The Froehlich/Kent

ENCYCLOPEDIA OF TELECOMMUNICATIONS

VOLUME 10

Editor-in-chief: Fritz E. Froehlich

Coeditor: Allen Kent

The Froehlich / Kent

ENCYCLOPEDIA OF TELECOMMUNICATIONS

VOLUME 10

The Froehlich/Kent
ENCYCLOPEDIA OF TELECOMMUNICATIONS

Editor-in-Chief

Fritz E. Froehlich, Ph.D.
Professor of Telecommunications
University of Pittsburgh
Pittsburgh, Pennsylvania

Co-Editor

Allen Kent
Distinguished Service Professor of Information Science
University of Pittsburgh
Pittsburgh, Pennsylvania

Administrative Editor

Carolyn M. Hall
Pittsburgh, Pennsylvania

VOLUME 10

INTRODUCTION TO COMPUTER NETWORKING to METHODS FOR USABILITY ENGINEERING IN EQUIPMENT DESIGN

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First published 1995 by Marcel Dekker, Inc.

Published 2021 by CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

ISBN 13: 978-0-8247-2908-0 (hbk)
ISBN 13: 978-1-003-20988-1 (ebk)

DOI: 10.1201/9781003209881

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Library of Congress Cataloging-in-Publication Data

The Froehlich/Kent Encyclopedia of Telecommunications / editor-in-chief, Fritz E. Froehlich ; co-editor, Allen Kent.
p. cm.
Includes bibliographical references
ISBN 0-8247-2902-1 (v. 1 : alk. paper)
1. Telecommunication—Encyclopedias. I. Froehlich, Fritz E., Kent, Allen.
TK5102.E646 1990 90-3966
384′.03—dc20 CIP

CONTENTS OF VOLUME 10

CONTRIBUTORS TO VOLUME 10

Jill D. Austin, M.B.A., Manager, Multi-Site Marketing for Multi-Site Systems, Northern Telecom, Inc., Nashville, Tennessee: *ISDN Applications*

Joyce E. Bedi, Hagley Fellow, Department of History, University of Delaware, Newark, Delaware: *Jenkins, Charles Francis, 1867–1934; Marconi, Guglielmo*

Imrich Chlamtac, Ph.D., Associate Professor, University of Massachusetts, Amherst, Massachusetts: *Introduction to Computer Networking*

Charles A. Dvorak, Ph.D., Technical Manager, AT&T Bell Laboratories, Bedminster, New Jersey: *ISDN, Broadband Performance Using Asynchronous Transfer Mode Transport*

Magda El Zarki, Ph.D., Assistant Professor, University of Pennsylvania, Philadelphia, Pennsylvania: *Introduction to Computer Networking*

Jennette I. Floyd, M.B.A., Senior Manager, Marketing and Technology, Northern Telecom, Inc., Morristown, New Jersey: *ISDN Applications*

Henry J. Fowler, M.S., Member of Technical Staff, Bellcore, Red Bank, New Jersey: *ISDN—Broadband Services*

John M. Goodman, Alexandria, Virginia: *Meteor Burst Communication*

James P. Gordon, AT&T Bell Laboratories, Holmdel, New Jersey: *Long-Distance, High-Bit-Rate Transmission Using Solitons in Optical Fibers* (co-author of appendix)

Motoo Hoshi, Senior Research Engineer, Nippon Telegraph and Telephone Corporation, Tokyo, Japan: *ISDN Introduction Planning in Developing Countries*

Edmond W. Israelski, Ph.D., Technical Manager, Human Factors, AT&T Bell Laboratories, Middletown, New Jersey: *Methods for Usability Engineering in Equipment Design*

Simin Kamvar, Ph.D., Member of Technical Staff, AT&T Bell Laboratories, Holmdel, New Jersey: *ISDN, Broadband Performance Using Asynchronous Transfer Mode Transport*

