-known platform, it is usually constrained to a subset of the API to ensure that it can be ported.

13.10 Quick Review

- ❖ *Transport protocol* manages the end-to-end communication between applications in the two end devices (*hosts*).

- ❖ Each transport-layer segment has fields that help to perform the demultiplexing and multiplexing jobs.
- ❖ TCP is a connection-oriented transport protocol that sends data as an unstructured stream of bytes using a three-step hand shaking. It provides reliable packet delivery, congestion control, error controlling, and full-duplex data exchange.
- ❖ Sliding window flow control is achieved by maintain a variable called the receive window to give the sender an idea about how much free buffer space is available at the receiver.
- ❖ Congestion is the situation when too many packets are present in a part of the subnet, causing the performance to degrade.
- ❖ Slow start congestion control algorithm and Internet congestion control algorithm are used to prevent the Congestion from occurring.
- ❖ UDP) is a connectionless unreliable transport protocol, no handshaking between sending and receiving points occurs before sending a segment. It does not provide a reliable service. It does not provide acknowledgment. But it tends to run faster than TCP, less overhead. UDP is useful in applications that are command/response oriented and in which the commands and responses can be sent in a single datagram.
- ❖ In order to retain transport layer connections, a mobile host's address must be preserved regardless of its point of attachment to the network. If either ends of the connection moves, many problems will take place.
- ❖ Mobile computing systems are characterized a poor link quality typically causes to lose TCP data segments which lead to a possible timeout.
- ❖ Disallowing a sender to shrink its congestion window when packets are lost for any reason, serves as an option to solve this problem..
- ❖ The Indirect Transmission Control Protocol (I-TCP), and the fast transmit will be the focus of our discussion are two other protocols are use too to solve this problem.
- ❖ Since the traditional UDP does not use acknowledgments and does not perform flow control it is modified to accommodate the process of registering with a foreign agent.
- ❖ Any network application involves at least two processes in two different hosts communicating with each other over the network using *sockets*.
- ❖ The socket serves as an interface between the application layer and the transport layer within a host. It is a logical endpoint for communication between two hosts on a TCP/IP network.

13.11 Self Test Questions

A- Answer the following questions

1. Explain how the transport layer protocol provides logical communication between processes running on different hosts.
2. What are the services provided by the transport layer?
3. What are the three parameters used when a destination host receives data from the network layer, in order to forward this data to the appropriate process

4. What is the role of sequence and acknowledge field numbers contained in the TCP data unit?
5. List the main services provided by TCP?
6. Explain the structure of TCP data unit.
7. How does TCP setup the connection between the source and the destination?
8. How can the flow control be distinguished from the congestion control?
9. What are the main aspects of the sliding window algorithm?
10. How dose the **receive window** effectively grant the sender permission to send a certain number more bytes?
11. How does the round trip time affect the **Timeout** of the timer?
12. What are the reasons that may cause congestion?
13. What TCP does try to prevent congestion from occurring in the first place?
14. What are the differences between slow start congestion and the Internet congestion control algorithm?
15. List the main characteristics of the UDP.
16. What are the main fields in the UDP data unit?
17. Where are the UDP and TCP applicable?
18. How dose the correct amount of data stuffed one packet chosen?
19. What are the problems that will take place if either ends of the connection moves?
20. What are the differences between the Indirect and the fast transmit Transmission Control Protocols?
21. How is the UDP modified to accommodate mobility?
22. What are the differences between the server socket and the client socket?
23. How does the server socket work?
24. How does the client socket work?

B- Identify the choice that best completes the statement or answers the question.

1. Which two protocols carried within IP datagrams operate at the transport layer of the OSI model?

I. IMCP	II. TCP	III. UDP
IV. IGMP	V. ARP	VI. RARP
a. I, II and III		c. II and III
b. II, III and IV		d. V, VI
2. TCP is _____
 - a. a data-link layer protocol
 - b. an application layer protocol
 - c. a transport layer protocol
 - d. a network layer protocol
3. Which of the followin protocols uses a handshake to establish a connection before sending data?
 - a. Connection-oriented protocol
 - b. Routing protocol
 - c. Connectionless protocol
 - d. File Transfer Protocol

4. The Data Offset field in the TCP header specifies:
 - a. The length of the TCP header
 - b. The location of the current segment in the sequence
 - c. The length of the Data field
 - d. The checksum value used for error detection
5. _____ is a service that the UDP protocol provides.
 - a. Flow control
 - b. Guaranteed delivery
 - c. Error detection
 - d. None of the above
6. _____ is responsible for managing the three-way handshake.
 - a. IP
 - b. UDP
 - c. TCP
 - d. ARP
7. The _____ are a kind of Transport layer protocols that are more useful in situations where data must be transferred quickly.
 - a. connectionless protocols
 - b. SYN-oriented protocols
 - c. connection-oriented protocols
 - d. ACK-oriented protocols
8. What is the transport layer protocol that establishes a connection with another node before they begin transmitting data?
 - a. connectionless protocols
 - b. SYN-oriented protocols
 - c. connection-oriented protocols
 - d. ACK-oriented protocols
9. TCP/IP _____.
 - a. comprises several subprotocols
 - b. comprises only one protocol
 - c. has been replaced by ARP
 - d. has been replaced by IPX/SPX
10. TCP/IP has grown extremely popular because _____.
 - a. It is expensive
 - b. It cannot be routable
 - c. Its private nature made its programming code secure
 - d. Its open nature
11. TCP operates on _____ layer of the OSI Model.
 - a. Physical
 - b. Session
 - c. Data Link
 - d. Transport
12. TCP _____.
 - a. is a connectionless protocol
 - b. is a connection-oriented protocol
 - c. does not use checksums
 - d. does not ensure reliable data delivery
13. TCP _____.
 - a. is a connectionless protocol
 - b. is a connection-oriented protocol
 - c. does not use checksums
 - d. does not ensure reliable data delivery

- a. does not use checksums
 - b. is a connectionless protocol
 - c. provides flow control
 - d. does not ensure reliable data delivery
14. What is the address on a host where an application makes itself available to incoming or outgoing data?
- a. IP address
 - b. NIC address
 - c. MAC address
 - d. Port
15. _____ field indicates how many bytes the sender can issue to a receiver while acknowledgment for this segment is outstanding.
- a. Acknowledge number
 - b. Reserved
 - c. Window
 - d. Checksum
16. _____ field allows the receiving node to determine whether the TCP segment became corrupted during transmission.
- a. Checksum
 - b. TCP header length
 - c. Flags
 - d. Padding
17. _____ is the only TCP/IP core protocol that runs at the Transport layer of the OSI Model.
- a. UDP
 - b. TCP
 - c. IP
 - d. ARP
18. _____ is a connectionless transport service.
- a. TCP
 - b. IP
 - c. UDP
 - d. HTTP
19. UDP_____.
- a. is less efficient than TCP
 - b. is more reliable than TCP
 - c. also uses checksums
 - d. produces less transmission overhead than TCP
20. UDP contains _____ header fields.
- a. 4
 - b. 13
 - c. 10
 - d. 15
21. The client uses _____ to broadcast a DHCP discover packet?
- a. ARP
 - b. IP
 - c. TCP
 - d. UDP
22. _____ port numbers indicate which application service is desired.
- a. IP
 - b. TCP
 - c. PVC
 - d. WAP
23. The Secure Sockets Layer is an additional layer of software added between the _____ layer and the _____ layer.
- a. transport (TCP); physical
 - b. data link; network
 - c. presentation; network

- d. application; transport (TCP)

24. Which protocol is used by network-monitoring applications that do not require the same level of reliability as offered by TCP?
a. IP
b. UDP
c. FTP
d. NCP

25. Which TCP/IP protocol is responsible for reliable delivery of data?
a. SPX
b. UDP
c. TCP
d. FTP

26. _____ is found in a TCP header but not in a UDP header.
a. Source port
b. Window size
c. Destination port
d. Checksum

27. _____ is found in a TCP header and in a UDP header.
a. Sequence number
c. Acknowledgment number
b. Window size
d. Checksum

28. Which of the following services use UDP?
I. DHCP II. SMTP III. SNMP
IV. FTP V. HTTP VI. TFTP
a. I,III and VI
b.I,II and V
c. II,IV and V
d. III, IV and VI

29. Which of the following services use TCP?
I. DHCP II. SMTP III. SNMP
IV. FTP V. HTTP VI. TFTP
a. I,III and VI
b.I,II and V
c. II,IV and V
d. III, IV and VI

30. Which TCP/IP protocol is responsible for reliable delivery of data?
a. SPX
b. UDP
c. TCP
d. FTP

31. Which of the following uses TCP as its transport protocol?
a. NFS
b. RTP
c. TFTP
d. HTTP

32. ITCP connection is composed of _____.
a. one wireless and the other fixed connections
b. one wireless connection
c. one fixed connection
d. two wireless connections

33. Fast Retransmit Mobile TCP connection is composed of _____.
a. one wireless and the other fixed connections
b. one wireless connection
c. one fixed connection

- d. two wireless connections
34. ____ is not a transport socket attribute
- a. The host's IP address
 - b. The type of service
 - c. The application
 - d. The Maximum Segment Size MSS
35. The application developer on the transport-layer side doesn't have the control over
- a. the choice of transport protocol
 - b. the ability to fix the maximum buffer size
 - c. the ability to fix the maximum segment size.
 - d. the choice of error checking method
36. One of the following is NOT true about the transport sockets
- a. Any network application involves at least two processes in two different hosts communicating with each other over the network using *sockets*.
 - b. The socket is a physical endpoint for communication between two hosts on a TCP/IP network
 - c. The socket serves as an interface between the application layer and the transport layer within a host.
 - d. The socket is a logical endpoint for communication between two hosts on a TCP/IP network

CHAPTER 14

THE APPLICATION PROTOCOLS

14.1 About This Chapter

There are several additional service protocols designed to assist TCP and IP. These protocols provide ways for applications to communicate in an IP environment to achieve a common task. It would be impossible to cover them adequately here.

The Hypertext Transfer Protocol (HTTP) could be described as *the* protocol that has made the Internet a popular success. It is used to publish and read hypertext documents across the World Wide Web—that is, to read web pages.

The Domain Name System protocol (DNS) is used to associate host and domain names with specific IP addresses allowing, for example, a Universal Resource Locator (URL) such as <http://www.elsevier.com> to be converted to an IP address to allow IP messages to be routed to the correct destination.

Telnet provides user access to remote systems. It is a popular method for users to log in and access the command line interfaces of computers and network devices without having to have a terminal that is directly attached.

The File Transfer Protocol (FTP) is used extensively in the Internet to copy files from one place to another. It is transaction oriented and focuses on the reliable transfer of bulk data using TCP as its transport protocol. The Trivial File Transfer Protocol (TFTP) achieves the same function as FTP but operates over UDP.

SMTP Simple Mail Transfer Protocol is the middleman that uses UDP to move data around from one internetwork host to another. Applications run on both hosts that make use of SMTP.

SNMP Simple Network Management Protocol is a network management standard widely used with TCP/IP networks. SNMP provides a method of managing network nodes (servers, workstations, routers, bridges, and hubs) from a centrally located host. SNMP performs its management services by using a distributed architecture of management systems and agents.

This chapter is intended to give the background to the above mentioned standardized application protocols and to illustrate how they function and how they make use of IP and IP transport services by examining a few of the very common and most important protocols.

14.2 Learning Outcome

After this chapter, you should be able to:

1. Be familiar with the services provided by application layer protocols.
2. Understand the client-server model used by many application layer protocols.

3. Explain the role and the function of HTTP and make a comparison between its versions.
4. Be familiar with the TELNET Protocol.
5. Determine the functions of FTP and RFTP.
6. Understand DNS protocol and DNS directory look-up service.
7. Understand the Internet mail transfer system and email Protocols
8. Explain the Management Information Base (MIB) and how the Simple Network Management Protocol (SNMP) works

14.3 The Application Protocols

Many application protocols associated with bulk transfer of data use TCP. These include the File Transfer Protocol (FTP), the Hypertext Transfer Protocol (HTTP), and email protocols such as the Simple Mail Transfer Protocol (SMTP) and the Post Office Protocol (POP3).

Telnet is an interesting example of a protocol that commonly transfers small amounts of data but still uses TCP. The command–response nature of Telnet and its immediate visibility to a human user is such that it is essential to ensure that messages are delivered correctly.

TCP is also used by control and routing protocols to transport their data. The Border Gateway Protocol (BGP-4) and the Label Distribution Protocol (LDP) are good examples. The use of TCP makes sense for them because they establish clear and long-lived associations with “adjacent” nodes over which they need to keep exchanging information. Using TCP means that these protocols do not need to include methods to track the data that is exchanged—they are heavily dependent on the reliability of TCP. On the other hand, many control and routing protocols that use TCP need to include their own keep-alive mechanisms to ensure that the TCP connection is still active and to detect connection failures in a timely manner.

There are several additional service protocols designed to assist TCP and IP. Since routing is so important on a packet-switched network like the Internet, specialized protocols have been designed to assist in this function. Special protocols for determining addressing on the Internet have also been devised. Additionally, some additional protocols may be involved in error checking and flow control, just to name a few. Let's explore some of these additional protocols that are included in the TCP/IP suite of protocols.

14.3.1 Application Layer Protocols Services

Processes that are running within end systems are communicating with each other using interprocess communication (IPC). IPC are governed by the end system's operating system. A sending process creates and sends messages into the network; a receiving process receives these messages and possibly responds by sending messages back. It is the rule of application-layer protocols to define the format and order of the messages exchanged between processes, as well as the actions taken on the transmission or receipt of a message.

Application Layer provides network services to user applications. The application layer defines and performs such applications as electronic mail (e-mail), remote access to computers, file transfers, newsgroups, and the Web, as well as streaming video, Internet radio and telephony, P2P file sharing, multiuser networked games, streaming stored video clips, and real-time video conferencing.

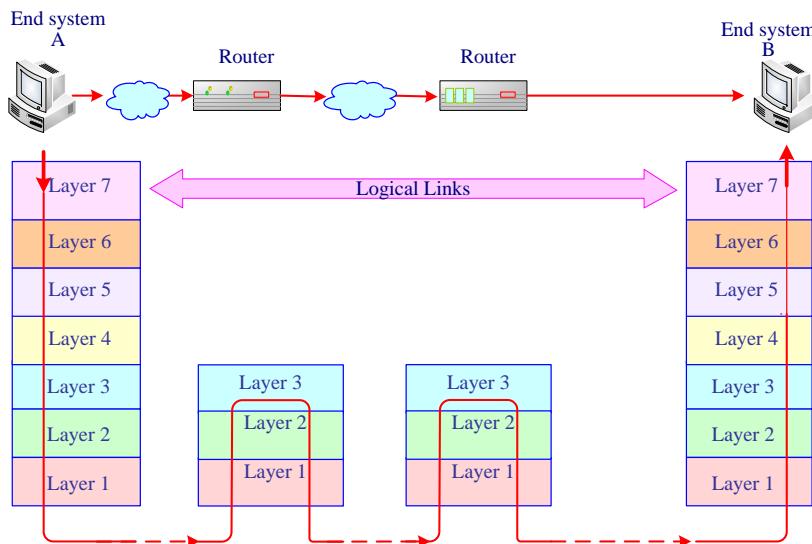


Figure 14.1: Communication between two end systems

The application layer protocols handle the details of the particular application. The primary functions of these protocols include formatting, presenting and transporting data. In particular, an application layer protocol defines the following:

- The types of messages exchanged, e.g., request messages and response messages;
- The syntax of the various message types, i.e., the fields in the message and how the fields are delineated;
- The semantics of the fields, i.e., the meaning of the information in the fields;
- Rules for determining when and how a process sends messages and responds to messages.

When a new application is developed, its software must be able to run on multiple machines, so that it does not need to be rewritten for networking devices, such as routers, that function at the network layer. In client/server architecture for example, a client end host requests services from a server host. A client host can be on sometimes or always. Figure 14.1 shows an example of application-layer communication.

14.3.2 Client and Server Model

A network application protocol typically has two sides. The client side in one end system communicates with the server side in another end system. This model provides specific computational services, such as partial-time usage services to multiple machines. Reliable communication protocols, such as TCP, allow interactive use of remote servers as

well. For example, we can build a server that provides remote image-processing services to clients. Implementing such a communication service requires a server loaded with the application protocol to accept requests and a client to make such requests. To invoke remote image processing, a user first executes a client program establishing a TCP connection to a server. Then, the client begins transmitting pieces of a raw image to the server. The server processes the received objects and sends the results back. There are many popular examples such as Web browser which implements the client side of HTTP and a Web server implements the server side of HTTP. In another example, e-mail, the sending mail server implements the client side of SMTP and the receiving mail server implements the server side of SMTP.

For many applications, a host will implement both the client and server sides of an application. FTP, used for transferring files between two hosts is a good example of this type. When an FTP session exists between two hosts, then either host can transfer a file to the other host during the session.



The host that initiates the session is labeled the client and that respond with a service is labeled the server. Furthermore, a host can actually act as both a client and a server at the same time for a given application.

14.4 HyperText Transfer Protocol (HTTP)

The Hypertext Transfer Protocol (HTTP) is one of the most extensively used Internet application protocols. Each time you open a Web browser to surf the Internet, you are using HTTP over TCP/IP. HTTP forms the basis of what most people understand the Internet to be—the World Wide Web. Its purpose is to communicate between web browsers and web servers, to read information from web pages, or to send responses such as completed forms or checked boxes.

HTTP is based on the client/server idea, having a client and a server program, both of which can be executed on different end systems. The communication between the client and server is carried out through an exchange of HTTP messages. This protocol specifies the structure of these messages. HTTP defines how Web clients (i.e., browsers) request Web pages from servers (i.e., Web servers) and how servers transfer Web pages to clients.

HTTP uses TCP rather than UDP, since reliability of delivery is important for Web pages with text. The TCP connection-establishment delay in HTTP is one of the main contributing delay factors associated with downloading Web documents.

Web page consists of files, such as Hypertext Markup Language (HTML) file or an image that can be addressed by a single uniform resource locator (URL). A URL is a global address of an HTML document and has two parts. The first part indicates what protocol is used, and the second part determines the IP address of the associated resource.

14.4.1 HTTP Message Formats

HTTP messages are text-based. That is, the control part of each message is made up of a series of fields, each of which is a text string tag. Each HTTP message uses the standard encoding of an application text message. That is, the message is built up from a common request or status header, an arbitrary number of message headers, and a message body. There are two types of HTTP messages, request messages and response messages, both of which are discussed below.



A Web page consists of objects. An object is a simply file, such as a HTML file, a JPEG image, a GIF image, a Java applet, an audio clip, etc. that is addressable by a single URL. Most Web pages consist of a Base HTML file and several referenced objects.

There are three HTTP main types:

- **HTTP/0.9:** A simplistic first implementation of the protocol that only support the option to get a Web page.
- **HTTP/1.0:** This version addes many supplemental data fields, known as headers to the specification. This allowes other information passing between the client and server, alongside the request and consequent page. HTTP/1.0 uses non persistent TCP connection and works as follows Given that a client will typically have to retrieve multiple objects to make up a single Web page:

1. The HTTP client initiates a TCP connection to the server. It establishes socket associated with this TCP connection using port number 80.
2. The HTTP client sends a HTTP request message into the socket.
3. The HTTP server receives the request message via the socket associated with the connection. It sends the response message into the TCP connection with the required object encapsulated in the HTTP response message.
4. The HTTP server tells TCP to close the TCP connection.
5. The HTTP client receives the response message.
6. The TCP connection terminates. The message indicates that the encapsulated object is an HTML file. The client extracts the file from the response message, parses the HTML file and finds references to the ten JPEG objects.
7. The first four steps are then repeated for each of the referenced JPEG objects.

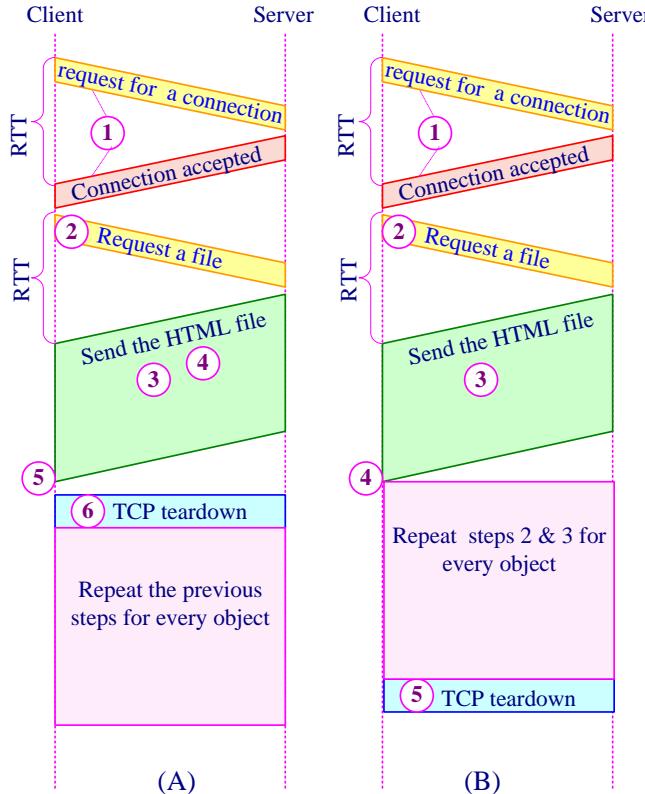


Figure 14.2: The difference in TCP handling between HTTP/1.0 and HTTP/1.1.

- **HTTP/1.1:** This version implements a number of improvements over and above the 1.0 specification. It has new features that make it more efficient. These new features include the following:
8. **Persistent connections:** An HTTP 1.1 server can keep TCP connections open after a file has been transferred, as shown in Figure 14.2 eliminating the need for a connection to be opened and closed each time a file is transferred, as is the case with HTTP 1.0.
 9. **Pipelining:** The HTTP client issues a request as soon as it encounters a reference. Thus the HTTP client can make back-to-back requests for the referenced objects. It can send multiple Internet Protocol (IP) packets to the server in parallel without waiting for the server to respond to each packet.
 10. **Buffering:** This process allows several HTTP requests by the client to be buffered into a single packet and sent to the server, which results in faster transfer times because fewer and larger packets are used.
 11. **Host headers:** This feature enables an HTTP 1.1-compliant Web server to host multiple Web sites using a single IP address.
 12. **Http put and http delete commands:** These commands enable Web browsers to upload and delete files from Web servers using HTTP.

The default mode of HTTP/1.1 uses persistent connections with pipelining. Most browsers these days offer support for both 1.0 and 1.1 implementations, with new browsers using 1.1 as a default but supporting the ability to fall back to earlier versions if required.



HTTP is the protocol through which Web servers communicate with Web browsers. It is a control language for passing commands between clients and servers.

14.4.2 HTTP Requests and Responses

HTTP request is generated by the http client or user agent (UA). It includes the following information (see Figure 14.3):

- request method: this is a command like PUT, GET, DELETE, etc. Table 14.1 shows the supported method types in HTTP/1.0 and 1.1.
- universal resource (document) identifier (URI): This is the file locator or ‘pointer’ which indicates where http can locate the requested file. It is equivalent to the combination of a universal resource locator (URL) and a universal resource name (URN).
- http protocol version;
- information about the client making the request;
- additional information forming part of the request (if required).

The first three elements listed above together form the http Request-Line. An example Request-Line might be:

GET http://www.company.com/sales/orders.html HTTP/1.1

The http server (the origin server) responds to an http request with an http response including:

- Response Status-Line (see Figure 14.3), which comprises the http protocol version number and a success or error code;
- Data file formatted in one of the standard MIME-formats containing information provided by the server in response to the request;
- Other response information (see Figure 14.4).

