Network Management
Principles and Practice

Mani Subramanian
Georgia Institute of Technology
Indian Institute of Technology Madras
NMSWorks Software Private Limited

With contributions from

Timothy A. Gonsalves
Indian Institute of Technology Madras

N. Usha Rani
NMSWorks Software Private Limited

PEARSON
Chennai • Delhi • Chandigarh

ISBN 978-81-317-2759-1

First Impression

Published by Dorling Kindersley (India) Pvt. Ltd., licensees of Pearson Education in South Asia.

Head Office: 7th Floor, Knowledge Boulevard, A-8(A), Sector-62, Noida 201 309, India.
Registered Office: 14 Local Shopping Centre, Panchsheel Park, New Delhi 110 017, India.

Typeset in 10.5/12.5 Times New Roman by Sigma Business Process, Chennai.

Printed in India

In loving memory of
Appa Mahadevan
Amma Kalyani

Affectionately dedicated to
Ruth, Ravi, and Meera Subramanian
for sustained support and persistent patience

With deep appreciation to
Stimulating Students
Who led me to learn by teaching

Endorsements

"I have been using the first edition since 2003 as core management principles and practical topics discussed therein made it an extremely useful reference even for practitioners. I am happy to note that the second edition is making the contents of the textbook even more applicable in the current technological context by incorporating management of Optical & MPLS networks widely deployed in the telecommunications network, discussing broadband wireless networks management that are now ubiquitous and the evolution of standards and technologies governing the actual implementation of the NMS itself. The addition of discussions around Cygnet NMS to illustrate the NMS architecture concepts and implementation considerations are quite useful. I am sure the book will serve the needs of both students in academics as well as the telecom and networking professionals."

Nagarajan, Sankar
Head, NMS R&D Services, Tech Mahindra, Chennai, India

"Many congratulations! It is a wonderful book with lots of minute details on Network Management. I am sure it will be a ready handbook for the student/professional communities.

My sincere thanks for your time and effort in bringing out the second edition of the textbook."

Seetharaman, V.
Head, ITMC & Cable NOC, Bharti Airtel Limited, Chennai, India

"Professor Subramanian has a remarkable ability to set complex network engineering and associated network management problems in context with well-written explanations and real-world examples that deal with the varied demands placed on converging telecommunications networks and the design and operation of the underpinning management systems and protocols.

This book will be extremely useful resource for graduate and postgraduate students on CS/EE courses including those studying in their first year of PhD in Telecommunications Engineering, as it provides a fantastic coverage of a wide range of fundamental network management issues. I for one will be using it for my graduate students."

Parr, Gerrard
School of Computing and Information Engineering, University of Ulster, Coleraine campus, Londonderry, Ireland

"Dr. Subramanian's *Network Management: Principles and Practice* provides the most thorough treatment of network management to date. There is no fluff in this book. It is for the serious, interested reader. It proceeds from the ground up, starting with common network management protocols and continuing to cover telecommunications management and broadband network management, focusing on WANs, optical networks, wireless networks, and home networks. Each chapter builds nicely upon previous chapters so that there is a logical delivery of information. Chapter 9, "Network Management Tools, Systems, and Engineering" is a very useful, practical chapter. It provides the reader with the know-how to perform hands-on network management with various management tools. Chapter 10 covers the classic model of the Telecommunications Management Network, indispensable for understanding network management. Chapter 11 covers other important aspects of network management, including fault management, performance management, security management, policy-based management, and service level management. Further, Chapter 11 includes a section on event correlation methods, typically not found in books on network management, and this is refreshing. These two chapters provide a solid foundation for understanding the management of WANs, optical networks, wireless networks, and home networks in the subsequent chapters. Chapter 16 covers forward-looking topics in network management, including web-based enterprise management and XML-based management approaches. There are appendices on Project Suggestions and Laboratory Tutorials that render the book quite well-suited for use in a course on network management. All in all, Dr. Subramanian's book provides a serious, first-rate treatment of the subject."

Lundy Lewis
Department Chair & Professor, Southern New Hampshire University, Manchester, USA

"This book fills a long-standing need. While there is an abundance of courses and textbooks that deal with typical topics in networking, there is a lack of such books for Network Management. Often, concepts and technologies related to Network Management are relegated to the last few chapters. This book brings out the fact that there is a wealth of detail in this area, which is important for practitioners as well as students.

This book gives comprehensive details of all aspects of network management, in different types of contemporary networks. Reading it would save practitioners considerable time and effort, which they might otherwise put into reading diverse online sources. This book also provides the syllabus structure required for a full-fledged course on Networking Management. It would be appropriate for students at the undergraduate as well as postgraduate levels."

Sridhar Iyer
Indian Institute of Technology Bombay, Mumbai, India

"It is a very comprehensive book on Network Management Systems addressing the needs of academia, industry both R&D and Operations. Coming from a person who has worked on all these functions in telecoms, the good thing about the second edition is the coverage of various technologies like Wireless, broadband, home networking and the challenges these technologies pose to the NMS."

Chalapathi Rao
Vice President & Head Global Delivery, Tata Communications Transformation Services Ltd., Chennai, India

"Mani Subramanian's book has been of great help in our undergraduate Network Management course.

The book provides both a top-down view on Network Management approaches and a bottom-up view of the management information available in almost any kind of network technology and environments. In particular, it offers quick and visual orientation in the jungle of MIBs available in all kinds of equipment.

The new edition kept the spirit of the first edition, but enhanced it significantly with new and helpful visualisations, examples and contemporary management scenarios.

The presentation is interspersed with the author's long-standing experience with Network Management and its tools, which helps the reader to gain a deep understanding of the reasoning behind Network Management models, protocols, services and tools."

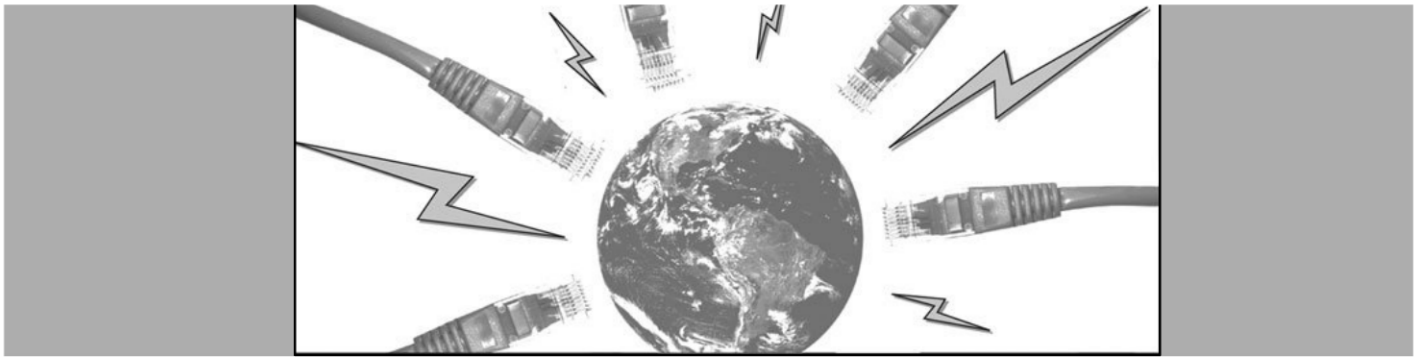
Markus Fiedler

Blekinge Institute of Technology, Karlskrona, Sweden

"This edition takes off from the previous one with a renewed perspective on network management, incorporating relevant developments over the past decade. The treatment of the topic beginning with a problem statement sets the scene for a detailed coverage on network management systems and their associated protocols. Mapping of TMN and eTOM gives a well-rounded view of both the technical and business process aspects of network management for the telecom operator. Real industry examples provide the much-needed meeting ground of theory and practical implementations. Dr. Subramanian's experience with the implementation of network management in major telcos lends authenticity to the treatment of this interesting subject. To summarize, the book would be valuable to students and professionals alike."

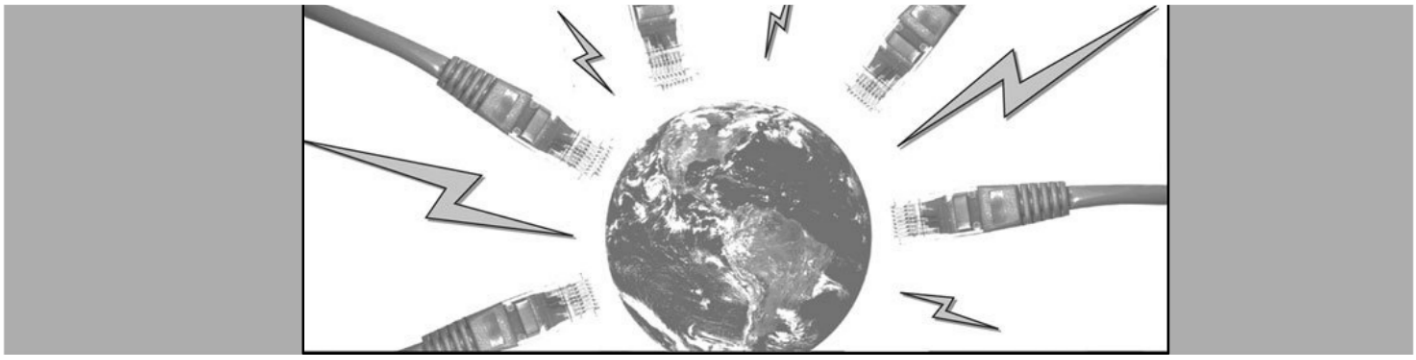
Aiyappan Pillai

Head, CNMS, Tata Communications Ltd., Mumbai, India



Brief Contents

This page intentionally left blank



Contents

Preface

Network-centric World and Role of Network Management

The world in the information era has become network-centric. Daily life, both personal and institutional, is network-centric. Century-old telephone technology has brought us today to the converged telecommunications and data communications technology era. We are linked to and interface with the globally "flat-world" via e-lifeline. The information era has built a world of information networks and systems that we need to operate, administer, maintain, and provision on an on-going basis. That is our challenge.

Areas of management of networks, systems, and applications in data and telecommunication services are not only the responsibility of telecommunications and networking industries and standards bodies but also of the academic world. Students graduating from technical colleges and universities are expected to be prepared to use a network and also to design and to manage one. The existing procedure to design and test some key networks is heuristic. Personnel with experience, and sometimes without, design networks and test them in live situations. A corporation hardly functions today without the deployment of local area networks (LANs) in their networking environment. The majority of homes in developed nations have a home network distributing voice, video, and data information. With the proliferating use of the Internet and Web technology, the subject of networking and network management has become part of the academic curriculum. This textbook, introduced ten years ago, has been part of this evolution. This new edition brings new technologies and services to undergraduate and graduate classrooms in the broad arena of what is known as network management.

Justification for a Textbook on Network Management

Over a decade ago when I started teaching a course on network management, there was a need for a textbook that satisfied quarter/semester requirements. The adoption of this book by colleges and universities across the world has partially filled that void. Just as networking education has been brought from the graduate to the undergraduate level, this edition of the textbook has been upgraded so that early parts of the book can be used at the junior and the senior undergraduate level and latter parts at the graduate level. It also addresses the audience of self-learners who want to get into or gain knowledge of network management.

Once again, a note about the title of this book: As noted in the earlier edition, the title does not truly reflect the contents of the book because we want to keep it succinct. The book covers management principles, practices, and technologies for managing networks, systems, applications, and services. The book is designed to be self-contained, so that the student does not have to traverse in and out of this book's domain. An attempt has been made to strike the right balance between theoretical background and practical aspects of networking. The treatment of practical aspects includes some real-world examples and "war stories." If "a picture is worth a thousand words," this book contains about a million. Just as a

programming course requires hands-on programming exercises, so does a network management course. So we have added laboratory tutorials to the appendix, which supplement classroom teaching.

A major addition to the book is the expanded treatment of broadband network management. It covers "triple play" services of voice, video, and data communications. It spans the network over the segments of wide area network (WAN), access networks to home, and home distribution networks including LANs. Multimedia communications is covered from the aspects of wired transmission media of cable, digital subscriber line, and optical fiber as well as fixed and mobile wireless.

This book exposes the student to current network management technology. At the completion of a course using this book, the student could either enter the industry with adequate networking knowledge or graduate school to pursue further research and specialization.

About the Contents

The book is divided into four parts. Part I deals with background material on networking and networking technologies. Part II addresses network management architectures and protocols. The focus is on SNMP and IP network management. Part III extends network management to the management of telecommunications, which includes networks, systems, operations and business services, and management applications. The last, and final, Part IV concludes with the management of broadband networks and the latest trends in management technology.

Part I consists of Chapters 1 and 2. Chapter 1 presents an overview of networking and network management. It is intended not only as a background and top-down information, but also as a motivation for the student. Chapter 2 reviews networking technology with a slant on management aspects. The course, for which this textbook is intended, assumes that the student has basic knowledge of data communications and networking. However, we review them briefly in Chapters 1 and 2. It is extremely difficult to cover much more than the basics of protocols, algorithms, and procedures of transport protocol layers 2, 3, and 4, as well as basic rudiments of components of LAN and WAN networks in such a course. Not much technology can be covered, and network management depends strongly on managing network components that are based on an ever-evolving technology, hence the presence of Chapter 2. It can be either skipped or covered in parts by the instructor. Relevant sections could also be used when dealing with subjects in Parts II, III, and IV. However, it would be useful as reference material for non-classroom learners who want an introduction to networking and network management.

Chapters 3 through 9 form Part II. Basic foundations of models that are needed to build various network management architectures and protocols are covered. OSI-based network management is rarely used, but has some strong fundamental concepts. For completeness of the subject, it is included in Appendix A. SNMP-based protocols that manage TCP/IP networks are covered in Chapters 4 through 8. Chapters 4 and 5 are devoted to learning the concepts and use of SNMP (version 1) in network management. Chapters 6 and 7 deal with the additional specifications defined in versions 2 and 3. Chapter 8 extends network management using remote monitoring capabilities. Chapter 9 discusses networking and network management tools. The architecture and features of some of the widely used network and system management systems are also covered.

Network management is more than just managing the network infrastructure. Part III addresses this from the service, business, and applications points of view. Chapter 10 extends the management area to cover broader aspects of network management from managing network elements and networks to service and business management as addressed in Telecommunications Management Network (TMN) standards. The knowledge acquired on management tools and systems, as well as on

principles in Part II, is applied to practical applications in managing fault, configuration, performance, security, and accounting, which forms the contents of Chapter 11.

The demarcation of telecommunications and data communications is becoming increasingly fuzzy in broadband communications. In Part IV, the broadband network is segmented into WAN, access network, and home distribution network. Chapter 12 deals with WAN. IP technology has been extensively dealt with in Parts I and II. The management of ATM network, MPLS network, and optical SONET/SDH/DWDM network management is covered in Chapter 12. Chapter 13 addresses wired broadband access networks in bringing services from core WAN to home. Management of cable, DSL, and PON are the three technologies that we cover. Fixed and mobile wireless access network management form the subject matter of Chapter 14. Having brought voice, video, and data of broadband service to home, it needs to be distributed inside customer premises and managed. This is the topic of discussion in Chapter 15.

The impact of emerging technologies in a Web-based and object-oriented management system is the future of management technology, which is addressed in Chapter 16.

Suggestions for Course Syllabus

Parts I and II along with the Laboratory Tutorials in Appendix C form a unit for undergraduate courses. Parts III and IV are suitable for graduate-level courses with senior-level students admitted with the consent of the instructor.

The complete contents of the book are more than can be covered in a quarter or even a semester course. The instructor may do a "mix and match" between chapters to suit local needs if SNMP basics and some of the broadband network management are to be covered in one semester. Independent of the choice, a project to accompany the course is recommended, and suggestions are given in Appendix B.

For a dedicated course on network management, there are several choices. If the focus is on SNMP management, then Chapters 6 through 8 covering SNMPv2, SNMPv3, and RMON, respectively, can be used. That can be followed with network management tools and systems (Chapter 9) and applications (Chapter 11).

If telecommunications is emphasized (this is more likely in computer engineering schools), then it would be good to include Telecommunications Management Network (Chapter 10).

If broadband services are taught at the school, then Part IV (Chapters 12–16) could be included.

Finally, if the school has a research program on network management, it is suggested that in addition to the special areas of interest, management applications in Chapter 11 be dealt with in depth. In addition, adequate treatment of Advanced Management Topics (Chapter 16) is strongly suggested.

To the Instructor

This textbook is designed as a dual-level book. It can be used for undergraduate courses at the junior or the senior level or for graduate-level courses. It assumes that the student has taken a prerequisite course in either data or telecommunication network or has equivalent knowledge. However, the book does review networking from a management focus prior to dealing directly with the main subject of network management.

With the prolific growth of networking, network management is expected to become part of the academic curriculum, and this book will be useful for both Computer Science and Electrical and Computer Engineering schools that specialize in networking.

Online Supplements: Solutions to exercises are available to instructors from the Pearson representative. Visual aids in the format of PowerPoint slides for instructors and students are available to all from the Pearson website that would facilitate teaching and note-taking in the class.

The book could also be used as a reference material if you are teaching a Continuing Education course on network management. The PowerPoint slides will come in handy as classroom aids. I have found that students like to take home knowledge in the form of a book in addition to the student manual. The author welcomes suggestions and material to be added and may be reached at manims@ieee.org.

To the Student

Although the book is written as a textbook to be adopted for a course, additional information is provided in the book that would serve as a reference book for students after graduation. For example, basic information is provided along with references to serve as a springboard to access additional in-depth details on any specialized management topic.

The book is also geared toward self-motivated engineers in the industry who are eager to learn network management. If the engineer has access to network resources, many of the hands-on exercises could be practiced. At the minimum, it would provide enough tools and knowledge for the frustrated worker when he or she cannot access the network resources and does not know why.

Grateful Acknowledgements

The major impetus for the contents of this book has come from students over the course offerings since 1996. It has been reviewed at various levels and to various depths by many students.

My thanks flow profusely to Professor Timothy Gonsalves and Dr. Usha Rani for making major contributions to Chapters 9 and 16, respectively. We have shared together teaching the Network Management course at Indian Institute of Technology Madras. I thank Professor Gerard Paar for motivating me to come out with a second edition; and it is unfortunate that he could not participate as a contributing author due to other commitments. I owe gratitude to several persons at NMSWorks who have helped in various ways in the preparation of the manuscript. My special thanks to Binu Raghavan for generating topological views of CygNet NMS that is customized for the textbook presentation, to Madangopal and Adithyan for SDH exercises, and to Santosh Chaudhari for help with network load statistics figures.

Many reviewers' comments and suggestions have contributed to the richness of the contents of the first edition that form the basis of this edition. I owe special gratitude to Lundy Lewis, who has made numerous and specific suggestions for improvement in the first edition. The results of interviews described in Chapter 1 generated positive feedback from reviewers and students; and I thank the following at Georgia Tech for consenting to be interviewed: Cas D'Angelo, Ron Hutchins, Dave Miller, John Mize, and John Mullin. Some of the case histories were provided by Rob Beverly, Ron Hutchins, and Dave Miller. Brandon Rhodes and Oleg Kolesnikov provided some interesting practical exercises to be included in the book.

My thanks go to Sojan Jose, Commissioning Editor, M. E. Sethurajan, Senior Production Editor, and Jennifer Samuel Sargunar, Associate Production Editor, of Pearson Education for their ever-willing cooperation in successfully seeing this second edition through to completion.

I am indebted to the Indian Institute of Technology Madras for providing time off for me to come out with the second edition. I also want to thank Professors Ashok Jhunjhunwala, Timothy Gonsalves, and Bhaskar Ramamurthy of TeNeT Group for providing me with an environment to fulfill my desire of the long-needed upgrade of the book.

My wife, Ruth, continued her contributing role to the book by inputting revisions, acting as the local copy editor, and being production manager of manuscripts. Thank you again, Ruth.

Mani Subramanian

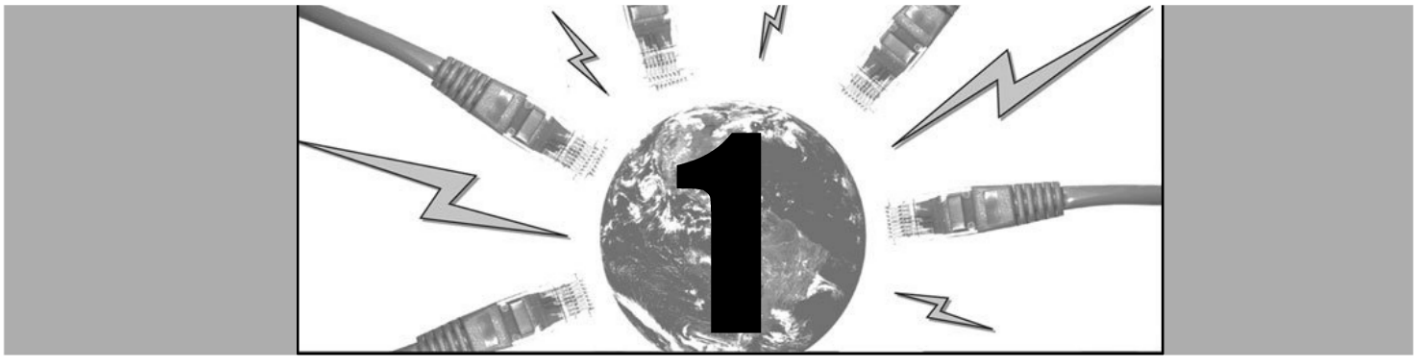
PART I

Background

Chapter 1 presents an overview of telecommunications, data communications, and network management. It is a broad review of networking and network management. It starts with an analogy of the telephone network. Telephone network almost always works, and there are reasons for its achieving quality and reliability. You will learn the relationship between data communications and telecommunications and how the distinction between the two is slowly disappearing. The influence of desktop computing and distributed computing environment based on client–server architecture has revolutionized computer communication. The Internet is a worldwide fabric and you will learn to appreciate how information travels across it around the globe. Basics of communication protocols and architecture are presented along with various standards. Select equivalent applications are used as illustrations comparing the Internet and OSI protocols.

Components of network management are described and complemented by interviews with network managers, whose experiences emphasize the need for network management and a network operations center. Network management is more than just managing networks. Network management is presented from the perspectives of service management, operations support systems, and business management. The platform for a network management system is discussed based on client–server architecture. Chapter 1 concludes with a note on future trends in network management technology.

Chapter 2 focuses on network technology. You may skip this chapter if you are familiar with the practical aspects of networking. If you are knowledgeable on principles of data communication, this chapter will help you appreciate the technological aspects of it. You will learn how various topologies are implemented in LAN and WAN networks. Basics of Ethernet, Token Ring, and FDDI networks are described from a practical point of view. Of these, Ethernet is the most widely deployed LAN today. LAN evolution from basic Ethernet to Gigabit Ethernet with half- and full-duplex configurations is presented. Switched Ethernet adds capability to expand the bandwidth and the flexibility of LAN. Virtual LAN is implemented using a switched Ethernet hub accomplishing flexibility in administration of workstations across multiple LANs. You will learn the various network components—hubs, bridges, routers, gateways, and protocol converters—that need to be managed. A brief review of wide area networking and transmission technology is also presented. Broadband technology is briefly described in this chapter, but a detailed discussion of it will be done in Part IV while addressing the management of broadband networks and services.



Data Communications and Network Management Overview

OBJECTIVES

- *Telecommunications overview*
- *Data communications overview*
- *Evolution of converged networks*
- *Desktop processors and LAN technology*
- *Client–Server architecture in networking*
- *Internet and intranet*
- *Network communication protocols*
- *OSI and Internet standards*
- *Broadband networks and services*
- *Need for network management and NMS*
- *Operations, Administration, Maintenance, and Provisioning*
- *Network management architecture and organization*
- *Concept of Network Operations Center*
- *Perspectives of network management*
- *Network management system*
- *Look-ahead of network management technology*

This chapter demonstrates the necessity of network system and service management in providing information technology (IT) services. The challenges that IT managers face are presented to motivate the student to get excited about network management. We start with the history of computer communication, walk you through some real-world case histories, and then present an overview of various aspects of network management.