Jagdish C. Kohli, Ph.D., Project Manager, Health Information Network, Pacific Bell, San Ramon, California: *Medical Communications*

Raymond W. Lawton, Ph.D., Associate Director, The National Regulatory Research Institute; Adjunct Associate Professor, School of Public Policy and Management, The Ohio State University, Columbus, Ohio: *Local Subscriber Loop Competition Issues*

Salomon Lederman, M.S.E.E., E.E., Distinguished Member of Staff, Bellcore (retired), Red Bank, New Jersey: *ISDN—Broadband Services*

Benjamin J. Leon, Sc.D., Distinguished Professor, Center for Telecommunication Studies, Department of Electrical and Computer Engineering, University of Southwestern Louisiana, Lafayette, Louisiana: *Introduction to Telecommunications Project Planning*

Gottfried W. R. Luderer, Dr.-Ing., ISS Chair Professor of Telecommunication, Telecommunications Research Center, College of Engineering and Applied Sciences, Arizona State University, Tempe, Arizona: *Introduction to Packet-Switched Technology*

John E. Midwinter, Ph.D., Pender Professor of Electrical Engineering, University College London, London, England: *Light-Wave Communication Systems and Technology*

Tetsuya Miki, NTT Transmission Systems Labs, Take, Japan: *Lightwave Fiber Cables and Optical Subscriber Loops*

Linn F. Mollenauer, Ph.D., Distinguished Member of Technical Staff, AT&T Bell Laboratories, Holmdel, New Jersey: *Long-Distance, High-Bit-Rate Transmission Using Solitons in Optical Fibers*

Mahmood R. Noorchashm, Ph.D., Member of Technical Staff, AT&T Bell Laboratories, Holmdel, New Jersey: *ISDN, Broadband Performance Using Asynchronous Transfer Mode Transport*

Paul E. Prozeller, M.E.E., Distinguished Member of Technical Staff, AT&T Bell Laboratories, Holmdel, New Jersey: *An Introduction to Telecommunications Operations and Network Management*

Marylin K. Sheddan, Vice President, Astro Tech, Inc., Daytona Beach, Florida; Research Associate, Embry Riddle Aeronautical University, Daytona Beach, Florida: *Jansky, Karl Guthe; Maxwell, James Clerk*

Joseph D. Straubhaar, Professor, Department of Telecommunications, Michigan State University, East Lansing, Michigan: *Liberalization and Privatization Patterns in Eastern Europe and the Third World*

John R. Whinnery, Ph.D., University Professor Emeritus, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, California: *Lasers for Optical Communication*

Mark A. Winther, Vice President, Worldwide Telecommunications, IDC/LINK Resources Corporation, New York, New York: *IVAN Services: International Value-Added Network Services*

The Froehlich/Kent

ENCYCLOPEDIA OF TELECOMMUNICATIONS

VOLUME 10

Introduction to Computer Networking

Introduction

What Are Communication Networks?

A communication network consists of a set of nodes that are interconnected via a transmission medium to permit the exchange of information. We distinguish between two types of connections that can exist in a network: point to point and multipoint. A point-to-point connection specifies a one-on-one communication between two end points, for example, a telephone conversation between two individuals. A multipoint connection involves several parties being active and communicating simultaneously, for example, a videoconferencing session between three or more people or a conference call. Communication networks can be broadly classified as switched or broadcast.

In a switched communication network (Fig. 1), only the parties involved in the communication receive the information, and switching nodes are used to relay the data over transmission links. Two types of networks fall within this class: circuit switched and packet switched.

In a broadcast communication network (Fig. 2), the information is broadcast over a common transmission medium to which all nodes are attached. No switching is involved as all parties listen to the transmission channel. Examples of such networks are packet-radio networks, satellite networks, and local networks.