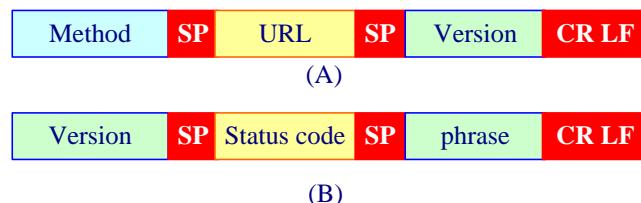


Figure 14.3: HTTP request (A) and response (B) status-lines

METHOD	DESCRIPTION	Version
GET	Retrieve the information specified.	1.0,1.1
HEAD	Identical to the GET request, but the server must not return any page	1.0,1.1

	content other than the HTTP headers.	
POST	Allows the client to submit information to the server, used for submitting information from a form, etc.	1.0,1.1
PUT	Allows the client to place an item on the server in the location specified.	1.1
DELETE	Allows the client to delete the item specified in the request.	1.1
TRACE	Allows the client to see the request it made to the server. This acts as a loopback in effect.	1.1
OPTIONS	Allows the client to determine the communications options available on the server.	1.1

Table 14.1: The HTTP Method Headers in HTTP/1.0 and HTTP/1.1

In terms of general Web browsing, the GET and POST methods are by far the most commonly used.

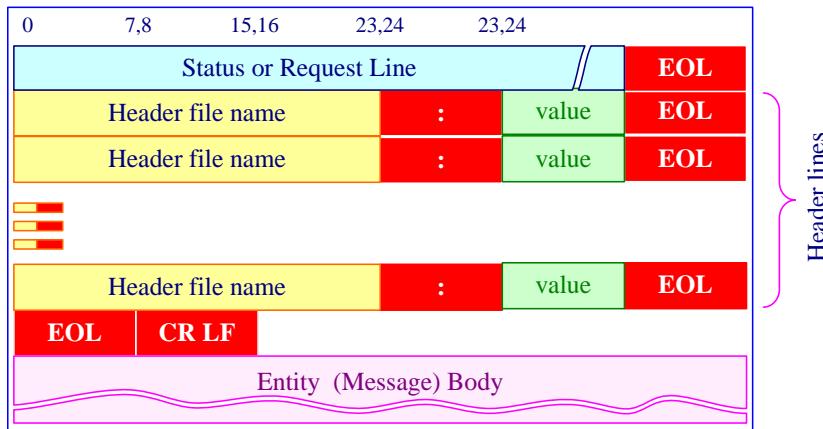


Figure 14.4: general format of a request message

14.4.3 HTTP Protocol Coding

The commands of the hypertext transfer protocol (http) have the appearance of a ‘classical computer programming language’, typically comprising a command or keyword, followed by colon and a list of parameter values (called arguments), and concluded at the end-of-line (EOL) by the _CRLF_ (carriage return, line feed sequence).

The HTTP generic request and response messages consist of:

- start line comprising either a request or a response,
- zero or more header fields; Header fields include the general header, together with the request header, the response header and/or the entity header. If necessary, header lines can be extended over multiple horizontal lines
- empty line to indicate the end of the header); and
- entity-body (if appropriate). This is typically an attached file coded in one of the MIME (multipurpose Internet mail extension) formats conceived for Internet mail attachments.

14.4.4 Uniform Resource Locators

The URL is the most important piece of information that the client browser includes in any GET request. The URL is defined as being a combination of the host where the site is located, the scheme used to retrieve the page, and the full path and filename. Optionally, the URL may include information such as the TCP port number to be used or a unique reference point within a larger page. Figure 14.5 shows the breakdown of an example URL.

Protocol	Host or IP address	Port	Full Path and document	Page marker
http:	// www.somehost.com:80	/	documenys/index.html	#middle

Figure 14.5: An example URL and its components.



The *URI* is also commonly used when referencing the location of documents within *HTTP*. The formal definition of the difference between a *URL* and a *URI* is simple: A *URI* is a *URL* without the scheme defined.

14.4.5 Web Caching (Proxy Server)

Normally, each organization or ISP should have its own cache providing a high-speed link to its users. An HTTP request from a user is first directed to the network proxy server, or Web cache which must contain updated copies of all objects in its defined proximity. The cache server stores all the http responses received in the response chain, thereby enabling it to respond to subsequent requests for the same file without requiring a repeat request to the origin server. The main reason for Web caching is to reduce the response time for a user request. Caching removes the need to send some requests across the network, thereby reducing network load and improving the response time perceived by the customer. Because cached data must be kept ‘fresh’ enough to be reliable, a time to live (TTL) parameter is used, after the expiry of which the cached copy is deleted and a new copy retrieved from the server on the occasion of the next client request. The details of Web caching are as follows:

1. The source browser makes a TCP connection to the Web cache.
2. The user browser transmits its HTTP request to the Web cache.
3. If it has a copy of the requested object, the Web cache forwards the object to the user browser. Otherwise the Web cache establishes a TCP connection to the requested server and asks for the object.
4. Once it receives the requested object, the Web cache stores a copy of it and forwards another copy to the requesting user browser over the existing TCP connection.



The proxy cache server can be used like a regular proxy server at the border of a private corporate network in order to cache the Web pages returned from the Internet when users in the private network request them.

14.5 TELNET Protocol

Telnet is one of the oldest remote login application protocols used within the Internet to provide a standardized way for terminals to communicate with host computers, regardless of their type. Telnet's history dates back to 1969 when the word "Telnet" came into being as an acronym for Telecommunications Network Protocol.

TELNET is used to establishing a connection to a remote system. It allows a user to log in to a remote machine across the Internet by first making a TCP connection and then pass the detail of the application from the user to the remote machine.

The advantage to the TELNET program is that a user may log on to any host on the TCP/IP internet. Sessions are set up over the TCP/IP network.



Remote login application is the mechanism that allows a client to establish a session on the remote server and then run its applications. A client may want to run such applications at a remote site, with results to be transferred back to its local site.

With TELNET, an application program on the user's machine becomes the client. The user's keyboard and its monitor also attach directly to the remote server. The remote-logging operation is based on timesharing, whereby an authorized user has a login name and a password.

Telnet applications are very common. Usually the user requests a connection to a specific host name or IP address, usually by typing **TELNET <domain name or IP address>**. If a host name is specified, the application will need to look up the correct IP address using the local mapping tables and possibly resorting to the DNS protocol. The TELNET application starts and attempts to establish a connection to the remote device.

The Telnet server listens on the well-known port 23 and responds to the client on the client's chosen port. The server may also offer other ports, and this can be useful to distinguish between connections to different devices when the connectivity is provided through a concentrator or terminal server.

Telnet transactions are remarkably simple. Telnet character flows are presented to TCP for transmission. In the normal case, the client does this only when the end of a line is reached—that is, when the user presses the “Enter” or “Return” key. There is nothing, however, that prevents the client from sending data to the server one character at a time, although such behavior is very inefficient. The server sends data to the client in blocks of

one or more lines, depending on whether it is spooling a job to the printer or just writing a message to the user's screen.

The TELNET program is extensible through the use of options. Each side of the connection requests or tells the remote end of the connection which of these options it can support and which one the remote end should support. This provides for symmetry.

TELNET has the following properties.

- Client programs are built to use the standard client/server interfaces without knowing the details of server programs.
- A client and a server can negotiate data format options.
- Once a connection is established through TELNET, both ends of the connection are treated symmetrically.

Different terminals and keyboards have different ways of representing characters and control commands, and different servers have different expectations. Clearly, for two computers to communicate using Telnet there may need to be a translation. The solution is embodied in Network Virtual Terminal (NVT). All workstations using Telnet are required to perform their own translations so that the data they send looks as if it had been generated by one of these virtual terminals. Each Telnet server is required to accept data formatted as though it had come from a virtual terminal. In this way each participating node, client, or server is responsible for implementing precisely one translation function, mapping data between its own format and the NVT format.

An NVT is defined to be a device capable of sending and receiving data. It has a keyboard through which a user can enter data to be sent, and a printer capable of displaying received data. The device operates in half-duplex mode, meaning that it buffers characters received from the keyboard until it has assembled a full line of text before it submits that line to the host server. This makes editing of the entered characters and cancellation of the whole line a local matter.

TELNET also offers several options that allow clients and servers to negotiate on nonroutine transactions. These options include:

1. The ability to change from 7-bit text to 8-bit binary
2. Allowing one side or the other to echo characters
3. Specifying a terminal type
4. Requesting the status of a TELNET option from the remote connection
5. Setting a timing mark to synchronize two ends of a connection
6. The ability to terminate a record with an EOR code
7. Setting line mode so that strings of characters may be sent instead of a character-at-a-time transmit
8. Stopping the go-ahead signal after data

The options are negotiated between the two network stations in the following manner:

Request	Response
WILL <option>	DO or DON'T <option>

For example, WILL ECHO from station A is requesting that station A provide the echoing of characters. The response will either be DO ECHO, meaning the remote end agrees, or DON'T ECHO, meaning the remote end will not allow station A to echo.

Using WILL, WON'T, DO, and DON'T provides symmetry. Either side of the connection can provide the command or the response. One side provides services in exactly the same manner as the other side.

14.6 DNS Domain Name System

To facilitate a variety of different types of organizations and their desires to have a scaleable, customizable naming scheme in which to operate, the IANA has created and maintains a hierarchical namespace called the Domain Name System (DNS).

DNS is a naming scheme that looks similar to the directory structure for files on a disk. However, instead of tracing a file from the root directory through subdirectories to its final location and its file name, a host name is traced from its final location through its parent domains back up to the root. The unique name of the host, representing its position in the hierarchy, is called its Fully Qualified Domain Name (FQDN). The top-level domain namespace is shown in Figure 13.5 with example second level and subdomains.

DNS is composed of a distributed data base of names. The names in the DNS data base establish a logical tree structure called the domain name space. A tree is structured with a maximum of 128 levels, starting at level 0 (root). Each node or domain in the domain name space is named and can contain subdomains. Domains and subdomains are grouped into zones to allow for distributed administration of the name space. The domain name identifies the domain's position in the logical DNS hierarchy in relation to its parent domain by separating each branch of the tree with a period "...". Figure 14.6 shows a few of the top level domains. Each level consists of nodes.

The last label of a domain name expresses the type of organization; other parts of the domain name indicate the hierarchy of the departments within the organization. The parts of the domain namespace are:

- The root domain represents the root of the namespace and is indicated with a "" (null).
- Top-level domains, those directly below the root, indicate a type of organization. On the Internet, the IANA is responsible for the maintenance of top-level domain names. Figure 14.8 shows a partial list of the Internet's top-level domain names.
- Below the top level domains are second-level domains, which identify a specific organization within its top-level domain. On the Internet, the IANA is responsible for the maintenance of second-level domain names and ensuring their uniqueness.
- Below the second-level domain are the subdomains of the organization. The individual organization is responsible for the creation and maintenance of subdomains.
- A domain name example is **ftpsrv.science.alzaytoonah.edu**.

Where:

- **edu** is the top-level domain, indicating an Educational Organization.
- **alzaytoonah** is the second-level domain, indicating Alzaytoonah University of Jordan.
- **science** is a subdomain of alzaytoonah.edu indicating the Collage of Science.
- **ftpsrv** is the name of the FTP server in the Collage of Science

Organizations not connected to the Internet can implement whatever top and second-level domain names they want.

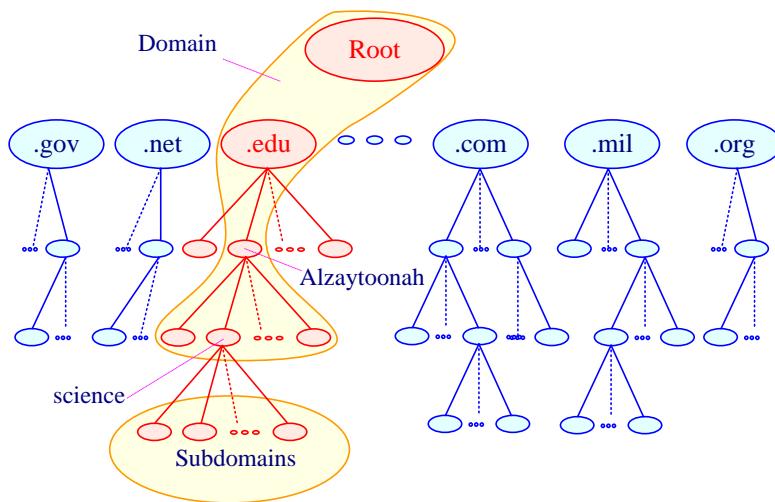


Figure 14.6: Hierarchy of domain name space

The domain name space is divided into subdomains, and each domain or subdomain is assigned a domain name server. This way, we can form a hierarchy of servers, just as we did for the hierarchy of domain names. A domain name server has a data base consisting of all the information for every node under that domain. Each server at any location in the hierarchy can partition part of its domain and delegate some responsibility to another server.

The country code top-level domains (ccTLDs) are generally administered and operated by national Internet domain registry authorities. Some of these country level domains are subdivided along similar lines to the .com/.org/.edu/.gov structure of the root domain. Thus the .jo (Jordan) domain is subdivided into separate domains: <.com.jo>_, <.edu.jo>, <.gov.jo>, <.org.jo> etc. Meanwhile, other country domain operators have elected for two-letter sub-domain names thus: co (commercial), e.g., <company.co.uk>, ac (academic). e.g., <ox.ac.uk>.

Some of the information-processing functions a DNS server handles are:

- Finding the address of a particular host
- Delegating a subtree of server names to another server

- Denoting the start of the subtree that contains cache and configuration parameters, and giving corresponding addresses
- Naming a host that processes incoming mail for the designated target
- Finding the host type and the operating system information
- Finding an alias for the real name of a host
- Mapping IP addresses to host names

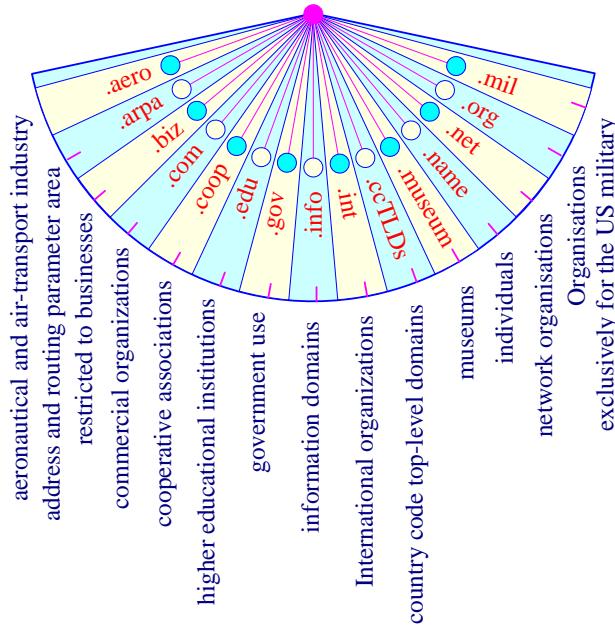


Figure 14.7: The root domain and the top-level domains



The root server supervises the entire domain name space. A root server typically does not store any information about domains and keeps references only to servers over which it has authority. Root servers are distributed around the world.

14.6.1 DNS Messages

DNS messages consist of requests and responses. Both message types have the 12-byte header format shown in Figure 14.8.

- The request message consists of a header and a question message only.
- The response message consists of a header and four message fields: question, answer, authority, and additional information.
- To help disambiguate responses to different requests, the response also contains the question.
- Multiple questions may be included in the same request, and so responses may include multiple answers

- Multiple answers could be provided for the same question.
- All messages start with a common header, and may end with additional information provided by the server, as shown in Figure 14.7.

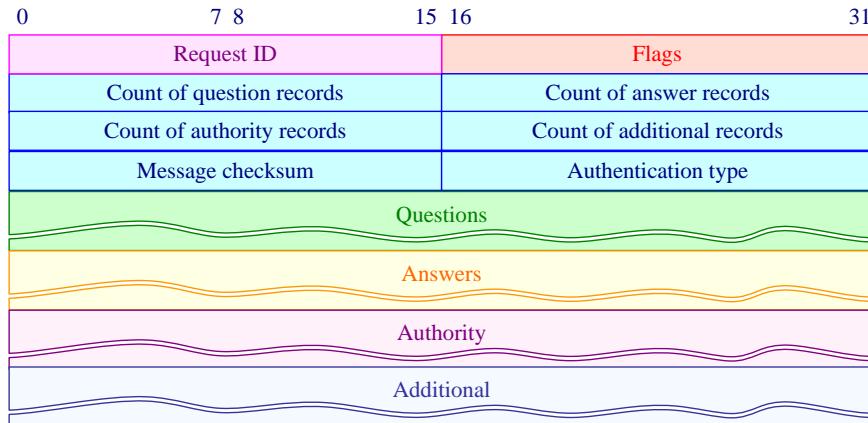


Figure 14.8: DNS Message format

The header contains the following fields:

- **Request ID:** It is to match the reply with the query. This field may appear with a different number each time a client transmits a query. The server copies this number in its reply.
- **Flags:** This field contains subfields that represent the type of the message, such as the type of answer requested or requested DNS recursive or iterative mapping.
- **Count of question records:** It indicates how many queries are in the question portion of the message.
- **Count of answer records:** It shows how many answers are in the answer field. For the query message, this field contains all zeros.
- **Count of authority records:** This field consists of the number of authoritative records in the authority portion of a reply message. Similarly, this field is filled by zeros for a query message.
- **Count of additional records:** It indicates how many records are in the additional information portion of a reply message and is similarly filled by zeros in a query message.
- **Questions:** This field can contain one or more questions.
- **Answers:** This field belongs only to a reply message and consists of one or more replies.
- **Authority:** It is present only in reply messages and provides the domain name information about one or more authoritative servers.
- **Additional information:** field is present only in reply messages and contains other information, such as the IP address of the authoritative server. This additional information helps a client further identify an answer to a question.



The form of the domain name allocated to you will be correspondingly in the form of [second level.top level], e.g. [alzaytoonah.edu]. You can then subdivide this domain by adding further sub-domains in a hierarchical fashion by prefixing further sub-domain-names and ‘dots’; e.g.: [ftpsrv.science.alzaytoonah.edu].

14.6.2 DNS Directory Look-up Service

Each host that needs to map an address to a name or vice versa should access the closest DNS server with its request. The server finds and releases the requested information to the host.

There is not one DNS name server, but instead a large number of name servers, at least one for each domain. Thankfully, all the name servers are linked according to a tree structure, and queries about unknown domain names can be channeled from the top (or root) of the tree downwards as appropriate.

The requesting process on the sending host accesses the DNS through an operating system call to the local DNS server. DNS server may need to make a number of requests to different DNS name servers and receive various referrals in order to resolve a particular address using either recursive or iterative method.

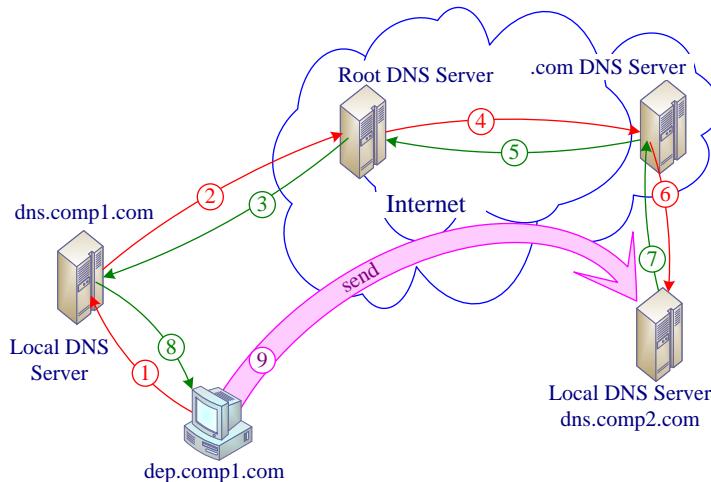


Figure 14.9: Recursive mapping

In recursive mapping (Figure 14.9), the client host makes the request to its corresponding DNS server. The DNS server is responsible for finding the answer recursively. The requesting client host asks for the answer through its local DNS server. If the information still has not been found, the root DNS server sends the query to the top level server of the destination. If the transaction still remains unsuccessful, the top level server of the destination sends the query to the local DNS server of the destination, and

finds the answer. The answer to a request in this method is routed back to the origin, as shown in the Figure 14.9.

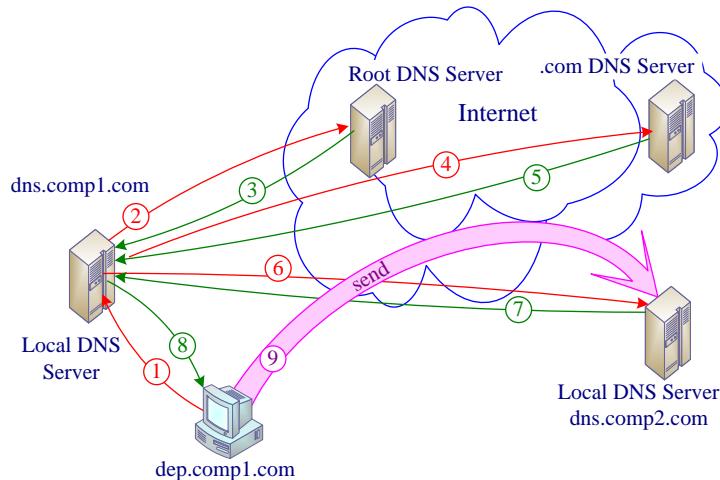


Figure 14.10: Iterative mapping

In the iterative approach, if the local DNS server of the sender does not have the name to provide, it must then repeat the query to the next DNS server that may be able to provide the name. This continues until the host succeeds in obtaining the name. The iterative mapping approach is shown in Figure 14.10.

14.7 File Transfer Protocol (FTP)

FTP exists primarily for the transfer of data between two end points. It differs from HTTP fundamentally as it is an application made up of two distinct TCP connections (see Figure 14.11):

The FTP connection actually comprises two separate connections:

- **FTP control connection:** It connects the user-PI (protocol interpreter) with the server-PI (protocol interpreter) for the purpose of exchange of FTP commands and replies on TCP port 21.
- **FTP data connection:** It is used for the transfer of the user's actual data (i.e., the file to be transferred) on TCP port 20.

A data transfer process (DTP) in each of the ends (user and server) coordinates the actual communication across the data connection. Using these two communication connections, two distinct modes of operation determine in which direction the connections are established: Active mode and Passive mode.

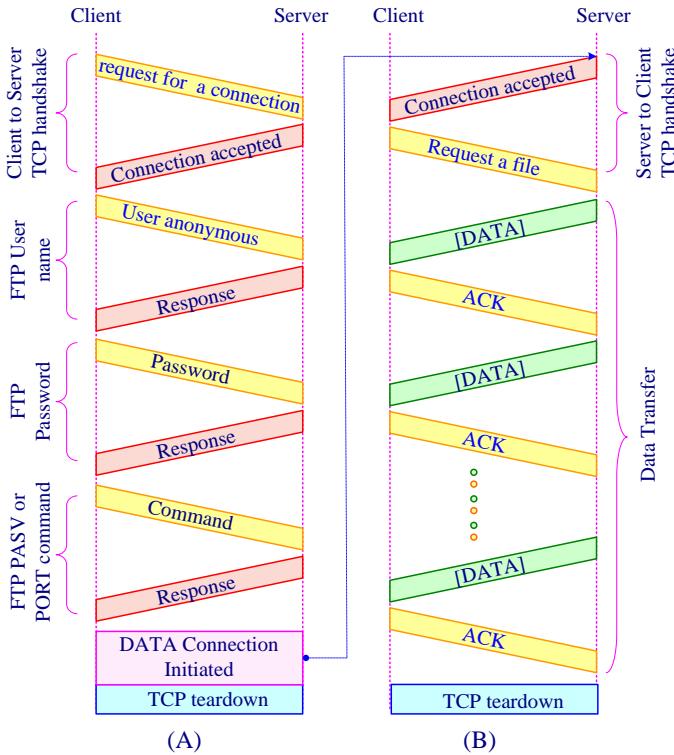


Figure 14.11: FTP connections lifecycle, (A) Control connection and (B) Data connection

Within an Active FTP session, the Control connection is established from the client to the server, with the Data connection established back from the server to the client. In order to do this, the client issues a PORT command to the server that contains the IP address and source and destination TCP ports that should be used during the Data connection.