The telephone system is known to be very reliable and dependable. One can make a telephone call from anywhere to anywhere at any time of the day and be reasonably sure that the connection will be made and the quality of connection will be good. This is partly due to the efficient management of the telephone network. Section 1.1 introduces the concept of management for the success of telephone network by using Operation Support Systems (OSSs).

Computer communication initially used the telephone network to carry digital data. There was a clear demarcation between the traditional telecommunication network and computer communication network. The evolution of early computer communication networks is dealt with in Section 1.2.

Computer communication technology radically changed with the advent of desktop computing power and distributed computing environments (DCEs) using local area networks (LAN) as described in Section 1.3. Global communication using Internet became a reality with the introduction of TCP/IP-based networks. Section 1.4 describes Internet and intranet followed by a discussion in Section 1.5 on the importance of communication protocols and standards.

The next phase in the evolution of IT was the introduction of broadband services. Voice, video, and data could be delivered on the same medium to homes. This has revolutionized the access network to home and the distribution network at customer premises. It has also initiated improvement in the core wide area network (WAN). Section 1.6 addresses these issues.

Networking is full of "war stories" as experienced by IT managers. Sections 1.7 and 1.8 present case histories experienced by IT managers and the challenges they face in today's computer and telecommunication environment. Interviews with them emphasize the importance of network and system management tools. Section 1.9 describes network management that comprises operations, administration, maintenance, and provisioning. Three groups perform these functions: Engineering, Operations, and Installation and Maintenance (I&M). Section 1.10 focuses on Network Management System (NMS) and relationships between its various components. Besides managing network components, application system resources also need to be managed. This is the subject of Section 1.11.

Network management technology is still in an evolutionary mode as network and software technologies advance. Section 1.12 briefly addresses NMS platforms based on Microsoft Windows and UNIX operating system. The future directions of network management technology form the content of Section 1.13. As with all chapters in the book, a summary section and exercises conclude this chapter.

1.1 ANALOGY OF TELEPHONE NETWORK MANAGEMENT

The need for data or computer communication network management is best illustrated by an analogy of telephone network management. The high degree of reliability of the telephone network is evidenced by the following illustration. We can pick up a telephone, call anybody, anytime, anywhere in the world, and be almost sure to be connected to the destination. It is reliable and dependable; and the quality and speed of connection are good. It is reliable because it almost always provides service of voice communication that we expect of it. It is dependable because we can be fairly sure that it works when we need it, especially in an emergency situation, such as 911 calls in the USA or military defense situations. The quality of service is generally good; and we can have a conversation across the world with the same clarity that we have when we call our neighbor.

The present-day telephone network is referred to as Public-Switched Telephone Network (PSTN), and is probably the best example of traffic engineering providing guaranteed Quality of Service. The reason for such reliability, dependability, and quality is more than careful planning, design, and implementation of a good telephone network using good and reliable components. The key is management and operation of the network. Much of the management of the network is so well automated that it becomes part of the operation. Let us first look at the telephone network architecture and then at some of the operations support systems that manage it. In the 1970s the telecommunications industry switched to digital services, which followed much the same pattern as voice services and conceived a vision of end-to-end circuit-switched services, known as the Broadband Integrated Services Digital Network (B-ISDN). B-ISDN is now being replaced by Internet and Broadband Service.

The architecture of a telephone network is hierarchical as shown in Figure 1.1 [AT&T 1977]. There are five levels of network switches and three types of trunks that connect these switches. A trunk is a logical link between two switches and may traverse one or more physical links. The end office (Class 5), which is lowest in the hierarchy, is the local switching office. The customer's telephone or Private Branch Exchange (PBX) is connected to the end office via a dedicated link called "loop." The other four higher levels of switches (Class 4 through Class 1) are tandem or toll switches carrying toll (long-distance) calls. Because of the advance in switching technology and economy of transmission, Classes 1 through 4 have been merged into a single class referred to as Class 4. A direct trunk connects two end offices, a toll-connecting trunk connects an end office to any toll office, and a toll (internal) trunk connects any two toll offices.

From the local Class 5 office to the called party's Class 5 office, there are multiple routes. A circuit connection is set up either directly using a local trunk or via higher-level switches and routers. Primary and secondary routes are already programmed into the switch. If the primary route is broken or facilities over the primary route are filled to capacity, an alternate route is automatically assigned. For example, on Mother's Day, which is the busiest telephone-traffic day of the year in the United States, a call to the neighboring town could travel clear across the country and back if that's the route where adequate bandwidth is available. Let us remember that there is a 3-hour time difference between the two coasts, and traffic in the West Coast starts 3 hours later than the East Coast.

To ensure the quality of service in a telephone network, operations support systems are implemented. They constantly monitor the various parameters of the network. For example, to ensure that there is adequate bandwidth to carry the traffic over the facilities, a traffic measurement system constantly measures traffic over switch appearances. The results are analyzed for facility-planning purposes. They also provide real-time input to a NMS when there is excessive blocking (traffic over the capacity of the trunk group) in any link.

The quality of the call, measured in terms of signal-to-noise (S/N) ratio, is measured regularly by a trunk maintenance system. This system accesses all the trunks in an office during the night and does a loop-back test to the far end. The results are analyzed in the morning and corrective actions taken. For example, if the S/N ratio of a trunk is below the acceptance level, the trunk is removed from service before the customer experiences poor performance.

For a given region, there is a network operations center (NOC) where the global status of the network is monitored. Traffic patterns are constantly observed and corrective operations are taken, if needed, in real time. The NOC is the nerve center of telephone network operations.

It is worth noting that the telephone network is managed from the users' perspective, and not from that of the system or the service provider, even though the objectives of both are the same. However,

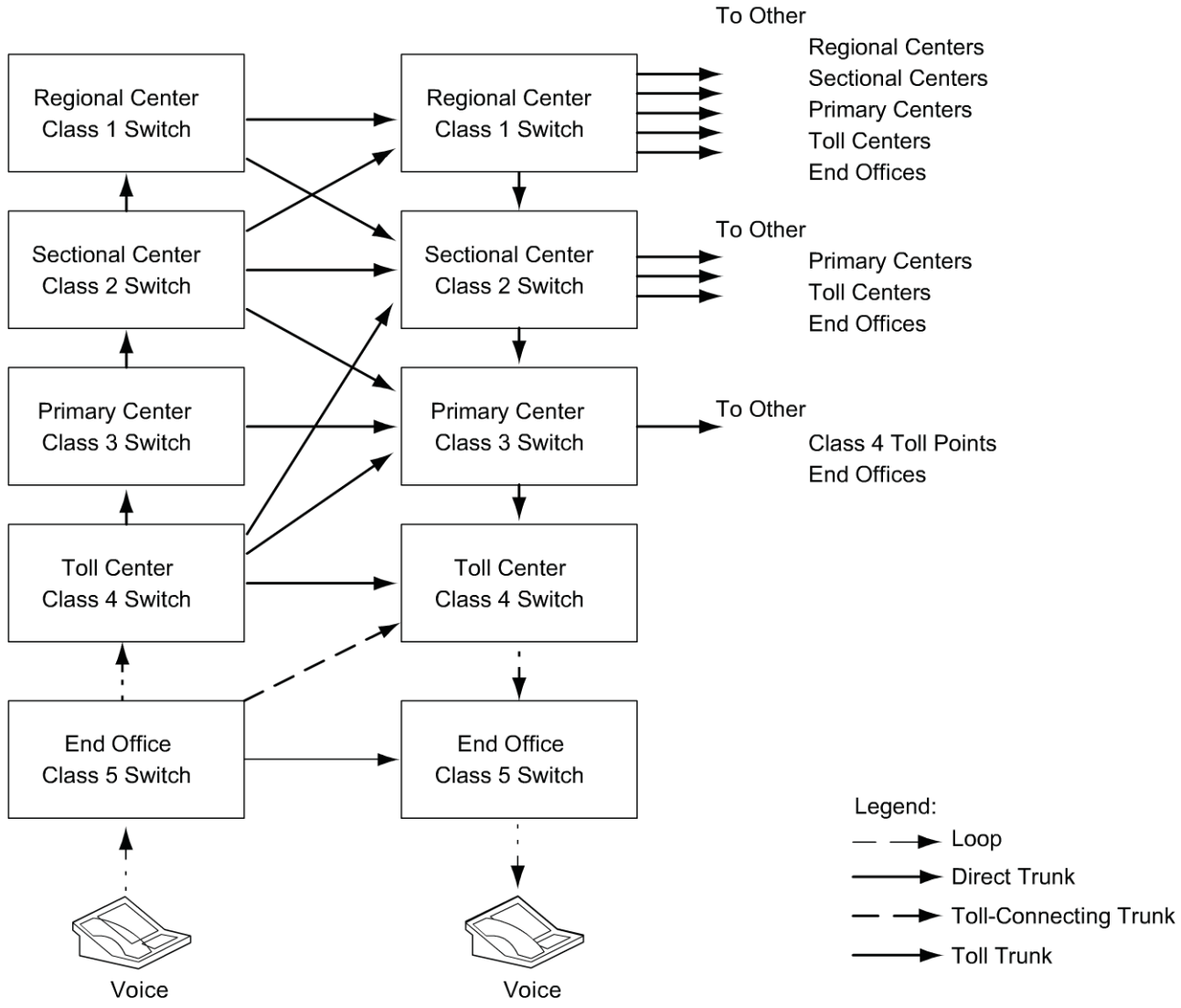


Figure 1.1 Telephone Network Model

with emphasis on the user's point of view, the first objective in operations is restoration of service and then the quality and economy of service. Thus, isolation of the problem and providing alternative means of service, by either manual or automated means, become more important than fixing the problem.

To manage a network remotely, i.e., to monitor and control network components from a central location, network management functions need to be built into the components of the network as much as possible. In that sense, network component designs should include network management functions as part of their requirements and specifications.

The computer or data communication network has not matured to the same extent as the telephone network. Data communications technology is merging with telephone technology. Data and modern telecommunication networks are evolving into broadband communication networks and are more complicated than the plain old telephone service (POTS). Analog audio and video services are migrating to digital services. The analog hierarchy of low-to-high bandwidth signals is being transmitted across the globe using a Synchronous Digital Hierarchy (SDH) mode.

Network management and operations of these digital networks are continuously being developed as new technologies emerge. Further, the telephone industry all over the world had been monopolistic and thus single-vendor oriented. This is no longer true. Digital-based computer communications started as a private industry and is hence multivendor oriented. Unfortunately, this has produced enormous problems to users because network components supplied by different vendors do not always communicate with each other. The network or information systems manager, who has the responsibility of keeping the service alive all the time, has been confronted with resolving the issue as new technology and new vendor products emanate. This situation has been recognized by various industrial and standard groups and is being continuously addressed.

1.2 DATA (COMPUTER) AND TELECOMMUNICATION NETWORK

Network communications technology deals with the theory and application of electrical engineering, computer engineering, and computer science to all types of communication over networks. It also addresses accessing of databases and applications remotely over LANs as well as switched and private lines. A basic network can be viewed as interconnected nodes and links as shown in Figure 1.2. A link carries information from one node to another that is directly connected to it. A node behaves as an end (terminating or originating) node, or an intermediate node, or both. If the node behaves as an end node, information either originates or terminates there. An intermediate node redirects the information from one link to another. End-office nodes mentioned in Section 1.1 behave as end nodes. A node can drop and add information channels and at the same time switch information transparently between two links. Each end node has a connection to a user interface if the information originates or terminates there. This interface could use any type of equipment—audio, video, or Data Terminating Equipment (DTE). A DTE is any equipment that generates or accepts digital data.

Data can be transmitted either in an analog or digital format. The analog data are sent either as a baseband (e.g., voice data from the switching office to the customer premises) or on top of a carrier (e.g., cable TV). Digital data are either directly generated by the user equipment (e.g., computer terminal) or as analog data and are converted to digital data (e.g., Integrated Services Digital Network (ISDN) connection to customer premises). The latter scenario of the ability to handle integrated digital and analog signals is becoming extremely important as in the case of multimedia broadband services. Management considerations associated with them are also very challenging, as we will see in Part IV. Long-distance data transmission today is mostly digital due to its superior price and performance.

Data are sent from the originating to the terminating node via a direct link or via a tandem of links and intermediate nodes. Data can be transmitted in one of three modes: circuit switched, message switched, or packet switched. In the circuit-switched mode, a physical circuit is established between the originating and terminating ends before the data are transmitted. The circuit is released or "torn down" after completion of transmission.

In message-switched and packet-switched modes, data are broken into packets and each packet is enveloped with destination and originating addresses. The message-switched mode is used to send long messages, such as email. The packet-switched mode is used to transmit small packets used in applications such as interactive communication. Bridges and routers open each packet to find the destination address and switch the data to the appropriate output links. The path between the two ends may change during the transmission of a message because each packet may take a different route. They are reassembled in

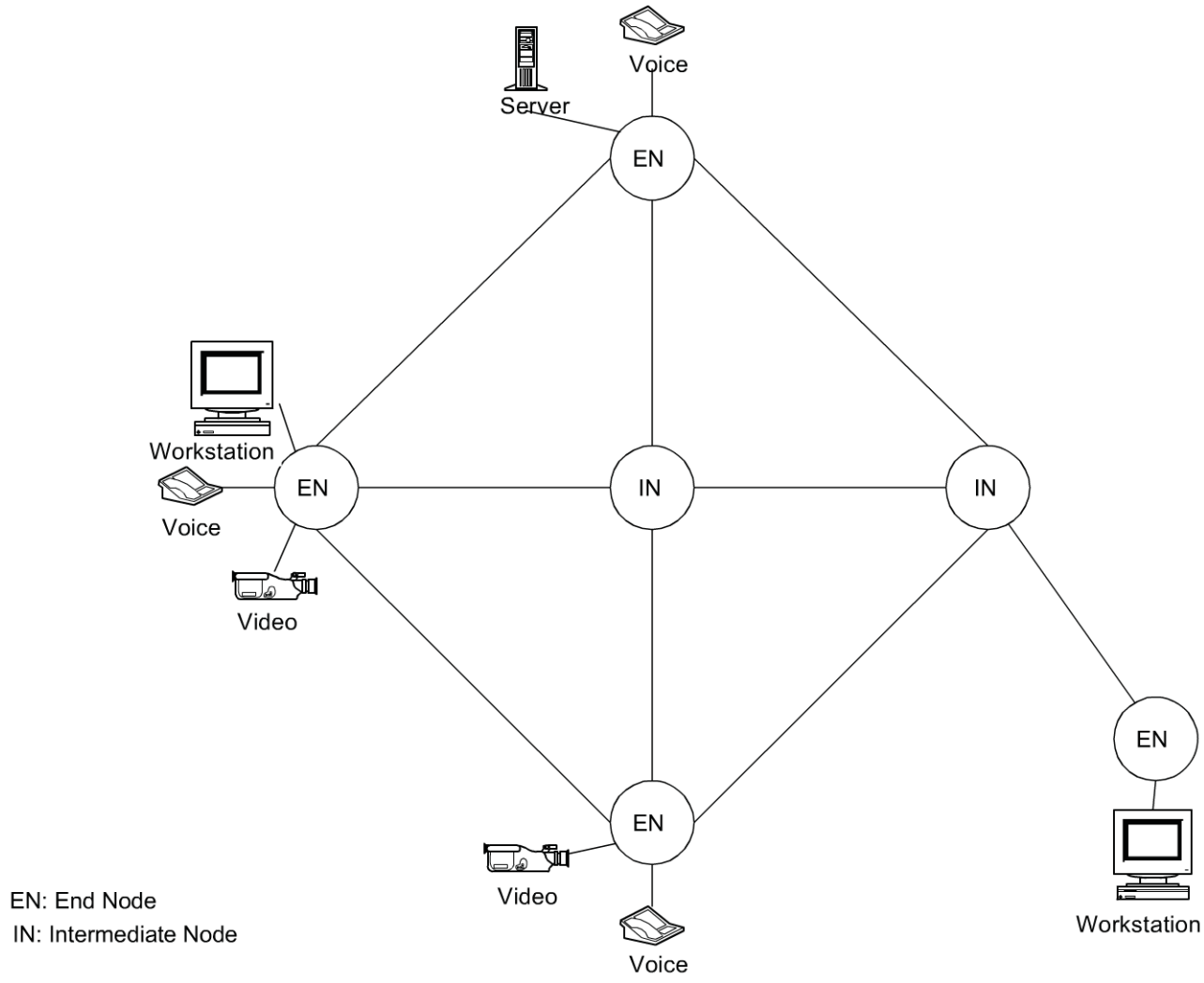


Figure 1.2 Logical Network Model

the right order at the receiving end. The main difference between message and packet switching is that in the former, data are stored by the system and then retrieved by the user at a later time (e.g., email). In the packet-switched mode, packets are fragmented and reassembled in almost real time. They are stored in the system only long enough to receive all the packets in the message. In Europe, X.25 packet-switched network was extensively used in Public-Switched Data Network (PSDN).

Network communications are commonly classified as either data communications or telecommunications. This classification is based on historical evolution. The telephone network, which came into existence first, was known as a telecommunication network. It is a circuit-switched network that is structured as a public network accessible by any user. The telephone network represents a telecommunication network. The organization that provides this service is called a telecommunication service provider (e.g., AT&T, British Telecom, NTT, BSNL, etc.).

With the advent of computers, the terminology data communication network came into vogue. It is also sometimes called computer communication network. The telecommunications infrastructure was, and is, still used for data communications. Figure 1.3 shows an early configuration of terminal-to-host and host-to-host communications, and how data and telecommunication networks interface with each

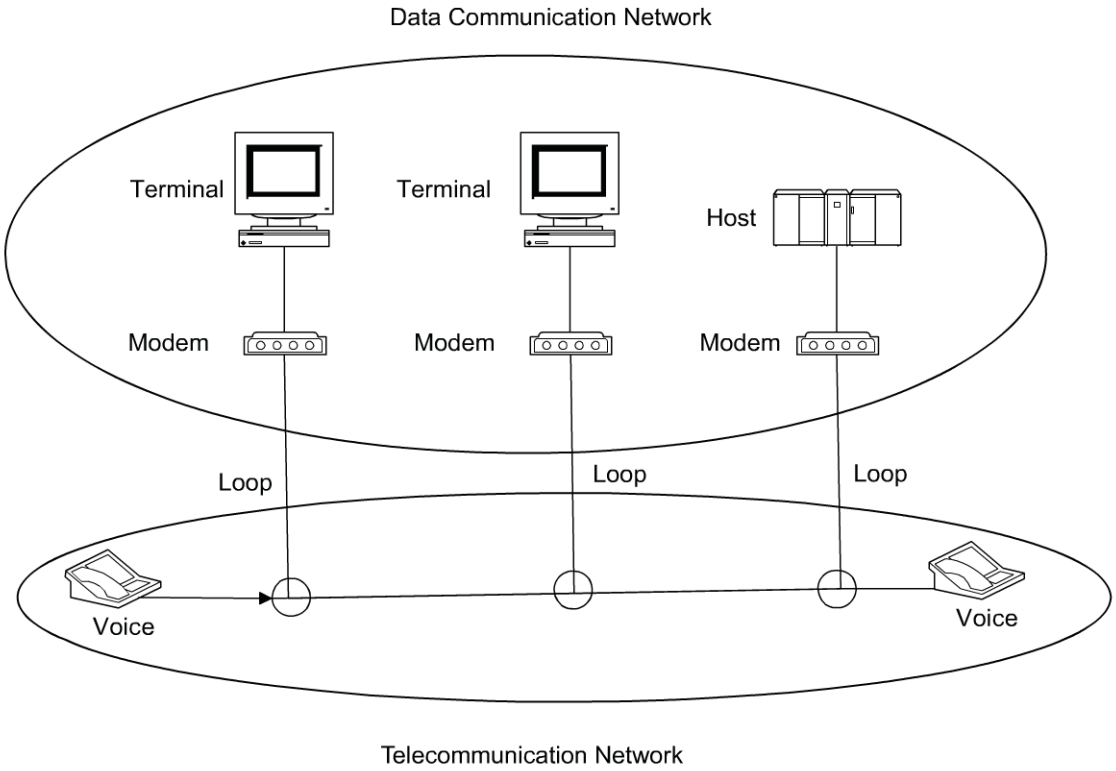


Figure 1.3 Analog and Data Telecommunication Networks

other. To interface, a terminal or host connected to an end-office switch communicates with the host connected to another end-office switch by modems at each end. Modems transfer information from digital to analog at the source (telephone networks carried analog signals) and back to digital at the destination.

Modern telecommunication networks mostly carry digital data. The nodes in Figure 1.4 are digital switches. Analog signals from telephones are converted to digital signals either at the customer premises or the central office. Figure 1.4 shows a corporate or enterprise environment in the stage of the evolution of data and telephone communications. A number of telephones and computer terminals at various corporate sites are connected by telecommunication network. Telephones are locally interconnected to each other by a local switch, PBX, at the customer premises, which interfaces digitally to the telephone network. The computer terminals are connected to a communication controller, such as a digital multiplexer, which provides a single interface to the telephone network.

With the advent of desktop computers and LAN, data communication was revolutionized. Desktop computers could communicate with each other over the LAN. This led to a Distributed Computing Environment (DCE), which is discussed in the next section.

1.3 DISTRIBUTED COMPUTING ENVIRONMENT

Figure 1.5 shows a LAN with hosts and workstations. Let us observe that they are workstations with processing power and not just dumb terminals as described in the previous section. Any workstation can communicate with any host on the LAN. There can be a large number of workstations and hosts depending on the type of LAN. DTEs connected to different LANs that are geographically far apart can

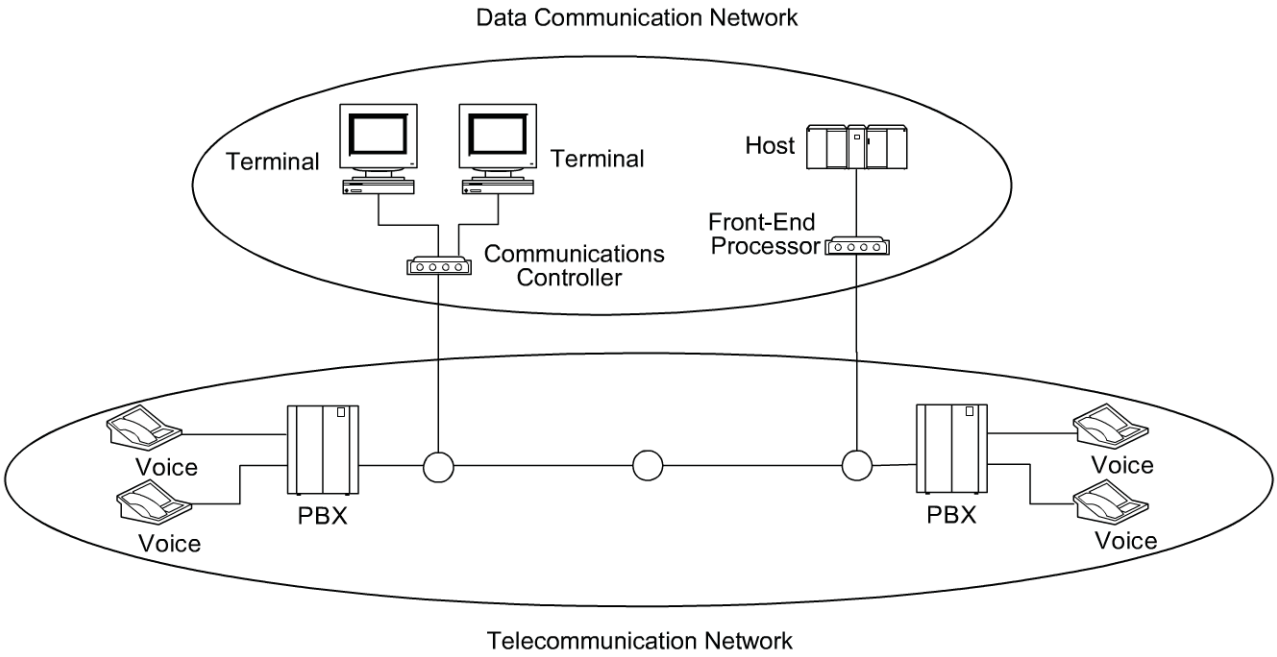


Figure 1.4 Digital Data and Telecommunication Networks

communicate via telecommunication network, either public or private switched. The system of links connecting remote LANs is called a WAN. A LAN is physically connected to a WAN by a bridge or a router as shown in Figure 1.5(b). We will discuss the types of LANs and WANs in Chapter 2. First, we want to bring out two important aspects of DCE in this section.