The Evolution of Communication Networks

The telephone network was the first example of a communication network. It started off by providing a very limited point-to-point communication service. This evolved to a meshed manual network in which switchboard operators were used to set up the circuits between various parties. Automated switching replaced the operators and now highly sophisticated electronic switches that are computer controlled not only set up circuits but also provide a whole set of services from call waiting and call forwarding to caller identification and so on.

The next step in networking came from the data-processing world. The desire to share expensive computer resources prompted the establishment of data communication networks by which users could gain access to a computer via remote terminals. With the advent of the workstation and the personal computer, it was not computing resources that needed to be shared but instead disks (file servers) and printers. With the proliferation of computers in the workplace, local networks were introduced to provide the necessary local connectivity. To gain access to the outside world and wider coverage, bridges and routers are used.

The current move is toward integration, with the goal to build a single network that will provide voice, video, and data services to everybody. Narrowband Integrated Services Digital Networks (NISDNs) are a first step in that

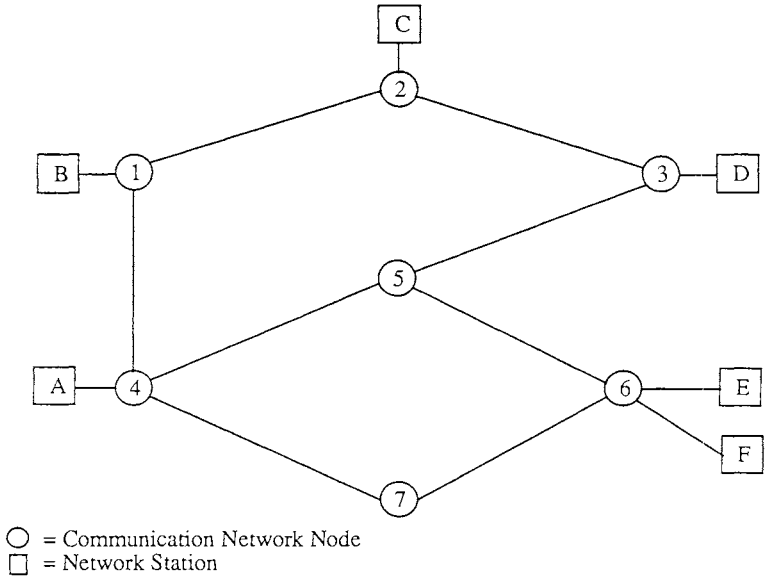


FIG. 1 Diagram of a switched communication network.