Passive mode FTP works similarly to Active mode FTP with one major exception: both the Control and Data connections within a Passive mode FTP session are established from the client to the server. To implement this, rather than use the PORT command, Passive mode FTP implements the PASV command, which instructs the server that it should listen for the incoming Data connection.

The commands, from client to server, and replies, from server to client, are sent across the control TCP connection in 7-bit ASCII format. Thus FTP commands are readable by people. Each command consists of four uppercase ASCII characters; some of the more common commands are given below:

- **USER** username : Used to send the user identification to server, the name required to access the server file system
- **PASS** password: Used to send the user password to the server.
- **LIST**: Command causes a list of all files and their details in the specified current directory or current information on the specified file to be returned.

- RETR: Command causes the server to transfer a copy of the file to the other end of the connection.
- STOR: Command causes the server to accept the data transferred and to store them.
- HELP: Server will return helpful information regarding its status and how to initiate next action.
- ABOR: Command tells server to abort the previous FTP service command and any associated data transfer.
- QUIT: Command terminates a user and closes control connection if file transfer is not still in progress.
- STAT: The reply to this command, sent over the control connection, indicates the status of the operation in progress.

There is typically a one-to-one correspondence between the command that the user issues and the FTP command sent across the control connection. Each command is followed by a reply, sent from server to client. Some typical replies, along with their possible messages, are as follows:

- 125: Data connection already open; transfer starting
- 150: File status OK
- 200: Command OK
- 202: Command not implemented: superfluous
- 211: System status or system help ready
- 214: Help message
- 230: User logged in
- 332: Need account for login
- 331: Username OK, password required
- 421 Service not available, closing control connection
- 425: Can't open data connection
- 452: Error writing file
- 500: Syntax error, command unrecognised
- 501: Syntax error, parameter or argument error
- 502: Command not implemented
- 503: Bad sequence of commands
- 504: Command not implemented for parameter specified
- 530: Not logged in



Trivial file transfer protocol (TFTP) is a very simple but unreliable file transfer protocol. It is not intended for ‘normal’ file transfer, but instead is typically used to transfer boot files or keyboard font files to terminals, diskless PCs or diskless workstations. TFTP operates on UDP port 69.

14.8 Electronic Mail (email) Protocols

Electronic mail (email) is a reliable and exceptionally fast means of message communication between human users equipped with computer terminals or personal

computers. The electronic mail protocols gave the users the ability to formulate a message, send, receive and store the message. The most popular protocols associated with e-mails are SMTP (simple mail transfer protocol), IMAP (Internet message access protocol) and POP (post office protocol).

14.8.1 Internet Mail Transfer System

All email messages comprise the message itself, called the content, and an envelope (Figure 14.12). The envelope provides commands to control and ‘steer’ the message transfer system (MTS), which allows the conveyance of messages across a network on a store-and-forward or store-and-retrieve basis.

As illustrated in the Figure the two basic components of the Internet mail system are the message user agent (MUA) and the message transfer agent (MTA). MUA function is undertaken by a combination of software on the user PC (originator) and his email server. It helps the human user to compose messages in a standard form suitable for transmission and provides a ‘filing cabinet’ for previously received and sent messages which may be read, filed or otherwise processed.

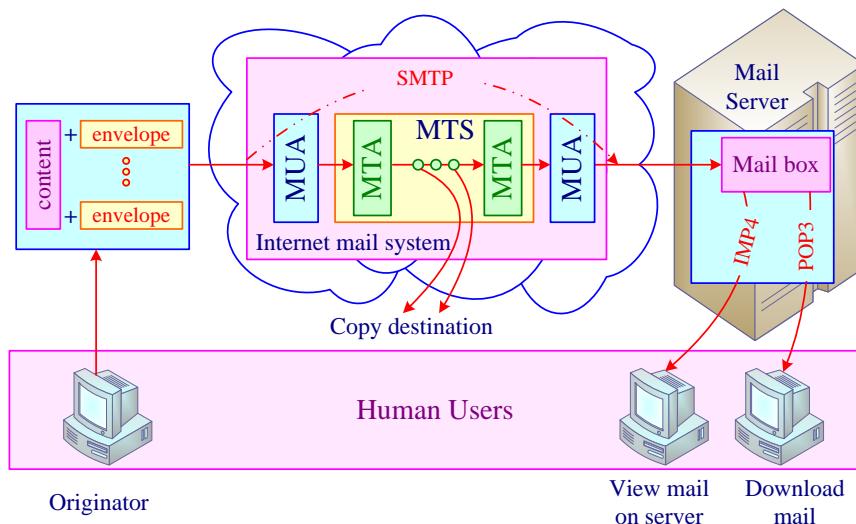


Figure 14.12: The operation of the Internet mail system.

The message is conveyed to its final destination via a number of MTAs, collectively called the message transfer system by means of the simple mail transfer protocol (SMTP). The first MTA in the connection is typically the electronic mail server associated with the sender. Intermediate MTA devices may then be used to relay the message to a destination postmaster server, where the mailbox of the intended recipient is located.

The Simple Mail Transfer Protocol (SMTP) plays a major role in transferring Internet electronic mail. This protocol transfers electronic mail (e-mail) from the mail server of a source to the mail servers of destinations. A user mailbox is a space in the mail server allocated to the user to keep its e-mail. Also, SMTP is designed to connect only the

two mail servers of the associated parties, regardless of the distance between the two users. Consequently, this protocol involves only the two mail servers of the communicating users.

Messages are carried between originator and recipient in a sealed electronic envelope. The envelope indicates the name of the recipient and records further information which may be necessary to cater for special delivery needs.

The simple mail transfer protocol (SMTP) is an application layer protocol which relies on the transmission control protocol (TCP) port 25 and the Internet protocol (IP) for data transport. The sending MTA is called the SMTP-sender (also called the SMTP client) and the receiving MTA is the SMTP-receiver (also called SMTP-server).

Once the mail message has traversed the message transfer system (MTS) to the recipient's mailbox on the destination email exchange server, the message is ready to be picked up by the human recipient. There are two normal means of final delivery. The IMAP4 (Internet mail access protocol version 4) allows a user to view the mail messages directly on the server, replying, copying, deleting or filing them without removing them from the server. The IMAP4 protocol may also be used to maintain a duplicate 'offline' mailbox (say, on a user's laptop PC), and to synchronize the contents of the laptop and server copies of the mailbox. Alternatively, the post office protocol (POP3) is a simple protocol for retrieving (i.e., downloading) all the messages from the server mailbox into the user's PC. Following a successful POP3 download, the copies of the messages left on the server are deleted.



IMAP4: An Internet standard protocol for storing and retrieving messages from Simple Mail Transfer Protocol (SMTP) hosts. IMAP4 provides mechanisms for storing messages received by SMTP in a receptacle called a mailbox. An IMAP4 server stores messages received by each user until the user connects to download and read them using an IMAP4 client.



Post Office Protocol version 3 (POP3) provides mechanisms for storing messages sent to each user and received by SMTP in a receptacle called a mailbox. A POP3 server stores messages for each user until the user connects to download and read them using a POP3 client.

14.8.2 The Internet Mail Message Format

An Internet mail message comprises an envelope and the message content (Figure 14.13).

- Envelope: It comprises a series of SMTP commands and replies which control the message transfer from message transfer agent (MTA) to message transfer agent (MTA) across the message transfer system (MTS).

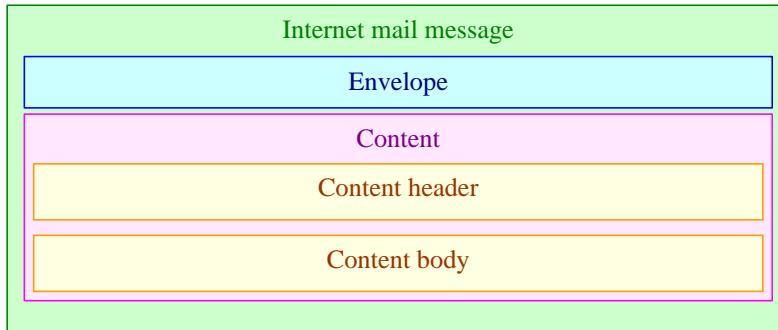


Figure 14.13: The Internet mail message format

- Message content: It is formatted according to the Internet message format. The content is sub-divided into a content header and a content-body; they are transferred together by SMTP as an SMTP protocol DATA unit (PDU).



SMTP protocol DATA units are divided into lines of characters each terminated with a _CRLF_ sequence. The maximum line length is 998 characters but it is recommended that a ‘normal line length’ of 78 characters be used (with _CRLF_, this is equivalent to a standard line length of 80 characters).

14.9 Network Management Protocols

The term network management is used to cover all aspects of configuration, control, and reporting that are useful to a network operator who is trying to understand how a network is functioning, commissioning new equipment, directing traffic along specific paths, or performing maintenance on parts of the network. The main purpose of network management is to monitor, manage, and control a network. Network management includes monitoring, testing, and analyzing the hardware, software, and human elements of a network and then configuring and controlling those elements to meet the operational performance requirements of the network.

Network management has three main components:

- **Managing center:** it consists of the network administrator and his facilities including the manager which is a network administrative device.
- **Managed device (agent):** this is the network equipment, including its software that is controlled by the managing center. Hubs, bridges, routers, servers, printers, or modems can be a managed device.
- **Network management protocol:** It is a policy between the managing center and the managed devices. It allows the managing center to obtain the status of managed devices. An agent can use the network management protocol to inform the managing center of an unexpected event.



Management systems are used to monitor network health, trap errors, perform diagnostics, and generate reports. SNMP is the most popular network management protocol in use.

14.9.1 Management Information Base (MIB)

The management information Base (MIB) defines the functions which the network element is capable of, the configuration options which are possible and the information it can provide in terms of a set of managed objects (MOs). A managed object is a standardized definition of a particular feature or capability of the network component, and the normalized states in which it can exist.

We require a common standardized way to represent the data while it is moved between management station and device. This helps us to decide how the statistics and configuration data should be represented, while each managed device has a different configuration requirements and internal data structures according to its implementation, and each network management tool has different commands and management screens displaying and requiring subtly different pieces of information. The management tools are free to collect and display the information in whatever way they choose, and the devices can store the information and use it or discard it as they see fit.

The MIB is an ordered, structured view of all of the information in all networks, all at the same time. It contains information about the configuration of the networking components, such as the type of hardware device or the version of the software running on the component. MIB functions as a kind of directory containing the logical names of the network resources and their configuration parameters that are managed by the management protocol. We can think about MIB as a logical representation of networking components. Data values or objects are given unique object identifiers (OIDs) in a hierarchical and somewhat long-winded way. Every MIB is a member of the MIB hierarchy, can be uniquely identified. The name is represented using a standard dotted naming system. For example:

iso.org.dod.internet.private.enterprises.lanmanager

- 1.3.6.1.4.1.77

To illustrate this, consider the part of the OID tree shown in Figure 14.14.

This shows the root of the tree and the branches down as far as some individual MIB modules. As can be seen, the MIB is broken into branches according to the standards-making body. Within the ISO branch, for example, the organization (3) branch is labeled sequentially from the root as 1.3. If we continue to follow the entries on this branch, we see a path over DoD (6), Internet (1), management (2), MIB-2(1), and IP (4). This path is identified by (1.3.6.1.2.1.4) to indicate all the labeled numbers from the root to the IP (4) entry. Besides that entry, MIB module represents a number of network interfaces and well-known Internet protocols at the bottom of this tree.



An entry is the equivalent of a single instantiation of a control block and is made up of a sequence of objects, each with its own object identifier.

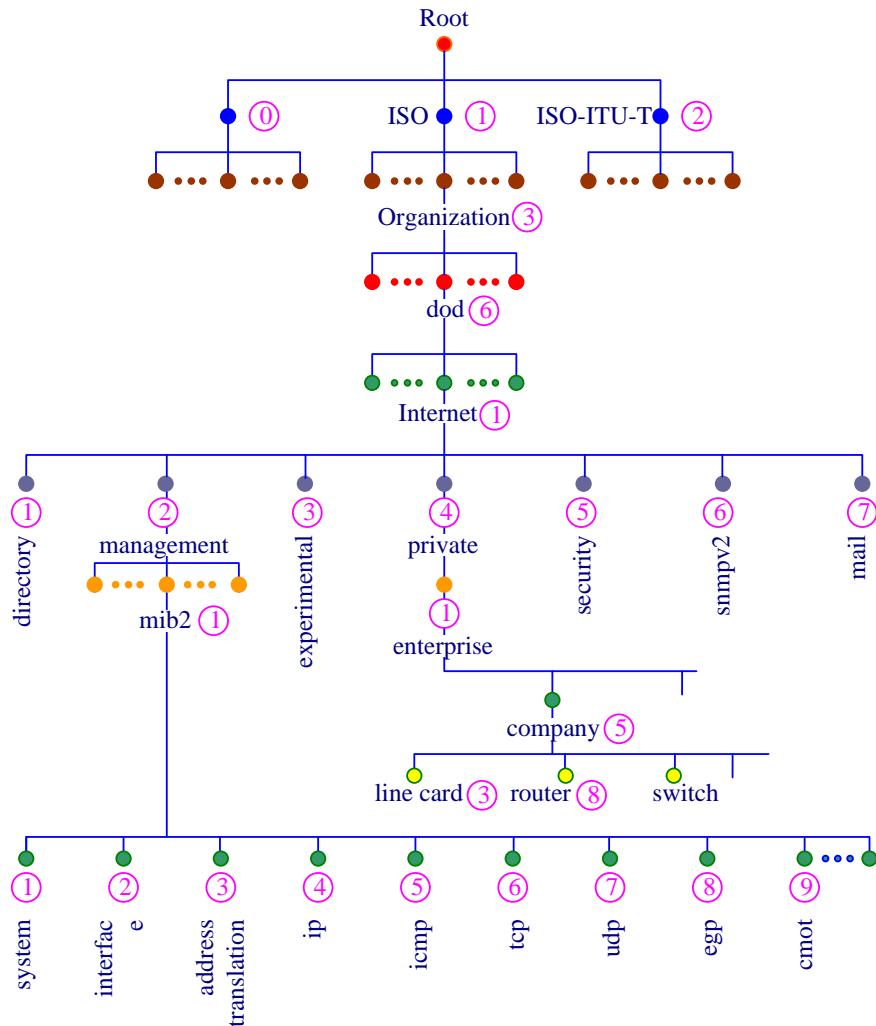


Figure 14.14: The OID tree from its root shown at the top of the example.

14.9.2 Simple Network Management Protocol (SNMP)

The simple network management protocol (SNMP) is a ‘simple’ protocol designed to enable remote network management including monitoring and control of Internet networking devices and protocols. It can use any transport mechanism. In

practice, it is most often used with UDP using port 161 since that is mandatory for conformance with the SNMP standards.

SNMP provides a standardized interface allows network management software and hardware provided by one manufacturer to be used to manage remote network devices (so-called network elements) provided by a different manufacturer.

The task of SNMP is to transport MIB information among managing centers and agents executing on behalf of managing centers. For each managed MIB object, an SNMP request is used to retrieve or change its associated value. If an unsolicited message is received by an agent, or when an interface or device goes down, the protocol can also inform the managing center.

The second version of this protocol, SNMPv2, runs on top of more protocols and has more messaging options, resulting in more effective network management. SNMPv3 has more security options.

SNMPv2 has seven PDUs, or messages, as follows.

1. **GetRequest:** Requests an agent to return attribute values for a list of managed objects.
2. **GetNextRequest:** Used to traverse a table of objects. Since the object attributes are stored in lexicographical order, the result of the previous GetNextRequest can be used as an argument in a subsequent GetNext-Request. In this way, a manager can go through a variable-length table until it has extracted all the information for the same types of objects.
3. **GetBulkRequest:** gets multiple values, equivalent to multiple get request but without using multiple overhead.
4. **InformRequest:** is a manager-to-manager message that two communicating management centers are remote to each other.
5. **GetResponse:** Returns attribute values for the selected objects or error indications for such conditions as invalid object name or nonexistent object.
6. **SetRequest:** Used to change the attribute values of selected objects.
7. **Trap:** Used by the agent to report certain error conditions and changes of state to the managing process.

Figure 14.15 shows the format of SNMP PDUs. Two types of PDUs are depicted: Get or Set and Trap. The Get or Set PDU format is as follows:

- PDU type indicates one of the seven PDU types.
- Request ID is an ID used to verify the response of a request. Thus, a managing center can detect lost requests or replies.
- Error status is used only by Response PDUs to indicate types of errors reported by an agent.
- Error index is a parameter indicating to a network administrator which name has caused an error.
- If requests or replies are lost, SNMP does not mandate any method for retransmission. Error status and Error index fields are all zeros except for the

one in a GetBulkRequest PDU. Figure 14.15 also shows the format of the Trap PDU, whereby the enterprise field is for use in multiple networks; the timestamp field, for measuring up time; and the agent address field, for indicating that the address of the managed agent is included in the PDU header.

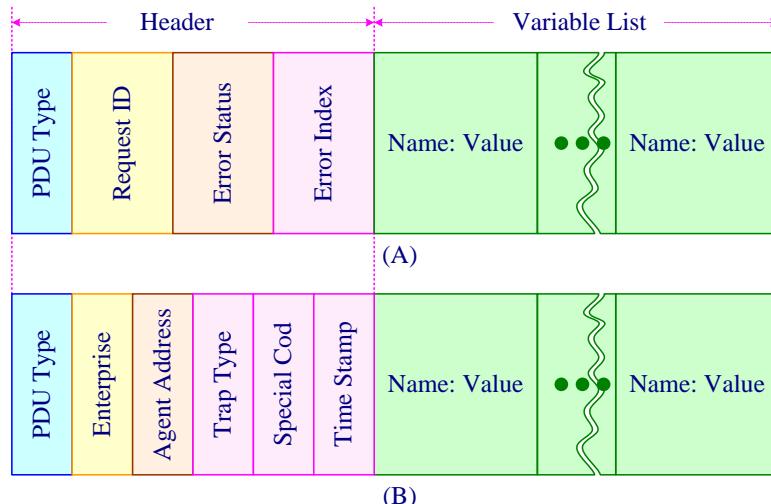


Figure 14.15: SNMP PDU format, A)getrequest PDU, B) trap PDU

Figure 14.16 shows the encapsulation of an SNMP packet. The community string is a simple password protection mechanism. Most are set to “public” for read access and “private” for read-write access. This field is established at set up time.

The variable binding indicates which groups or which objects in the groups are being requested for information.

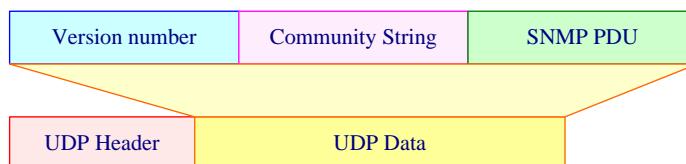


Figure 14.16: Encapsulation of an SNMP packet

 SNMP is most often used for collecting statistical information (the number of packets or frames sent or received per second, the number of errors per second, and so on) and configuration information (IP address of an interface on the device, the version of the operating system running on the device, and so on) about network devices such as computers, hubs, switches, routers, and even network printers..

14.10 Quick Review

- ❖ Many application protocols associated with bulk transfer of data use TCP. Many additional service protocols designed to assist TCP and IP.
- ❖ Application-layer protocols to define the format and order of the messages exchanged between processes and provide network services to user applications.
- ❖ The application layer protocols handle the details of the particular application. The primary functions of these protocols include formatting, presenting and transporting data.
- ❖ The Hypertext Transfer Protocol (HTTP) is one of the most extensively used Internet application protocols. It is based on the client/server idea. The communication between the client and server is carried out through an exchange of HTTP messages.
- ❖ HTTP uses TCP rather than UDP, since reliability of delivery is important for Web pages with text.
- ❖ A URL is a global address of an HTML document and has a part indicates what protocol is used, and another part determines the IP address of the associated resource.
- ❖ There are three HTTP main types: **HTTP/0.9**, **HTTP/1.0**, **HTTP/1.1s**.
- ❖ The use of proxy cache server removes the need to send some requests across the network, thereby reducing network load and improving the response time perceived by the customer.
- ❖ Telnet is one of the oldest remote login application protocols used within the Internet to provide a standardized way for terminals to communicate with host computers, regardless of their type.
- ❖ **DNS Domain Name System** is composed of a distributed data base of names. The names in the DNS data base establish a logical tree structure called the *domain name space*. Each node or domain in the domain name space is named and can contain subdomains.
- ❖ Domains and subdomains are grouped into zones to allow for distributed administration of the name space. The domain name identifies the domain's position in the logical DNS hierarchy in relation to its parent domain by separating each branch of the tree with a period ".".
- ❖ **FTP File Transfer Protocol** allows the transfer of copies of files between one node and another. FTP is not hardware-dependent so its services can function just about anywhere. Using this utility to copy data is typically referred to as "FTPing" a file. The FTP connection actually comprises two separate connections: **FTP control connection** and **FTP data connection** Trivial file transfer protocol (TFTP) is a very simple but unreliable file transfer protocol.
- ❖ **TELNET Remote Terminal Emulation** allows users to communicate with diverse hosts. The TELNET application provides terminal-type access to PCs.
- ❖ **SMTP Simple Mail Transfer Protocol** is the middleman that uses UDP to move data around from one internetwork host to another. Applications run on both hosts that make use of SMTP.
- ❖ **SNMP: Simple Network Management Protocol** is a network management standard widely used with TCP/IP networks and, more recently, with Internetwork

Packet Exchange (IPX) networks. SNMP provides a method of managing network nodes (servers, workstations, routers, bridges, and hubs) from a centrally located host. SNMP performs its management services by using a distributed architecture of management systems and agents.

14.11 Self Test Questions

A- Answer the following questions

1. What are the primary functions of the application layer protocols?
2. How can you distinguish a client from a server?
3. What is the transport layer protocol used by HTTP and why?
4. What is the difference between persistent and non persistent TCP?
5. What are the new features that make HTTP 1.1 more efficient than HTTP 1.0?
6. How can you differentiate HTTP request from HTTP response?
7. What do the HTTP generic request and response messages consist of?
8. How does the proxy cache server work?
9. Where is TELNET applicable?
10. What are the parts of the domain namespace?
11. List some of information-processing functions that are handled by DNS.
12. Why does the DNS response message also contain the question?
13. Explain the DNS directory look-up service.
14. What are the differences between recursive and iterative method that are used by DNS server to resolve a particular address?
15. What is the difference between passive mode FTP and active mode FTP?
16. What is the difference between TFTP and FTP?
17. What does the Internet mail transfer system (MTS) consist of?
18. Explain the operation of the Internet mail system.
19. What are the differences between SMTP and POP3?
20. What are the main components of Network management?
21. How you can describe the management information Base (MIB)?
22. What are the main functions of the simple network management protocol?
23. How is the SNMP data unit encapsulated in the UDP packet?

B- Identify the choice that best completes the statement or answers the question.