The first aspect is the question of whether the different platforms and applications running on DCEs have the ability to communicate with each other. In the early stage of communication network evolution, proprietary interfaces between platforms and processes were implemented by telecommunication service providers and computer vendors to communicate autonomously within each of their networks. For example, Bell System, a monopolistic telecommunication service provider, and IBM, the largest computer vendor, established transmission, switching, and interface standards and manufactured their own communications equipment to meet them. They made significant contributions to the standards bodies to make such specifications the industry standards. For customer premises equipment (CPE) interface, specifications are published for them to interface cleanly with the network. For example, Bell System published specifications for Customer Service Unit (CSU) for customer equipment to interface with the network. However, as the telecommunications industry rapidly grew, national and international standards needed to be established for communication between equipment provided by various vendors. Protocols and database standards for handshaking and information exchange are discussed in the following sections. For now, we will assume that the different processors and processes running on them could communicate with each other.

The second aspect of DCE is the ability of processors attached to LANs to do multiple functions. They could continue, as dumb terminals did, to request a host to perform the functions and return the results. Alternatively, they could request some special functions to be performed by a host—and it could be any processor in the network—and receive the results. In this scenario, the processor that requests a service is called the client; and the processor that provides the service is called the server. Such a configuration is termed a client–server environment. Although the terminology of client and server is

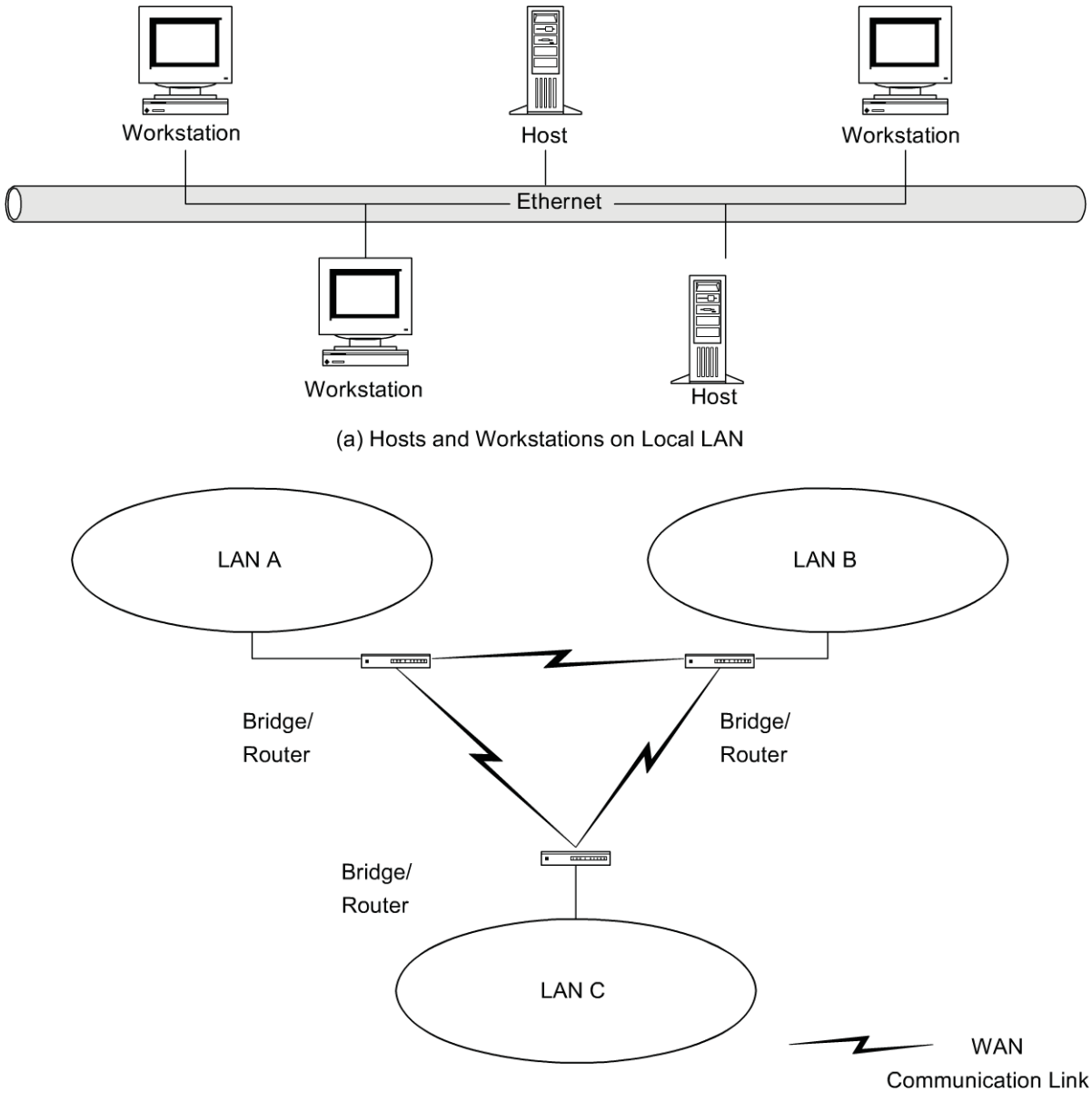


Figure 1.5 DCE with LANs and WANs

commonly associated with the processors, the more accurate definition should be associated with the processes. Thus, the process that initiates a transaction to run an application in either a local or a remote processor is called the client. The application process that is invoked by a client process is called the server. The server returns the results to the client. The application designed to take advantage of such a capability in a network is called a client–server architecture. With such an interpretation, the client and server processes can coexist in the same processor or in different processors.

We will now go into some detail on the salient characteristics and features of client–server architecture and models, as they are very pertinent to network management applications and architecture. A simple client–server model is shown in Figure 1.6. There is apt to be confusion between which is a client

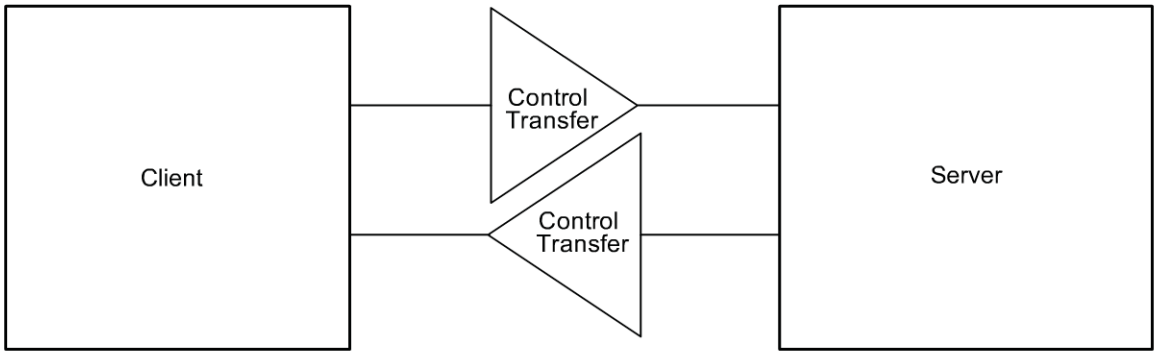


Figure 1.6 Simple Client–Server Model

and which is a server in distributed computing architecture. The best way to distinguish between the two is to remember that the client initiates the request and the server responds.

The client initiates a request to the server and waits. The server executes the process to provide the requested service and sends the results to the client. It is worth noting that the client cannot initiate a process in the server. Thus, the process should have already been started in the server and be waiting for requests to be processed.

A real-world analogy to the client–server operation is a post office. The clerk behind the counter is ready and waiting for a client. She is a server. When a customer walks in and initiates a transaction, for example, ordering stamps, the clerk responds. The customer is the client. After the clerk gives the stamps to the customer, i.e., she has delivered the results, the customer leaves and the clerk, as a server, goes into a waiting mode until the next client initiates a transaction.

As with any system, delays and breakdowns of communication need to be considered in this model. The server may be providing the service to many clients that are connected to it on a LAN, as shown in Figure 1.7(a). Each client's request is normally processed by the server according to the FIFO rule—first in first out. This delay could be minimized, but not eliminated, by concurrent processing of requests by the server. It is also possible that, due to either the communication link or some other abnormal termination, the server may never return the result to the client. The application on the client should be programmed to take care of such deficiencies in communication.

Since the client and application are processes running in a DCE, each of them can be designed to execute a specific function efficiently. Further, each function may be under the jurisdiction of different departments in an organization. An example of this is shown in Figure 1.7(b). joe.stone@source.com (Joe Stone's user id) using a client in a network sends a message to sally.jones@dest.com (Sally Jones' user id) on the network. The message first goes to the mail server on the network. Before it can process the request, the mail server needs to know the network address of sally.jones, which is dest.com. Therefore, it makes a request to the domain name server (DNS) on the network for routing information for the address of dest.com. When it receives that information, it sends out joe.stone's message via the bridge connected to the network. It then sends a message to joe.stone on the client stating that the message has been sent (or not sent because the dest.com address does not exist in the DNS). In this example, the mail server behaves both as a server and as a client. The three processes in this scenario, namely the client, the mail server, and the DNS, are considered cooperative computing processes and may be running in three separate platforms on remote LANs connected by a WAN. Communication between these processes is called peer-to-peer communication. We will soon learn how network management fits into such a model and manages components on the network that perform cooperative computing using peer-to-peer

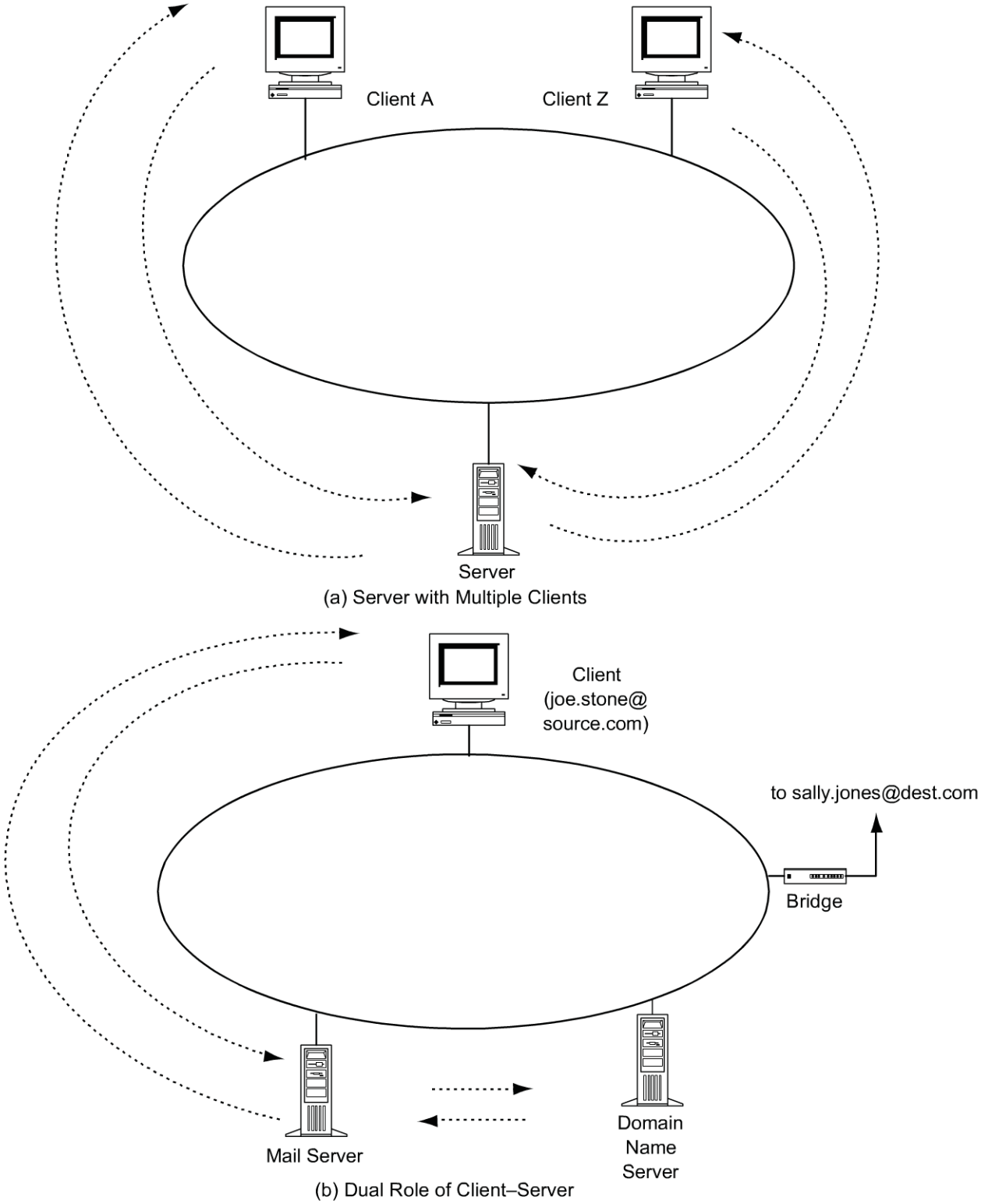


Figure 1.7 Client–Server in Distributed Computing Environment

communication. However, before we pursue that, let us first look at a new dimension that the DCE has caused networking to mushroom into—the Internet.

1.4 TCP/IP-BASED NETWORKS: INTERNET AND INTRANET

Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of protocols that enable networks to be interconnected. It forms the basic foundation of the Internet. Architecture and protocols are discussed in detail in Section 1.5. We will briefly describe the role TCP/IP plays in Internet. Nodes in the network route packets using network protocol, IP, a connectionless protocol. That means there is no guarantee that the packet will be delivered to the destination node. However, end-to-end communication can be guaranteed by using the transport protocol, TCP. Thus, if a packet is lost by IP, the acknowledgement process of TCP ensures successful retransmission of the packet.

TCP/IP suite of protocols contains more than TCP and IP protocols. TCP is a connection-oriented protocol. A complement to TCP is User Datagram Protocol (UDP), which is a connectionless protocol. Much of Internet traffic really uses UDP/IP due to the reliability of data transmission. For example, email and management messages are carried by connectionless transmission.

The Internet is a network of networks. Just as we can communicate over the telecommunication network using the telephone from anywhere to anywhere in the world today, we can now communicate worldwide over the computer network via email. We looked at the example of Joe Stone sending a message to Sally Jones in the previous section, Figure 1.7(b). Let us expand that example and visualize that Joe Stone, who is at the College of Computing building of Georgia Institute of Technology, is sending an email to Sally Jones at her home in Australia. Sally is connected to an Internet service provider, ostrich.com. Similar to a unique telephone number that each station has in the telephone world, each person has a unique address in the computer communication network. Joe's email address is joe@cc.gatech.edu and Sally's address is sally@ostrich.com.au.

Figure 1.8 shows an Internet configuration for our scenario. Assume that Joe is at Workstation A on LAN A sending the email to Sally at Workstation Z that is "teleconnected" to her Internet service provider's email server on LAN Z. Two servers shown on LAN A are mail server and DNS. It should be noted that the servers do not have to be on the same LAN as the sender's LAN, as shown in Figure 1.8. The two servers cooperatively transmit the email message to LAN C on the computer network made up of bridges and routers. The link between LAN A and LAN C could be a WAN. Information is transported exclusively based on TCP/IP-based protocols. We will explain TCP/IP protocol in Section 1.5.2.

Information from LAN C progresses via gateways and WANs to the computer communications network in Australia, as shown in Figure 1.8. The WAN network shown is composed of a series of networks, not all necessarily using TCP/IP protocol. Gateways between them serve as the interfaces between dissimilar and independent autonomous networks and perform many functions including protocol conversions. Autonomous networks have little knowledge of each other's attributes, configurations, and addresses and yet communication is automatically taken care of by a hierarchy of Internet servers along the path.

Joe's email message finally reaches the email server on LAN Z in Australia and is stored there until Sally retrieves it via her Internet link with an Internet service provider's server. In fact, email messages are transmitted by a "store-and-forward" scheme all along the path. In addition, the final stage in the Internet link uses a TCP/IP suite of protocols.

Thus, via the Internet, any user can communicate with any other user in any part of the world as long as both are connected to a network that is part of the Internet. This has also revolutionized the software user interface providing capabilities like web pages so that you can gather information about anything in the world instantly through the Internet.

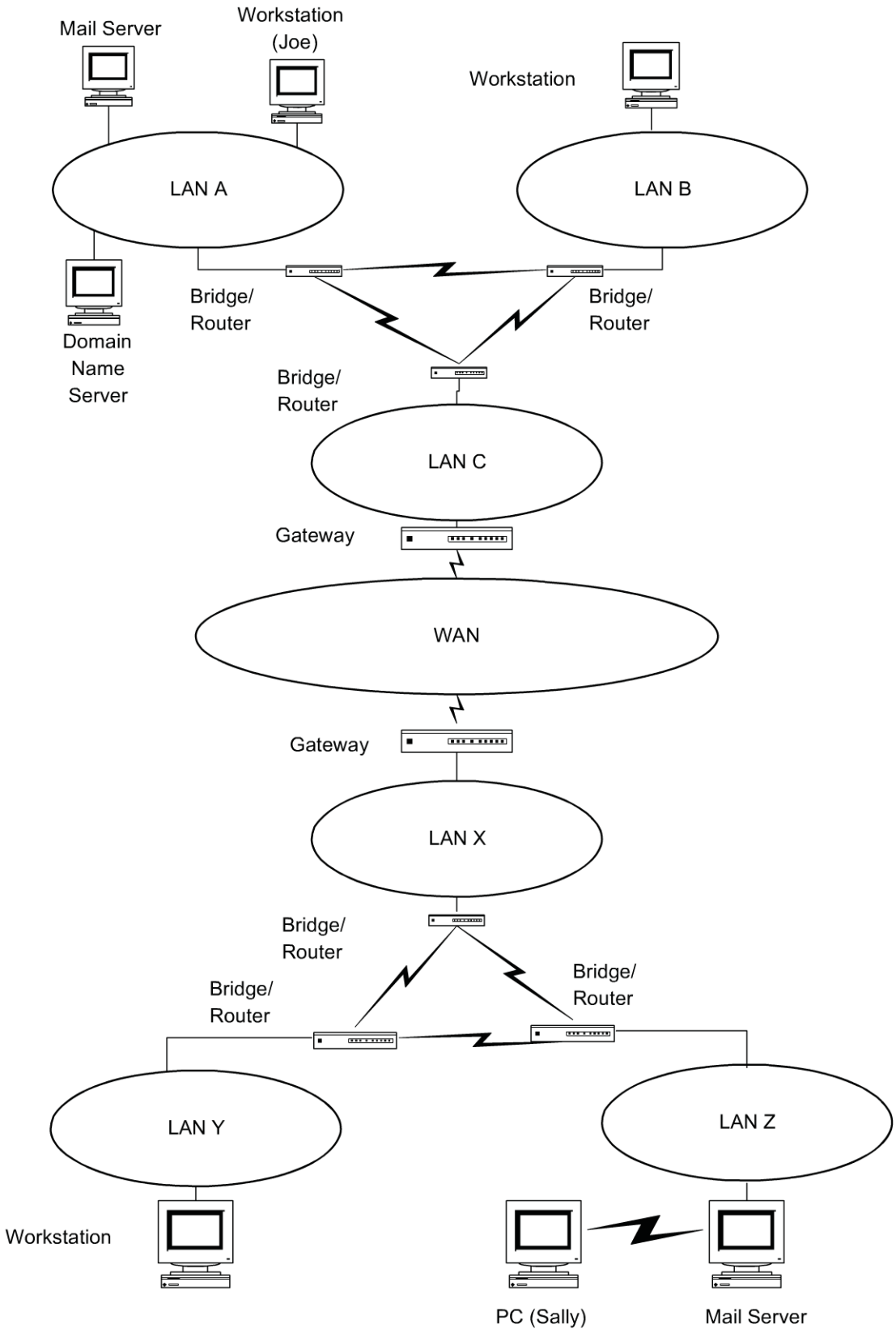


Figure 1.8 Internet Configuration

Another perspective of the Internet is to view it as a layered architecture, as shown in Figure 1.9. This architecture shows the global Internet as concentric layers of workstations, LANs, and WANs interconnected by fabrics of Medium Access Controls (MACs), switches, and gateways. Workstations belong to the user plane, LANs to the LAN plane, and WANs to the WAN plane. The interfaces are defined as the fabrics. MAC fabric interfaces the user plane to the LAN plane. LAN and WAN planes interface through switching fabric. WANs in the WAN plane interface with each other via the gateway fabric.

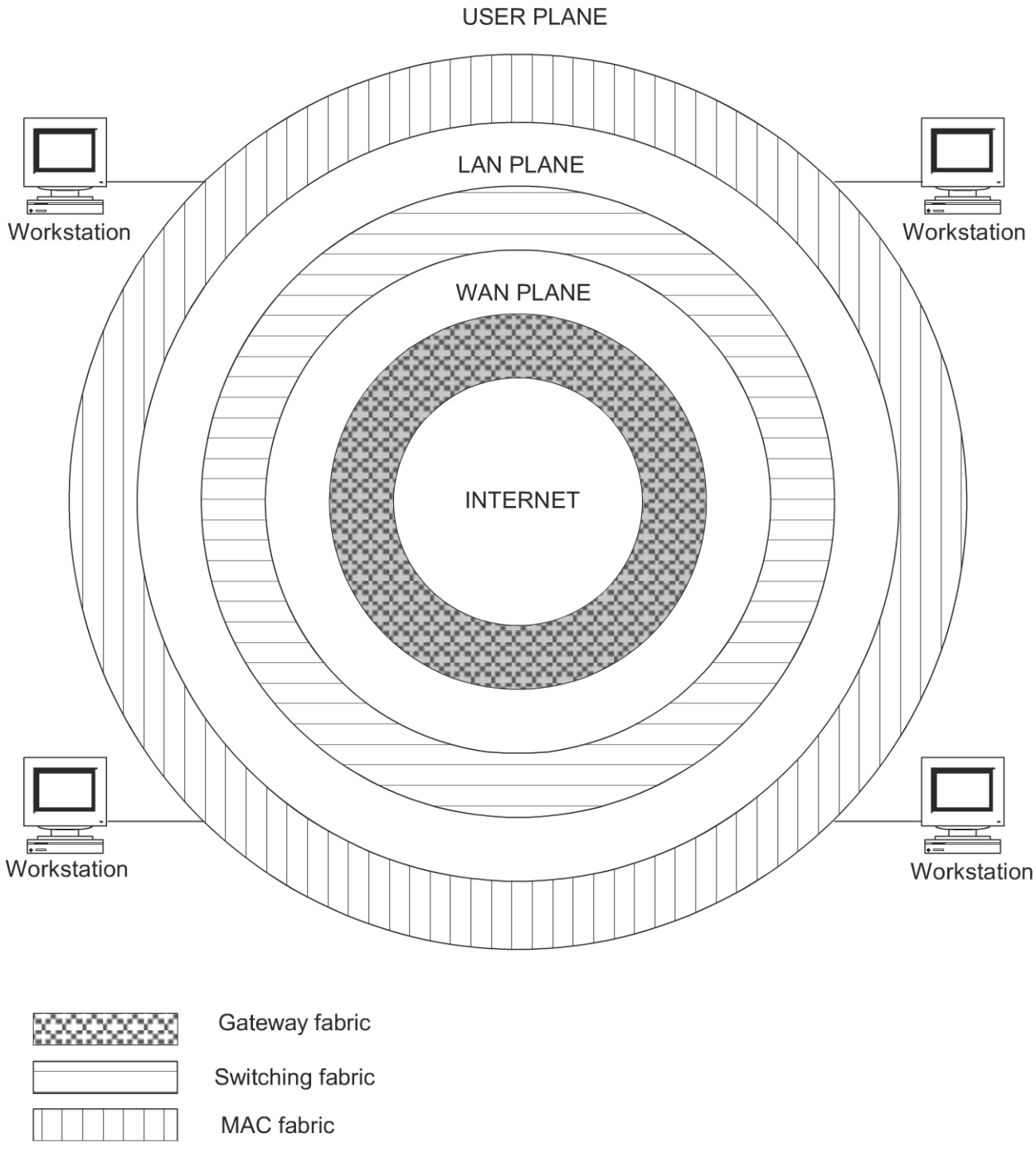


Figure 1.9 Internet Fabric Model

The user's workstation interfaces to a LAN via a MAC, which will be explained in Chapter 2. LANs interface to a WAN by a switching fabric of bridges, routers, and switches. Each WAN may be considered as an autonomous network, and hence needs a gateway to communicate with another WAN. Gateway fabric interconnects different WANs. Thus, a single Internet plane at the core of the model multiplies into millions and millions of users at the user plane, with virtually no limits in sight.

Communication between two users in the user plane, i.e., logical link connection on the user plane, takes the following path. The physical path traverses the MAC fabric, the LAN plane, the switching fabric, the WAN plane, and the gateway fabric to the core and then returns to the user plane going through all the planes and interface fabrics in reverse.

The huge success of Internet technology has spawned intranet technology. The main distinction between the two is similar to that between public and private switched networks. An intranet is a private network and access to it is controlled by the enterprise that owns it, whereas the Internet is public.

The impact of the Internet in networking is enormous. How do we manage the Internet? For example, if an email does not reach its destination, how do we detect where the communication broke down? How do we take advantage of Internet capabilities to implement network management? We have not yet defined network management and how it fits into the client–server environment. However, before we define what network management is, let us briefly look at the protocols and protocol architecture that enable successful communication between different components on the network.

1.5 COMMUNICATION PROTOCOLS AND STANDARDS

Consider a fax machine and a modem bought from a local store successfully sending a fax to a modem and fax machine anywhere in the world, even though each fax machine and attached modem were manufactured by local vendors. Likewise, isn't it a technological miracle that two computers located anywhere in the world can transmit messages to each other as long as each is connected to the Internet? The key to the practical success of these and other such technologies is the interoperability of the two end devices. More and more vendors in more and more countries have recognized that in this world of shrinking cyberspace and advancing modern communication technology, interoperability is the key to the success of their business.

Universal interoperability is achieved when all participants agree to establish common operational procedures. In communications lingo, commonality can be interpreted as standards and procedures as protocols. Let us consider the scenario of Joe sending an email from Georgia Institute of Technology (GA Tech) in Atlanta to a colleague in a Japanese Telecommunications Company (JTC) in Tokyo. Joe composes the message on his computer terminal and sends it to his colleague (yoho@jtc.com.jp). Joe's message with his user id (joe@cc.gatech.edu) and IP address (169.111.103.44) goes through several changes before it is transmitted on the physical LAN medium at GA Tech. The message goes to its College of Computing (cc)'s email server, which obtains the IP address of the destination and sends the message out on the Internet. The message traverses several nodes and links and arrives at the post office box of Yoho's mail server at JTC. She establishes a session in her computer and gets the complete message that Joe transmitted. In this scenario, Joe's message is wrapped with several layers of control information at various times and is broken down into packet units and reassembled at the destination. All these steps happen each time without any loss or error in the message due to standardization and modular (layered) architecture of data communication protocols. As we will soon learn in this section, the popularity of Internet as a peer-to-peer network has been made possible by the peer-to-peer protocol TCP/IP suite.

Architecture can be defined as modeling a system into functional components and the relationship among them. Thus, communication architecture describes the functional components of communication network as well as the operational interface between them. Operational procedures—both intra- and inter-modules—are specified in terms of protocols. Just as human communication is made mutually understandable by speaking a common language, communication protocols are standardized for service interfaces from the perspectives of both a service provider and a service user. If different vendors implement the same standards in their system components, then communication between their different components can be universal. Standardization of protocols involves agreement in the physical characteristics and operational procedures between communication equipment providing similar functions. Thus, looking at our example, all fax machines are able to communicate with each other because all vendors have implemented standards recommended by International Telecommunication Union—Telecommunications Sector (ITU-T). Similarly, email exchange across the world is possible because most vendors have adopted Internet standard Simple Mail Transport Protocol (SMTP) in their software. However, there are email software packages other than SMTP, and the user has to install a gateway in those systems to convert back and forth between SMTP and the vendor-specific proprietary protocol. For example, IBM Lotus uses cc:mail (now defunct), and any network that uses cc:mail has to implement a gateway to send an email over the Internet. Note that there are different mail protocols (SMTP, IMAP, POP, etc.), which have different procedures. We will now look at the details of communication architecture.

1.5.1 Communication Architectures

Communication between users (human beings using a system) and applications (programs that run in a system) occurs at various levels. They can communicate with each other at the application level, the highest level of communication architecture. Alternatively, they can exchange information at the lowest level, the physical medium. Each system can be broadly subdivided into two sets of communication layers. The top set of layers consists of application layers and the bottom set transport layers. The users—and users include application programs—interface with the application level layer, and the communication equipment interfaces with the physical medium. The basic communication architecture is shown in Figure 1.10. In Figure 1.10(a), the two end systems associated with the two end nodes communicate directly with each other. Direct communication occurs between the corresponding cooperating layers of each system. Thus, transport layers can exchange information with each other, and so can the application layers and the users.

This can be illustrated with a real-life example. A hearing-impaired person, accompanied by an interpreter, attended one of my classes. As I lectured, the interpreter translated to the student using sign language. If the student had a question, the interpreter translated the information from sign language, orally to the class and me. In this illustration, the hearing-impaired student and I are at the application layer. The interpreter did the protocol conversion at the application layer level. The transport layer is the aural and visual media.

Figure 1.10(b) shows the end systems communicating via an intermediate system N, which enables the use of different physical media for the two end systems. System N converts the transport layer information into the appropriate protocols. Thus, system A could be on a copper wire LAN and system Z could be on a fiber optic cable.

Various standard organizations propose, deliberate, and establish standards. One of the internationally renowned standard organizations is International Standards Organization (ISO). ISO has developed a highly modular, or layered, architecture for communication protocols that is called the Open Systems

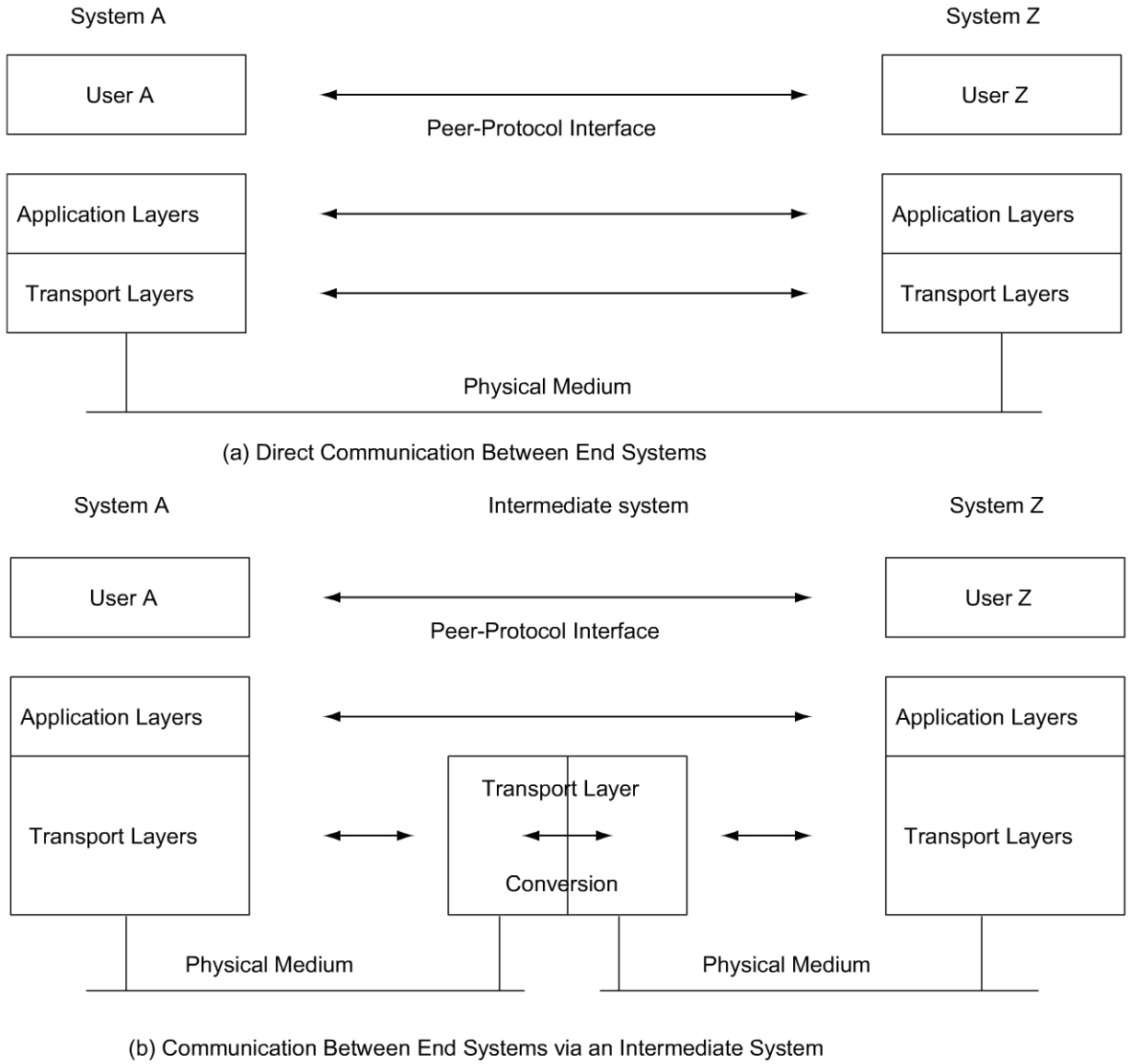


Figure 1.10 Basic Communication Architecture

Interconnection (OSI) Reference Model, published as OSI RM—ISO 7498. This model was developed based on the premise that the different layers of protocol provide different services; and that each layer can communicate with only its own neighboring level. Two systems can communicate on a peer-to-peer level, that is, at the same level of the protocol. The OSI protocol architecture with all seven layers is shown in Figure 1.11. Table 1.1 describes the salient features of, and services provided by, each layer. Layers 1–4 are the transport system protocol layers and layers 5–7 are application support protocol layers.

OSI protocol architecture truly enables building systems with open interfaces so that networks using systems from different vendors are interoperable. Figure 1.12 expands the basic communication architecture shown in Figure 1.10 to an OSI model. Figure 1.12(a) is a direct end-to-end communication model. The corresponding layers in the two systems communicate with each other on a peer-to-peer protocol interface associated with those layers. In Figure 1.12(b), the end systems communicate with each other by going through an intermediate node/system. Again, notice that the physical media

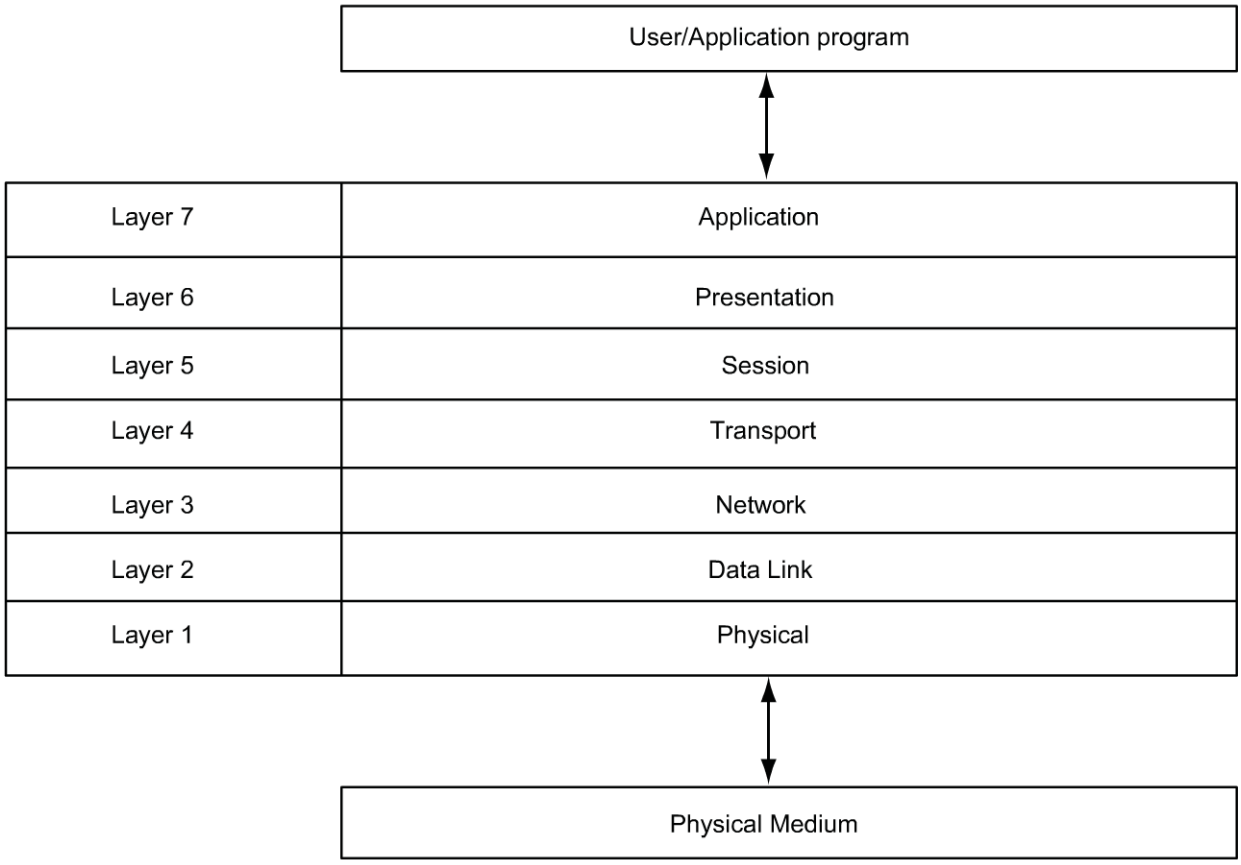


Figure 1.11 OSI Protocol Layers

connected to the end systems could be different. The intermediate system is involved only up to the first three layers in the process. Layers 4–7 are not involved in the intermediate system. This is analogous to a mail container with letters enclosed in envelopes being transported from one town to another town anywhere in the world. It does not matter what network of intermediate cities (nodes) it goes through, or what network of transportation media—surface, air, or water—it takes to get to the destination. The letter in the envelope and contents of packages are untouched at the transfer points and are only handled by the sender and the receiver, i.e., user applications.

The message in each layer is contained in message units called protocol data unit (PDU). It consists of two parts—protocol control information (PCI) and user data (UD). PCI contains header information about the layer. UD contains the data that the layer, acting as a service provider, receives from or transmits to the upper layer/service user layer. The PDU communication model between two systems A and Z, including the users at the top and the transmission medium at the bottom of the PDU layers, is shown in Figure 1.13. As you can see, the size of the PDU increases as it goes towards lower layers. If the size of the PDU exceeds the maximum size of any layer specifications, it is then fragmented into multiple packets. Thus, a single application layer PDU could multiply into several physical PDUs.

1.5.2 Protocol Layers and Services

We will now go into some detail regarding services provided by the seven layers of OSI protocols.

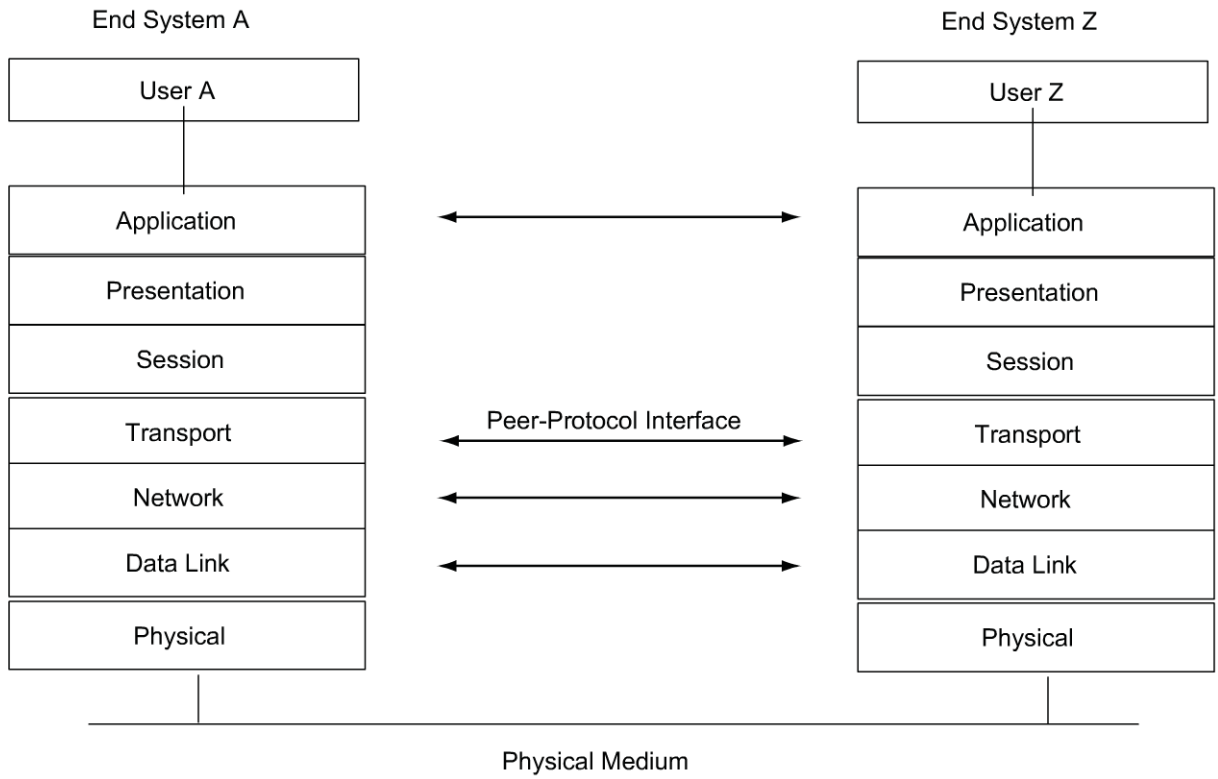
Table 1.1 OSI Layers and Services

LAYER NO.	LAYER NAME	SALIENT SERVICES PROVIDED BY THE LAYER
1	Physical	–Transfers to and gathers from the physical medium raw bit data
		–Handles physical and electrical interfaces to the transmission medium
2	Data link	–Consists of two sublayers: Logical link control (LLC) and Media access control (MAC)
		–LLC: Formats the data to go on the medium; performs error control and flow control
		–MAC: Controls data transfer to and from LAN; resolves conflicts with other data on LAN
3	Network	Forms the switching/routing layer of the network
4	Transport	–Multiplexing and de-multiplexing of messages from applications
		–Acts as a transparent layer to applications and thus isolates them from the transport system layers
		–Makes and breaks connections for connection-oriented communications
		–Data flow control in both directions
5	Session	–Establishes and clears sessions for applications, and thus minimizes loss of data during large data exchange
6	Presentation	–Provides a set of standard protocols so that the display would be transparent to syntax of the application
		–Data encryption and decryption
7	Application	–Provides application-specific protocols for each specific application and each specific transport protocol system

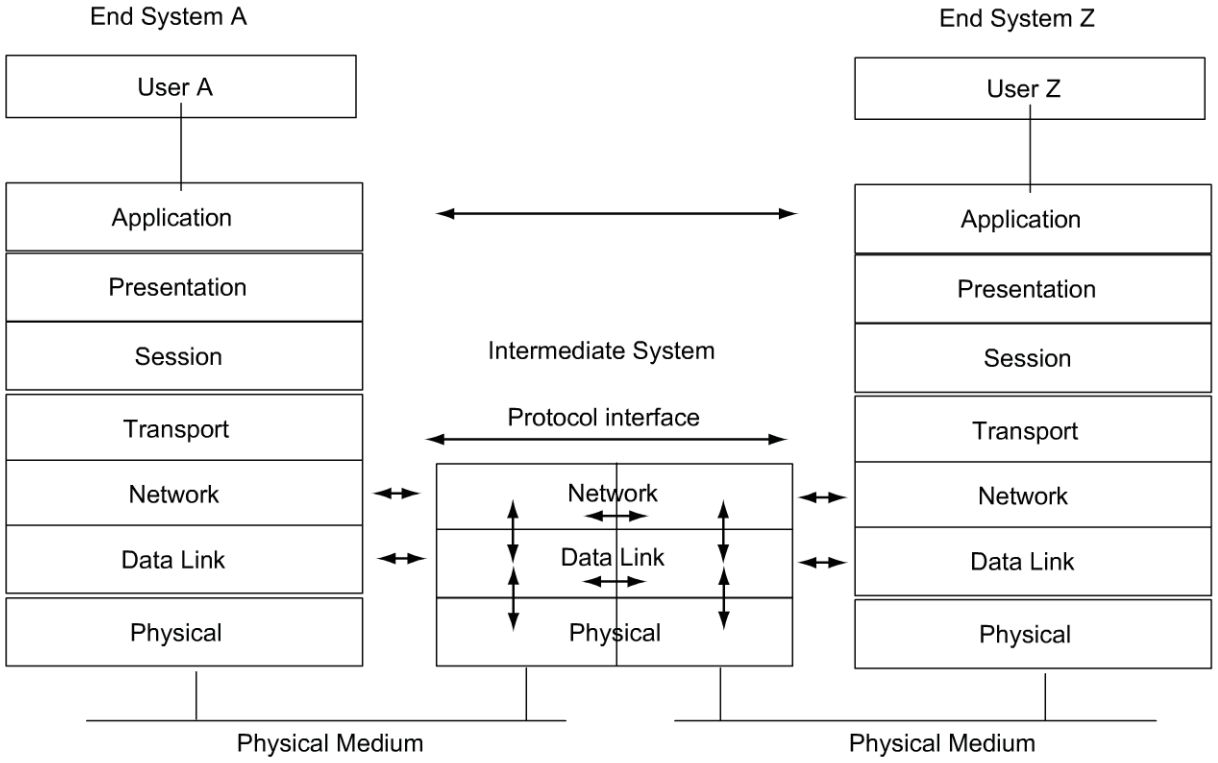
Layer 1, physical layer, is responsible for physically placing the electrical signal on the physical medium and picking up the signal from it. It controls and manages the physical and electrical interfaces to the physical medium including the connector or the transceiver. The physical medium could be copper in the form of a twisted pair or coaxial cable, optical fiber, or wireless media such as radio, microwave, or infrared. The signal could be either analog or digital. There are various protocol standards for a physical-layer interface depending on the transmission medium and the type of signal. The two classes of standards have been established by ITU-T and Electronics Industries Association (EIA).

Layer 2 is the data link control layer, or data link layer for short. Data communication between two DTEs is controlled and managed by this layer. Note that in contrast to a byte-oriented transmission across a computer bus, the data communication is a serial-bit-oriented stream. The data link layer needs to do basic functions: first establish and clear the link, and second transmit the data. Besides these, it also does error control and data compression. Flow control on data link layer is done on a hop-to-hop basis.