1. To communicate with another node, a device initiates a data exchange through _____ layer of the OSI Model.

a. Transport	c. Physical
b. Network	d. Application
2. _____ is used to transfer Web pages over the Internet.

a. UDP	c. ARP
b. HTTP	d. DHCP
3. Each country has its own _____ domain name.

a. bottom-level	c. top-level
-----------------	--------------

- b. intermediate d. network

4. _____ is used in sending and receiving e-mail.
a. SMTP c. MIME
b. IMAP4 d. D-HTML

5. What is the software that allows the user to save e-mail messages in a server mailbox and download them when desired from the server?
a. SMTP c. POP3
b. MIME d. IMAP4

6. _____ is used to transfer Web pages.
a. UDP c. ARP
b. HTTP d. DHCP

7. HTTP is a(n) _____ layer protocol.
a. network c. application
b. transport d. data link

8. What is the portion of the URL that specifies a particular server at a particular site that contains the requested item?
a. service type c. directory
b. domain name d. server type

9. Which of the following service types performs remote logins?
a. http:// c. news://
b. telnet:// d. mailto://

10. _____ service type is used to send an electronic mail message.
a. http:// c. ftp://
b. mailto:// d. sendto://

11. Which part of the URL identifies the protocol that is used to transport the requested document?
a. service type c. top-level domain
b. domain name d. filename

12. Which of the following is a set of codes inserted into a document intended for display on a Web browser?
a. HTTP c. FTP
b. HTML d. Telnet

13. Which of the following is a client/server protocol in which e-mail is received and held for you at your Internet server?
a. MIME c. POP3
b. IMAP4 d. SMTP

14. Which of the following is a terminal emulation program for TCP/IP networks such as the Internet that allows users to log in to a remote computer?
a. FTP c. HTTP
b. Telnet d. TTY

37. A domain name is represented by a series of ____.
- Decimal numbers separated by dots
 - Binary numbers separated by dots
 - Labels separated by colons
 - Labels separated by dots
38. On a domain name a label represents ____.
- A level in the domain naming hierarchy
 - A part of the organization name
 - A part of the organization IP address
 - None of the above
39. ____ is a hierarchical way of associating domain names with IP addresses.
- | | |
|--------|---------|
| a. ARP | c. RARP |
| b. DNS | d. IP |
40. DNS includes ____ components?
- | | |
|------|------|
| a. 1 | c. 3 |
| b. 2 | d. 4 |

ANSWER TO SELF TEST QUESTIONS

Chapter1

- | | | | | | |
|-----|----|-----|---|-----|---|
| 1. | a. | 15. | a | 16. | b |
| 2. | c. | 16. | a | 17. | a |
| 3. | c. | 17. | a | 18. | b |
| 4. | d. | 18. | d | 19. | a |
| 5. | a. | 19. | c | 20. | d |
| 6. | b. | 20. | b | 21. | c |
| 7. | c. | 21. | c | 22. | d |
| 8. | c. | 22. | a | 23. | d |
| 9. | a. | 23. | a | 24. | c |
| 10. | b. | 24. | c | 25. | b |
| 11. | a. | 25. | d | 26. | b |
| 12. | c. | 26. | b | 27. | a |
| 13. | b. | 27. | d | 28. | a |
| 14. | b. | 28. | a | 29. | d |
| 15. | a. | 29. | d | 30. | b |
| 16. | c. | 30. | a | 31. | b |
| 17. | b. | 31. | d | 32. | d |
| 18. | d. | 32. | c | 33. | c |
| 19. | c | 33. | c | 34. | a |
| 20. | d. | 34. | a | 35. | d |
| 21. | b. | 35. | c | 36. | d |
| 22. | a. | 36. | a | 37. | a |
| 23. | c. | 37. | c | 38. | c |
| 24. | b. | 38. | a | 39. | d |
| 25. | a. | 39. | b | 40. | b |
| | | 40. | a | 41. | a |
| | | 41. | c | | |

Chapter 2

- | | |
|-----|---|
| 1. | a |
| 2. | b |
| 3. | c |
| 4. | c |
| 5. | d |
| 6. | c |
| 7. | a |
| 8. | a |
| 9. | a |
| 10. | d |
| 11. | d |
| 12. | c |
| 13. | d |
| 14. | c |

Chapter 3

- | | |
|-----|---|
| 1. | c |
| 2. | c |
| 3. | b |
| 4. | d |
| 5. | c |
| 6. | c |
| 7. | a |
| 8. | a |
| 9. | a |
| 10. | b |
| 11. | b |
| 12. | a |
| 13. | a |
| 14. | c |
| 15. | a |

Chapter 4

- | | |
|-----|---|
| 1. | c |
| 2. | d |
| 3. | b |
| 4. | a |
| 5. | b |
| 6. | c |
| 7. | b |
| 8. | c |
| 9. | d |
| 10. | b |
| 11. | a |
| 12. | a |
| 13. | c |
| 14. | c |
| 15. | a |
| 16. | b |

- | | | | | | |
|-----|---|-----|---|-----|------------------|
| 17. | b | 14. | b | 16. | c |
| 18. | b | 15. | b | 17. | b |
| 19. | a | 16. | a | 18. | a |
| 20. | b | 17. | d | 19. | c |
| 21. | c | 18. | c | 20. | d |
| 22. | a | 19. | a | 21. | c |
| 23. | b | 20. | d | 22. | a |
| 24. | b | 21. | d | 23. | d |
| 25. | b | 22. | b | 24. | b |
| 26. | b | 23. | b | 25. | a |
| 27. | d | 24. | c | 26. | d |
| 28. | c | 25. | a | 27. | b |
| 29. | c | 26. | c | 28. | c |
| 30. | a | 27. | b | 29. | a |
| 31. | c | 28. | b | 30. | d |
| 32. | c | 29. | c | 31. | d |
| 33. | d | 30. | c | 32. | c |
| 34. | d | 31. | d | 33. | c |
| 35. | b | 32. | c | 34. | c |
| 36. | b | 33. | a | 35. | b |
| 37. | c | 34. | a | | |
| 38. | a | 35. | c | | Chapter 7 |
| 39. | b | 36. | a | 1. | a |
| 40. | d | 37. | d | 2. | d |
| 41. | b | 38. | b | 3. | c |
| 42. | c | 39. | c | 4. | d |
| 43. | b | 40. | a | 5. | a |
| 44. | a | 41. | b | 6. | c |
| 45. | c | 42. | c | 7. | b |
| 46. | a | | | 8. | c |
| 47. | b | | | 9. | a |

Chapter 5

- | | | | | | |
|-----|---|-----|---|-----|---|
| 1. | c | 1. | b | 10. | b |
| 2. | d | 2. | c | 11. | a |
| 3. | b | 3. | a | 12. | b |
| 4. | c | 4. | d | 13. | b |
| 5. | c | 5. | c | 14. | c |
| 6. | a | 6. | d | 15. | b |
| 7. | b | 7. | c | 16. | d |
| 8. | c | 8. | b | 17. | d |
| 9. | b | 9. | b | 18. | b |
| 10. | b | 10. | c | 19. | b |
| 11. | c | 11. | a | 20. | c |
| 12. | b | 12. | d | 21. | c |
| 13. | c | 13. | d | 22. | b |
| | | 14. | b | 23. | c |
| | | 15. | a | 24. | a |

25.	c	16.	a	1.	d
26.	c	17.	b	2.	a
27.	a	18.	b	3.	d
28.	a	19.	d	4.	c
29.	d	20.	a	5.	b
30.	a	21.	c	6.	c
31.	b	22.	b	7.	a
32.	d	23.	a	8.	b
33.	b	24.	d	9.	a
34.	a	25.	c.	10.	b
35.	a	26.	d	11.	c
36.	c	27.	c	12.	d
37.	a	28.	a	13.	a
38.	c	29.	c	14.	a
39.	b	30.	b	15.	a
40.	a	31.	c	16.	b
41.	c	32.	d	17.	a
42.	c	33.	a	18.	d
43.	b	34.	d	19.	c
44.	a	35.	d	20.	b
45.	d	36.	c	21.	a
46.	b	37.	a	22.	c
47.	a	38.	a	23.	d
48.	b	39.	a	24.	b
49.	d	40.	d	25.	b
50.	a	41.	c	26.	c
51.	d	42.	b	27.	a
52.	b	43.	b	28.	b
53.	d	44.	b	29.	b
		45.	a	30.	c

Chapter 8

1.	d	46.	c	31.	b
2.	c	47.	b	32.	b
3.	a	48.	b	33.	c
4.	c	49.	a	34.	b
5.	d	50.	a	35.	a
6.	d	51.	c	36.	b
7.	d	52.	b	37.	b
8.	d	53.	c	38.	d
9.	a	54.	a	39.	b
10.	d	55.	b	40.	a
11.	d	56.	c	41.	c
12.	a	57.	b	42.	a
13.	a	58.	a	43.	d
14.	a,d	59.	a	44.	c
15.	b			45.	a
				46.	c

Chapter 9

47.	a	24.	c	32.	d
48.	c	25.	a	33.	c
49.	d	26.	d	34.	c
50.	c	27.	a	35.	a
51.	b	28.	b	36.	b
52.	c	29.	c	37.	c
53.	a	30.	b	38.	a
54.	b	31.	a	39.	b
55.	b	32.	b	40.	d
56.	d	33.	c	41.	c
57.	c	34.	c	42.	a
58.	a	35.	d	43.	b
59.	b	36.	c	44.	b
60.	a			45.	c.

Chapter 11

61.	d	1.	a	46.	d
62.	c	2.	c	47.	a
63.	c	3.	a	48.	a
64.	d	4.	d	49.	c
65.	d	5.	b	50.	b
66.	b	6.	a	51.	a
67.	d	7.	d	52.	c
		8.	a	53.	c
				54.	b
				55.	d

Chapter 10

1.	a	9.	c	1.	b
2.	d	10.	d	2.	c
3.	d	11.	b	3.	a
4.	a	12.	b	4.	b
5.	c	13.	c	5.	c
6.	b	14.	C	6.	c
7.	a	15.	d	7.	d
8.	d	16.	a	8.	b
9.	a	17.	b	9.	c
10.	c	18.	b	10.	c
11.	d	19.	b,d	11.	b
12.	b,d	20.	c	12.	d
13.	c	21.	d	13.	c
14.	b	22.	d	14.	a
15.	a	23.	a	15.	c.
16.	c	24.	b	16.	a
17.	b	25.	b	17.	c
18.	d	26.	d	18.	c
19.	c	27.	a	19.	d
20.	a	28.	a	20.	c
21.	a	29.	b		
22.	c	30.	d		
23.	d	31.	c		

Chapter 12

- | | | | | | |
|-----|----|-----|---|-----|---|
| 21. | c | 23. | d | 31. | d |
| 22. | c | 24. | b | 32. | c |
| 23. | a | 25. | c | 33. | d |
| 24. | b | 26. | b | 34. | b |
| 25. | d | 27. | d | 35. | b |
| 26. | a | 28. | a | 36. | c |
| 27. | a | 29. | c | 37. | d |
| 28. | d | 30. | c | 38. | a |
| 29. | a | 31. | d | 39. | b |
| 30. | c | 32. | a | 40. | c |
| 31. | c | 33. | a | | |
| 32. | d | 34. | d | | |
| 33. | c. | 35. | d | | |
| 34. | b | 36. | b | | |
| 35. | a | | | | |
| 36. | c | | | | |
| 37. | d | | | | |
| 38. | a | 1. | d | | |
| 39. | d | 2. | b | | |
| 40. | b | 3. | c | | |
| 41. | b | 4. | a | | |
| 42. | a | 5. | c | | |
| | | 6. | b | | |
| | | 7. | c | | |
| | | 8. | b | | |

Chapter 14

- | | | | |
|-----|----|-----|---|
| 1. | c | 9. | b |
| 2. | c | 10. | b |
| 3. | a | 11. | a |
| 4. | a | 12. | b |
| 5. | c. | 13. | b |
| 6. | c | 14. | b |
| 7. | a | 15. | a |
| 8. | c | 16. | d |
| 9. | a | 17. | b |
| 10. | d | 18. | a |
| 11. | d | 19. | b |
| 12. | b | 20. | a |
| 13. | c | 21. | a |
| 14. | d | 22. | b |
| 15. | c | 23. | d |
| 16. | a | 24. | b |
| 17. | b | 25. | a |
| 18. | c | 26. | d |
| 19. | d | 27. | b |
| 20. | a | 28. | a |
| 21. | d | 29. | b |
| 22. | b | 30. | b |

Chapter 13

GLOSSARY

- 1000BaseTX:** Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 1 Gbps (gigabits per second) with a distance limitation of 220 meters per segment.
- 100BaseT:** Ethernet specification for unshielded twisted pair cabling that is used to transmit data at 100 Mbps (megabits per second) with a distance limit of 100 meters per segment.
- 10Base2:** Ethernet specification for thin coaxial cable transmits signals at 10 Mbps (megabits per second) with a distance limit of 185 meters per segment.
- 10Base5:** Ethernet specification for thick coaxial cable transmits signals at 10 Mbps (megabits per second) with a distance limit of 500 meters per segment.
- 10BaseF:** Ethernet specification for Optical fiber cable transmits signals at 10 Mbps (megabits per second) with a distance limit of 2000 meters per segment.
- 10BaseT:** Ethernet specification for unshielded twisted pair cable (category 3, 4, or 5), transmits signals at 10 Mbps (megabits per second) with a distance limit of 100 meters per segment.
- 802.11:** standards are a group of wireless specifications developed by the IEEE. The standards cover items such as frequency ranges, modulation, security, etc. Below are a few of the key 802.11 standards:
- 802.11a:** Operates in the 5-GHz frequency range (5.125 to 5.85 GHz) with a maximum transmission rate of 54Mbit/sec. The 5-GHz frequency band has more radio channels than the 2.4-GHz frequency (used in 802.11b/g) and is less crowded. However, it has a smaller range than 802.11b/g. It is not generally used in domestic wireless networks, but is supported by high-end wireless equipment for business use from vendors such as Cisco Systems.
- 802.11b:** Operates in the 2.4-GHz band (2.4 to 2.4835 GHz) and provides transmission rates of up to 11Mbit/sec. Generally used standard for domestic and business wireless networks, but can suffer from interference from other devices in the frequency range, such as microwave ovens, cordless phones, and Bluetooth devices. Forward compatible with 802.11g standard and many dual-standard devices are referred to as 802.11b/g.
- 802.11e:** Quality-of-service specification designed to guarantee the quality of voice and video traffic over wireless networks.
- 802.11g:** Operates in the same frequency range as 802.11b, but supports transmission rates of up to 54Mbit/sec. It 802.11g is backward compatible with the older 802.11b standard and many dual-standard devices are referred to as 802.11b/g. NOTE:- Although compatibility between 802.11g and 802.11b is useful for migrating to newer technology, it should be remembered that all devices will work to the standard of the slowest device on the network. This means that all devices will

work at 11Mb/sec whilst there are still 802.11b devices connected to the network.

802.11i: A standard for improving wireless LAN security, generally referred to as WPA2 (see below). It adds new encryption protocols, such as AES (Advanced Encryption Standard).

Access Line: That portion of a leased telephone line that permanently connects the user with the serving central office or wire carrier.

Access method: The way in which data may pass onto a physical network medium.

Access Port: The physical gateway between a customer's local loop and the frame relay network.

Access Time: The amount of time it takes the computer to find and read data from a disk or from memory. The average access time for a hard disk is based on the time it takes the head to seek and find the specified track, the time for the head to lock onto it and the time for the head to spin around until the desired sector is beneath the head.

Acknowledgment: A message indicating that data has been correctly received.

Ad hoc mode: An ad hoc network is one where wireless devices, such as PCs can communicate directly with one another without using an Access Point. An Access Point Based network, known as an infrastructure network, is more generally used.

Adapter: The device that connects a piece of equipment to the network and controls the electrical protocol for communication with that network; also called network interface card, or NIC.

Adaptive Channel Allocation: Used in multiplexing signals. Bandwidth is only afforded a signal by request.

Adaptive Differential Pulse Code Modulation (ADPCM): A voice digitization technique requiring a bandwidth of 32 kbps.

Adaptive Routing: Using intelligent methods for selecting routes for packet transmission.

Adaptive Technology: An Intel technology (supported in adapters and switches) that automatically and dynamically customizes product performance to match network operating conditions, thus helping to optimize network performance.

Address: A set of numbers that uniquely identifies a data processing entity, such as a workstation in a network, a location in computer memory, or the destination of a packet of data traveling through a network. A sequence of bits, a character, or a group of characters that identifies a network station, user, or application. Used mainly for routing purposes.

Advanced Communications Function (ACF): Official product name for all IBM SNA products (i.e. ACF/VTAM).

Alternate Mark Inversion (AMI): Line coding method for T-1 lines.

American National Standards Institute (ANSI): The national standards body that represents the United States as an ISO member.

American Standard Code for Information Interchange (ASCII): A common code for representing alphanumeric characters in computers.

Amplifier: A device used to boost the strength of an electronic or optical signal, which is weakened (attenuated) as it passes through the transport network.

Analog-To-Digital (A/D) & Digital-To-Analog (D/A) Converters: Devices that can change analog impulses into digital impulses and vice versa for use with digital equipment.

Antenna: A structure, which transmits or receives electromagnetic signals.

Application Layer: In the OSI Model, the highest of the seven layers that are reflected in the ISDN standards being developed by the CCITT. Functions of the Application Layer include the interface between the user (person or program) and the communications network.

Application Oriented Layer: Layers 5, 6, and 7 of the OSI Reference Model. They are also referred to as the “Network Independent” or “Communications” Layers. These layers are concerned with the protocols that allow two end user application processes to interact with each other, normally through a range of services offered by the local operating system.

Architecture: The principles that govern the design of hardware or software. Architecture typically describes how a system is structured and how its components fit together. A system’s architecture defines the formats and procedures used for communication between components and with other systems.

ARCnet: Attached Resources Computer network. Developed by Datapoint in the late 70's to provide data transfers at 2.5 Mbps. Very inexpensive products with great product interoperability.

Asymmetric digital subscriber line (ADSL): here asymmetric means data speed does not same in both directions (upload and download) and provides high speed on already exiting telephone lines and same time you can use internet and as well as your line for phone.

Asymmetric Digital Subscriber Line (ADSL): A new technology that allows more data to be sent over existing copper telephone lines. ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

Asynchronous protocol: Protocol designed for async. data transfers including ASCII, TTY, Kermit and XMODEM.

Asynchronous Transfer Mode (ATM): A network protocol that transmits data at a speed of 155 Mbps and higher. It is very fast and reliable data transmission connection line that can carry data, audio, video, imaging and multimedia transmission etc.

Attachment Unit Interface (AUI) Connector: A 15 pin connector found on Ethernet cards that can be used for attaching coaxial, Optical fiber, or twisted pair cable.

Attenuation: The decrease in the power of some sort of signal.

Backbone: A segment of a network that connects LANs together. Often Optical fiber cabling is used for this purpose.

Backhaul Capacity: Capacity on terrestrial Optical fiber cables from undersea cable landing stations to metropolitan areas.

Bandwidth: The difference between the highest and lowest frequencies used for a communication channel. Generally, more bandwidth means greater transmission capacity.

Baseband: A network transmission technique that uses voltage to represent data; similar to turning a light switch on and off.

Basic Input/Output System (BIOS): The BIOS is responsible for handling the input/output operations of a computer.

Baud rate: The maximum number of signal pulses that a communication line can handle per second. Higher baud rates indicate greater transmission capacities.

Bearer Channel: The ISDN communications channel that provides a means of transmitting and recording voice and nonvoice information in real time and without changing message content. The B channel runs at 64 kbps. Voice information is digitally encoded using pulse modulation (PCM). Nonvoice information may be circuit-switched synchronous data or packet-switched data.

Bipolar: Transmission method that alternates between positive and negative voltages to represent bits.

Bit: A binary digit, the representation of a signal, wave, or state, as either a binary zero or a one.

BNC Connectors: This connector used to connect coaxial and 10Base2 cables.

Border Gateway Protocol (BGP): A routing protocol used in interdomain routing in large networks to maintain integrity of the network. It allows the routers to exchange only prespecified information with prespecified routers in other domains.

Bridge: Devices that connect and pass packets between two similar networks at the OSI Data Link layer and passes data between them.

Broadband: A network transmission technique that uses radio frequencies on a cable; a broadband cable is typically shared with other networks or services, such as TV or teleconferencing.

Broadcast: A network transmission sent to all nodes on the network.

Broadcast Radio: It is a wireless transmission medium that is used to communicate information through radio signals in air, over long distance such as between cities and countries.

Brouter: An internetworking device that functions as a router for protocols that it understands, and as a bridge for those that it does not.

Buffer: A temporary storage place for data being received or transmitted.

Bus topology: A physical layout of network devices in which all devices must share a common medium to transfer data, and no two devices may transmit simultaneously.

Byte: Eight bits. A byte can represent whole numbers from 0 to 255. Typically, one byte holds a single character.

Cable: Cable is a transmission medium and there are different types of cables that are used in a network like coaxial cable, UTP/STP and Optical fiber cables.

Capacity: The information-carrying ability of a telecommunications system, as defined by its design (number of fibers, system length, and optoelectronic equipment) and its deployed equipment (amount of optoelectronics in the station) and measured in bits per second.

Carrier detect: Circuit that detects the presence of a carrier.

Carrier Sense Multiple Access Collision Avoidance (CSMA/CA): is a network access method in which each device signals its intent to transmit before it actually does so. This prevents other devices from sending information, thus preventing collisions from occurring between signals from two or more devices.

Carrier Sense Multiple Access Collision Detection (CSMA/CD): is a network access method in which devices that are ready to transmit data first check the channel for a carrier. If no carrier is sensed, a device can transmit. If two devices transmit at once, a collision occurs and each computer backs off and waits a random amount of time before attempting to retransmit. This is the access method used by Ethernet.

Carrier Signal: A continuous waveform that is capable of being modulated to convey information. The signal conveys no information until its amplitude, frequency, or phase is changed (modulated). The changes in the signal convey the information.

Cellular Radio: Cellular radio is a form of broadcast radio that is used for mobile communication such as cellular and wireless modems.

Central Office (CO): The telephone company switching facility or center, at which subscribers' local loops terminate. It handles a specific geographic area, identified by the first three digits of the local telephone number. Since divestiture, these are the facilities of the local Bell operating company. Central Processing Unit (CPU) .The main operating portion of a computer that performs all system functions as directed by the user or a peripheral.

Channel Bank: Equipment typically located in a telephone central office that performs multiplexing of lower speed channels into a higher speed composite channel. The channel bank also detects and transmits signaling information for each

channel and transmits framing information so the receiver can identify time slots allocated to each channel.:.

Channel: A physical or logical path allowing the transmission of information, the path connecting a data source and a data receiver. A radio frequency assignment (which is dependent upon the frequency band and geographic location). Part of a circuit path through several entities in communications systems. A channel runs between two nodes.

Checksum: A value created by adding up bits in a packet. The resultant value is computed at the sender and receiver of data. Mismatches will cause error-recovery routines to be followed.

Circuit Switching: The process of establishing and maintaining a circuit between two users on demand, such that the users have exclusive use of the circuit until the connection is released.

Cladding: A covering of glass or plastic surrounding a Optical fiber core designed to prevent light waves from leaving the core.

Client/Server: A networking system in which one or more file servers (Server) provide services; such as network management, application and centralized data storage for workstations (Clients).

Client: A node on a network that requests services from a network server.

Coaxial Cable: Coaxial Cable is also referred to as coax. It consists of a single copper wire surrounded by insulating materials. Usually, it is surrounded by three layers. Insulating material Solid metal shield External plastic cover

Codec (Coder/Decoder : An integrated circuit (IC) or circuit made of ICs that performs a specific analog-to-digital and digital-to-analog conversion, such as conversion of an analog signal to a 64 kbps digital bit stream or an analog television signal to a digital format.

Collision Domain: The maximum length of the wiring medium that allows collision detection. For example, the collision domain in Fast Ethernet using 100BASE-TX is 205 meters.

Collision: When electrical signals from two or more devices sharing a common data transfer medium crash into one another. this commonly happens on Ethernet-type systems.

Common carrier: A company that provides telecommunications services to the public. Telephone companies are an example.

Common Channel Signaling (CCS): A way of providing the interexchange signaling capabilities required for an ISDN using out-of-band signaling. CCS provides greater flexibility and information content than in-band systems for interexchange signaling.