For point-to-point communication using a dedicated facility, like the loop link from a customer telephone to the telephone company switching office, the data link control is simple and straightforward to implement. However, if the DTE is connected to a LAN, or which is shared transmission media and is



(a) Direct Communication Between End Systems



(b) Communication Between End Systems via Intermediate System

Figure 1.12 OSI Communication Architecture

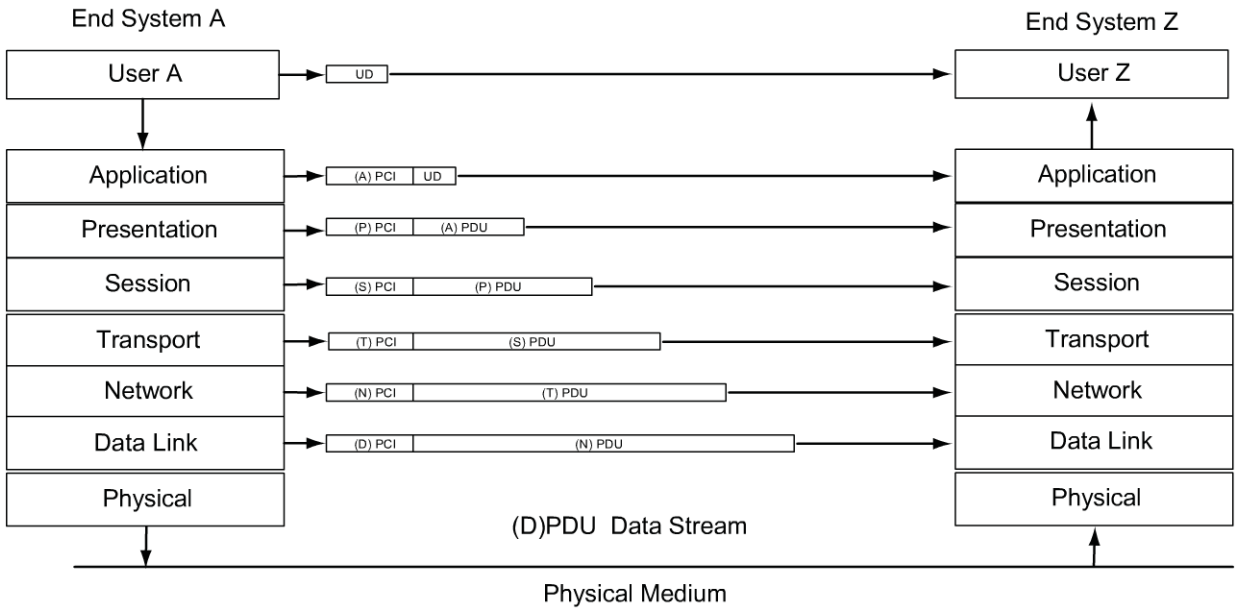


Figure 1.13 PDU Communication Model between End Systems

accessed simultaneously by many users, then the data link control becomes more complex. In the case of point-to-multipoint transmission, the head end controls the access of the medium. LAN is a distributed environment and thus access control is distributed. In an OSI-layered model, the data link layer is divided into two sublayers—logical link control (LLC) and media access control (MAC), as shown in Figure 1.14. The lower MAC layer controls the access and transmittal of data to the physical layer in an algorithmic manner. There are three basic types of LANs. Ethernet LAN is a bus type and the media is accessed using a distributed probabilistic algorithm, Carrier Sensing Multiple Access with Collision Detection (CSMA/CD). The second type of LAN is a ring type used in token ring (TR) and Fiber Distributed Data Interface (FDDI). A deterministic token-passing algorithm is used in this case. The third type of LAN is deployed in wireless medium and is referred to as wireless LAN or WLAN. The probabilistic algorithm, Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA), is used to access the medium. Random-access protocol will be covered in Chapter 2.

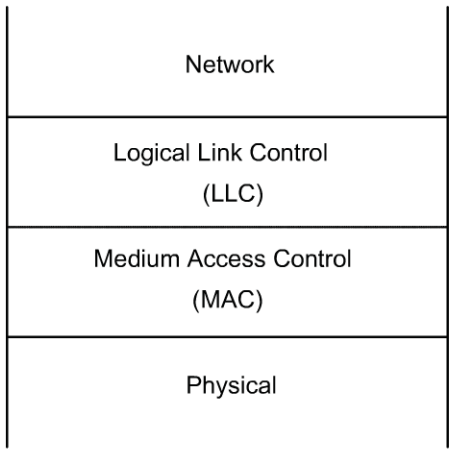
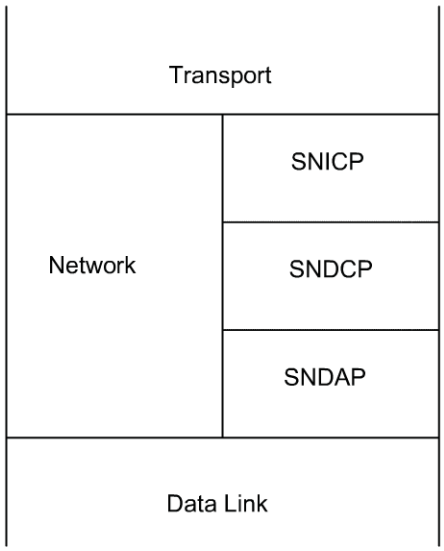


Figure 1.14 Sublayer Structure of a Data Link Protocol Layer

LLC performs link management and data transfer. Link management includes formatting the data to go on the medium, performing error control, and flow control. If there is security required, it could be included in the LLC sublayer.

The network layer is the third layer in the OSI protocol stack. It controls and manages the switching fabric of the network. It provides both connectionless network service (CLNS) and connection-oriented network service (CONS). The former is used when lower layers are highly reliable, such as LANs and bridges, as well as when messages are short. CONS is the method for transmitting long messages, such as file transfer. It is also used when the transmission medium is not reliable. It subdivides the transport PDUs into frames of appropriate size based on transmission parameters. The destination address of each packet is read in both CLNS and CONS at the network layer and routed on the appropriate link.

A router, or a routing bridge, at the nodes of a network performs the function of routing and switching data. Any subnetwork of the node is under the control of that router. The subnetwork(s) can be anything from a simple-single segment LAN to complex subnetworks operating under a proprietary protocol. OSI architectural model handles this by dividing the network layer into three sublayers as shown in Figure 1.15. The top sublayer is the Subnetwork-Independent Convergence Protocol (SNICP) layer that interfaces to the transport layer. The Internet communicates between nodes using Internet address and SNICP. The nodes in turn communicate with subnetworks using the Subnetwork-Dependent Convergence Protocol (SNDCP), which depends on the subnetwork protocol and could be any proprietary protocol. In such a situation, the SNDCP communicates with its data link layer via the third network sublayer, the Subnetwork-Dependent Access Protocol (SNDAP). This subnetwork architecture isolates transport and the above layers from the subnetwork dependencies. It also enables communication between a DTE on the Internet and a DTE on a subnetwork node, as shown in Figure 1.16. Figure 1.16(a) depicts network configuration in which DTE-A connected to end node A communicates with DTE-N1 connected to subnetwork node N1 via the intermediate system gateway node N.

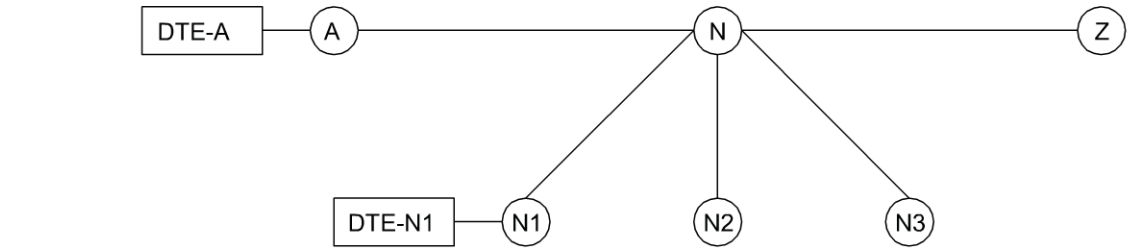


SNICP: Subnetwork-Independent Convergence Protocol

SNDCP: Subnetwork-Dependent Convergence Protocol

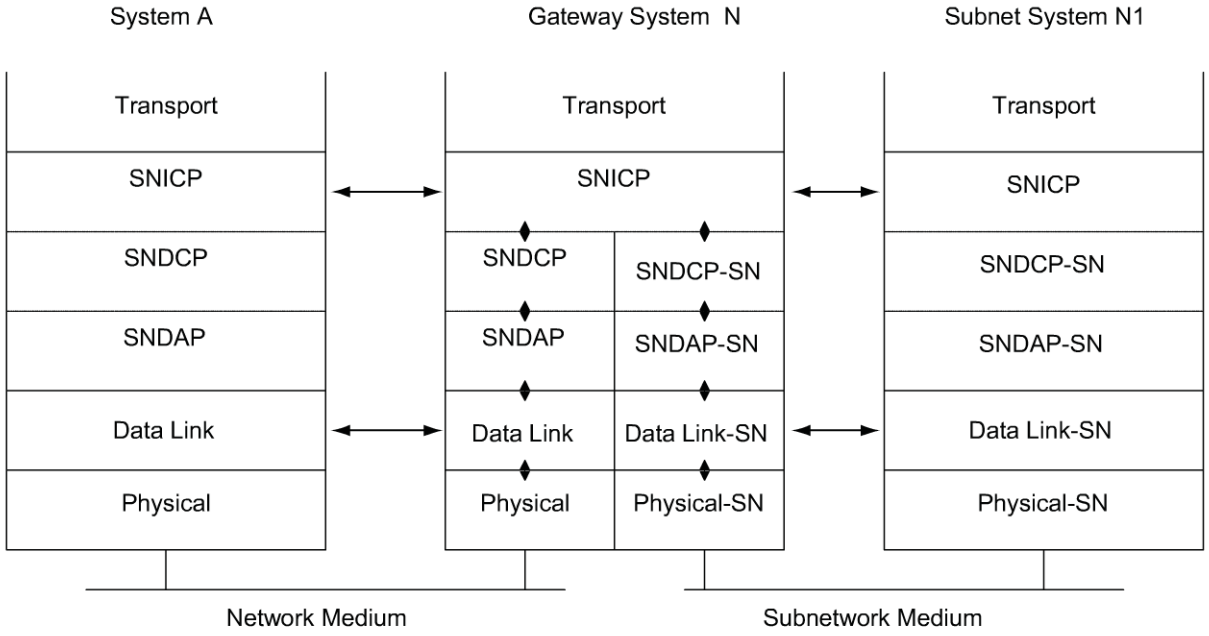
SNDAP: Subnetwork-Dependent Adapter Protocol

Figure 1.15 Sublayer Structure of a Network Protocol Layer



A–N–Z Standard Network
N–N1–N2–N3 Subnetwork Under Node N

(a) Network Configuration



(b) Protocol Communication

Figure 1.16 Gateway Communication to Private Subnetwork

Figure 1.16(b) describes the path of communication through different protocol layers from the originating end system to the terminating end system via the intermediate node gateway. The formats of the PDUs are identical in all three systems at SNICP layer levels and above. Access networks having their own addressing scheme using Network Address Translator (NAT) or Dynamic Host Configuration protocol (DHCP) can be implemented using this scheme.

The most used network protocol is the Internet Protocol (IP) and has been popularized by the Internet. It is part of the Internet suite of the TCP/IP and is a CLNS protocol. In OSI terminology, it is called ISO-IP or ISO CLNP. A connection-oriented OSI protocol is X.25 PLP, Packet Layer Protocol.

A popular scheme of implementing private subnetwork is to establish a network with a private IP address, such as 10.x.y.z. In this instance, the gateway node, known as NAT, converts the global IP address to the local proprietary IP address, for example, LAN Z in Figure 1.8.

The transport layer is the fourth layer of the OSI protocol. It multiplexes the UD provided by application layers and passes packets to the network layer. Its service is independent of the network on which

the packets are transmitted. The transport layer can again be connectionless or connection oriented and is implemented in both Internet and OSI protocols. As mentioned earlier, TCP is a component of the IP suite and is connection oriented. The connectionless transport protocol in a TCP/IP suite is called the UDP. Flow control is also implemented in transport layers and functions as data rate manager between application programs and the network layer. ISO has five transport layer specifications, TP0 to TP4. TP4 is analogous to TCP.

Layers 5–7 are application layer protocols. Except in the OSI Reference Model, the three application layers are not clearly separated and independent. Let us look at each layer as if they were independent, like in the OSI model, to understand their specific functions and services provided. An application process communicates with another application process during a session. The session layer services establish communication at the beginning of the session, monitor, synchronize, and error correct the information exchanged during the session, and then release the logical link at the end of the session. It is very strongly related to the presentation layer, which is the medium of presentation of the context of the message to the user or application program. In that sense, the presentation layer is a context-sensitive layer. It can be interpreted as the common language and image that the users at both ends of the system use and understand—shared semantics of the two end users. A common abstract syntax that is used for semantics is Abstract Syntax Notation Number One (ASN.1). Although the primary function of the presentation layer is the conversion of syntax, data encryption and data compression are also generally done in that layer.

The top and the seventh protocol layer is the application layer. The application process interfaces with the application support processes that are provided by this layer. Like the other two layers in the set of application layers (session and presentation), it is strongly coupled with the rest of the application layers. In the OSI Reference Model, one can separate these processes from the presentation and session layers, but in other models there is no clear distinction of the functions. Figure 1.17 presents a comparison of the models—OSI Reference Model and Internet model.

The Internet model does not specify the two lower layers although it is obvious that they use distributed LAN and WAN configurations. The transport and network layers form the suite of TCP/IP protocols that we mentioned earlier. Application layers are combined into application-specific protocols.

Figure 1.18 shows a comparison of four common application-specific protocols in OSI and Internet models. There are more OSI application-specific protocols, which we will not discuss here. All application-specific protocol services in OSI are sandwiched between the user and presentation layers. In the Internet model, they are sandwiched between the user and the transport layer. The boxes on the right-hand side of Figure 1.18 describe the comparable services offered in the two models. A user interfaces with a host as a remote terminal using Virtual Terminal (VT) in the OSI model and TELNET in the Internet model. File transfers are accomplished using File Transfer Access and Management (FTAM) in the OSI model and File Transfer Protocol (FTP) in the Internet. The most common used mail service function in the Internet is Simple Mail Transfer Protocol (SMTP). A similar protocol in the OSI model is the Message-Oriented Text Interchange Standard (MOTIS). Network management is accomplished using the Common Management Information Protocol (CMIP) in the OSI model and the Simple Network Management Protocol (SNMP) in the Internet. We will extensively discuss the details of SNMP in this book. CMIP is briefly discussed in Appendix for completeness. However, it is important to understand the overall picture of protocol layers and other application protocols to appreciate network management functions that are accomplished using network management protocols.

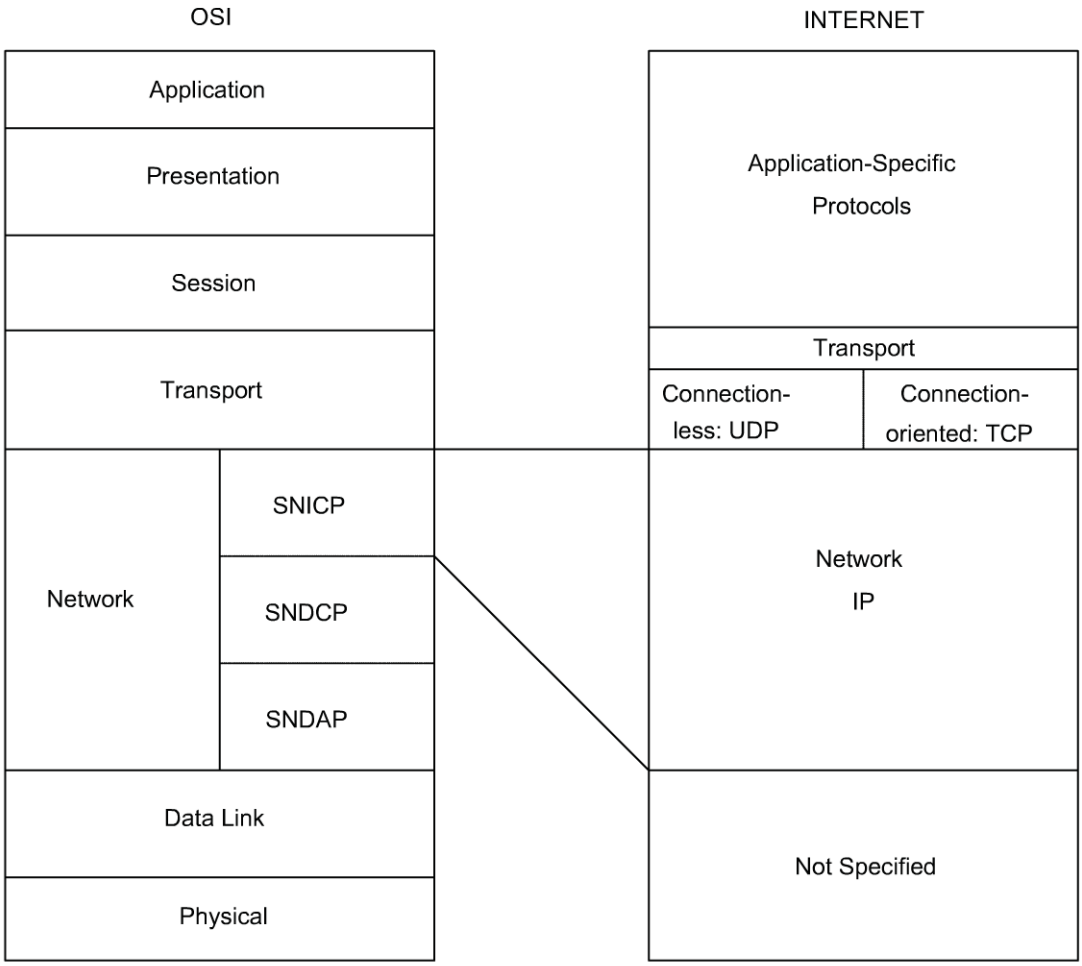


Figure 1.17 Comparison of OSI and Internet Protocol Layer Models

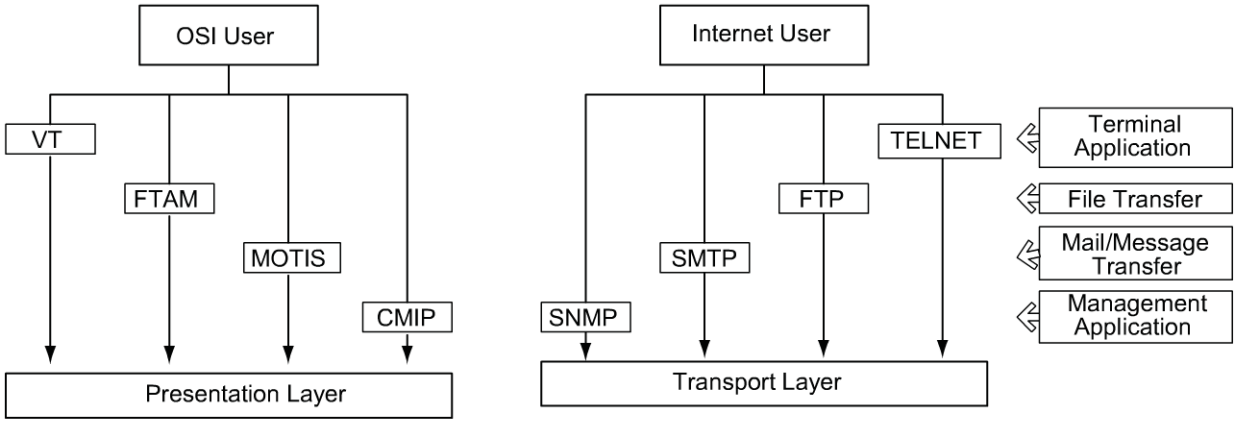


Figure 1.18 Application-Specific Protocols in OSI and Internet Models

1.6 NETWORKS, SYSTEMS, AND SERVICES

We described a network comprising nodes and links in Section 1.2. The physical embodiment of a network can be defined as a system. Thus, the nodes and links are components of a network system. Just as

a network can be subdivided into subnetworks, a system comprises subsystems. A system or subsystem is made up of network elements. Network elements can be either active or passive. Thus, a router is an active network element, whereas a splitter or a combiner that divides or combines signal energy is a passive element. A link could also be an active or a passive component. In the case of an active transmission link, it can be subdivided into active nodes and passive transmission media.

Services are functions that users derive out of networks and systems. Networks and systems exist to provide service to the users. Service providers provide telecommunication services to subscribers and customers using networks and systems.

1.6.1 Broadband Networks, Systems, and Services

A broadband communication system can be defined as one that provides broadband service to homes and enterprises. The common interpretation of this definition in practice varies in different countries as well as among various service providers. In the most comprehensive definition of the term, we will define broadband communication system as one that provides voice, video, and data services over the same medium to customer premises. Broadband service comprising audio, video, and data is also known as multimedia service.

Audio service includes telephone, telephone conference, and radio broadcast. Although the end terminals could be either analog or digital devices, information is carried digitally in the context of broadband service. A system providing this service is truly a real-time information system.

Video service includes broadcast television, interactive television, video-on-demand, and video conference services. Video service could be either real-time or quasi (near) real-time service. Once again, the presentation could be on either analog or digital terminals.

Data service includes numerous applications, which can be classified into three categories: store-and-forward, audio streaming, and video streaming. Some examples of store-and-forward service are email, messaging, and Web-based applications. Audio and video broadcast and streaming services mentioned above such as MP3 and video-on-demand can in a sense be considered under this category. They are not sensitive to absolute delay time between the source and the destination, but are affected by delay variations or jitter.

Broadband services are provided using broadband networks. There are numerous types of networks to choose from depending on what segment and what type of service one needs. It is like ordering ice cream in an ice-cream parlor—cone or cup, hard or soft, size small/medium/large, choice of flavor, choice of topping, etc.

The three segments of broadband network are WAN, broadband access network, and CPE network. In broadband terminology, the CPE network is also called home network when the customer premises is a residence. Network segments and choices in various segments are shown in Figure 1.19.

The WAN and access network interface with each other via the edge router. The demarcation point between the access network and CPE network is shown as the residential gateway. Although this is the logical demarcation point, the physical demarcation point between the access network of the service provider and the customer-owned CPE, or home network, could be different. As an example in the cable network, the demarcation point is called Network Interface Unit (NIU) or Network Interface Device (NID) and is the physical termination of the cable access network outside the house. The residential gateway may or may not exist, and if it does, it is a part of CPE network.

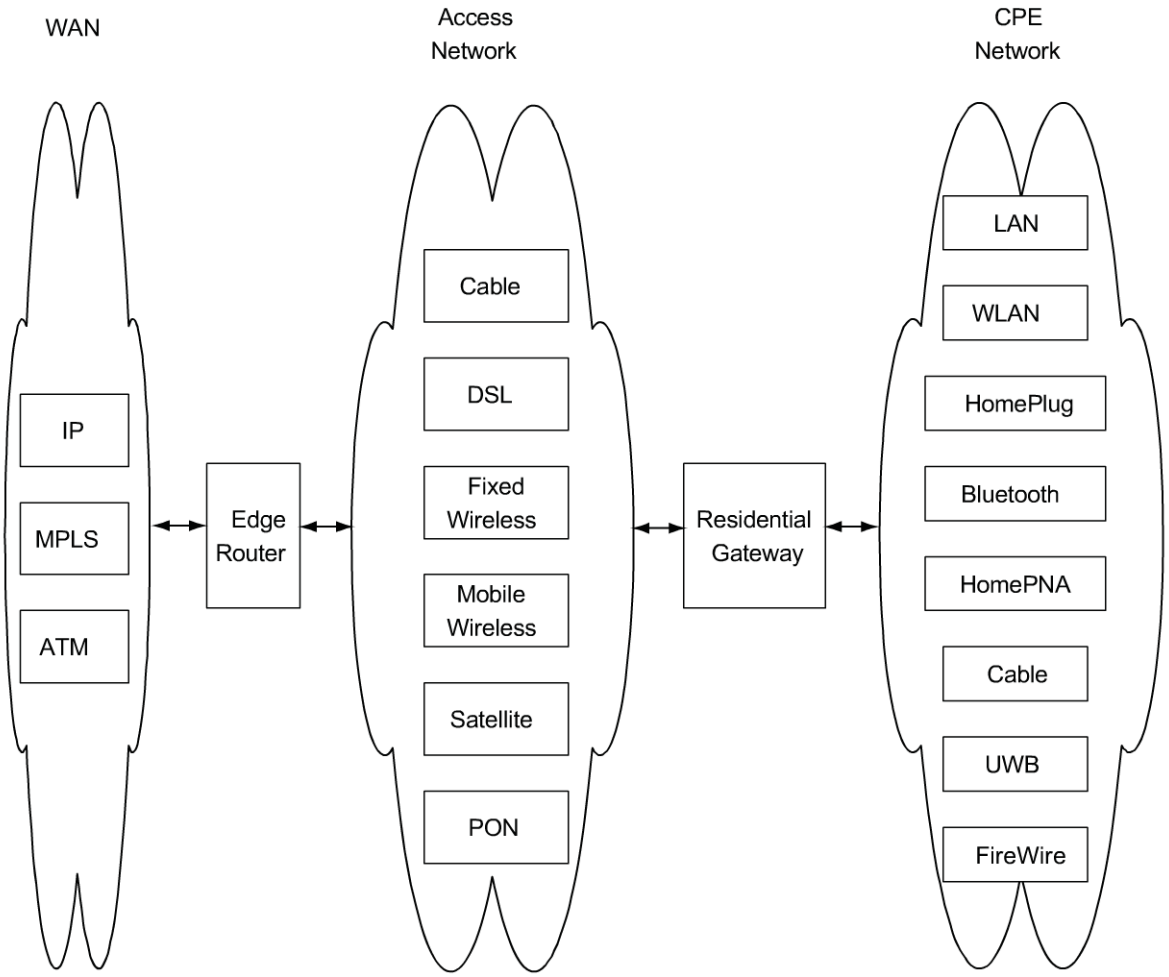


Figure 1.19 Broadband Network Segments and Technologies

1.6.2 Wide Area Networks

The four leading networks and protocols that are used in broadband WAN are Internet using Asynchronous Transfer Mode (ATM), Synchronous Optical Network (SONET), IP, and Multiprotocol Label Switching (MPLS) network.

ATM network: ATM network is ideally suited for WAN or core network. It has fast layer 2 switches that can be configured to function in parallel and thus can process high data rate cell-oriented packets. Latency can be set in ATM switches by setting priorities to the different services—real-time and non-real-time—being provided. Further, traffic performance is increased by establishing Virtual Path–Virtual Circuit (VP–VC).

Four classes of traffic have been defined in ATM network to implement quality of service. Constant bit rate (CBR), real-time variable bit rate (VBR-RT), non-real-time variable bit rate, (VBR-NRT), and available bit rate (ABR) or user bit rate (UBR). Transmission of voice is assigned CBR. An example of VBR-NRT is transmission of still images. Data traffic and store-and-forward traffic get the lowest priority, ABR.

SONET: An optical fiber medium can be used to carry multiplexed lower bandwidth signals implementing SDH. This mode of transmission is known as SONET. The optical transmission network

contains regenerators, digital cross-connect elements, and add-and-drop multiplexers (ADM). Modern optical networks use dense wavelength division multiplexers (DWDM) and very high bandwidth signals can be transmitted through this optical network.

Internet: The Internet backbone WAN using IP is highly matured, has a full set of application-oriented features, and can interface with access and CPE network in a more seamless manner. However, its main drawback is that it is difficult to meet quality-of-service requirements needed for multimedia broadband service. Because of its variable packet size and packets choosing possible alternate paths between the source and the destination, the performance of routers and other transmission devices is not as efficient as in an ATM network.

Quality of service in IP-oriented WAN traffic is improved by implementing one of two different approaches. They are integrated service [RFC 2205] and differentiated service [RFC 2474]. In one form of implementation, *Intserv* packets in the Internet are classified into three classes: guaranteed, controlled or predictive, and best effort. *Intserv* reserves bandwidth from the source to the destination on a per-flow basis for a guaranteed class-of-service call or session using reservation protocol, RSVP. Once the reserved path with the necessary bandwidth is established, data are transmitted. The bandwidth is released after the call/session is completed. *Intserv* is not an efficient scheme for establishing quality of service in the backbone network as there is no guarantee that the resources will be available when needed. Further, the scheme does not scale well.

In the differentiated service, *diffserv*, packets belonging to the same class are grouped at each hop and then prioritized. There are four classes and each class has three subclasses for dropping packets—low, medium, and high. The present trend in providing quality of service for backbone is to use differentiated service complemented with some form of reservation capabilities of RSVP.

MPLS network: MPLS attempts to combine the benefits of ATM quality of service with feature benefits of the IP-based Internet. Conventional routers examine the packet headers and classify them into forwarding equivalence classes (FEC). They are then assigned the next hop. In MPLS this is done once, possibly at the ingress router, and a label is attached to it. At each router, only the label lookup is done for determining the next hop. Label lookup can also be done using a switch. A router that supports MPLS is known as a Label Switching Router (LSR). MPLS can support any network layer protocol. RFC 3031 describes MPLS architecture for an IP network layer protocol.

1.6.3 Broadband Access Networks

Figure 1.20 shows six types of broadband access networks that provide broadband service to homes, Small Office Home Office/Small and Medium Enterprise (SOHO/SME), and enterprises. The core network is IP/ATM/MPLS WAN. The link from the head end or the edge router to business customers is shown as an optical carrier-n (OC-n) link, although it could be any other transport scheme. Hybrid fiber coax (HFC) cable network and Digital Subscriber Line (DSL) network are the matured access networks. Fixed wireless is being offered as point-to-multipoint service or meshed network, WiMax, to metropolitan areas. Mobile wireless could be offered using either 3G technology or wireless LAN. The former has the limitation on data rate and the latter on range. Fiber network as Passive Optical Network (PON) is still in an embryonic stage for economic reasons.

Cable Access Network has its head end interfacing to the edge router. Analog and digital signals from various services are multiplexed at the head end and are converted from an electrical signal to optical wavelength signals. The optical signal is then carried over fiber up to an intermediate point, optical node, where it is down-converted to radio frequency and transmitted the rest of the way to the customer

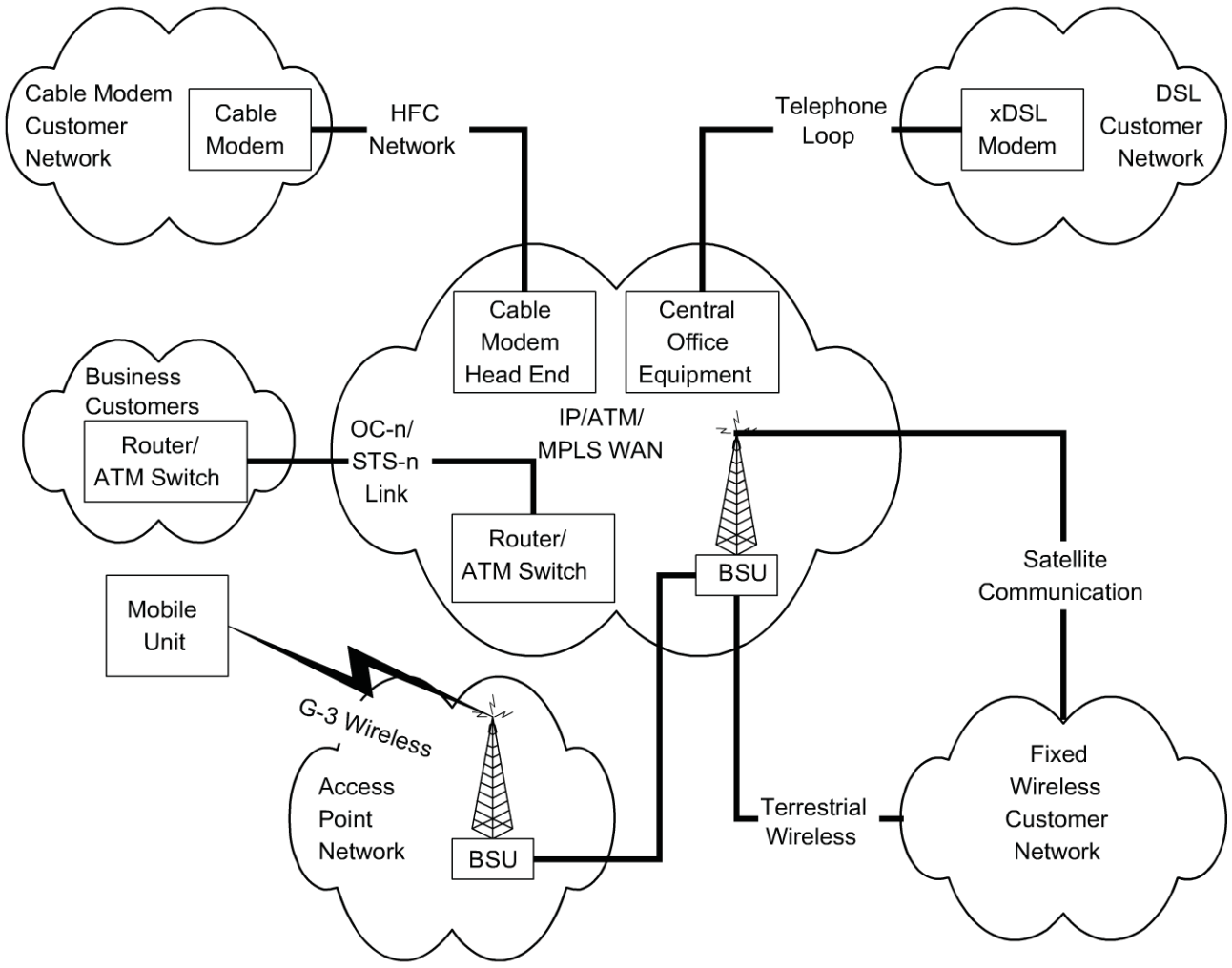


Figure 1.20 Broadband Access Networks

premises over two-way coaxial cable, hence the term hybrid fiber coax (HFC). At the customer premises, the TV analog signal is split from the digital data. The latter is demodulated to a baseband digital signal using a cable modem and is fed to the digital devices, such as computer and appliances.

Digital Subscriber Line access network uses a telephone line and can be deployed using different implementations, referred to as XDSL. Of these, Asymmetric DSL (ADSL) shown in Figure 1.20 is the most prevalent deployed all over the world. Although cable network is more commonly used in the United States by a ratio of approximately 2 to 1, the reverse is the case in the rest of the world. The technology uses the existing unshielded twisted-pair (UTP) wire that carries the **analog** voice to transmit data in addition to voice. The voice is carried as an analog signal at the low end of the frequency spectrum (0–4 kHz) and the digital data over the higher band of the spectrum. It is termed asymmetric as the downstream data rate (from the central office to customer premises) is much higher than the upstream (from customer premises to the central office) data rate. The analog voice and digital data are separated at both ends of the access network using a filter, and the digital data are modulated and demodulated at both ends using ADSL modems. At the central office, voice circuit interfaces with the central office switch and the digital data with the edge router.

Wireless Access Networks: Figure 1.20 shows three types of wireless access networks. The terrestrial wireless network, also known as fixed wireless, is a point-to-multipoint transmission. A base station with multiple antennas covers multiple sectors, each serving many subscribers. The two well-known deployed technologies are Multichannel Multipoint Distribution Service (MMDS) for rural areas and WiMax for urban areas. Satellite wireless systems are primarily used for one-way television broadcasting service. Mobile wireless has limited bandwidth and is currently used in phones such as smart phones, providing broadband service.

1.6.4 Home/CPE Networks

CPE network in enterprise environment is either an IEEE 802.3-based Ethernet LAN or IEEE 802.11-based wireless LAN, also known as WiFi, or a hybrid of both. Home network provides the opportunity to utilize multiple technologies besides Ethernet LAN and WiFi. HomePNA is implemented using twisted-pair telephone cable medium, HomePlug takes advantage of power line wiring in the house, and cable utilizes the television coaxial cable. FireWire is also a wired medium and is based on IEEE 1394 protocol to transmit high-speed digital data. Universal Serial Bus (USB) is used for low data rate peripherals. Wireless home network technologies include Bluetooth and ultra-wide band (UWB) personal area networks (PANs) for short distances.

1.6.5 Quality of Service in Broadband Systems

Quality of service could be interpreted in technical terms in many different ways. However, from the users' point of view, people are used to reliable, dependable, and good quality analog telephone and television service. They expect the same quality of service when the telecommunication and cable services are extended to broadband service that includes voice, video, and data. Networking technology has to prioritize real-time voice and video traffic over store-and-forward data traffic, and provide the end-to-end quality of service. For real-time applications of voice and video, the delay and jitter should be imperceptible. Service should be highly dependable (always available) and reliable (quality is consistent). Monitoring and managing these parameters is a challenge for network management.

1.6.6 Security and Privacy in Broadband Systems

With universal ID and multiple service providers delivering multiple services on shared media to multiple subscribers, the security and privacy of information becomes a primary concern. This is especially critical with e-business over the Internet. Besides implementing security and privacy—authentication, authorization, and encryption—of the data and management information, there has to be a cultural change in the perception of the subscribers that the information link is secure.

1.7 CASE HISTORIES ON NETWORK, SYSTEM, AND SERVICE MANAGEMENT

Network Management is more than just managing the network. In standards bodies it is referred to as Operations, Administration, Maintenance, and Provisioning (OAMP). Of course, networking and network management existed before network management became a formalized discipline. Network

management and its complementary functions of system management and application management are all means to the end of service management in providing the subscriber or customer quality of service. As one IT manager commented, the configuration and use of a NMS formalizes what a network administrator would have otherwise done. The network administration "war stories" in the following subsections illustrate that network management (especially without proper tools) could present a challenge to IT managers.

1.7.1 Case History 1: Importance of Topology ("Case of the Footprint")

A stable corporate network consisting of several minicomputers and about 100 desktop workstations and personal computers suddenly started "crashing" frequently (a legacy network example). How often have we heard a network coming down without any apparent reason? Here is how one Vice President of Information Systems describes an incident.

Part of the network went down in the engineering area one morning. Since there were a whole series of users and at that time we were not using a STAR (hub) topology, but rather the old-fashioned serial topology (where all the users were daisy chained to the coax), we suspected a break in the chain, probably at a transceiver tap. Lacking sophisticated NMS tools, Information Systems personnel started walking the hallways asking the users if anyone had just been doing anything out of the ordinary, which might have broken the chain and caused the problem.

The guys came back and reported that no one had said that they had "done anything." So I (VP) started back down the halls with the guys and peeked into each office. Finally, I stopped and said "Let's look up in the ceiling here." Sure enough, we found a transceiver that someone had been fooling with and that was not properly connected, which had caused the break. Once connected, the network segment came back up.

The guys asked "Why did you say—try here?" particularly since the engineer in that office claimed ignorance. I calmly pointed to a dusty image of a sneaker footprint on the engineer's desk and the ceiling tile that was ajar above the desk and said—"you need to use all the diagnostic tools at your disposal!"

1.7.2 Case History 2: Centrally Managed Network Issues

There are numerous war stories that we can describe relating to heavy load on a NMS managing the network and network elements. We will choose one that illustrates several issues related to network design, configuration, and maintenance. An integrated network management system (INMS) was integrating alarms from multiple element management systems (EMSs) in a service provider network. Each EMS manages a domain of network elements and passes the relevant events to the INMS as shown in Figure 1.21. The service provider is able to monitor in its centrally located NOC faults occurring in its global network. As simple as this sounds, its implementation could be extremely complex. Let us consider a simple real-world situation in which a few EMSs were integrated into an INMS and the alarm occurrence time in the INMS was at variance with the individual EMSs.

Each EMS records and displays the receipt time of the alarm. The same is transmitted to the INMS. It was observed that the indication of the time at which the alarm occurred was significantly different in INMS from that indicated in the EMSs that were sending the alarms. The alarm occurrence time was considerably delayed, sometimes by hours, in INMS. The challenge in a centrally managed network is to

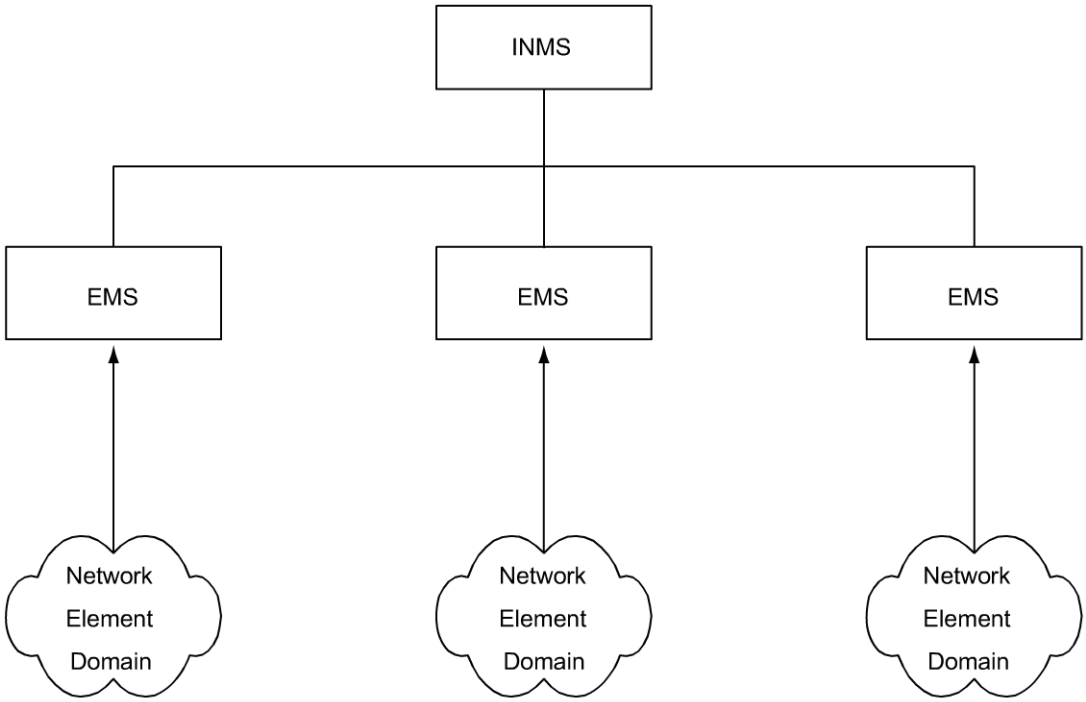


Figure 1.21 Case History 2: Centrally Managed Network Issues

find the root cause of the problem. Is it network delay? Is the delay due to excessive number of events? Is it due to input/output (I/O) limitation of the input port of the INMS? Is it due to I/O output port of EMS? Is it in the software of either EMS or INMS or both? If it is in the INMS software, should the filtering of unnecessary events at the input take care of the problem? The answers to most of these questions were affirmative for each, but to a varying degree in each case. The predominant cause is the stress on NMSs, although it can be traced sometimes to network elements in the various domains. Transmission of unnecessary alarms also causes a stress on the network and networks have gone down due to uncontrolled generations of network management messages.

1.7.3 Transaction Delays in Client–Server Network

In current national and global enterprise organizations, application servers serve thousands of clients over international networks. In a study of banking industry, transaction delays were measured and analyzed to determine the root cause of the delay as reported by tellers of branches. The propagation time of individual transactions was monitored as they traversed through the LAN networks and servers of the branches, through the WAN, and centrally processed by an application server. Some of the transactions were discovered to time-out due to long transaction delays. Study results identified the source of the problem to be gateways and applications; and appropriate actions were initiated to resolve the problem. This case illustrates the need for management of end-to-end communication and the influence of network components, applications, and client–server architecture in a network.

1.7.4 Service Impact in End-to-End Service of Customers

End-to-end communication is further illustrated by the need to proactively identify the service of the customers affected by a network element failure. This is illustrated by the following case. In an optical

fiber transport network using TDM SDH network element that carries thousands of channels, the failure of a single component affects services of hundreds of customers. An end-to-end communication breakdown is to be traced to the failure of a single or multiple network elements by root cause analysis and dynamically determine all clients whose services are impacted. The service provider detects the problem even before customer complaints are received and informs the customers that the problem is already being addressed to restore service as soon as possible.

1.7.5 Some Common Network Problems

The most common and serious problems in network are connectivity failures and are handled under the category of fault management. Fault is generally interpreted as failures in accessing networks and systems by users. Network failure is caused more often by a node failure than failure of passive links (except when it is cut by construction crew). Even node failures are more often limited to specific interface failures. When this happens, all downstream systems from that interface are inaccessible. Such failures are associated with failure of the network interface card.

Node failures manifest as connectivity failures to the user. There are networking tools available to the manager to localize the fault, as we shall learn in Chapter 9 on Network Management Systems and Tools.

Another cause of network connectivity failure is procedural, but very common. Network connectivity is based on the IP address, which is a logical address assigned by the network administrator. The IP address is uniquely associated with a physical MAC address of the network component. However, mistakes are made in assigning duplicate IP addresses, especially in an enterprise environment with multiple system administrators.

A host or system interface problem in a shared medium can bring the entire segment down, sometimes intermittently, as shown in Case History 1 above. This could be a nightmare for the network manager to isolate without causing interruption in service. A network manager uses intuitive knowledge to look for patterns such as change in configuration, addition of new equipment or facility, etc. in resolving such problems.

Intermittent problems could also occur due to traffic overload causing packet loss. Sometimes the management system may indicate failures, when in actuality data traffic is flowing normally. Performance monitoring tools could be useful in tracking such problems.

Power hits could reset network component configuration, causing network failure. The network has a permanent configuration (default) and a dynamic configuration (run-time), and thus a power hit could change the configuration.

Finally, there is the non-problem, which really means that the cause of failure is a mystery. There is nothing else that a network manager could do except turn the system off and then on. Bingo! The problem is resolved.

Performance problem could also manifest as network delay and is more an annoyance to the network manager, who needs to separate network delay from the application program or application processes delay. Then the network manager has to convince the user and then the person responsible for the application to rectify the situation.

With the ever-increasing size of the network and connectivity to the Internet, security violation in network management is a frequently encountered problem. This is more a policy problem than technical, which we will address in Chapter 11 when we discuss security management.

1.8 CHALLENGES OF IT MANAGERS

Managing a corporate network is becoming harder as it becomes larger and more complex. When we talk about network management, it includes not only components that transport information in the network, but also systems that generate traffic in the network. What use is a computer network if there are no systems in the network to provide service to users? The systems could be hosts, database servers, file servers, or mail servers. In the client–server environment, network control is no longer centralized, but distributed. Computer and telecommunication networks are merging fast into converged network with common modes and media of transportation and distribution. As in the case of broadband networks, the IT manager needs to maintain both types of networks. Thus, the data communications manager functions and telecommunication manager functions have been merged to that of the IT manager. With the explosion of information storage and transfer in the modern information era, management of information is also the responsibility of the IT manager, with the title of CIO, Chief Information Officer. For example, the IT manager needs to worry in detail about who can access the information and what information they can access, i.e., authentication and authorization issues of security management. The corporate network needs to be secured for privacy and content, using firewalls and encryption. Technology is moving so fast and corporate growth is so enormous, that a CIO has to keep up with new technologies and the responsibility for financial investment that the corporation commits to. This amounts to millions of dollars, and the success or failure of making the right guess—not choice—could make or break the CIO's job. Notice that the word "guess" was used instead of "choice" deliberately because it is not always clear which of the options are a dead end, and hence need to be avoided. Since they are not obvious, the IT manager needs to make provisions for contingencies to change direction when the IT industry does.