Communication channel: The medium through which information is transmitted.

Communications Satellite: A “relay system” in orbit above the earth’s surface for telecommunications signals such as voice, video and data. Requires earth stations to transmit and receive the signals at the ground locations (downlinks). Commonly called a “bird.”

Communications server: A specialized network node that provides clients with access to communications capabilities. A typical example is a computer that provides other nodes with access to a shared modem.

Compression: Algorithm that minimizes the redundancy in the signal to be transmitted.

Computer Conferencing: Allows users to communicate with other systems via a computer network. The transmission of data, text, questions and answers can be accomplished quickly and easily. Computer conferences can be either synchronous or asynchronous. The former requires that all participants be online simultaneously. An asynchronous system allows participants to access at their convenience, thereby avoiding “telephone tag.”

Concentrator: A device that provides a central connection point for cables from workstations, servers, and peripherals. Most concentrators contain the ability to amplify the electrical signal they receive.

Configuration: the physical and electronic arrangement of equipment (hardware and software) that allows for successful work, especially for interchange of data over communications lines.

Connectionless: No relationship is set between sender and receiver for reliability's sake.

Connection-oriented: A relationship is set up between sender and receiver to provide increased data transfer reliability.

Connectivity: The attachment of devices on a network. The devices may be similar or dissimilar.

Crosstalk: Interference caused by "leaks" from a nearby communication channel.

Cryptography: The process of concealing the contents of a message from all except those who know the key. Cryptography is used to protect e-mail messages, credit card information, and corporate data. As the Internet and other forms of electronic communication become more prevalent, electronic security is also becoming increasingly important.

Dark Wavelength: Refers to a virtual channel in a Optical fiber system utilizing DWDM. Each virtual channel is supported through a specific wavelength of light, with many channels riding over the same fiber. Once the fiber system is deployed and the DWDM equipment is activated, some of the wavelengths may be activated immediately and others may be left dark for future needs. When the need arises, those dark wavelengths are lit up.

Data compression: A procedure that uses mathematical techniques to encode data so that it uses less space. In most cases, data must be decompressed into its original form to be usable.

Data encryption: A security procedure that encodes data so that it cannot easily be understood. To be usable, data must be decrypted into its original form by reversing the procedure that was used to encrypt it.

Data Link Layer: In the OSI Model, the network processing entity that establishes, maintains, and releases data link connections between elements in a network. This layer ensures reliable transport of information between communicating devices.

Data Terminal Equipment (DTE): A PC hooked to a modem is an example of this.

Data base server: A device set aside to assist in data base storage and retrieval. The data base itself is not necessarily stored in this machine.

Data base server: A network computer that specializes in retrieving and storing data, providing that service to clients.

DataBase: A collection files containing data that are related and accessed by a data base management program.

Datagram: A TCP/IP packet containing data and a source and destination address. It uses an unreliable delivery method.

De facto standard: A standard that exists through popular practice.

Decibel (dB): A decibel is a logarithmic unit used to describe signal ratios.

DECnet: A network developed by Digital Equipment Corporation that connects DEC computers, PCs, and Macintoshes.

Decoder: Device that reconstructs or “unscrambles” an encrypted signal.

Decryption: Code conversion of digitally coded signal values in order to cancel encryption.

Dedicated line: Transmission line servicing only one type of data. Pathway is permanent.

Delta Modulation (DM): A differential pulse code modulation, where the polarity of the difference between the actual samples value and a prediction value is transmitted only by one bit.

Demodulation: In general, this term refers to any device, which recovers the original signal after it has been modulated onto a high frequency carrier.

Demodulator: A device, which removes a signal from a carrier for subsequent conversion to digital data. Modems do this.

Dense Wavelength Division Multiplexing (DWDM): A technique which employs more than one light source and detector operating at different wavelengths and simultaneously transmits optical signals through the same fiber while message integrity of each signal is preserved.

Desktop computer: generic term for personal computer (Mac or IBM) in an office or home, as opposed to a special-purpose computer like a server or router or workstation, or a laptop or notebook machine.

Differential Pulse Code Modulation (DPCM): A pulse code modulation in which the coded value transmitted for each sample represents the quantized difference between the present sample value and a prediction value. For signals having strong correlation between successive samples, a reduction of information can be attained, since fewer levels may be used to quantize differences than would be required for quantizing sample values with comparable precision.

Digital data: Information that is digital (1s and 0s) in nature.

Digital Modem: The modem that is used to send and to receive data to and from a digital telephone line is called digital modem. ISDN modem and DSL modem are the best example of digital modem.

Digital Multiplex Hierarchy: A series of digital multiplexes defined by CCITT graded to combine at one level a defined number of digital signals, each having a digit rate prescribed for a lower level, into a digital signal having a prescribed digit rate.

Digital Network Architecture (DNA): A network architecture developed by Digital Equipment Corporation.

Digital Network: A telecommunications network where information is encoded in binary form. Digital networks encode voice communications in binary form and eliminate the need for modems for data communications. Digital networks are typically more flexible and more reliable than analog networks.

Digital Signal Level 0 (DS0): Designates a 64Kbps digital signal, a channel, comprised of 8,000 8-bit bytes of customer data.

Digital Signal Level 1 (DS1): Designates the combination of 24 DS0 channels plus overhead bits into a 1.544Mbps T1 data stream.

Digital Subscriber Line (DSL): DSL provides high speed on already exiting telephone lines and same time you can use internet and as well as your line for phone. In DSL, both ends of connections require the network cards and DSL modems for data communication.

Digital Switching: The process of establishing and maintaining a connection, under stored program control, where binary-encoded information is routed between two or more end-users.

Digital Terminating Equipment (DTE): Customer premise equipment. Includes the DSU functionality, which may or may not be physically incorporated into the same equipment package as other DTE functions at the manufacturers' or customers' option.

Digital Transmission: Method of storing, processing and transmitting information through the use of distinct electronic or optical pulses that represent the binary digits 0 and 1.

Digital Transport: A portion of the telecommunications network using digital methods for the transmission of signals from one point to another to complete

transmission service channel. A transmission service channel may have one or more digital transport portion(s).

Digital: A form of information that is represented by signals encoded as a series of discrete numbers, intervals or steps, as contrasted to continuous or analog circuits.

DIN: A plug and socket connector consisting of a circular pattern of pins in a metal sleeve. This type of connector is commonly seen on keyboards.

Diskless workstation: A networked computer that does not have local storage.

Distributed application: An application that runs on two or more networked computers.

Distributed processing: A system in which processing of applications stored on the network is done by client computers. "Distributed processing" is also sometimes used to refer to "distributed applications."

Domain Name System (DNS): naming conventions (including 4-part "dotted quad" version as well as text name) for hooking a server into the big network and making sure it can be addressed. For example, UCD's "bullwinkle" server is a domain known by the IP address 128.120.8.167 in machine-talk; the "peseta" mail server is 128.120.2.149. When a Web browser like Netscape cannot find a particular host computer's location (or if the host doesn't answer) the error message includes "cannot locate DNS."

Domain Name Resolver (DNR): a piece of software living in a Mac's System Folder that helps "resolve" domain names into machine-comprehensible form; you will not know this item exists until something goes wrong with it, in which case you will get the an error message referring to "Domain Name Reslover" (yes, with the picturesque typo there).

Domain: a defined Internet location or set of addressable computers, usually indicated in the last parts of an Internet address; for example the ucdavis.edu part of the hierarchical designation like fzstenze@peseta.ucdavis.edu, with the .edu signifying a US educational domain; company domains are designated with .com (as in timewaste.com), organizations with .org (as in dogooders.org).

Disk Operating System (DOS): From Microsoft, that little computer company in Redmond, WA.

Downlink: An earth station that receives satellite signals.

Dumb terminal: An entry and display device that has no processing capability. Used in networks based on central processing.

Duplex: Simultaneous two-way transmission of data. (Also referred to as full duplex.)

E-1: Similar to the North American T-1, E-1 is the European format for digital transmission. E-1 carries signals at 2.048 Mbps (32 channels at 64Kbps), versus the T-1, which carries signals at 1.544 Mbps (24 channels at 64Kbps). E-1 and T-1 lines may be interconnected for international use.

E-mail: An electronic mail message sent from a host computer to a remote computer.

Emulation: Act like something else. An example would be when a PC appears to be a dumb terminal to a host.

Encoder: A device that electronically alters a signal (encrypts) so that it can be clearly seen only by recipients that have a decoder which reverses the encryption process.

Encryption: The process of electronically altering or “scrambling” a signal. Encryption is usually used as a security method for satellite transmissions. Code conversion of digitally coded signal values, performed, in general, without any increase of bit rate, in order to prevent unauthorized reception of a signal. Often a specific code or “key” is required to restore the original data.

End User: End user is a person who executes the applications on the workstations.

Ethernet address Each networking node has its own unique, pre-programmed Ethernet address, the address is obtained automatically when required by network transmission. This number identifies the node or networking device as a unique communication device and enables direct communications to and from the device.

Enterprise network: A network comprised of all the LANs or other networks within a single organization.

Error Correction: Technique of transmitting a small amount of redundancy to the coded information that can be used to restore the integrity of corrupted received data.

Error Detection: Process of detecting errors affecting a digital transmission. By a suitable selection of a redundant transmission code, those code words being affected by transmission errors can be detected as being erroneous.

Error Rate: The ratio of the number of incorrectly received code elements, code words or blocks to the total number received. Consequently, distinction is made between bit, word or block error rate.

Ethernet card: add-on circuit board that plugs into the parallel port on the back of a computer, and allows high-speed data communication via 10BASE-T.

Ethernet port: a cable jack or socket allowing a user to plug in an Ethernet-ready notebook computer and gain Internet access; the library is adding Ethernet ports, as are other areas on campus, although the process of configuring IP addresses and protocols is still being streamlined so that non-experts can do it easily.

Ethernet: A popular local network design, which is the trademarked product of Xerox Corporation. It is characterized by 10 mbps Baseband transmission over a coaxial cable and employs CMSA/CD for access control.

Fast Ethernet: The high-bandwidth networking technology based on the 802.3 Ethernet standard (100BASE-T); supports 100Mbps performance, a tenfold increase over original 10Mbps Ethernet (10BASE-T).

Fault Tolerance: The ability of a system to respond gracefully to an unexpected hardware or software failure. There are many levels of fault tolerance, the lowest being the ability to continue operation in the event of a power failure.

Fiber Distributed Data Interface (FDDI): FDDI is a communication protocol that is used to interconnect two or more local area networks that are often over large distances

Optical fiber: A cable that uses light to communicate; the fastest and most noise-resistant cable available for network wiring, but also the most expensive.

Field: One of the two or more equal parts into which a frame is divided in interlaced scanning.

File Server: File server is a Server Computer that contains the data, applications and gives logon access to the other computers on the network. If the file server is dedicated only then it is connected to the client/server network.

File Transfer Protocol (FTP): Communications protocol used to copy files from one computer to another.

Flag: Typically a certain bit that has meaning in bit-oriented protocols.

Frame relay: A high-speed, low-latency packet switching technology, based on a switched virtual network topology, used for WANs; popular for LAN-to-LAN connections.

Frame: A block of data in bit-oriented protocols.

Frequency Bandwidth: The portion of the audible band 20 to 20,000 Hertz over which the power output was measured.

Frequency Division Multiplexing (FDM): The official term for placing several different signals on a wire each has its own unique frequencies (i.e. broadband LANs).

Frequency Modulation (FM): Used to encode data into a carrier of a set frequency. The changes in frequency represent 1s and 0s.

Frequency: Cycles per second. Measured in Hertz (Hz).

Full Duplex: A communication channel over which both transmission and reception are possible in two directions simultaneously.

Functional Signaling: A signaling system under ISDN that assumes intelligent terminals. Functional signaling allows the terminal, rather than the central office, to monitor call status and send appropriate signals to the central office for action. Initially functional signaling will be limited to basic call set-up procedures (see stimulus signaling).

Gateway: A network station used to interconnect two or more dissimilar networks or devices; may perform protocol conversion.

Gigabit Ethernet: A developing technology for 1 gigabit per second (1Gbps) Ethernet; equivalent to 1000Mbps and 10 times faster than Fast Ethernet.

Half-Duplex: A communications channel over which both transmission and reception are possible but only in one direction at a time.

Handshaking: Signals sent by communicating devices to initiate and synchronize the communication.

Head-End: The electronic equipment located at the start of a cable system, usually including terrestrial and earth station receiving antennas, preamplifiers, frequency converters, demodulators, modulators, scramblers, descramblers, and related equipment.

High Level Data Link Control (HDLC): A generic link layer protocol standard for point-to-point and multi-point communications that is bit oriented and in which control codes differ according to their bit positions and patterns.

Higher Layer Functions: In the seven-layer OSI Model, layers 4 through 7 provide higher layer functions, which manage and control data communications applications, such as teletext, videotext, and electronic mail

Home page: The main page of a Web site and the first screen that a visitor sees displayed when connecting to that site; usually has links to other pages, both within that site and to other sites.

Hop count: A term used when counting components and sections of wire in an Ethernet network to determine whether Ethernet compliance has been met.

Host: computer (or server) that can connect *as a computer* to other computers on the Internet, and identifiable as such through IP address.

Hot spot: A place, such as a hotel, restaurant or airport, that offers wireless access, either free or for a fee.

Hub: A hardware device that contains multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat but merely split signals sent through them).

Hybrid System: A system that combines two or more communications technologies (e.g., a system that integrates freeze-frame video images and an electronic tablet for free-hand drawings).

Hyperlinks: Embedded "hot spots" in Web pages that allow users to jump from one document to another related document, regardless of where it "lives" on the Internet.

HyperText Markup Language (HTML): the authoring language of the Internet; used to create Web pages.

Impulsive Noise: Noise characterized by non-overlapping transient disturbances commonly introduced by devices such as switches and relays.

In-Band Signaling: Signaling that occurs over the same channel that carries user information. Contrast this with out-of-band signaling.

Infrared: Electromagnetic waves whose frequency range is above that of microwaves, but below that of the visible spectrum.

Integrated Digital Network (IDN): A network that can transmit or receive both voice and data information digitally. This network provides the ability to access a variety of services.

Integrated Services Digital Network (ISDN): A network evolved from the telephony Integrated Digital Network (IDN) that provides end-to-end digital connectivity to support a wide range of services, including voice and nonvoice services, to which users have access by a limited set of standard multipurpose customer interfaces. It is a telecommunications network driven by the communications needs (both voice and nonvoice) of the customers.

Interactive Medium: Refers to telecommunications channels that allow the two-way exchange of information.

Interactive: A way of describing time-dependent data communications, typically where a user enters data and waits for a response from the destination before continuing.

Intercarrier Sound: A method used to recover audio information in the NTSC system.

Interface: A common boundary between two systems over which the intersystem communication occurs. A physical point of demarcation between two dissimilar devices where the electrical signals, connectors, timing, and handshaking are defined.

Interleaving (Shuffling): Process of changing the bit pattern of a stream of code words, usually as part of the channel coding, in order to reduce the influence of error bursts that may occur during transmission.

Internal Commands: DOS commands that are loaded into memory when the computer is booted.

Internet Packet Exchange (IPX): a NetWare protocol that provides connectionless communications between devices on a network.

Internet Service Provider (ISP): A for-profit provider of equipment and software furnishing Internet access, usually for a monthly fee. ISP's have purchased modem banks and run servers, but lease space on digital fiber-optic data trunk lines from firms like MCI and Sprint.

Internet: A worldwide collection of computer networks that use the TCP/IP protocol and provide connectivity for Web browsing and other network communication.

Internetwork: A combination of multiple networks joined together through connecting devices (i.e. bridges, routers).

Interoperability: The ability of disparate systems to share network resources.

Intranet: An Internal network of an organization that uses Internet protocols. For example a University's Intranet, in which the students of the university can access their university computer network through Internet.

IP Addressing: IP stands for internet protocol. Basically it is a unique identifier for a computer on the internet. It is numerical address with four numbers separated with dots and the format of an IP address is a 32-bit. Each number can start from 0 and end with 255. For example IP address looks like this: 131.200.1.1

Latency: The amount of time it takes a packet to travel from source to destination. Together, latency and bandwidth define the speed and capacity of a network.

Layer: In the OSI Reference Model, it refers to a set of related data communications functions that make up one level of a hierarchy of functions.

Leased Line: A dedicated circuit, typically supplied by the telephone company that permanently connects two or more user locations. It is generally voice-grade and supports voice communications or data communications using modems.

Link: The combination of communication devices, medium and software information that is required to effect data communications.

Local Area Network (LAN): A network in a centralized location it is limited to a small geographic area.. The network lets users at that location share files, printers and other services. See WAN.

Local Loop: The physical facility, leased from a LEC, which provides connectivity between the customer's location and the carrier's point of presence.

MAC address: Unique address assigned to each active infrastructure end station (including adapters, LAN on motherboard, switch ports and router ports).

Management Information Base (MIB): A data base of objects that stores information used by SNMP-enabled management devices.

Medium-Access Control (MAC): Portion of the Data Link layer that controls access to the communication channel.

Message switching: A strategy that enables communication channels to be used simultaneously by more than one node. At each transfer point in the connection, incoming data is stored in its entirety, then forwarded to the next point. This process continues until the data reaches its destination.

Message: Grouping of data into a discrete unit containing a header, data and a trailer.

Metropolitan Area Network (MAN): A network connecting computers over a large geographical area, such as a city or school district.

Microwaves: Microwaves are radio waves that provide a high speed transmission. Microwaves station contains an antenna, transceiver and other equipments that are required for microwave communication. The data transmission speed of microwave transmission is up to 150 Mbps.

Modem (Modulator/Demodulator): Devices that convert digital and analog signals. Modems allow computer data (digital) to be transmitted over voice-grade telephone lines (analog).

Modem bank: set of modems connected to a server, furnishing each remote user a temporary connection to a campus computer, either as an IP-addressed Internet machine (using a PPP or SLIP line), or as a terminal to a multi-user host (using a POP connection).

Modem speed: the approximate number of bits-per-second (bps) that a given connection can accommodate; phone lines limit the effective speed of a modem to between 14400 and 28800 bps; if the fiber-optic cable is a huge water main of data, the phone line is a small garden hose.

Modulate: A process imposing message information on a carrier by varying the amplitude, frequency, or phase of a wave.

Modulator: A device, which converts the video signal and audio signal onto a viewable television channel

Multicasting: The ability of one network node to send identical data to a number of end servers on the multicast backbone.

Multimedia: The electronic conversation between two or more people or groups of people in different places using two or more types of digitally integrated communication for voice, sound, text, data, graphics, video, image or presence at the same time. Applications include conferencing, presentations, training, referencing, games, etc.

Multiplexer: A device that allows multiple logical signals to be transmitted simultaneously across a single physical channel.

Multiplexing: An electronic or optical process that combines two or more lower bandwidth transmissions onto one higher bandwidth signal by splitting the total available bandwidth into narrower bands (frequency division) or by allotting a common channel to several transmitting sources one at a time in sequence (time division).

Multipoint: Pertaining or referring to a communications line to which three or more stations are connected. It implies that the line physically extends from one station to another until all are connected.

Narrowband: The copper-based technology of today's services. A telecommunications medium that carries lower frequency signals.

NetWare: Novell, Inc.'s market-leading network operating system accompanied by lots of manuals which, when properly displayed, create what is fondly called "the red shelf".

Network adapter: A device that enables a computer to attach to a network.

Network Address: Network layer address referring to a logical, rather than a physical, network device. Used by the network layer. Compare with MAC address.

Network Architecture: A set of design principles, including the organization of functions and the description of data formats and procedures, used as the basis for the design and implementation of a communications network (see architecture).

Network Dependent Layers: Layers 1, 2, and 3 of the OSI Reference Model. They are also referred to as the “Connection” or “Access” Layers. These layers are concerned with the protocols associated with the data communication network being used to link two communicating computers together.

Network File System (NFS): A distributed file-system protocol suite developed by Sun Microsystems that allows remote file access across a network.

Network Interface Card (NIC): A board that provides network communication capabilities to and from a computer.

Network Layer: In the OSI Model, the entity that services the transport layer. The network layer is responsible for ensuring that data passed to it from the transport layer is routed for delivery through the network.

Network management system (NMS): System responsible for managing a network. An NMS is generally a powerful and well-equipped computer such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

Network Operating System (NOS): Software that manages the resources of a network; typically provides file sharing, e-mail, print services, security measures, etc.

Network segment: An uninterrupted length of the network communication channel. For example, a single cable between two repeaters, bridges, or routers is a segment.

Network termination equipment (NT1): Network channel termination equipment that meets a specific ISDN standard. NT1 equipment terminates the network at the customer’s premises but does not provide switching or control (see network channel terminating equipment).

Network termination equipment (NT2): Network termination equipment that meets a specific ISDN standard. NT2 equipment connects terminal equipment to the NT1 network channel termination. NT2 can provide switching and control capabilities. NT1 functions can be built into NT2 equipment.

Network Topologies: network topology is defined as: the schemes of joining a number of computers in the form of a network are called Network Topologies.

Network: A collection of hardware and software that enables a group of computers to communicate and provide users with access to shared resources.

Networking Hardware: Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data-processing and communications within the network..

Network-only application: A software program that runs only on, or is useful only on a network.

Network-to-Network Interface (NNI): ATM Forum standard that defines the interface between two ATM switches that are both located in a private network, or are both located in a public network.

Node Devices: Any peripheral devices or computer that is connected to a network
PCMCIA - An expansion slot found in many laptop computers.

Node: End point of a network connection. Nodes include any device attached to a network such as file servers, printers, or workstations.

Noise: An extraneous electrical disturbance tending to interfere with the normal reception of transmitted signals. Undesired sound or sounds. Sounds, which are non-periodic and generally have random pitch and loudness characteristics.

Open Systems Interconnection (OSI): A proto-type for network communication that promotes interconnectivity.

Optical Fiber: Any filament or fiber made of optically transparent materials that are used to transmit laser or LED-generated light signals. Optical fiber usually consists of a core, which carries the signal, and cladding, a substance with a slightly higher refractive index than the core, which surrounds the core and reflects the light signal back into it.

Packet Mode: An information transmission mode supported by the ISDN standards. In packet mode, equipment will use packet-switching techniques to transmit information in X.25 packets.

Packet Switching: A process where messages are broken into finite-sized packets that are always accepted by the network. The message packets are sent across different circuit paths. The packets are reassembled into the original message at the end of the circuit.

Packet: A chunk of data bits and associated information, including source address and destination address, formatted for transmitting from one node to another.

Parallel Transmission: Method of transmission of a digitally coded signal where at least two distinct transmission paths are used for the simultaneous transmission of the code elements representing the code words of a digital signal. A system that uses eight lines to send eight bits at a time, or one whole byte.

Parallel-To-Serial Converter: Circuit or device in which a group of code elements, all of which are presented simultaneously, is converted into a corresponding sequence of code elements.

Parity Bit: Code element appended to a code word for the purpose of error detection. The value of this parity bit is chosen such that the total number of code elements to which the number (1) is allocated yields a prescribed parity. This parity can be even or odd.

Peer-to-peer: Describes a network environment where there is no central server for all clients, rather all devices may act as server or client. LANtastic is a common peer-to-peer NOS.

Peripheral Component Interconnect bus architecture PCI: This is a 32/64 bit local bus architecture on the motherboard of a computer. It is used by network interface cards and runs faster than an ISA bus.

Phase modulation: The encoding of data into a carrier signal by altering the carrier's phasing.

Phase: The phase of the colors can be adjusted and this changes the "hue" or "tint" of the colors themselves.

Physical Layer: Within the OSI model, the lowest level of network processing concerned with electrical, mechanical, and handshaking procedures that connect a device to a transmission medium.

Physical Topology: The physical layout of the network; how the cables are arranged; and how the computers are connected.

Physical Transmission medium: In physical Transmission medium, communication devices are directly linked with each other via cables or other physical materials for data communication.