A good example of indeterminacy in the fast-moving technology industry was competition between the two technologies of Ethernet and ATM to desktop. ATM was predicted to be the way to go a few years ago. However, this has not been the case because of the development of enhanced capability and speed of Ethernet. Another current example related to this is the decision that one has to make in the adoption and deployment of WAN—whether it should be IP, ATM, or MPLS.

Perspectives of Network Managers In order to appreciate challenges that IT managers face, several of them were interviewed by the author. They face network administration and management problems day in and day out. These are the folks who carry a cell phone with them all the time since most corporate networks run 24/7—i.e., available 24 hours a day 7 days a week! The questions that were posed, with a summary of the answers edited for the current status of IT, follow. They are not an exhaustive list of questions and answers, since that would make the contents of a separate book, but are only intended to indicate the complexity of managing a network and thus motivate a student in networking. Notice that it is not just a technical function, as Case History 1 exemplifies. Also, even use of the best NMS does not solve the problems associated with building and maintaining a network, but it is a necessary tool. Thus, learning network management involves more than understanding network and network management protocols. The author's recent in-depth study of service providers also raises similar comments.

General

- People expect a network to function like a telephone network.
- Reliability in a data network as in a telephone is unrealizable. The telephone network was monopolistic and had expensive redundancy. The data network is ad hoc, decentralized, has loosely

specified interfaces, and has dynamic routing. Thus, it is a lot more flexible than the telephone network though less reliable.

- Designing, deploying, and managing networks that can handle real-time and non-real-time data.
- Integration of multivendor and multitechnology equipment and their network management systems.

1. **What are your top challenging activities in managing the network?**
   - Rapid advance of technology
   - Problem analysis—needs human intuition and skill besides sophisticated management tools
   - Anticipate customer demands
   - Acquire and retain human resources
   - Manage client–server environment in converged networks
   - Networking with emerging technology necessitates the need for continuing education
   - Collaborative research between academic institutions and industry
   - Maintain reliability, that is, make changes, upgrades, etc. without disrupting the network and impacting business
   - Diagnose problems or outages in a non-disruptive manner (without impacting other users on the network)
   - Estimate the value of a technology transition. For example, should one transition over to accommodate the increasing number of IP addresses with IPv6 or continue with IPv4 with Network Address Translation (NAT) as a hierarchical addressing scheme?
2. **Which elements of managing your network require most of your time? What percentage of time do you spend on maintenance compared to growth?**
   - A 30–80% growth, 20–70% maintenance based on the organization.
   - Configuring the management system itself takes most of the time.
   - Expanding the network.
   - Gathering and analyzing statistics for upper management review to conduct business.
3. **How did you or would you manage your network without an NMS?**
   - Reactively, not proactively; firefighting
   - Troubleshooting tools, e.g., sniffer, ping, etc.
   - Home-grown systems using an open source, e.g., Multi Router Traffic Grapher (MRTG)
   - Rely on consultant advice and technical information for growth decisions
4. **Do you need an NMS? Why?**
   - For proactive management of network
   - Verify customer configuration
   - Diagnose problems
   - Provide statistics on performance
   - Help remove bottlenecks
   - NMS formalizes the manual practice of network management
   - NMS products reflect the company's practice that develops them
   - To see the trend in growth
5. **What problems would you expect the NMS to resolve, and how?**
   - Enhance customer satisfaction by meeting the Service Level Agreement (SLA)
   - Save time and people resource and thus enhance productivity

- Turn-around shorter for resolution of problems
- Gather statistics and predict trends for planning purposes
- Document events
- Troubleshooting
- Remove constraints and bottlenecks
- Fault isolation
- Expect the NMS to do a root cause analysis and pinpoint failures

We will now briefly introduce the subject of network management functions and system in the following sections.

1.9 NETWORK MANAGEMENT: GOALS, ORGANIZATION, AND FUNCTIONS

Network Management can be defined as Operations, Administration, Maintenance, and Provisioning (OAMP) of network and services. The Operations group is concerned with daily operations in providing network services. The network Administration is concerned with establishing and administering overall goals, policies, and procedures of network management. The Installation and Maintenance (I&M) group handles functions that include both installation and repairs of facilities and equipment. Provisioning involves network planning and circuit provisioning, traditionally handled by the Engineering or Provisioning department. We will describe each of these functions in this section. Although we continue to use the terminology of network management, in the modern enterprise environment this addresses all of IT and IT services.

1.9.1 Goal of Network Management

The goal of network management is to ensure that the users of network are provided IT services with a quality of service that they expect. Toward meeting this goal, the management should establish a policy to either formally or informally contract an SLA with users.

From a business administration point of view, network management involves strategic and tactical planning of engineering, operations, and maintenance of network and network services for current and future needs at minimum overall cost. There needs to be a well-established interaction between the various groups performing these functions.

Figure 1.22 presents a top-down view of network management functions. It comprises three major groups: (i) network and service provisioning, (ii) network and service operations, and (iii) network I&M. It is worth considering the different functions as belonging to specific administrative groups, although there are other ways of assigning responsibilities based on local organizational structure. Network provisioning is the primary responsibility of the Engineering group. The Customer Relations group deals with clients and subscribers in providing services planned and designed by the Engineering group. Network I&M is the primary responsibility of the Plant Facilities group. Interactions between the groups are shown in Figure 1.23. Normal daily operations are the function of the Network Operations group, which controls and administers a NOC. This is the nerve center of network management operations. The functions of NOC are primarily concerned with network operations; its secondary responsibilities are network provisioning and network I&M. The associated service operations are handled by a subscriber operation center (SOC) and customer relations management (CRM). Our focus here is on NOC.

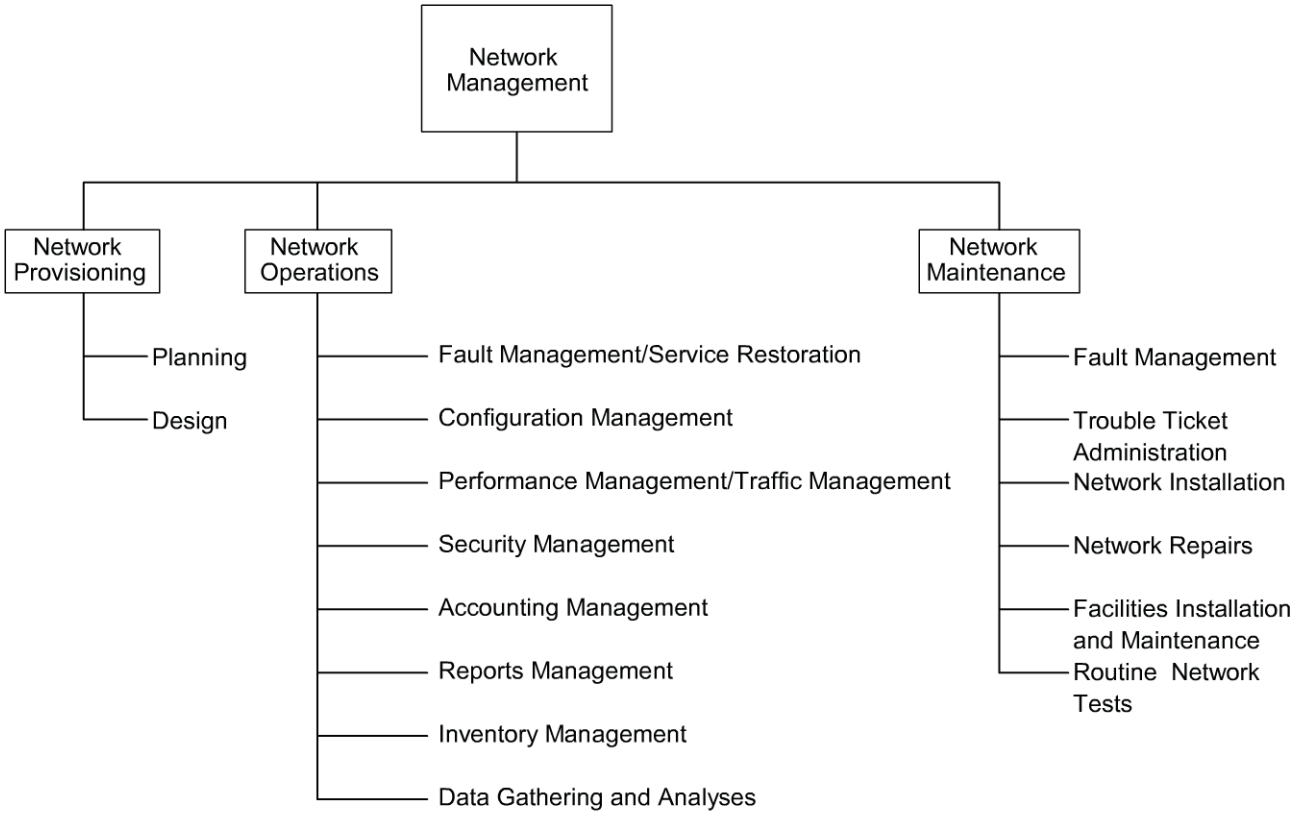


Figure 1.22 Network Management Functional Groupings

1.9.2 Network Provisioning

Network Provisioning consists of network planning and design and is the responsibility of the Engineering group. The Engineering group keeps track of new technologies and introduces them as needed. What is needed and when it is needed are determined from analysis of traffic and performance data provided by the network operations. New or modifications to network provisioning may also be initiated by management decisions. Planning and efficient use of equipment can be achieved with good inventory management of current and future modifications of network configuration by the Network Provisioning group.

Network management tools are helpful to the Engineering group in gathering statistics and studying trends in traffic patterns for planning purposes. Automated operations systems help in the design of circuits and measuring the performance tune-up.

1.9.3 Network Operations and NOC

The functions of network operations listed in Figure 1.22 are administered by the NOC. They are concerned with daily operations of the network and providing network services. ISO has defined five OSI network management applications, which are fault, configuration, performance, security, and account management. They are also responsible for gathering statistics and generating reports for management, system support, and users. NMS and tools are a necessity for NOC operations. They are used in various management applications described below.

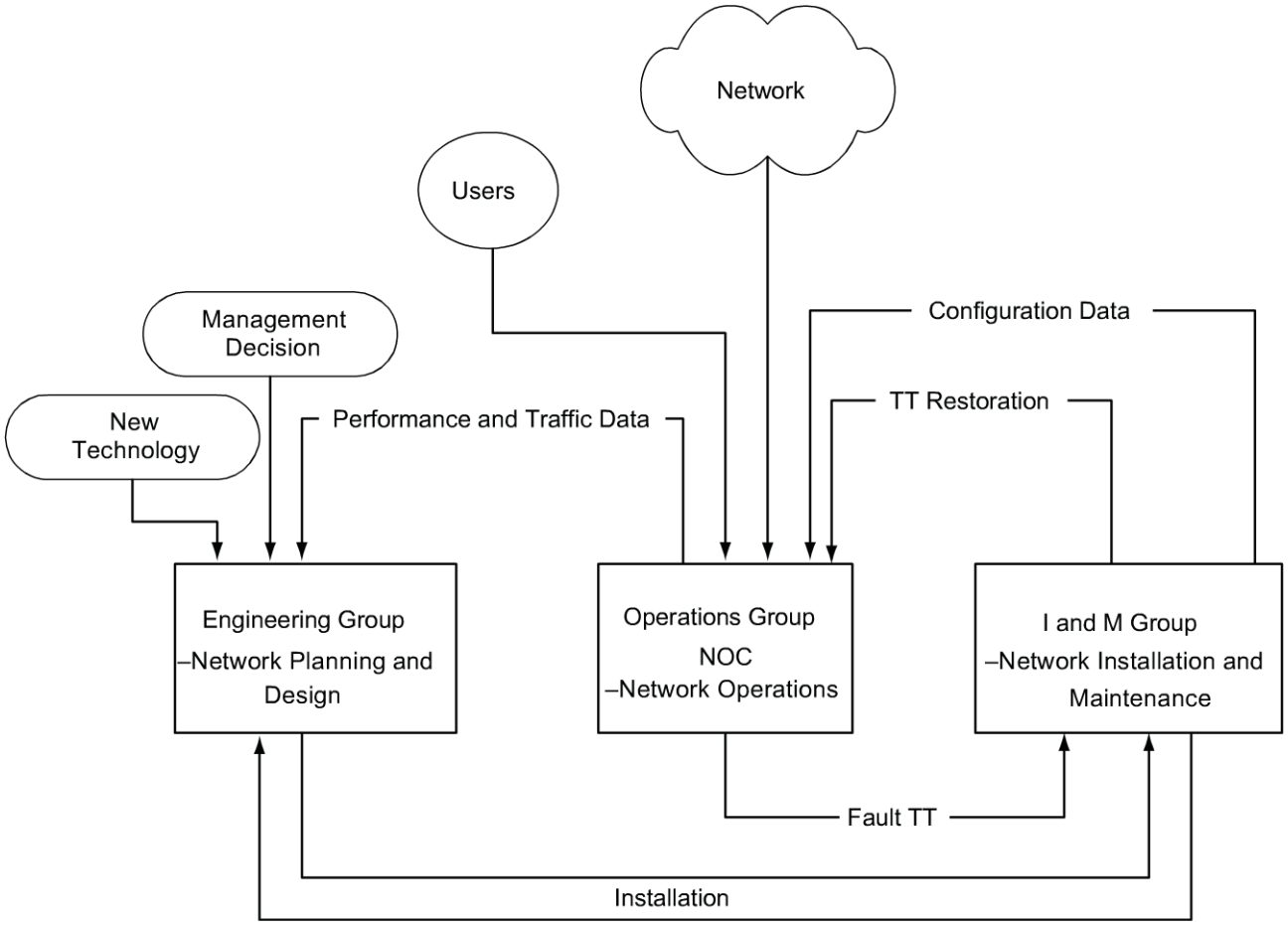


Figure 1.23 Network Management Functional Flow Chart

Fault Management/Service Restoration: Whenever there is a service failure, it is NOC's responsibility to restore service as soon as possible. This involves detection and isolation of the problem causing the failure, and restoration of service. In several failure situations, the network will do this automatically. This network feature is called self-healing. In other situations, NMS can detect failure of components and indicate with appropriate alarms. Restoration of service does not include fixing the cause of the problem. That responsibility usually rests with the I&M group. A trouble ticket is generated and followed up for resolution of the problem by the I&M group.

Trouble Ticket Administration: Trouble ticket administration is the administrative part of fault management and is used to track problems in the network. All problems, including non-problems, are to be tracked until resolved. Periodic analysis of the data, which are maintained in a database, is done to establish patterns of the problems for follow-up action. There are trouble-tracking systems to automate the tracking of troubles from the automatic generation of a trouble ticket by an NMS to the resolution of the problem.

Configuration Management: There are three sets of configuration of the network. One is the static configuration and is the permanent configuration of the network. However, it is likely that the current running configuration, which is the second, could be different from that of the permanent configuration.

Static configuration is one that the network would bring up if it is started from an idle status. The third configuration is the planned configuration of the future when the configuration data will change as the network is changed. This information is useful for planning and inventory management. The configuration data are automatically gathered as much as possible and are stored by NMSs. NOC has a display that reflects the dynamic configuration of the network and its status.

The status of the network is displayed by a NMS and indicates any failure of components of the network, as well as the traffic pattern and performance. Any configuration changes needed to relieve temporary congestion in traffic are made by NOC and are reflected in the dynamic display at NOC.

Performance Management: Data need to be gathered by NOC and kept updated in a timely fashion in order to perform some of the above functions, as well as tune the network for optimum performance. This is part of performance management. Network statistics include data on traffic, network availability, and network delay. Traffic data can be captured based on volume of traffic in various segments of the network. They can also be obtained based on different applications such as Web traffic, email, and network news, or based on transport protocols at various layers such as TCP, UDP, IP, IPX, Ethernet, TR, FDDI, etc. Traffic statistics are helpful in detecting trends and planning future needs. Performance data on availability and delay are useful for tuning the network to increase the reliability and to improve its response time.

Security Management can cover a very broad range of security. It involves physically securing the network, as well as access to the network by users. Access privilege to application software is not the responsibility of NOC unless the application is either owned or maintained by NOC. A security database is established and maintained by NOC for access to the network and network information. There are other aspects of security management such as firewalls and cryptography, which will be introduced later in Chapter 11.

Accounting Management administers cost allocation of the usage of network. Metrics are established to measure the usage of resources and services provided.

Since the network consists of components manufactured by multiple vendors, commonality in the definition and relationship of component attributes is needed. This is defined by Management Information Base (MIB), which we will discuss in Part II. Some of the data acquisition has to be manual (because of legacy systems), but most data can and should be acquired in an automated mode. The SNMP is the most popular protocol to acquire data automatically using protocol- and performance-analyzing tools.

As part of implementing the above standards, we need to ensure that adequate reports are generated and distributed to relevant personnel. There are, in general, three classes of reports: systems, management, and user. System reports are needed for network operations to track activities. Management reports go to the managers of network management group to keep them informed about the activities and performance of NOC and the network. User reports are distributed to users on a periodic basis or are available on-line to let them know the status of network performance.

1.9.4 Network Installation and Maintenance

The Network I&M group takes care of all activities of installation and maintenance of equipment and transmission facilities. This group is the service arm of the Engineering group for installation and fixing

troubles for network operations. The group works closely with the Help Desk in responding to the problems reported from the field.

Having introduced what network management is from an operations, administration, maintenance, and planning viewpoint, let us next consider the architecture and organization of an NMS.

1.10 NETWORK MANAGEMENT ARCHITECTURE AND ORGANIZATION

We need to distinguish at the outset the difference between network management and network system and service management. Remember that a user may not make that distinction when he or she cannot access an application on a server from a client application in his or her workstation. This could be either due to a problem in the application program in the server affecting one or more clients or due to a transport problem from the client workstation to the server platform. The former is a network system problem affecting the service offered and falls under the category of network system and service management. The latter is a connectivity problem and falls under network management. We can generalize system and service management as the management of systems and system resources in the network and services offered by the network. Network management is concerned with network resources such as hubs, switches, bridges, routers, and gateways, and the connectivity among them via a network. It also addresses end-to-end connectivity between any two processors (not application processes) in the network.

As we saw in Section 1.1, a network consists of network components and their interconnection. Each vendor, who manufactures a network component or a set of network components, is best qualified to develop an NMS to manage that product or set of products. This involves getting data from each instance of that component in the network to one or more centralized locations and displaying their status on an NMS; for example, failure of a bridge. This would set up an alarm in the NMS to alert operations personnel of the failure. This would enable operations personnel to follow up on the problem and restore service, even before the user calls in a complaint.

As mentioned above, each type of component is managed most efficiently by its respective management system. There is need for an NMS to manage all the components that are connected to a network. Again, it is relatively simple for a vendor to develop an NMS to manage a network comprising only their components. However, a user, such as a global corporation, buys components from many different vendors, and the information systems manager of the corporation has the responsibility of maintaining the network of all vendor components. This might require the installation of multiple NMSs for an enterprise or an NMS that can manage multiple vendor components of a network. Thus, common management system, as well as the integration of different management systems and the interoperability between them, has played a major role in the network management arena. Standards organizations and industrial communities have established standards for this purpose, which are still evolving. The two major management standards are the Internet developed by the Internet Engineering Task Force (IETF) and OSI developed by the ISO. We will look at the former in detail in this book. There are also standards that are developed by industrial consortiums associated with specific technologies, such as DSL Forum and CableLabs.

Network management dumbbell architecture for interoperability is shown in Figure 1.24(a) where two vendor systems A and B exchange common management messages. The messages consist of management information data (type, id, and status of managed objects, etc.) and management controls

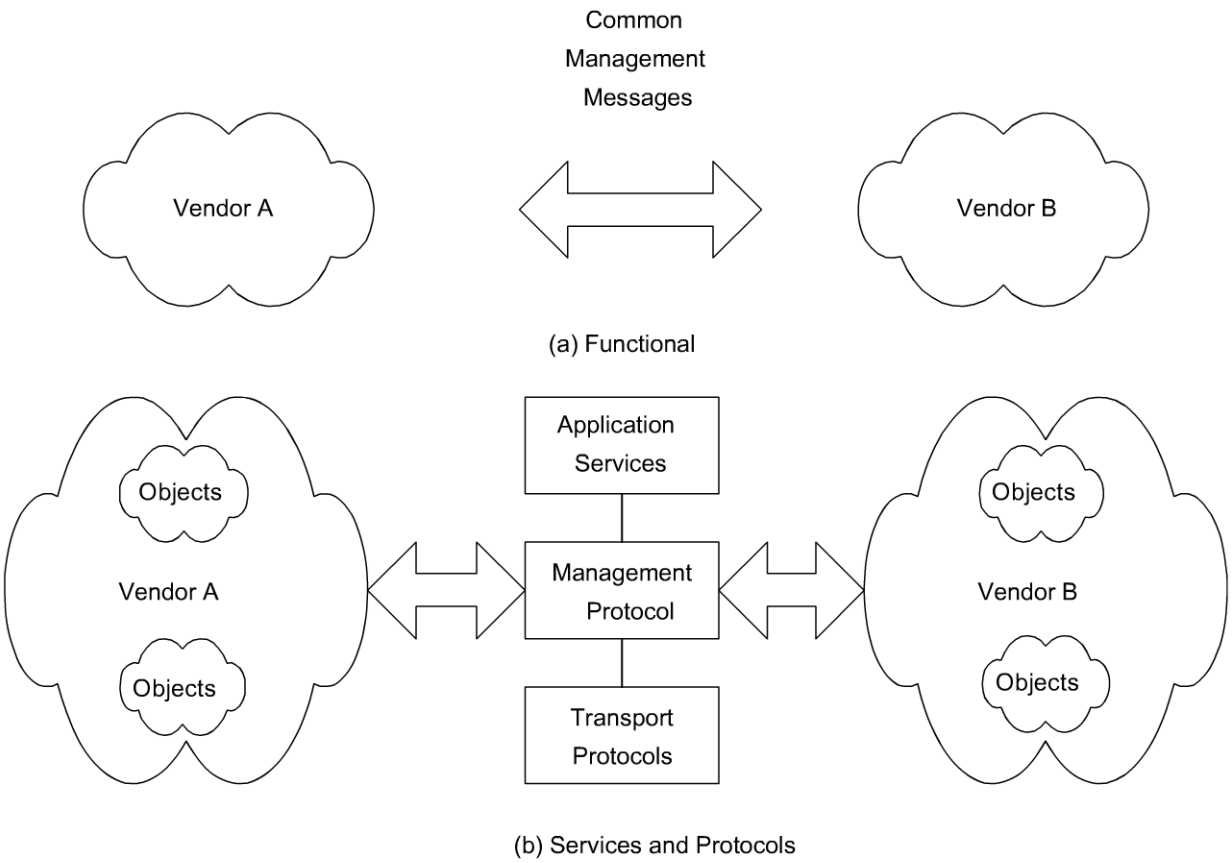


Figure 1.24 Network Management Dumbbell Architecture

(setting and changing configuration of an object). The protocols and services associated with dumb bell architecture are presented in Figure 1.24(b). Application services are the management-related applications such as fault and configuration management. Management protocols are CMIP for the OSI model and SNMP for the Internet model. Transport protocols are the first four OSI layers for the OSI model and TCP/IP over any of the first two layers for the Internet model.

Figure 1.25 models a hierarchical configuration of two network agents monitoring two sets of managed objects. The agent could be an embedded agent in a network element or an EMS communicating with agents embedded in the network elements. An NMS is at the top of the hierarchy. Each network agent monitors its respective objects. Either in response to a polled query from the NMS or triggered by a local alarm, the agent communicates to the NMS the relevant data.

Peer networks can communicate network management messages and controls between each other, as shown in Figure 1.26. An example where such a configuration could be implemented would be two NMSs associated with two telecommunication networks belonging to two network service providers; for example, an interexchange carrier and a local access provider. As the two NMSs communicate with each other, each NMS can superimpose the data from the other and present an integrated picture to the network administrator.