Point-to-Point Protocol (PPP): a type of dial-in modem connection that establishes a direct IP-addressed Internet connection, instead of a terminal connection to a single multi-user host. Users with PPP or SLIP connections can run Netscape or other Web browsers, unlike users with terminal connections; with a PPP or SLIP connection the processor in your desktop computer is more actively involved in manipulating the data from the network, instead of just passively receiving and displaying it.

Post-Office-Protocol (POP): the mode of connecting to a large multi-user server (like chip, dale, etc) and extracting mail or other information. Currently modem access to e-mail servers is through POP connections, but your login only fetches mail from the POP server to another machine; you do not log in directly to a POP machine.

Port: point of entry / exit for a data stream, either at the back of a computer, or (in the network sense), for wiring from a desktop's IP address to a hub in an IDF closet; each hub generally serves 12 or 24 ports. Activating another IP address in a local network may be as simple as throwing a switch (if a port is free) or as complex as buying and hooking-up a whole new hub if no ports are left.

Presentation Layer: In the OSI model, the layer of processing that provides services to the application layer, allowing it to interpret the data exchanged, as well as to structure data messages to be transmitted using a specific display and control format.

Primary Rate Interface (PRI) or Primary Rate Access (PRA): A higher speed S/T interface classification defined by the CCITT where the typical delivery medium will be a T-carrier. The standard configuration for the digital transmit and receive channels is 23 B channels and 1 D channel, where the D channel operates at 64 kbps (see B channel, D channel, S interface, T interface). An ISDN channel rate not to exceed 1.536 mbps.

Print server: An application-specific computer that manages printers and requests for print services; allows multiple users to share a network printer.

Private Branch Exchange (PBX): A telephone switch located on a customer's premises that primarily establishes voice-grade circuits over tie trunks, between individual users and the switched telephone network. PBXs typically provide switching within a customer's premises or over a limited local area and usually offer enhanced features.

Private Line: A leased line, a nonswitched circuit connecting two or more end-user locations.

Private Network: A network established and operated by a private organization or corporation for users within that organization or corporation.

Protocol: Formal set of rules governing the format, timing, sequencing, and error control of exchanged messages between similar devices or between similar functions within a device. The protocol may also include facilities for managing a communications link.

Public Packet-Switched Network (PPSN): A network established and operated by communications common carriers or telecommunications administrations for the provision of packet-switched facilities to the public.

Pulse Code Modulation (PCM): A voice digitization technique requiring 64 kbps bandwidth. PCM is the ISDN standard for voice communications. Method of source coding where the code words are obtained by sampling, quantizing and coding of the analog input signal.

Quadrature AM: A process, which allows two different signals to modulate a single carrier frequency.

Quantizing Noise: Distortion resulting from the process of quantizing, caused by the difference between the true value and the quantized approximation.

Quantizing: Process of dividing a continuous range of values into a finite number of distinct values.

Receiver: The component on the "hearing" end of a transmission.

Reflector: The antenna's main curved "dish," which collects and focuses signals onto the secondary reflector or the feed.

Remote Terminal: Any device that connects ISDN terminal equipment to a distant ISDN central Office. These devices allow customer access to ISDN even though a nearby ISDN central office does not serve the customer.

Repeater: A device for regenerating a signal that has attenuated due to distance limitations. Works on the physical layer.

RF (Radio Frequency): In television applications, RF generally refers to the television signal after the picture carrier modulation process.

Ring topology: A network cabling configuration in which each system is connected in a series, forming a closed loop.

RIP: Routing Information Protocol: Supplies routers with data to update their routing tables.

RJ-11 connector: A standard modular telephone connector.

RJ-45 connector: The connector on each end of 10Base-T or 100Base-TX twisted-pair cable. RJ-45 connectors are slightly larger than RJ-11 modular telephone connectors and connect eight wires instead of the four used in RJ-11 connectors. RJ-45 connectors snap into the RJ-45 jack on a network adapter card and the RJ-45 port on a network hub or switch.

Router: A device for connecting networks. A router selectively routes particular packet types along various network pathways. It functions on the transport layer.

Routing: The process of selecting the correct circuit path for a message.

RS-232: A communication standard created by the EIA. It governs communications on the physical level (i.e. between a PC and modem). RS stands for "Recommended Standard".

Sampling: Process of obtaining a series of discrete instantaneous values of a signal, usually at regular intervals.

Segment: Refers to a section of cable on a network. In Ethernet networks, two types of segments are defined. A populated or trunk segment is a network cable that has one or more nodes attached to it. A link segment is a cable that connects a computer to an interconnecting device, such as a repeater or concentrator, or connects a interconnecting device to another interconnecting device.

Sequenced Packet eXchange (SPX): Novell's connection-oriented reliable delivery protocol akin to TCP/IP's TCP packet. Based on XNS from Xerox and used by NetWare printing facilities as well as Remote Console and SAA services.

Serial Transmission: Method of transmission of a digitally coded signal where only one single transmission path is used for the time-sequential transmission of the code elements representing the code words of a digital signal. The transmission of one bit at a time over a single line.

Serial-To-Parallel Converter: Circuit or device in which a sequence of code elements is converted into a corresponding group of code elements, all of which are presented simultaneously.

Server: computer dedicated to interact with other networked computers to share resources (files, printing capabilities, a modem bank); depending on scale can be anything from a garden-variety PC or Mac to a very-high-power Sun Microsystems or SGI workstation serving hundreds of remote terminal connections the way chip, dale, and rocky do. Computer classrooms have their own servers providing storage for class files and programs.

Server-Based network: A network in which all client computers use a dedicated central server computer for network functions such as storage, security and other resources.

Service Access Point (SAP): The point at which processes on certain layers of the OSI Model access data from other layers.

Service Access Point Identifier (SAPI): The SAPI identifies a logical point at which data link layer services are provided by a data link layer entity to a layer 3 entity.

Session Layer: In the OSI Model, the network-processing layer responsible for binding and unbinding logical links between end-users and maintaining an orderly dialogue between them.

Session: A logical relationship or connection set up between two nodes that wish to communicate with one another.

Shielded Twisted Pair (STP): a thin-diameter network wire, wrapped with a metal sheath for extra protection against electrical interference.

Shielding: A metal foil or mesh surrounding a conductor to reduce electromagnetic interference.

Signal-To-Noise Ratio (SNR): The ratio of the signal power to the noise power, expressed in dB. Usually a Baseband signal measurement. Higher values indicate less background noise.

Simple Network Management Protocol (SNMP): A de facto standard for managing network devices, including adapters, switches, routers, servers and workstations; garners information from various agents.

Simplex: One-way data transmission, with no capability for changing direction.

Small Computer Serial Interface (SCSI): An interface controller that allows several peripherals to be connected to the same port on a computer.

Source Timing Modules: A synchronizing generator on a module that is used to adjust the timing of a specific piece of source equipment, and is kept in time by a reference sync pulse generator.

Source: Video producing equipment such as cameras, tape recorders, graphics or character generators. When copying a diskette, the origin, or diskette to be copied from.

Speed of Data Transfer: The rate at which information travels through a network, usually measured in megabits per second.

Stand-alone network application: An application that is processed locally by client computers, but stored on the network, typically providing access to network features.

Star Topology: LAN topology in which each node on a network is connected directly to a central network hub or concentrator.

Start bit: A bit that signals the start of a byte in asynchronous communications.

Stop bit: A bit signaling the end of a byte in asynchronous transmissions.

Store-and-forward The most accurate data transferring technique used by switches. When the network is busy, packets are stored until the network is able to carry

the traffic and packets are transmitted without error. The switch examines each packet of a transmission to verify accuracy, and ensure bad or misaligned packets are eliminated, and then sends good packets to their destination.

Subnet: A network segment connected by hubs. Subnets can stand alone, or connect to other subnets to form a larger network.

Switch Multigabit Data Service (SMDS): High-speed service used for MANs.

Switch Similar to but more sophisticated than a hub, a switch provides a private line across the network. When two devices communicate through a switch, it sends signals directly from one port to the other port, instead of transmitting to all ports, like on a hub. You can connect a computer or a fully populated hub to each port on a switch.

Synchronous Optical NETwork (SONET): Part of the ISDN system. Allows broadband transmission over Optical fiber cable at throughputs ranging from 51 Mbps to over 13 Gbps.

Systems Network Architecture (SNA): IBM's popular layered communications protocol that controls information transmission through data processing networks. In IBM networks, the layered logical structure, formats, protocols, and procedures that govern information transmission.

Systems Network Architecture (SNA): A network developed by IBM to interconnect IBM's family of computers.

T connector: A special connector used in bus systems that allow attachment of coax cable to a network node or a terminator.

T Interface: An interface standard defined for the CCITT and used to connect switching and controlling equipment (NT2), TE1s, or TAs to network channel termination equipment (NT1).

TAP: A coupling device that obtains CATV signals from the coaxial cable in the distribution feeder, and connects it to the drop. Modern systems use directional couplers.

Tariff: The formal process whereby services and rates are established by and for communications common carriers. Tariffs are submitted by carriers for government regulatory review, possible amendment, and final approval.

T-Carrier: A time-division multiplexed transmission facility. It usually operates at an aggregate data rate of 1.544 mbps or higher. In its simplest form, a T-carrier system puts 24 digitized voice calls or twenty-four 64 kbps data calls on two copper wire pairs.

TCP: TCP/IP packet protocol providing connection-oriented reliable delivery.

Telecommunications: The use of wire, radio, optical, or other electromagnetic channels to transmit or receive signals for audio, data, and/or video. Communications over distances using electrical means.

Teleconferencing: Electronic communications between two or more groups, or three or more individuals, who are in separate locations. Includes communications via audio, data, and/or video systems. Interactive communication between persons at one or more locations using electronic means.

Telnet: Tool used to connect directly to other computers.

Terminal equipment (TE1): ISDN designation for ISDN-compatible terminal equipment. TE1 connects to an ISDN by an S/T interface.

Terminal equipment (TE2): ISDN designation for non-ISDN-compatible terminal equipment. Most current terminal equipment, including analog telephones, digital data terminals, and large and small computers, are not ISDN compatible and are, therefore, designated TE2. TE2 connects to an ISDN by an R interface and appropriate terminal adapters.

Terminal: Point in a network at which data can either enter or leave. A device, usually equipped with a keyboard, often with a display, capable of sending and receiving data over a communications link. An ISDN station set is also considered a terminal.

Terminator: A device that provides electrical resistance at the end of a transmission line. Its function is to absorb signals on the line, thereby keeping them from bouncing back and being received again by the network.

Thick Ethernet: The original Ethernet cable specification, requiring an AUI connector; noise-resistant, but expensive and difficult to install.

Thinnet: (Thin Ethernet) A CSMA/CD network based on thin coaxial cable (also called thin Ethernet) that requires a BNC connector; based on the 10BASE-2 IEEE standard.

Throughput: The measure of how much data travels from one point to another in a given time frame. Usually represented in bits per second.

Time Division Multiplex (TDM): A technique for transmitting a number of separate data, voice and/or video signals simultaneously over one communications medium by quickly interleaving a piece of each signal one after another.

Time Division Multiplexing (TDM): Used for placing several lower speed signals onto one high-speed line by slicing a little of each signal at a time. The slices are reconstituted at the receiving end.

Time Slot: Time interval, uniquely defined, which occurs at regular, in general, periodic instants. In the case of multiplex transmission, definitive time slots are allocated to each individual signal.

Token passing: A network transmission method that requires a node to have control of a "token" before it can send messages; typically fairer than CSMA/CD on busy networks, but more complicated to implement.

Token Ring: A network protocol developed by IBM in which computers access the network through token-passing. Usually uses a star-wired ring topology.

Token: A special packet that contains data and acts as a messenger or carrier between each computer and device on a ring topology. Each computer must wait for the messenger to stop at its node before it can send data over the network.

Topology: There are two types of topology: physical and logical. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical topology is the method used to pass the information between workstations. Issues involving logical topologies are discussed on the Protocol chapter

Transceiver (Transmitter/Receiver): A Device that receives and sends signals over a medium. In networks, it is generally used to allow for the connection between two different types of cable connectors, such as AUI and RJ-45.

Transmission Channel: The medium by which a signal is sent and received between separate locations.

Transmission Control Protocol/Internet Protocol (TCP/IP): Originally two separate protocols, now they are almost always used together. The term TCP has evolved to mean the family of common Internet protocols. It is the protocol for the Internet.

Transmission Loss: The decrease in signal along a circuit due to resistance or impedance.

Transmission Service Channel: The one-way path between two designated points.

Transmitter: The component on the "speaker" end of a transmission.

Transport Layer: In the OSI Model, the network processing entity responsible (in conjunction with the underlying network, data link, and physical layers) for the end-to-end control of transmitted data and the optimized use of network resources to ensure the end-to-end integrity of the signal path.

Transportation Trunk: A high quality multi-channel transmission system that links the head-end to the distribution system(s) or to other (associated) head-ends.

Tree Topology: LAN topology similar to linear bus topology, except that tree networks can contain branches with multiple nodes.

Trunk: A multi-line connection between Telephone Company switching centers. If you get a rapid busy tone, it usually means that the trunk into someone's switch is full.

Twisted Pair: Network cabling that consists of four pairs of wires that are manufactured with the wires twisted to certain specifications. Available in shielded and unshielded versions.

U Interface: An ISDN interface standard for connecting NT1 network channel termination equipment to the network. The U interface is necessary in the United States because the NT1 network channel termination equipment is considered customer premise equipment. The U interface ensures that signals entering the network meet ISDN standards. The U interface provides for portability of NT1s between different vendors' switches.

Unavailable Signal State: Occurs when 10 consecutive severely ESs occur. Ends when 10 consecutive seconds of data are processed and no severely ESs occur. For every second an unavailable signal state exists, a UAS results.

Unguided medium: Product that transmits data through the air, such as radio or microwave.

Uniform Resource Locator (URL): the standard way to write the address of a specific site or piece of information on the Web; for example, <http://www.pcxcomputers.com/>.

Universal Serial Bus (USB): A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

Uplink: An earth station that transmits a signal to a communications satellite.

Upstream: Direction of transmission from the subscriber(s) to the central distribution point.

Usenet News: A large collection of topic-specific discussion groups. Users read and post articles that are often answered in a matter of hours.

Video: The visually displayed images of video teleconferencing/video telephony,

Virtual LANs (VLANs): a switching technology that enables logical segmentation of switched networks, independent of physical grouping or collision domains.

Virtual terminal: A terminal emulation program that makes a workstation appear to be a dumb terminal connected to some remote system, such as a mainframe.

Virtual: Being such in essence or effect though not formally recognized or admitted (Webster). Something that may be essentially present, but not in actual fact.

Virus: Destructive code that is embedded in a computer program. The virus is usually self-replicating and will often copy itself onto other programs.

Voice over Internet Protocol (VOIP): in common terms voice connection using internet protocol through internet. In technical words VOIP is a technology used to transmit voice using broadband internet connection instead of old analog phone lines.

Voice-Grade Channel: A telecommunications circuit used primarily for speech transmission but suitable for the transmission of analog or digital data or facsimile, typically supporting a frequency range of 300 to 3,400 Hz. also voice band.

Voice-Switching: An electrical technique for opening and closing a circuit in response to the presence or absence of sound.

Wavelength Division Multiplexing (WDM): A way of increasing the information-carrying capacity of an optical fiber by simultaneously operating at more than one wavelength. With WDM you can multiplex signals by transmitting them at different wavelengths through the same fiber.

Wavelength: The distance between two crests of a signal or a carrier and is measured in terms of meters, millimeters, nanometers, etc. In lightwave applications, because of the extremely high frequencies, wavelength is measured in nanometers.

Web server: a computer running Web server software and permanently connected to the Internet, dedicated to maintaining web pages on its hard drive; accessible from outside via Internet protocols, hence must have its own DNS address, and thus physically have its own NAM-->port-->hub-->router connection.

Wide Area Information Server (WAIS): WAIS servers search for information spread around the Internet. Users tell the WAIS servers which dataBases they wish to search, and then specify one or more keywords for the search. WAIS returns a list of articles matching the search criteria.

Wide Area Network (WAN): A network connecting computers within very large areas, such as states, countries, and the world.

Wideband: A communications channel offering a transmission bandwidth greater than a voice-grade channel. Data transmission speeds on wideband facilities are typically in excess of 9.6 kbps and often at rates such as 56 kbps and 1.544 mbps.

Wireless Adaptor/Wireless Card: A Wireless Adaptor is a device used to provide wireless capability to a device such as a PC. Many newer laptop computers have the capability built in and so do not require a separate card. Note also that wireless capability can also be provided by a USB connected device rather than an internal card.

Wireless local-area networks (WLAN): use radio waves instead of a cable to connect a user device, such as a laptop or other computer, to a LAN. They provide Ethernet connections over a wireless connection and operate under the IEEE 802.11 group of specifications.

Wireless Network Equipment: Access point: A Wireless Network transceiver or "Base station" that can connect a wired network to a number of wireless devices. APs can also bridge to one another.

Wireless Networking: In Wireless transmission medium, communication devices communicate with each other and data is communicated through the air or space using broadcast radio signals, microware signals and infrared signals.

Wireless Router: A Wireless Router combines an Access Point with a router (frequently capable of direct connection to a broadband network). A Wireless broadband router is a cost-effective means of connecting wireless enabled computers to the Internet.

Workgroup server: powerful computer dedicated to performing network tasks like printing, file storage, Web page storage, etc; each computer classroom has its own workgroup server, parts of which are accessible from the individual student computer stations.

Workgroup: A collection of workstations and servers on a LAN that are designated to communicate and exchange data with one another.

Workstation: A computer connected to a network at which users interact with software stored on the network.

World Wide Web (WWW): Internet tool that is capable of displaying both text and graphics in full color on the same page. Before the web, users navigated the Internet using command-line interfaces and exchanged only textual information. The WWW provides graphics, sound, video, an easy-to-use interface, and the ability to follow hypertext links to other places on the Internet.

X.25: A CCITT recommendation that specifies the interface between user data terminal equipment (DTE) and packet-switching data communications equipment (DCE), which provides a user access to an X.25 standard packet-switched network.

X.400: A CCITT standard that describes electronic-mail protocols.

xDSL: A term referring to a variety of new Digital Subscriber Line technologies. Some of these varieties are asymmetric with different data rates in the downstream and upstream directions. Others are symmetric. Downstream speeds range from 384 kbps (or "SDSL") to 1.5-8 Mbps (or "ADSL").

REFERENCES

1. Ahamed, S., and Lawrence, Victor B. Intelligent Communication Systems, AT&T Bell Laboratories, NJ, to be published by Kluwer Academic Publishers, Boston, 1996.
2. Artech House, 2003
3. Aziz, A., and Diffie, W. Privacy and Authentication for Wireless Local Area Networks, IEEE Personal Communications, First Quarter 1994.
4. Barbutta F. Network Security: Examining your Arsenal, Business Communications Review, Volume 25, number I, November 1996
5. Bertsekas, D. and Gallager, R., Data Networks, Second Edition, Prentice-Hall, 1992.
6. Blank, Andrew G., TCP/IP Foundations, John Wiley and Sons, 2004
7. Chen, Jyh-Cheng, and Zhang, Tao, IP-Based Next-Generation Wireless Networks: Systems, Architectures, and Protocols, Wiley-IEEE, 2004
8. Clark M. Networks and Telecommunications: Design and Operations, John Wiley & Sons, 1993.
9. Comer, D.E., Computer Networks and Internets with Internet Applications, Third Edition, Prentice-Hall, 2001.
10. Comer, Douglas E., Computer Networks and Internets , Prentice Hall; 5th edition, 2008
11. Comer, Douglas E., Hands-on Networking with Internet Technologies, Prentice Hall; 2nd edition 2004
12. Comer, Douglas E., Internetworking with TCP/IP, Vol 1 , Prentice Hall; 5th edition , 2005
13. Comer, Douglas E., The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works, Prentice Hall; 4th edition 2006
14. Comer, Douglas, Internetworking with TCP/IP: Principles, Protocols and Architecture, Edition: 5, Prentice Hall, 2006
15. Comerford, R. "Interactive Media: An Internet reality", IEEE Spectrum, pp. 29-32, April 1996.
16. Dixit, Sudhir and Prasad, Ramjee, Technologies for Home Networking, Wiley-Interscience, 2007
17. Duck, Michael and Read, Richard, Data Communications and Computer Networks: For Computer Scientists and Engineers, Edition: 2, Pearson/Prentice Hall, 2003
18. Erik, J. H. ,and others, Mobile Virtual Work: A New Paradigm, Springer, 2006
19. Fantauzzi, G. Digital Switching Control Architectures", Artech House, Norwood, MA, 1990.
20. Greenfield. A. and Gupta, A. "Taking Aim at Wide Area ATM," Business Communications Review, Vol. 25, No 12, December 1995.
21. Gruber J., and Williams G. Transmission Performance of Evolving Telecommunications Networks, Artech House, Inc., Norwood, MA, 1992.
22. Guizani, Mohsen, Wireless Communications Systems and Networks, Springer, 2004
23. Hac, A. and Mutlu, B, "Synchronous Optical Network and Broadband ISDN Protocols", IEEE Computer, Nov. 1993, pp26-34
24. Halsall F. "Data Communications: Computer Networks and OSI", 2nd., d., Addison-Wesley, Reading, M.A., 1990.

25. Halsall, F., Computer Networking and the Internet, Fifth Edition, Addison-Wesley, 2005.
26. Halsall, F., Data Communications, Computer Networks, and Open Systems, Addison Wesley; 4 1996
27. Handel, R., and others, ATM Networks - Concepts, Protocols, Applications, Second Edition, Addison-Wesley, 1994.
28. Hossain, Ekram, and Leung, Kin, Wireless Mesh Networks: Architectures and Protocols, Springer, 2008
29. Huang, Xu and others, Advances in Communication Systems and Electrical Engineering, Springer, 2008
30. Huitema, C., Routing in the Internet, Second Edition, Prentice-Hall, 2000.
31. Ifeatchor, E. Digital Signal Processing, A Practical Approach, Addison-Wesley Publisher Ltd., pp. 77, 1994.
32. Information Discovery and Dissemination, 124 illus., 2009
33. Jia, Weijia and Zhou, Wanlei, Distributed Network Systems: From Concepts to Implementations, Springer, 2005
34. Jiraud D., "Broadband CDMA for Wireless Communications", Applied Microwave & Wireless, 1995.
35. Kasera, Sumit, ATM Networks: Concepts and Protocols, McGraw-Hill Professional, 2007
36. Kasim, Abdul and others, Delivering Carrier Ethernet: Extending Ethernet Beyond the LAN, McGraw-Hill Professional, 2007
37. Katz, R. "Adaptation and Mobility in Wireless Information Systems," IEEE Personal Communications, First Quarter 1994, pp. 6-17.
38. Kenyon, Tony, High-performance Data Network Design: Design Techniques and Tools, Digital Press, 2002
39. Kikkert,C. Digital Communication Systems and their Modulation Techniques, James Cook University, October 1995.
40. Kozierok, Charles, The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference, No Starch Press 2005
41. Kumar, B. Broadband Communications, New York: McGraw-Hill, 1994
42. Kurose, J.F. and Ross, K.W., Computer Networking, A Top-Down Approach Featuring the Internet, Third Edition, Addison-Wesley, 2005.
43. Kurose, James F. , and Ross, Keith W., Computer Networking: A Top-Down Approach, Addison Wesley; 4 edition, 2007
44. Kyas, O. ATM networks, International Thomson Publishing, New York, NY, 1995.
45. Left, B, Making sense of wireless standard and system designs, Microwaves & RF, pp. 113-118, February 1994.
46. Leon-Garcia, A. and Widjaja, I., Communication Networks, Fundamental Concepts and Key Architectures, Second Edition, McGraw-Hill, 2003.
47. Luckenbach, Reiner, and others, Heterogeneous Wireless Access Networks: Architectures and Protocols, Edition: 4, Springer, 2008
48. Maier, Martin, Optical Switching Networks, Cambridge University Press, 2008
49. Martin, James, and others, Local Area Networks: Architectures and Implementations, Edition: 2, PTR Prentice Hall, 1993

- 50.Minoli, D and Dobrowski, Pub. Principles of Signalling for Cell Relay and Frame Relay. Artech House 1994
- 51.Misic, Jelena, and Misic, Vojislav, Wireless Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15.4, John Wiley and Sons, 2008
- 52.Muller N., and Davidson R.P. LAN to WAN, Artech House, Norwood, MA, 1990.
- 53.Nolle T. "Evolving toward a modular public network", Business Communications Review, Vol. 24, May 1994.
- 54.Norman H. LAN/WAN Optimization Techniques, Artech House, Norwood, MA, 1992.
- 55.Papadopouli, Maria, and Schulzrinne, Henning, Peer-to-Peer Computing for Mobile Networks
- 56.Partridge, C., Gigabit Networking, Addison-Wesley, 1994.
- 57.Pecar J., O'Connor R. J., and Garbin D.A. Telecommunications Factbook, McGraw-Hill, Inc., 1992.
- 58.Perkins, C. and Bhagwat, P. "A Mobile Networking System based on Internet Protocol," IEEE Personal Communications, First Quarter 1994.
- 59.Perlman, R., Interconnections - Bridges and Routers, Addison-Wesley, 1992.
- 60.Perlman, Radia, Interconnections: Bridges, Routers, Switches, and Internetworking Protocols ,Addison-Wesley Professional; 2nd edition 1999
- 61.Peterson Larry L., and Davie, Bruce S., Computer Networks: A Systems Approach, Edition: 4, Morgan Kaufmann, 2007
- 62.Peterson, L. and Davie, B., Computer Networks, A Systems Approach, Third Edition, Morgan Kaufman, 2003.
- 63.Peterson, Larry L. and Davie , Bruce S. Computer Networks: A Systems Approach, Morgan Kaufmann; 4 edition, 2007
- 64.Plunkett, Jack W., Plunkett's Wireless, Wi-Fi, Plunkett Research, Ltd., 2006
- 65.Prasad, Luis Muñoz, WLANs and WPANs Towards 4G Wireless, Edition: 2, Programmers Press, 1994.
- 66.Prycker, M. Asynchronous Transfer Mode, Ellis Horwood, London, 1991
- 67.Quartermann J. The Matrix - Computer Networks and Conferencing Systems Worldwide, Digital Press, USA, 1990.
- 68.Rappaport, T. Wireless Communications, Principle & Practice", IEEE Press, Prentice Hall, pp. 3, 1996.
- 69.Rudd S. and Johnson M. "Here Comes the Virtual Public Network", Business Communications Review, Volume 25, number II, November 1995, pp. 51-54.
- 70.Rutkowski A. Integrated Services Digital Networks, Artech House, Norwood, MA, 1985.
- 71.Smounts M. Packet Switching Evolution from Narrow band to Broad ISDN, Artech House, Norwood, MA, 1991.
- 72.Stallings, W., Local and Metropolitan Area Networks, Sixth Edition, , Prentice-Hall, 1999.
- 73.Stallings, W.S., Data and Computer Communications, Eighth Edition, Pearson Prentice-Hall, 2007.
- 74.Stallings, William, Data and Computer Communications, 7th edition, Prentice Hall, 2004
- 75.Stallings, William, Business Data Communications, Edition: 6, Prentice Hall, 2008

76. Stallings, William, Data and Computer Communications, Edition: 8, Prentice Hall, 2007
77. Stallings, William, High-speed Networks and Internets: Performance and Quality of Service, Edition: 2, Prentice Hall, 2002
78. Steenstrup, M., Routing in Communications Networks, Prentice-Hall, 1995.
79. Swales, S. and Beach, M. "Third Generation Wireless Networks", University of Bristol, Future Communication Systems course, April 1994.
80. Sypser R. Communications for Cooperating Systems, Addison-Wesley, Reading, M.A., 1991.
81. Tan, Teik-Kheong and others, The World Wide Wi-Fi: Technological Trends and Business Strategies, John Wiley and Sons, 2003
82. Tanenbaum, A., Computer Networks, Fourth Edition, Prentice-Hall, 2003.
83. Tanenbaum, A.S., Computer Networks 4th Edition, Prentice Hall, Upper Saddle River, NJ, 2003
84. Tse, David and Viswanath, Pramod, Fundamentals of Wireless Communication, Cambridge University Press, 2005
85. Yahya (Tamimi), Abdelfatah A. and Aboeid, Imad M., Computer Networks and Internet, Dar Alyazori, Amman, Jordan, 1999
86. Yahya (Tamimi), Abdelfatah A. Traffic congestion, connectivity and optimality in national networks, City University of NY,NY,, 1996
87. Zhang, Yan, and Chen, Hsiao-Hwa, Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks, CRC Press, 2007
88. <http://www.networktutorials.info/>; feb,2008
89. <http://www.webproforum.com/>; June,2008
90. (<http://www.wia.org>); Dec,2007
91. http://80211b.weblogger.com/turnkey_hotspots.html; May,2008
92. <http://computer.org/internet/v2n1/perkins.htm>; Aug,2008
93. <http://easy.intranet.gr/>; May,2008
94. <http://fcit.usf.edu/network/>; March,2008
95. <http://gaia.cs.umass.edu/kurose/Contents.htm>; April,2008
96. <http://grouper.ieee.org/groups/802/3/efm/public/index.html>; Aug,2008
97. <http://learnlinux.tsf.org.za/courses/build/net-admin/index.html>; March,2008
98. <http://learn-networking.com/network-design>; March,2008
99. http://members.tripod.com/ATM_protocols/PtoP/Q_2931.html; Aug,2008
100. <http://mobility.tamu.edu/>; May,2008
101. <http://playground.sun.com/pub/png/html/specs/standards.html>; Aug,2008
102. <http://search.techrepublic.com.com/search/network+topology.html>; March,2008
103. <http://standards.ieee.org/getieee802/802.11.html>; Aug,2008
104. <http://standards.ieee.org/regauth/oui/tutorials/EUI64.html>; Aug,2008
105. <http://technet.microsoft.com/en-us/library/bb742616.aspx>; feb,2008
106. <http://wareseeker.com/free-subnet-addresses/>; feb,2008
107. <http://williamstallings.com/CNIP/CNIP1e.html>; feb,2008
108. <http://world.std.com/~jimf/papers/sockets/sockets.html>; Dec,2007
109. <http://www.10gea.org>; Aug,2008

-
110. <http://www.3com.com/technology/>; Dec, 2007
 111. <http://www.3gpp.org/>; Aug, 2008
 112. <http://www.80211-planet.com/tutorials/article.php/1495031>; May, 2008
 113. <http://www.atmforum.com/>; April, 2008
 114. <http://www.atmforum.com/>; June, 2008
 115. <http://www.att.com/>; April, 2008
 116. <http://www.bluetooth.com/>; May, 2008
 117. <http://www.boingo.com/>; Aug, 2008
 118. <http://www.cablemodem.com/>; Aug, 2008
 119. <http://www.caida.org/>; Dec, 2007
 120. <http://www.cisco.com/>; April, 2008
 121. <http://www.ciscopress.com/>; April, 2008
 122. <http://www.comptechdoc.org/independent/networking/>; March, 2008
 123. <http://www.computer.org/internet/v2n1/mobile.htm>; Aug, 2008
 124. <http://www.cs.columbia.edu/~hgs/rtp/>; June, 2008
 125. http://www.cybergeography.org/atlas/isp_maps.html; Dec, 2007
 126. <http://www.data.com/>; Dec, 2007
 127. <http://www.dns.net/dnsrd/docs/>; Dec, 2007
 128. <http://www.eurecom.fr/~ross/CacheTutorial/>; Dec, 2007
 129. <http://www.frforum.com/>; June, 2008
 130. <http://www.gigabit-ethernet.org/>; June, 2008
 131. <http://www.gsmworld.com/>; Aug, 2008
 132. <http://www.hill.com/>; June, 2008
 133. <http://www.iana.org/>; June, 2008
 134. <http://www.icann.org/>; Aug, 2008
 135. <http://www.iec.org/>; March, 2008
 136. <http://www.iol.unh.edu/training/ge.html>; June, 2008
 137. <http://www.ipass.com/>; Aug, 2008
 138. <http://www.ipv6.org/v6-www.html>; Aug, 2008
 139. <http://www.ipv6forum.com/>; Aug, 2008
 140. <http://www.isc.org/>; Dec, 2007
 141. <http://www.iso.org/>; Aug, 2008
 142. <http://www.isoc.org/internet/history/>; April, 2008
 143. <http://www.ist-tequila.org/>; Aug, 2008
 144. <http://www.itu.ch/>; Dec, 2007
 145. <http://www.itu.ch/>; June, 2008
 146. <http://www.javvin.com/protocol/>; Aug, 2008
 147. <http://www.kfu.com/~nsayer/6to4/>; Aug, 2008
 148. <http://www.netapp.com/>; Dec, 2007
 149. <http://www.NetworkRouting.net/>; Aug, 2008
 150. <http://www.nw.com/zone/WWW/top.html>; April, 2008
 151. <http://www.nwfusion.com/>; Aug, 2008

152. <http://www.pbs.org/nerds/>; June, 2008
153. <http://www.prenhall.com/tanenbaum/>; May, 2008
154. http://www.psc.edu/networking/tcp_friendly.html; May, 2008
155. <http://www.real.com/devzone/library/fireprot/rtsp/>; June, 2008
156. <http://www.softpedia.com/get/Network-Tools/>; feb, 2008
157. <http://www.stabdards.ieee.org/>; Aug, 2008
158. <http://www.TCPIPGuide.com>; feb, 2008
159. <http://www.tcpipguide.com/index.htm>; feb, 2008
160. <http://www.techsoup.org/learningcenter/networks/>; March, 2008
161. <http://www.thinworld.com/>; April, 2008
162. <http://www.w3.org/>; Aug, 2008
163. <http://www.wapforum.org>; Aug, 2008
164. <http://www.webstart.com/jed/papers/Components/>; March, 2008
165. <http://www.weca.net/>; Aug, 2008
166. <http://www.wi-fi.org/>; Aug, 2008
167. <http://www.wirelessbroadbandalliance.com>; Aug, 2008
168. <http://www.wireless-data.com>; May, 2008
169. <http://www.wirelessip.net>; May, 2008
170. <http://www.wireless-world-initiative.org>; Aug, 2008
171. <http://www.wireless-world-research.org>; Aug, 2008
172. <http://www2.rad.com/networks/1994/hd1c/hd1c.htm>; Aug, 2008
173. <http://www-aml.cs.umass.edu>; Dec, 2007
174. www.80211hotspots.com; May, 2008
175. www.apnic.net; Aug, 2008
176. www.arin.net; Aug, 2008
177. www.internetworldstats.com; May, 2008
178. www.internic.net; June, 2008
179. www.isoc.org/internet/history/brief.shtml; May, 2008
180. www.itu.int/publications; June, 2008
181. www.metroethernetforum.org; May, 2008
182. www.ripe.net; Aug, 2008
183. www.unicode.org; June, 2008
184. www.wirelessdevnet.com/news/2003/169/news7; Aug, 2008

INDEX

1

10 Gigabit Ethernet
10GBase-CX4, 199
10GBase-ER, 199
10GBase-LR, 199
10GBase-LRM, 199
10GBase-LW, 10GBase-EW, 10GBase-SW,
 199
10GBase-LX4, 199
10GBase-SR, 198
10GBase-T, 199
applications, 201
frame format, 201
types, 198
100VG-AnyLAN, 205

A

Access
 enterprise, 67
 global, 4
 institutional, 67
 mobile, 67
 residential, 65
Access protocol
 ALOHA, slotted ALOHA, 163
 Carrier Sense Multiple Access (CSMA), 163
 Carrier Sense Multiple Access with Collision
 Avoidance, 221
 Carrier Sense Multiple Access with collision
 avoidance (CSMA/CA), 164
 Carrier Sense Multiple Access with collision
 detection (CSMA/CD), 164
 Carrier Sense Multiple Access/Collision
 Detection (CSMA/CD), 193
 channel partitioning, 162
 code division multiple access, 163
 frequency division multiple access, 162
 polling, 165
 random access, 163
 round robin, 165
 taking turns, 165
 time division multiple access, 162
 token passing, 165
Acknowledgment, 170, 433
Adapter
 node, 161
Address
 anycast, 355
 automatic IP address allocation, 372
 broadcast, 355
 destination, 161, 186

destination IP, 395
destination, source, 209, 214
foreign, 415
forwarding, 391
forwarding IP, 395
gateway, 395
global unicast, 377
home, 415
illegal, 371
IP, 161
link local unicast, 377
logical, 161, 343
MAC, 161, 374
Managing the Address Space, 379
multicast, 355, 378
Network Address Translation (NAT), 371
Network Service Access Point (NSAP), 379
next hop, 389
physical, 343
pool of IP addresses, 371
Prioritization of automatic IP addresses, 374
private, 369
private address space, 369
public, 369
site local unicast, 378
source, 186
table, 245
unicast, 355
Addressing
 IP v6 Address
 address space, 377
 general format, 375
 global routing prefix, 375
 interface ID, 375
 subnet ID, 375
 types of address inscription, 374
 IPv4 addressing, 356
IPv4 Addressing
 class A, 356
 class C, 357
 class D, 358
 Class E, 358
 classful, 356
 classless, 356
 dotted-decimal notation, 358
 IP address format, 357
Agent
 foreign, 412
 home, 412
 managed, 472
Algorithm
 centralized, 398
 cyclic redundancy check (CRC), 175
 distance vector, 398
 distributed, 398

distributed spanning tree, 242
 error checking, 175
 flow control, 433
 Internet congestion control, 436
 link-state, 401
 sliding window, 168, 433
 slow start congestion control, 435
 spanning tree. *See* distributed spanning tree
 stop-and-wait, 167
 American Registry for Internet Numbers (ARIN), 379
 Amplifier, 236
 ANSI, 22, 291
 AppleTalk, 31
 Application layer
 protocol, 453
 services, 453
 ASCII, 32
 Asia Pacific Network Information Center (APNIC), 379
 ATM, 224, 301
 cell format, 302
 cell header, 302
 cell routing, 304
 cell structure, 303
 general description, 301
 Generic Flow Control (GFC), 302
 higher layers, 38
 management plane, 38
 protocol reference model, 39
 switch, 303
 terminal, 302
 user plane, 38
 Attenuation, 87
 Autonomous system (AS), 408
 Autonomous system border routers (ASBRs), 408

B

BGP
 data unit, 410
 data unit format, 411
 Bluetooth, 146
 chain, 146
 piconet, 146
 scatternet, 146
 Bridge, 239
 adaptive or learning, 241
 characteristics, 241
 encapsulating, 240
 general description, 239
 remote, 240
 source-rout translation, 240
 source-rout transperant, 240
 transperant, source-rout, 239
 types, 239

Broadband Wireless Access system (BWA), 306
 Broadband Wireless Access (BWA), 306
 Broadcasting radio, 143
 Brouter, 254

C

Cable
 coaxial, 129
 electrical, 123
 Hybrid fiber coaxial, 66
 optical fiber, 5, 131, 194
 RG 58, 189
 RG-8, RG-11, 187
 STP, 124
 twisted pair, 124
 twisted pair application, 128
 twisted pair category, 127
 twisted-pair, 5
 UTP, 124, 189, 239
 Carrier sensing, 164
 Carrier System, 283
 analog, 283
 digital, 284
 E-1, 285
 E-3, 288
 primary rate, 284
 standards, 285
 T1, 284
 T-3, 288
 Category
 Cat3, 189, 193
 Cat5, 190
 CATV, 139, 192
 CCITT, 22, 291
 Cellular
 frequency reuse, 149
 Channel
 bandwidth, 122
 Bandwidth, 90, 97
 bank, 286
 capacity, 90
 data transmission, 93
 Efficiency of a digital transmission, 92
 Service Unit/Data Service Unit (CSU/DSU), 121
 voice, 284
 Channel Service Unit/Data Service Unit (CSU/DSU), 61, 121
 Clear to send (CTS), 219
 Client/Server
 model, 8
 network, 7
 network operating system (NOS), 11
 Coaxial cable

- application, 130
- Baseband, 129
- broadband, 129
- physical description, 129
- RG-8, RG-58, RG-59, RG-62, 129
- transmission characteristics, 131
- Coding
 - line, 94
- Collision, 162
 - domain, 241
- Collision detection, 164
- Common Object Request Broker Architecture, 14
- Communicating Processes, 441
- Communication
 - data, 77
 - Effective Worldwide Communications, 4
 - interprocess, 452
 - logical, 426
 - protocols, 24
 - socket, 442
- Computer
 - client, 6
 - peer computer, 6
 - server, 6
- Concentrator, 237
- Connector
 - BNC, BNC-T, 189
 - BNC, BNC-T, BNC terminator, 129
 - optical, FC, SC, LC, MT-RJ, 134
 - RJ 45, 190
 - RJ-45, RJ-48, RJ-11, 127
 - vampiretap, 130
- Converter
 - Analog to Digital, 106
 - analog-to-digital, 81
 - Digital to Analog, 106
 - optical fiber, 266
- D**
- Data
 - analog, 107
 - analog transmission channel, 93
 - Asynchronous mode transmission, 85
 - Baseband mode transmission, 86
 - broadband mode transmission, 86
 - channel, 90
 - communication equipment (DCE), 50, 120, 121
 - digital, 280
 - digital transmission channel, 93
 - flow, 83
 - full-duplex transmission, 83
 - half-duplex transmission, 83
 - parallel mode transmission, 84
 - serial mode transmission, 84
- simplex transmission, 83
- synchronous mode transmission, 85
- terminal equipment (DTE), 50, 120
- transmission, 77, 83
- transmission channel, 93
- Data communication equipment (DCE), 50
- Data terminal equipment (DTE), 50
- Data unit*, 40
- Data Unit
 - cell, 40
 - datagram*, 39
 - frame, 39
 - message, 40
 - packet, 39
 - Segment*, 39
- Destination
 - access point, 160
- Digital, 312
- Digital Hierarchy
 - ITU-T, 287
 - North American, 286
- Digital Subscriber Line
 - Access Multiplexer (DSLAM), 299
 - Asymmetric, 66
 - equipment, 298
 - general description, 297
 - transceiver, 299
- Digital Subscriber Line (DSL), 297
- Digital Terminal Equipment, 101
- Direct-sequence spread spectrum (DSSS), 218
- Dispersion, 87
- Distortion
 - amplitude, 87
 - delay, 88
 - phase, 88
- DNS
 - directory look-up service, 466
 - Iterative mapping, 467
 - message, 464
 - message format, 465
 - Recursive mapping, 466
- Domain
 - country code top-level domains (ccTLDs), 463
 - frequency, 80
 - hierarchy, 463
 - root, 462
 - time, 80
 - top-level, 463
- Domain Name System (DNS), 462
- Drive Designators, 12
- DSL
 - Asymmetric DSL (ADSL), 300
 - High-bit-rate DSL (HDSL), 300
 - ISDN DSL (ISDL), 300
 - Multirate Symmetric DSL (MSDSL), 300
 - Rate Adaptive DSL (RADSL), 300
 - Symmetric DSL (SDSL), 300

- variation, 300
 - Very high bit-rate DSL (VDSL), 300
 - Voice-over DSL (VoDSL), 300
 - Duplexing
 - frequency division, 307
 - time division, 307
 - Dynamic Data Exchange, 14
- E**
- EBCDIC, 32
 - Electronic collaboration, 3
 - Electronic Data Interchange (EDI), 68
 - Encoding, 105
 - 4B/5B, 99, 212
 - 5B/6B, 99
 - 8B/10B, 99
 - 8B/10B, 197
 - 8B/10B, 198
 - 8B/6T, 100
 - AMI, 97
 - differential, 97
 - differential Manchester, 98
 - digital, 106
 - intermediate, 99
 - End Systems, 5
 - Error
 - check mechanism, 172
 - checksum, 173
 - correction, 178
 - detection, 170
 - Ethernet
 - 10 Gigabit Ethernet, 198
 - 1000Base SX, 1000BaseLX, 1000BaseCX, 1000BaseT. *See* Gigabit Ethernet
 - 10Base2, 189
 - 10Base5, 187
 - 10BaseF, 190
 - 10BaseFB, 10BaseFL, 10BaseFP. *See* 10BaseF
 - 10BaseT, 189
 - 10Broad36, 191
 - auto-negotiation, 202
 - Fast Ethernet, 193
 - frame, 245
 - frame format, 186
 - Gigabit, 195
 - Thick Ethernet. *See* 10Base5
 - ThickNet. *See* 10Base5
 - ThinEthernet. *See* 10Base2, ThinNet, cheaperNet
 - traditional, 192
 - Ethernet auto-negotiation, 203
 - Extension Header
 - authentication, 332
 - destination, 332
- encapsulating security payload, 332
 - fragment, 332
 - general structure, 331
 - hop-by-hop, 332
 - routing, 332
- F**
- Fast Ethernet
 - 100BaseFX, 194
 - 100BaseT, 193
 - 100BaseT2, 194
 - 100BaseT4, 193
 - 100BaseTX, 194
 - FDDI
 - dual attachment concentrator (DAC), 212
 - dual attachment station, 212
 - frame format, 214
 - operation, 212
 - port, 212
 - ring, 212
 - single attachment station, 212
 - specifications, 212
 - Fiber Distributed Data Interface (FDDI), 211
 - Flow Control
 - data link, 166
 - Fragmentation, 333
 - fragmentation and reassembly, 333
 - maximum transmission unit (MTU), 333
 - more fragment offset, 333
 - more fragments flag, 333
 - Frame
 - broadcast, 241
 - check sequence, 159
 - check sequence, 176
 - check sequence, 186
 - check sequence, 214
 - chek sequence, 209
 - control, 214, 220
 - data, 186
 - filtrng, 241
 - format, 160
 - statuse, 214
 - stause, 209
 - structure, 159
 - type, 186
 - Frame relay, 61
 - Framing, 159
 - SONET, 289
 - Frequency-hopping spread spectrum (FHSS), 218
 - FTP
 - active mode, 468
 - active session, 468
 - connections lifecycle, 468
 - control connection, 467
 - data connection, 467