We want to make one final note before we leave this section. Some of the issues associated with the management of telecommunication network by the telecommunication service providers are unique and involve more than just management of networks. This has given birth to the Telecommunication Management Network (TMN) framework and related standards. We will address these in Chapter 10.

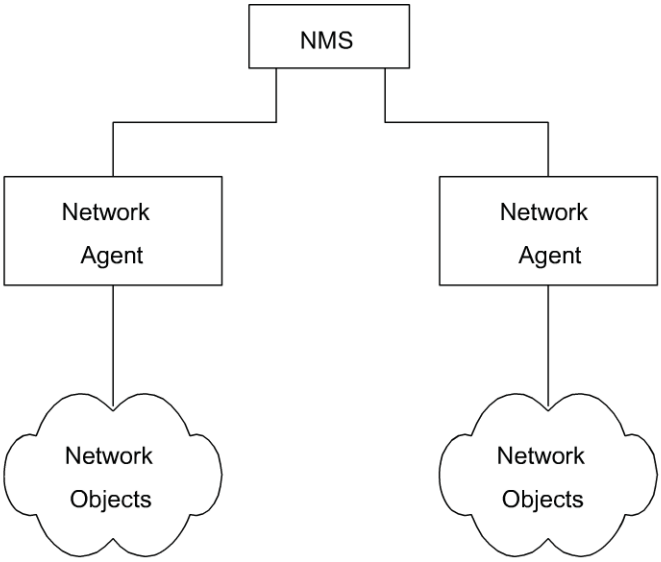


Figure 1.25 Network Management Components

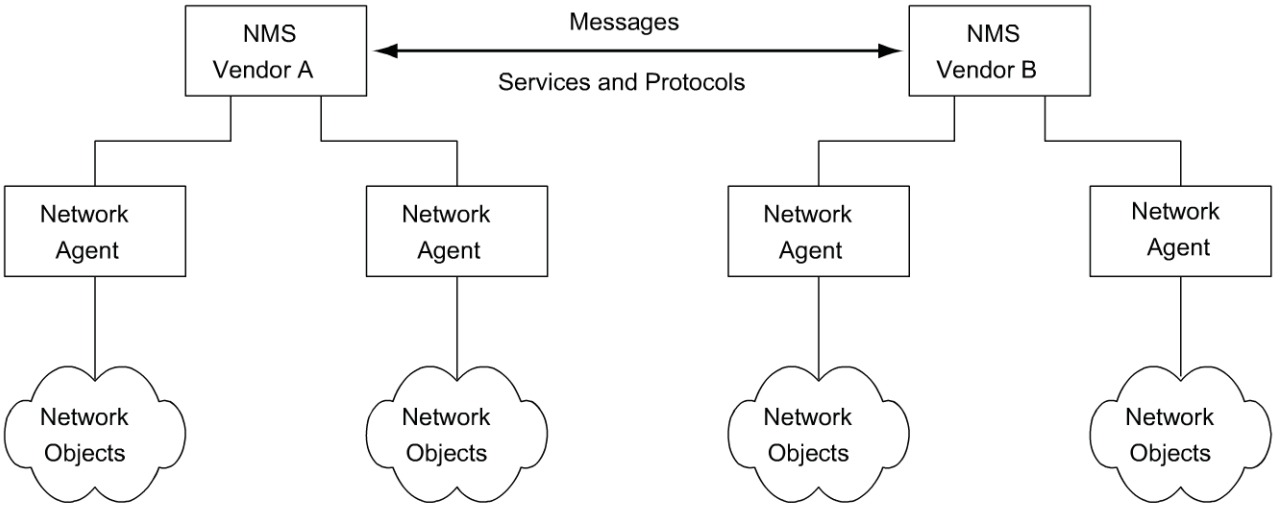


Figure 1.26 Network Management Interoperability

1.11 NETWORK MANAGEMENT PERSPECTIVES

As we said earlier, the NMS primarily manages the networks that transport information. However, from a user's perspective, networks are means to an end, namely to have access to information across the networks. Thus, the users' needs require a total solution to manage the networks, system resources, and applications that run on systems. Applications could be specific user applications, or general-purpose servers such as file servers, database servers, and DNSs. Software products have since been developed to address such system-wide solutions.

An IT manager is interested in more than managing networks, systems, and applications. He or she would like to automate other functions such as back up of databases and programs, downloading of software updates from a central location, and a host of other support functions. These are required to run an IT operation efficiently and in a cost-effective manner.

Another area of system management is logging and archiving of events. This is illustrated by a case history when the system performance during normally slow activity time at night was poor. Further probing the system resources indicated that the system was busy with processes being executed from outside the institution. The system had been "compromised," i.e., had been broken into. The intruder could manipulate the normal system resource tools so as to hide the intruder programs. The intruder was finally discovered from the archival system log.

Solutions to the total IT services are currently being offered by commercial vendors. We will discuss them along with network and system management tools and systems in Part III of the book. We will present here a high-level view of some of the alternate perspectives of the broad aspects of network management.

1.11.1 Network Management Perspective

Domains: The network management overview given so far in the chapter can be perceived as management of a domain. The domain can be any of a selected group of parameters having common attributes. Thus, a geographical domain refers to the subdivisions of a large geographical region. For example, in India the telecommunication administration is divided into circles, and each circle maintains its own telecommunication network.

Another classification of a domain can be based on vendor products. Thus, we could have different vendors' management systems managing their respective products. A third perspective of looking at domains can be from the technology perspective. For example, IP-based products, telecommunication products, broadband communication products, and digital transport products such as SDH could each define a domain managed by a separate NMS, as well as a different administrative group.

Protocols: Network management can be perceived from the protocol used to manage the network such as Internet-based SNMP and OSI-based Common Management Information Protocol/Common Management Information Service Element (CMIP/CMISE). Traffic use of various protocols at each protocol layer can be monitored.

Network and Transmission Technologies: An end-to-end network system could be viewed as comprising multiple network technologies traversing different transmission media and carrying information in different transmission modes, each managed from a different network management perspective. Thus, an end-to-end communication, which can be represented as a logical circuit, could be made up of network elements comprising IP-based routers and ATM-based switches. It can traverse globally through coaxial cable in an access network, wireless transmission over continents, fiber optic cable over land on a WAN, and twisted copper wire at home. The transmission mode could be digital TDM, or ATM, or a broadband access mode. An integrated NMS is used to manage end-to-end availability of a circuit that deploys multivendor and multitechnology network elements.

1.11.2 Service Management Perspective

The network is used to provide service to customers and consequently what needs to be managed are the services. The real concern of service providers is more about service management. Providing quality of service to satisfy the customers' needs requires network management. However, while network management focuses on the physical network, service management focuses on services offered over the network and those services meeting customer needs and satisfaction. Various quality of service (QoS)

parameters are defined and an SLA is reached between the service provider and the customer. There are several OSSs that provide different types of service management.

Communication services can be offered as public switched network services, Internet services, virtual private network, real-time interactive audio and video services, and others too numerous to list. Computing services are offered to clients using applications running on servers. These servers and applications running on them need to be managed centrally by the service provider or enterprise that owns them. This management is also known as enterprise management. It monitors the health of system resources, as well as the applications that run on them. There are managed service offerings available to manage multiple enterprise networks from a common management facility.

1.11.3 OSS Perspective

While the EMS, NMS, and enterprise management system are designed to manage the network and network resources, OSSs support the operation of network and service management systems. In Section 1.9 we described the supporting functions of networking needed to provide communication services as operations, administration, maintenance, and provisioning (OAMP).

Provisioning System: The logical and physical network has to be provisioned to provide the desired service to the customer. An OSS, provisioning management system, does this function using several other OSSs such as the inventory management system, the service order system, and the element and NMSs. Provisioning management includes circuit provisioning, service provisioning, and network provisioning.

Inventory Management System includes inventory of equipment and facilities. We can generalize equipment as active components forming nodes of a network and facilities as passive components linking the nodes.

Customer Relations Management (CRM) operation support system manages complaints reported by the customers. A proactive approach to CRM is the service provider calling the customer on detecting a service outage indicated by NMS.

Trouble Ticket and Work Force Management manages the troubles detected by the NMS and generates work **order** in the Work Force Management System. Various OSSs help with the remote testing, either on-demand or automated, in installation and maintenance.

IP Telecommunication Application Management: The traditional analog services of voice and video are now offered as digital services. Such services as voice-over-IP and video-over-IP applications require not only management of data, but also connection management. Sessions that are equivalent to a circuit need to be established and managed.

1.11.4 e-Business Management

The e-business management and privacy requirements are associated with e-commerce applications. This includes application management in Internet retail activities, as well as banking automated teller machines.

1.12 NMS PLATFORM

NMSs and tools are available in various platforms—hardware and operating system. Popular high-end systems are housed on UNIX-based servers. Low-end NMSs run either on Windows or Linux-based platforms.

Most high-end NMSs are equipped with remote client capability and can be accessed either via Java client or Web browser. Client platforms are either Windows or UNIX based.

Common troubleshooting and monitoring of network element parameters could be done by using simple networking and network management tools. These are part of TCP/IP stack. For example, network connectivity could be tested using *ping* and *traceroute* commands in UNIX and *tracert* in Microsoft Windows. We will discuss NMSs and tools in detail in Chapter 9.

1.13 CURRENT STATUS AND FUTURE OF NETWORK MANAGEMENT

Current NMSs are based on SNMP protocol. Most commercial network components have embedded SNMP agents. Because of the universality of the IP, transport of management information for SNMP management, which is TCP/IP-based, is automatically resolved. In addition, most of the popular host-operating systems come with TCP/IP protocol suite and thus are amenable to SNMP management.

Current NMSs, however, suffer from several limitations. One of the limitations of SNMP-based management system is that values of managed objects should be defined as scalar values. OSI-based management protocol, CMIP, is object oriented. However, it has not been successful due to the complexity of specifications of managed objects and the limitation of large memory in computer systems in the past. Another limitation of SNMP-based management is that it is a poll-based system. In other words, NMS polls each agent as to its status, or for any other data that it needs for network management. Only a small set of transactions is initiated by a management agent to an NMS as alarms. To detect a fault quickly, or to obtain good statistics, more frequent polling of agents needs to be done by the NMS, which adds to network traffic overhead. There is an alternative solution to this problem, which is deployment of remote monitors as discussed in Chapter 8.

Some of the above constraints in SNMP-based management have been overcome by emerging advanced network management discussed in Chapter 16. Object-oriented technology has reached a matured stage, and the hardware capacity to handle object-oriented stacks is now commercially available. Thus, object-oriented network management is being reconsidered. This has potential application in Telecommunications Management Network discussed in Chapter 10. Network management systems are currently built with object-oriented protocols and schema, such as Common Object Request Broker Architecture (CORBA) protocol and Extended Markup Language (XML) schema.

An active network, which is the direction of next generation network, would include embedded network management applications. Besides the advancement of research and development in network management in standards, protocols, methodology, and new technology, there is considerable activity in management applications, which form the topic of Chapter 11. Of particular significance are event correlation technology in fault management, and secured network and communication in security management.

With the proliferation of the Internet, secured network and communication has become extremely important. Existing management standards do not go far enough in this. However, security management

has taken on the role of a special topic in network management. Topics of high interest in this field are firewalls that establish secure networks and cryptography that assure secure communication.

IT itself is exploding and gives rise to new challenges for expanding the horizon of network management. Transport of voice, video, and data is integrated in broadband multimedia services. Broadband multimedia service is based on ATM, IP, and MPLS in a WAN and several emerging access technologies such as HFC, Asymmetric Digital Subscriber Loop (ADSL), and fixed and mobile wireless. Quality of Service in integrated services is important. Managing these new service offerings forms the content of Part IV.

Another re-emerging technology for network management is the wireless technology. This is being widely deployed for WAN, mobile, broadband access, and home networks. Much work on standardization of management of this technology needs to be done in this area.

Summary

We presented in this chapter an overview of data and telecommunication networks, as well as converged networks and how these networks are managed. The telephone network was shown as a model to be followed in accomplishing a reliable, dependable, and quality data communication network. We explained the difference between data communication and telecommunication networks, although this distinction is fast disappearing. Desktop processors and LAN technology have contributed to the client–server distributed computing environment, which has changed the future direction of data communication.

We briefly talked about the Internet and intranet in today's environment. Adoption of standards has played a significant part in the popularity of the Internet. OSI and IPs play an important part in data communication today. We also treated difficulties associated with real-time and non-real-time management of different segments of broadband networks and services. We have presented some practical day-to-day experiences of network managers, including "war stories" to make us realize the importance of network management.

We saw a bird's-eye view of network management and described how network components and networks are managed by network management systems. We extended the concept of network management to managing networks and systems and all of IT services. The future direction of IT management is undergoing changes due to advancements in software and IT. Possible future directions in network management technology were addressed at the end of the chapter.

Exercises

Note for Problems 1–4: It is important that a network administrator be familiar with both the protocols employed in the network and the tools with which its operation may be investigated. There are several tools that are fundamental for administration of an IP network; the after used ones are *ping*, *nslookup*, and *traceroute*. These commands should be available on UNIX platforms. You may get the syntax of their usage by logging into a UNIX system and accessing the on-line manual by invoking the command *man commandname*. Similar tools or commands are available in Windows 95/NT machines (*ping*, *tracert*, *nslookup* either built in or external software) connected to the Internet. Problems 1–7 are intended to familiarize you with exploring a network. You should be able to do these exercises using the commonly available networking tools and on the Internet using websites such as whois.domaintools.com and iternic.net.

In doing these exercises, if you have a problem reaching the destination host, you may use any other equivalent destination site. It is important for you to learn to use tools and interpret results.

1. Who is the primary Internet service provider (ISP) in your institution? Find another institution served by the same ISP by using a traceroute tool.

2. Educational institutions in your state or province are networked. Discover that network by tracing the route from your institute or organization to other institutes or organizations.
3. Draw the route diagram identifying each node for the following data obtained using a trace routing tool. What is the average time a packet takes to travel from noc2 host to *netman* host?
   noc2% traceroute netman.cc.gatech.edu
   traceroute to netman.cc.gatech.edu (130.207.8.31), 30 hops max, 40 byte packets
   main-rtr.gcatt.gatech.edu (199.77.147.1) 1.045 ms 1.012 ms 0.971 ms.
   130.207.251.2 (130.207.251.2) 2.198 ms 1.404 ms 1.837 ms.
   netman.cc.gatech.edu (130.207.8.31) 3.528 ms 1.671 ms 1.602 ms.
4. Between which two hosts on the route between your site and www.president.lv is the largest geographic distance probably traversed? Support your answer with evidence.
5. Ping ns1.bangla.net in this exercise. State what data you gathered and how it determined your conclusion.
   (a) Measure the percent packet loss between a host at your site and the machine ns1.bangla.net, and record the time of your measurement.
   (b) Then determine where along the route to ns1.bangla.net the packets are getting lost.
6. For each host on the route between your location and ns1.bangla.net (or any other foreign country), determine the name of the administrative contact responsible for it (use *whois* command from your UNIX system or from internic.net). List these names alongside the hosts. If you can't find an administrative contact for some of the hosts, then at least state what you did find.
7. You can discover the hosts in your subnetwork by using the ping command with your network IP address and host address of decimal 255. Discover all the hosts in the subnetwork that you are logged on.
8. In Problem 5, identify the gateway from your subnetwork to others.
9. Identify the hosts in the neighboring subnetworks and draw the configuration of interconnected subnetworks.
10. The email system is based on client–server architecture. Send an email to a wrong node address (for example, misspelling the remote node address). Explain the error message(s) that you get and the servers that you get them from.
11. Send an email to a remote site with a wrong user id, but correct node address. Explain the error message(s) that you get and the servers that you get them from.
12. Explain the decimal notation in representing the classes of IPv4 addresses. Give an example for each class.
13. You are given a class B IP address of 145.45.x.y for your network node. As a network engineer, you are asked to configure your network for 126 subnets. (Remember that 0 and 1 are reserved.)
    (a) How would you configure your address for subnets and hosts?
    (b) What is the maximum number of hosts that each subnet can accommodate?
14. An IP network is connected to a Novell IPX network via a gateway as shown. Draw the protocol layers of the gateway in Figure 1.27.
15. MBI Corporation uses cc:mail, which is not Internet standard. The company also uses Novell LAN. Novell has Internet Exchange Protocol, IPX (connectionless datagram service), as its equivalent to Internet TCP/IP. As you know well, most of the global email traffic is on the Internet with SMTP as the mail protocol. Figure 1.28 shows the high-level configuration of the two networks connected through a gateway. Fill in the protocol layers of the gateway.

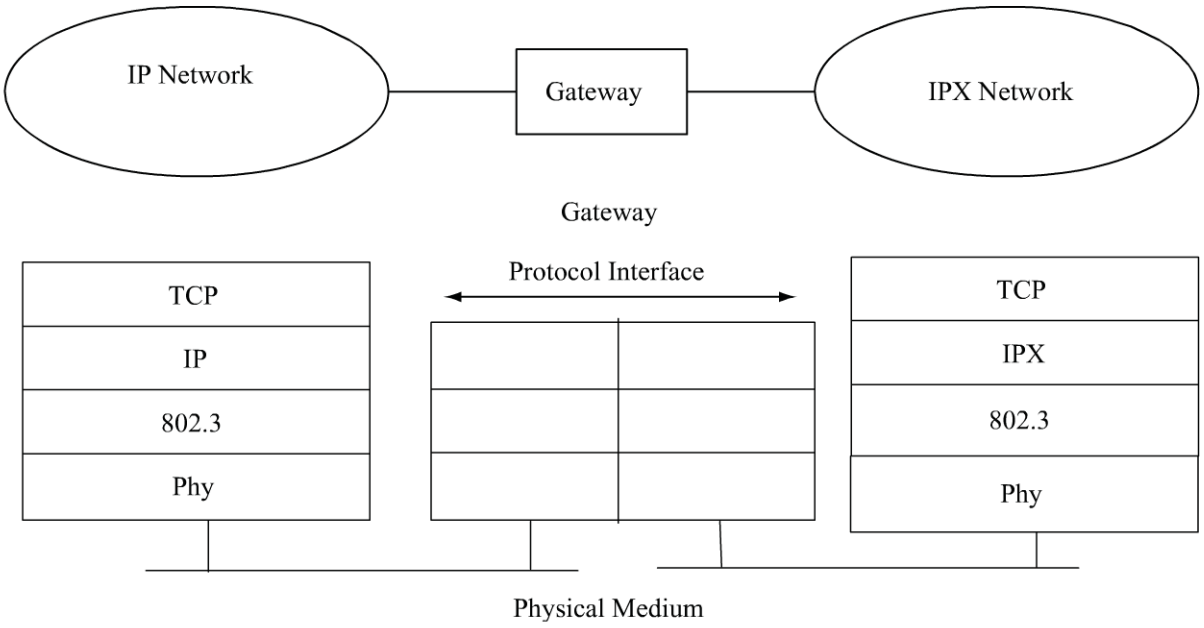


Figure 1.27 Exercise 14

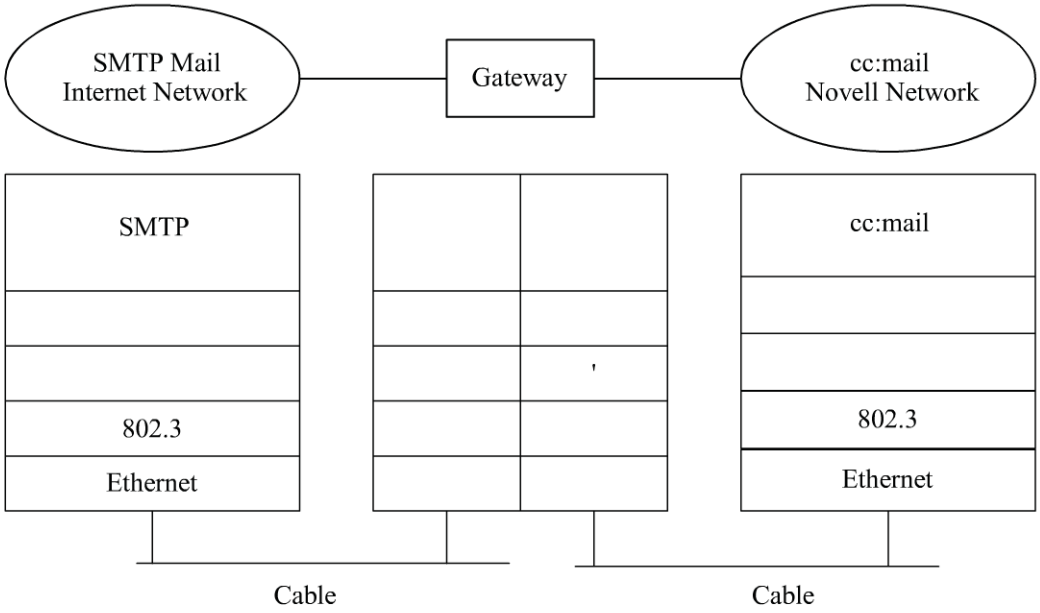
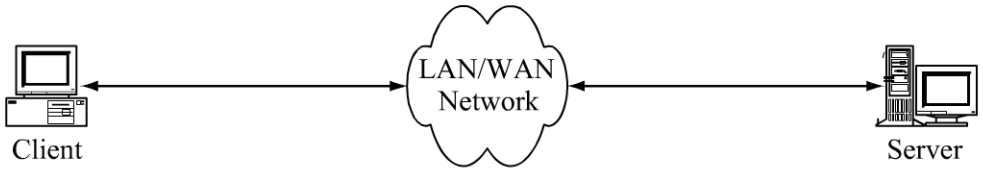
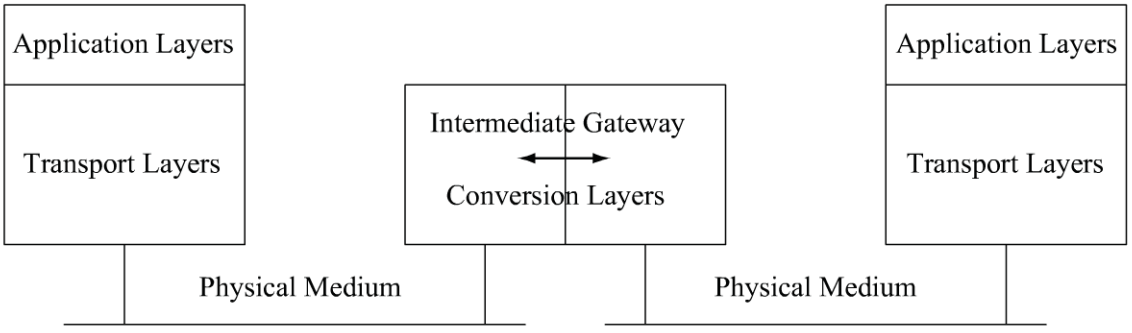


Figure 1.28 Exercise 15

16. Picture a scenario where you are downloading a file from a server, located in Europe, which has an X.25 protocol based on the OSI Reference Model. Its physical medium interface is X.21. Your client machine is connected to the Internet with Ethernet as the physical medium.
    (a) Draw the details of the communications network in Figure 1.29(a) using bridges, routers, and a gateway between the server and the client.
    (b) Complete the protocol architecture in Figure 1.29(b) for the intermediate gateway system.
17. In Case History 2 described in Section 1.7.2, the delay in alarm indication in INMS was attributed to several possible causes. Give an example for each of these causes.



(a) Communication Network Between Client and Server



(b) Communication Between End Systems via an Intermediate System

Figure 1.29 Exercise 16

18. As a network engineer in a Network Operations Center, you are following up on two trouble tickets. You do not have a network management system and you have to use the basic network tools to validate the problem before you can resolve them. Please explain what tools you would use in each case and how it would validate the customer complaint

    (a) Trouble Ticket 100: Customer says that when he receives messages, the message is periodically missing some characters.

    (b) Trouble Ticket 101: Customer in Atlanta complains that when she tries to log into the system *server.headquarters.com* in New York, she gets disconnected with a time-out. However, her colleague in her New York office reports that he is able to access the system.