Fully Qualified Domain Name (FQDN), 462

G

Gateway, 255

H

Header, 26

 tag, 257

 TCP, IP, LLC, MAC, 159

Host

 fixed, 440

 mobile, 412, 440

 roaming, 412

HTTP

 host header, 456

 message, 454

 message format, 455

 persistent connection, 456

 pipelining, 456

 protocol coding, 458

 request status-line, 457

 response status-line, 457

 types, 455

Hub, 236, 237

 connection, 237

 distributed, hybrid, 237

 layer, 204

 passive, active, intelligent, 237

 priority, 204

 stackable, 238

 types, 237

Hypertext Transport Protocol, 8

I

IEEE, 23, 33

IEEE Standard

 802, 33

 802 Specification Categories, 34

 802.11, 215

 802.11a, 218

 802.11b, 219

 802.11g, 216, 219

 802.16, 307

 802.16a, 307

 802.16e, 310

 802.20, 310

 802.3, 98, 187

 802.3ab, 197

 802.3ak, 199

 802.3U, 193

 802.3z, 196

 802.5, 98, 208

IETF, 23

Infrared, 144

 diffused, 145, 217

 directed beam, 144

 omnidirectional, 144

Interface, 294, 391

 application programming interface (API), 442

 basic rate, 293

 outgoing, 389

 Physical, 120

 Physical, 121

 primary rate, 293

Internet

 accessing Method, 65

 checksum, 173

 Internet Assigned Numbers Authority (IANA), 369

 Internet Assigned Numbers Authority (IANA), 379

 Internet Corporation for the Assignment of Names and Numbers (ICANN), 380

 Internet Network Information Center (InterNIC), 353, 379

 Internet Registry (IR), 379

 Internet service provider (ISP), 371

 Internet service provider (ISP), 353

 local IRs, 379

 mail message format, 471

 regional IRs, 379

 Services Provider (ISP), 65

 Internet mail transfer system (MTS), 470

 Internet Protocol (IP), 326

 datagram, 327

 Internet Protocol v4 (IPv4)

 checksum, 329

 data unit, 328

 header, 328

 packet, 328

 Internet Protocol v6 (Ipv6)

 data unit, 330

 extension header types, 331

 header, 330

 hop limit, 331

 next header, 331

 Internetwork, 347, 481

 Internetworking

 Extranet, 68

 Internet, 63

 Intranet, 68

IP

 datagram, 443

 IP v6 Address, 374

 address space, 377

 format, 377

 general format, 375

 global routing prefix, 375

 interface ID, 375

 subnet ID, 375

types of address inscription, 374

IPv4 Addressing

 class B, 357

 space, 358

IPv4 IP classes, 356

ISDN

 application, 297

 equipment configuration, 295

 network termination, 296

 services, 293

 terminal, 295

 terminal adapter, 296

ISO, 23

ITU, 22

K

Keying

 Amplitude-Shift(ASK), 102

 Frequency-Shift (FSK), 102

 Multi-level-Shift, 103

 Phase-Shift (PSK), 103

L

LAN

 architecture, 185

 Ethernet, 185

 extended, 233

 private, 371

 segment, 190

 switch, 243

 technology, 185, 233

 virtual LAN, 233

 wireless, 215

Layer, 23

 application, 32

 Application, 36

 ATM, 38

 ATM Adaptation, 38

 dat link, 157

 data link, 30

 data link, 239

 Internet, 35

 logical-link control, 158

 medium access control (MAC), 158

 network, 31

 Network Access, 35

 Network Interface, 35

 OSI Layers, 29

 physical, 29, 37

 presentation, 32

 session, 31

 transport, 31

 Transport, 36

layer management. *See* management plane

Layered

 model, 24

Lifetime, 391

Line Coding

 bi-phase, 95

 NRZ, 94

 RZ, 95

Link layer

 frame, 159

M

Management

 Data base Management System, 15

 Network Management Services, 14

 Secure, 4

Management information Base (MIB), 473

Managing the Address Space, 379

Maximum Segment Size MSS, 443

Maximum Transmission Unit (MTU), 391, 405

Medium

 shared, 162

Message

 transfer agent (MTA), 471

 transfer system (MTS), 471

Message user agent (MUA), 470

Microwave

 point-to-point, omnidirectional, 137

 satellite, 140

 system, 137

 terrestrial, 136

Mobile, 149

 Base station, 149

 care-of address (COA), 415

 cellular, 147

 Fast Retransmit Mobile TCP, 441

 host, 440

 Indirect TCP, 440

 IP, 414

 Node Registration Reply messages, 414

 Node Registration Request message, 414

 routing with IPv6, 416

 switching center, 149

 switching center (MSC), 440

 TCP, 440

 transport protocol, 439

 UDP, 441

 user, 150

Mobile Broadband Wireless Access (MBWA),

 310

Model

 ATM protocol reference, 39

 client-server, 453

 Equal-Size Packet Protocol, 37

 hybrid, 10

 layered, 24

- peer-to-peer, 6
- reference, 24
- Reference, 28
- TCP/IP, 35
- Modem, 101
- Modulation
 - amplitude (AM), 107
 - DSB-SC, 108
 - Five level Pulse Amplitude Modulation, 197
 - Five-level Pulse Amplitude Modulation, 194
 - Frequency (FM), 110
 - LSB, 109
 - Phase (PM), 111
 - pulse amplitude, 199
 - pulse code (PCM), 106
 - Quadrature Amplitude (QAM), 104
 - Sigle Sideband (SSB), 109
 - USB, 109
- More Fragments, 220
- Multicasting, 338
 - address, 338
 - multicast group, 338
- Multiplexing, 276
 - frequency division, 277
 - statistical time division, 278, 281
 - super group, 284
 - time division, 278
 - wavelength division, 283

N

- Network
 - access points (NAPs), 65
 - architecture, 21
 - building blocks, 5
 - Cell switching, 63
 - cellular, 148
 - Circuit-switched, 58
 - Classification Methods, 47
 - client/server
 - computer, 78
 - connection- oriented, 59
 - connection-oriented, 61
 - core, 5
 - dedicated WAN, 58
 - destination, 391
 - Ethernet, 187
 - foreign, 412
 - fully switched, 244
 - home, 412
 - hybrid, 10
 - I, 249
 - integrated services digital, 293
 - Integrated Services Digital Network, X, 275
 - intelligent, 83
 - interface card, 189

- interface card (NIC), 5, 6
- Local Area (LAN), 49
- Local Area LAN, 131
- mask, 391
- Metropolitan Area (MAN's), 53
- mobile data networks (MDNs), 55
- mobile IP, 412
- model, 28
- operating system (NOS), 1, 6, 10
- Packet switching, 58
- peer-to-peer, 6
- private, 55
- protocols*, 25
- PSTN, PSDN, 149
- public, 56
- public switched telephone network, 275
- Services, 14
- switched WAN, 57
- Technologies, 64
- Topologies, 49
- topology, 30
- virtual private, 69
- virtual private network (VPN), 56
- Wide Area (WAN), 54
- WiFi, 309
- WiMax, 309
- wireless, 412
- wireless mesh, 308
- Network Operating System (NOS), 16
- client software, 12
- client/server, 11
- Drive Designator, 12
- hybrid, 16
- peer-to-peer, 11
- redirector, 12
- Noise, 97
 - crosstalk, 89, 127, 129, 131, 277
 - electromagnetic interference, 127
 - impulse, 90
 - intermodulation, 89
 - Intermodulation, 131
 - thermal, 88
- Nyquist frequency, 105

O

- Object identifiers (OIDs), 473
- Object Linking and Embedding, 14
- OID tree, 474
- Open Systems Interconnection (OSI), 29
- Optical fiber
 - application, 134
 - components, 132
 - graded index, 133
 - multimode, 133, 190, 194, 212
 - passive star, 191

- physical description, 132
- single mode, 133
- single mode, 191
- single mode, 194
- single mode, 212
- step-index, 133
- transmission characteristics, 136
- types, 133
- Orthogonal frequency division multiplexing (OFDM), 218
- OSPF
 - packet format, 407
- P**
- packet, 306
- Packet, 27, 539
 - IP, 160
 - Link State, 402
- Parity
 - check, 172
 - odd, even, bit, 172
 - two-dimensional, 173
- Path
 - cost, 396
 - least cost, 396, 397
- Peer-to-Peer
 - model, 6
 - network, 6
 - network operating system (NOS), 11
- Physical Interface, 120, 121
 - parallel, 121
 - serial, 121
- Physical Star-Logical Ring, 206
- plane management. *See* management plane
- Point
 - rate reference, 296
 - system reference, 296
 - terminal reference, 296
 - user reference, 296
- Point-to-point, 142
- Port, 36
- Power save poll (PSPoll), 219
- Prioritization of automatic IP addresses, 374
- Private Branch Exchange (PBX), 295
- Protocol, 27
 - (IMAP4), 471
 - Address Resolution Protocol (ARP), 35, 342
 - ARP query, 344
 - packet, 344
 - packet format, 345
 - table, 343
 - AppleTalk, 253
 - application, 451
 - ARP, RARP, 161
 - Bootstrap protocol (BOOTP), 373
- Border Gateway Protocol, 409
- border gateway protocol (BGP), 410
- Border Gateway Protocol (BGP-4), 452
- border gateway protocol (EBGP), 410
- Border Gateway Protocol is an EGP, 409
- data transfer process (DTP), 467
- Domain Name System (DNS), 36
- Dynamic Host Configuration, 262
- Dynamic Host Configuration Protocol (DHCP), 372
- Electronic Mail (email) Protocol, 469
- Exterior Gateway Protocol (EGP), 409
- File Transfer Protocol (FTP), 36
- File Transfer Protocol (FTP), 467
- High-level Data Link Control (HDLC), 327
- Hypertext Transfer (HTTP), 36
- Hypertext Transfer Protocol (HTTP), 454
- interdomain, XI, 389
- InterDomain Routing Protocol (CIDR), 357
- Interior Gateway Protocols (IGPs), 408
- Internet Control Message (ICMP), 35
- Internet Control Message Protocol (ICMP),
 - 334
 - code, 336
 - data unit, 334
 - messages, 337
 - packet type, 334
 - ping, 334
 - version 6, 336
- Internet Group Management Protocol (IGMP),
 - 337
 - function, 340
 - IP group address, 341
 - maximum response time, 341
 - membership, 341
 - message, 340
 - message encapsulation, 340
 - report and queries, 342
- Internet Group Management(IGMP), 35
- internet protocol (IP), 35
- Internet Protocol (IP), 323
- intradomain, XI, 389
- Intradomain, 408
- intradomain routing, 405
- Label Distribution Protocol (LDP), 452
- link layer, 157
- mobile IP, 333
- multiple-access, 162
- Name Binding Protocol (NBP), 31
- Neighbor Discovery protocol, 342
- network layer, 325
- network management, 472
- Open Shortest Path First (OSPF), 407
- post office protocol (POP3), 471
- Reverse Address Resolution Protocol (RARP),
 - 346
- routable, 404

routing, 404
 Routing Information, 253
 routing information (RIP), 405
 Routing protocol, 389
 Session Control Protocol (SCP), 32
 Simple Mail Transfer Protocol (SMTP), 36, 470
 Simple Network Management (SNMP), 36
 Simple Network Management Protocol, 240
 simple network management protocol (SNMP), 474
 spanning tree, 264
 suites, 28
 TCP/IP suite, 324
 Telnet, 460
 Telnet, a terminal emulation, 36
 Transmission Control Protocol (TCP), 425
 Transport Control Protocol (TCP), 428
 User Datagram Protocol (UDP), 425, 437
 segment, 438
 User Datagram Protocol (UDP)segment structure, 438
 VLAN Trunking Protocol (VTP), 260
 Zone Information Protocol (ZIP), 32

Q

Quality of Service, 195

R

Rate
 Baud, 92
 bit error, 93, 94
 data, 94
 data signaling, 92
 line, 291
 modulation, 92
 Nyquist, 106
 sampling, 105
 Redirector, 12
 Réseaux IP Européens (RIPE), 379
 Reference Model, 28
 Repeater, 234
 characteristics, 235
 Drawbacks, 235
 Request to send, 219
 Resource sharing, 3
 RIP
 command, 405
 data unit foramt, 405
 message, 405
 router, 406
 routing table, 406
 Route
 Default Route, 392

determination process, 394
 Directly Attached Network ID Route, 392
 Host Route, 392
 matching, 395
 Remote Network ID Route, 392
 Router, 249, 391
 buffer, 251
 characteristics, 252
 functions, 252
 ID, 408
 physical structure, 250
 Routing
 algorithm, 394
 centralized, 398
 distance, 396
 distributed, 398
 dynamic, 392
 information, 404
 interdomain, 404
 intradomain, 404
 mobile, 412
 policy, 396
 principles, 390
 protocol, 389, 394, 403
 static, 392
 table, 390, 400
 table entries, 392
 unicast, 405
 Routing Algorithm
 classification, 398

S

Sampling, 105, 279
 Satellite
 radio spectrum, 5
 Satellite Microwave
 C-Band, Ku-Band, Ka-Band, L-Band, 141
 GEO, MEO, LEO, 140
 physical description, 140
 SDH
 framing, 292
 multiplexing, 291
 Secure Management, 4
 Server
 application, 15
 cache, 459
 communication, 15
 data base, 15
 File, 15
 mail, 15
 Print, 15
 proxy, 16, 370, 459
 SMTP, 471
 software, 14
 terminal, 15

- web, 15
- Service**
 - Application Services, 14
 - Connection-less, 59
 - Connection-oriented, 60
 - Data base Services, 14
 - DNS directory look-up service, 466
 - Fax/Print Services, 13
 - Message Services, 14
 - Network Management Services, 14
 - Network Services, 14
 - Remote Boot Services, 13
 - remote procedure call for service (RPC), 13
 - Remote Services, 13
 - request for Service, 13
 - Switched Multimegabit Data Service (SMDS), 40
 - Utility Services, 13
 - Window Services, 13
- Shannon's formula, 91
- Shift keying**
 - quadrature phase, 307
- Signal**
 - amplitude, 78
 - analog, 81
 - bandwidth, 81
 - Baseband, 94
 - digital, 82
 - frequency, 78
 - optical, 131
 - parameters, 78
 - phase, 79
 - spectrum, 80
 - transmission, 80
 - types, 81
- Signaling
 - bipolar, 96
 - multi-level, 96
 - NRZ-I, 97
 - NRZ-L, 97
 - polar, 95
 - unipolar, 96
- SMTP
 - server, 471
- SNMP
 - packet encapsulation, 476
 - PDU format, 476
- Socket, 36, 441
 - basic operation, 442
- SONET, 291
 - framing, 289
 - STS-N frame format, 290
- Source
 - access point, 160
- Spectrum
 - electromagnetic, 124
- Standard, 21
- Stop bit, 85
- Sublayer**
 - Logical Link Control, 30
 - Medium Access Control, 30
 - physical medium, 38
 - transmission convergence, 38
- Subnetting, 353
 - default subnet mask, 361
 - design an IP addresses, 367
 - Enumerate IP addresses, 365
 - enumerating subnetted network IDs, 364
 - host bits, 363
 - host ID, 361
 - host per subnet, 363
 - network bits, 363
 - network ID, 362
 - network ID, 360
 - schame, 363
 - subnet mask, 359
 - subnetted network ID, 359
- Switch**
 - address table, 245
 - bus-architecture, 248
 - cut-through, 246
 - feature, 249
 - fragment-free, 246
 - full availability, limited availability, 247
 - function, 246
 - general description, 243
 - input ports, output ports, 246
 - matrix, 247
 - packet-based, 245
 - physical structure, 246
 - shared-memory, 247
 - store-and-forward, 246
- Switching
 - Cell, 62
 - Circuit, 58
 - Frame, 61
 - Packet, 58
- Switching Technologies, 245
- Synchronous**
 - digital hierarchy, 288
 - digital hierarchy, 291
 - optical network, 288
 - optical technology, 288
 - transport signals, 288
- System, 284
 - cellular, 147

T

- Table**
 - ARP table, 343
 - routing, 249, 390, 400
 - routing information, 303

- simple routing, 393
- static routing, 253
- switching, 245
- TCP/IP
 - layers, 35
 - Model, 35
 - Protocol Architecture, 36
- TCP/IP suite, 452
- TDM
 - bit-interleaved, 279
 - frame, 280
 - pulse stuffing, 281
 - word-interleaved, 279
- Telnet
 - Remote Terminal Emulation, 477
 - request, 461
 - response, 461
- Terrestrial
 - radio, 5
- Terrestrial Microwave
 - application, 138
 - physical description, 137
 - transmission characteristics, 138
- Token Ring
 - dedicated, 210
 - frame format, 208
 - IBM, 210
 - IBM Token Ring, 207
 - multistation access unit (MSAU), 206
 - operation, 209
 - specifications, 206
 - topology, 206
- Token Rings, 205
- topology, 50
- Topology
 - bus, 50, 189
 - interface, 377
 - mesh, 53
 - public, 377
 - ring, 52
 - site, 377
 - star, 51
 - tree, 52
 - WiMax Point-to-Multipoint topology, 308
- Trailer, 26
- Transmission
 - analog, 100, 107
 - Asynchronous mode, 85
 - Baseband mode, 86
 - broadband mode, 86
 - data, 77
 - digital, 105
 - impairments, 87
 - medium, 119, 120, 122
 - parallel mode, 84
 - reliable, 166
 - serial mode, 84
 - signal, 78
 - standard, 286
- Transmission medium
 - frequency consideration, 123
 - general classification, 123
 - guided, 124
 - unguided, 136
- Transport Control Protocol (TCP)
 - congestion, 429
 - congestion control, 434
 - connection setup, 431
 - flow control, 432
 - Round Trip Time and Timeout, 434
 - segment, 429
 - Sequence number, 429
 - source port, destination port, 429
 - three-way handshake, 431
- Transport layer
 - congestion control, XI, 425
 - connectionless service, 425
 - connection-oriented service, 425
 - flow control, XI, 425
 - multiplexing/demultiplexing, 426, 427
 - protocols, 425
 - services, 426
- Trunk
 - digital carrier, 286
 - link, 260
 - long-haul, metropolitan, rural exchange, 134
- Twisted pair
 - transmission characteristics, 128
- U**
- UDP, 481
- Uniform Resource Locators, 459
- V**
- VG-AnyLAN, 203
- Virtual
 - channel, 302
 - channel identifier, 302
 - path, 302
 - path identifier, 302
 - tributary, 288
- Virtual LAN, 256
 - frame format, 257
 - general description, 256
 - identification number, 258
 - standared, 257
 - trunking protocol, 260
 - workgroups, 259

W

W3C, 23
Web Caching, 459
WiMAX, 307
Wireless
 access point, 261
 base station, 307
 basic service set, 262
 basic service set identifier, 262
 bridge, 263
 distribution system, 264
 extension point, 262
 MAN (WMANs), 307
 mobile wireless router, 265
 point-to-multipoint bridge, 263
 point-to-point bridge, 263
 router, 265
 subscriber's station, 308

switch, 265
Wireless LAN, 215
 Access Point (AP), 217
 ad hoc, 217
 architecture, 216
 Basic Service Set (BSS), 218
 direct sequence, 217
 frame format, 219
 frequency hopping, 216
 general characteristics, 215
 Independent Basic Service Set (IBSS), 217
 infrastructure, 217
 MAC methods, 221
Workgroup, 6
World Wide Web, 4

Z

Zone Information Protocol (ZIP), 32

ACRONYMS

AAL:	ATM Adaptation Layer
ACK:	Acknowledgment
ADSL:	Asymmetric DSL
ADU:	Application Data Units
ALP:	Application Layer Protocols
AM:	Amplitude Modulation
ANSI:	American National Standards Institute
API:	Application Programming Interface
ARIN:	American Registry for Internet Numbers
ARP:	Address Resolution Protocol
ARQ:	Automatic Repeat Request
ASCII:	American Standard Code for Information Interchange
ASK:	Amplitude-Shift Keying
ATM:	Asynchronous Transfer Mode
BGMP:	Border Gateway Multicast Protocol
BGP:	Border Gateway Protocol
BOOTP:	Bootstrap Protocol
BRI:	Basic Rate Interface
BWA:	Broadband Wireless Access
CBR:	Constant Bit Rate
CDMA:	Code-Division Multiple Access
CIDR:	Classless Interdomain Routing
CLP:	Cell-Loss Priority
CO:	Central Office
CRC:	Cyclic Redundancy Check
CS:	Circuit Switching
CSMA/CA:	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD:	Carrier Sense Multiple Access with Collision Detection
CSMA:	Carrier Sense Multiple Access
CSU/DSU:	Channel Service Unit/Digital Service Unit
CTS:	Clear To Send
DCE:	Data Communication Equipments
DHCP:	Dynamic Host Configuration Protocol
DLC:	Data Link Control
DNS:	Domain Name System
DOD:	Department Of Defense
DSL:	Digital Subscriber Line
DSLAM:	Digital Subscriber Line Access Multiplexers
DSR:	Dynamic Source Routing
DSSS:	Direct-Sequence Spread Spectrum
DTE:	Data Terminal Equipments
DVA:	Distance Vector Algorithm
FC:	Frame Control

FDM:	Frequency-Division Multiplexing
FDMA:	Frequency-Division Multiple Access
FEC:	Forward Error Correction
FFDI:	Fiber Distrusted Data Interface
FHSS:	Frequency-Hopping Spread Spectrum
FM:	Frequency Modulation
FSK:	Frequency Shift Keying
FSK:	Frequency-Shift Keying
FTP:	File Transfer Protocol
FTP:	File Transfer Protocol
GUI:	Graphical User Interface
HDSL:	High-Bit-Rate Digital Subscriber Line
HFC:	Hybrid Fiber-Coaxial
HL:	Header Length
HTTP:	Hypertext Transfer Protocol
ICANN:	Internet Corporation For Assigned Names And Numbers
ICMP:	Internet Control Message Protocol
IDRP:	Interdomain Routing Protocols
IETF:	Internet Engineering Task Force
IFS:	Interframe Space
IGMP:	Internet Group Management Protocol
IP:	Internet Protocol
ISDN:	Integrated Services Digital Network
ISI:	Intersymbol Interference
ISP:	Internet Service Providers
I-TCP:	Indirect Transmission Control Protocol
LAN:	Local Area Network
LLC:	Logical-Link Layer
MAN:	Metropolitan Area Networks
MAU:	Multistation Access Unit
MBWA:	Mobile Broadband Wireless Access
MF:	More-Fragment
MIB:	Management Information Base
MSC:	Mobile Switching Center
MSS:	Maximum Segment Size
MTS:	Internet Mail Transfer System
MTU:	Maximum Transmission Unit
NAP:	Network Access Points
NAT:	Network Address Translation
NCP:	Netware Core Protocols
NFS:	Network File System
NIC:	Network Interface Card
NNI:	Network-Node Interface
NOS:	Network Operating System
NRZ:	Non-Return-To-Zero
NRZ-I:	NRZ- Inverted

NRZ-L:	Nonreturn-To-Zero-Level
NVT:	Network Virtual Terminal
OFDM:	Orthogonal Frequency Division Multiplexing
OSI:	Open Systems Interconnection
OSPF:	Open Shortest Path First
P2P:	Peer-To-Peer
PAM:	Pulse Amplitude Modulation
PBX:	Private Branch Exchange
PCM:	Pulse Code Modulation
PDU:	Protocol Data Unit
PEP:	Packet Exchange Protocol
PPP:	Point-To-Point Protocol
PRI:	Primary Rate Interface
PS:	Packet Switching
PSK:	Phase-Shift Keying
PWM:	Pulse Width Modulation
QAM:	Quadrature Amplitude Modulation
QoS:	Quality of Service
QPSK:	Quadrature Phase Shift Keying
RARP:	Reverse Address Resolution Protocol
RF:	Radio Frequency
RIP:	Routing Information Protocol
RTS:	Request To Send
RTT:	Round-Trip Time
RZ:	Return-To-Zero
SDH:	Synchronous Digital Hierarchy
SDH:	Synchronous Digital Hierarchy
SDMA:	Space-Division Multiple Access
SDSL:	Symmetric Digital Subscriber Line
SNMP:	Simple Network Management Protocol
SNR:	Signal-to-Noise Ratio
SONET:	Synchronous Optical Network
SSB:	Single Sideband
STA:	Spanning-Tree Algorithm
STDM:	Statistical Time-Division Multiplexing
STP:	Shielded Twisted Pair
SYN:	Synchronize
TCP:	Transport Control Protocol
TDM:	Time-Division Multiplexing
TDMA:	Time-Division Multiple Access
Tos:	Type of Service
TTL:	Time to Live
UTP:	Unshielded Twisted Pair
VCC:	Virtual Channel Connection
VCI:	Virtual Channel Identifier
VDSL:	Very High Bit-Rate Digital Subscriber Line

VLAN:	Virtual LAN
VoIP:	Voice over IP
VPC:	Virtual Path Connection
VPI:	Virtual Path Identifier
VPN:	Virtual Private Network
WAN:	Wide Area Network
WAP:	Wireless Access Points
WDM:	Wavelength-Division Multiplexing
WiFi:	Wireless Fidelity
WiMAX:	Worldwide Interoperability for Microwave Access
WMAN:	Wireless MAN
WRP:	Wireless Routing Protocol
ZIP:	Zone Information Protocol