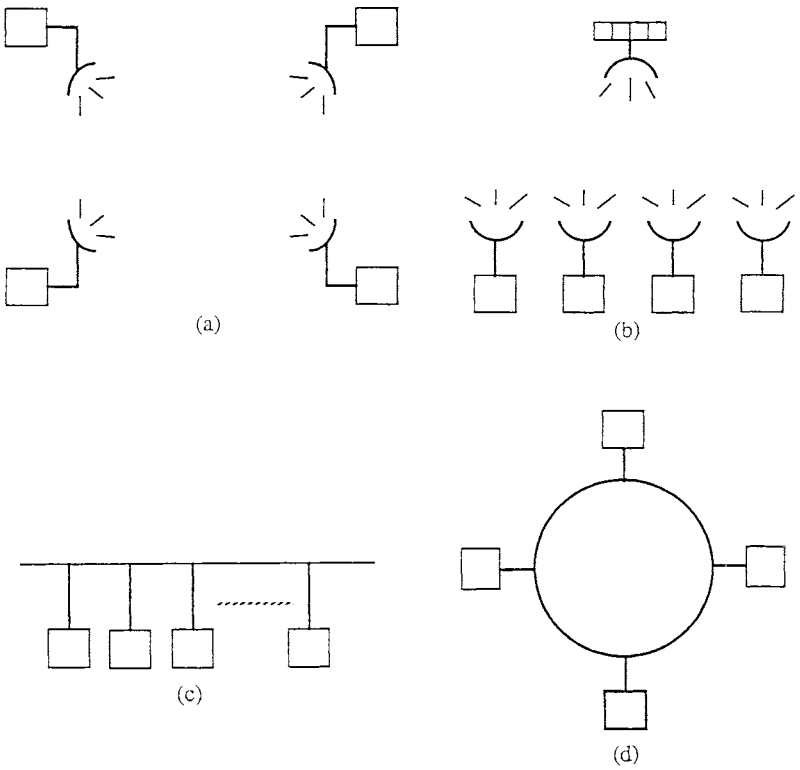


FIG. 2 Examples of broadcast communication networks: *a*, packet terrestrial radio; *b*, satellite; *c*, local network with bus topology; *d*, local network with ring topology.

direction. The future lies in optical technology, Broadband ISDN (BISDN), and wireless communication networks.

Standards and Standards Organizations

Standards and the organizations responsible for making them come into play whenever more than one organization participates in the following activities: the dissemination of information, the specification of performance and quality attributes, compatibility, the reduction of the variety of interfaces, and the definition of standardized tests and measurement methods. Standards fulfill one or several of these functions (1). There are both advantages and disadvantages to standards. The main advantage that standards can offer is compatibility among vendors' equipment, offering the user the option for interchangeability, and providing purchasing flexibility. On the larger scale, standards offer a means for competitive entries into a particular market, and can be seen as a method to distribute technical information.

There are several disadvantages to standards that can be seen at the development and corporate levels. These include the time that it takes to release a standard (often several years) and the effective freezing of technology once a standard has been accepted (the elapse of time between updates of a standard can be on the order of two to four years). In some cases, a standard is developed while still within the research phase, causing a release of a nonoptimal standard or even a faulty one. All in all, the advantages gained by standards far outweigh the disadvantages, with one of the primary goals being the economically driven market to supply the end users with compatible, inexpensive and reliable products.

What standards organizations are involved in making decisions concerning telecommunications standards on the international and national levels? On the international level, the International Telecommunication Union (ITU) allows membership from national governments, is recognized by private companies (i.e., AT&T, IBM), and allows international organizations to participate on its committees. Most activities are within its International Telegraph and Telephone Consultative Committee (CCITT) (renamed ITU-T in 1994) and the International Radio Consultative Committee (CCIR). Another large player is the International Organization for Standardization (ISO), which is a nongovernmental organization that produces standards using a balloting procedure among its members every two to four years.

Within the United States, the key standards organizations include the American National Standards Institute (ANSI), a nonprofit organization that coordinates voluntary standards and is the U.S. representative to the ISO. Other organizations are the Institute of Electrical and Electronics Engineers (IEEE), which is a professional association interested in areas of computer communications, and the National Bureau of Standards (NBS).

In the European Community (EC), the key standards group is the European Telecommunication Standardization Institute (ETSI), formed in the late 1980s,

with members that may be from within or outside the EC. These members can be telecommunication administrators, public network operators, manufacturers of telecommunications equipment, private service providers, and users (1). Another standards group is the Conference of European Postal and Telecommunications Administrators (CEPT).

Network Architectures and Protocols

The goal of a communication network is to provide services to users. These services consist of transfer of information (voice, data, video, etc.), signaling (both user and network oriented), and accounting and billing. These services are defined by network architectures and protocols.

A *network architecture* defines the manner in which a complex service is decomposed into a set of simpler services, where each service is to be performed, and what will perform the service. The internals of the services are hidden and services can interact only via specified interfaces. A *layered architecture* is one in which services are layered; service layer N uses service layer $N - 1$, and so on (see Fig. 3). Layer N interacts with Layers $N + 1$ and $N - 1$, providing services to Layer $N + 1$ and exchanging information with other N layers. A service of Layer N is executed by peer communicating entities. The set of rules that governs the flow of information between peer layers is called a *protocol*. In the next few sections, we discuss some network architectures and protocols that are currently in use.

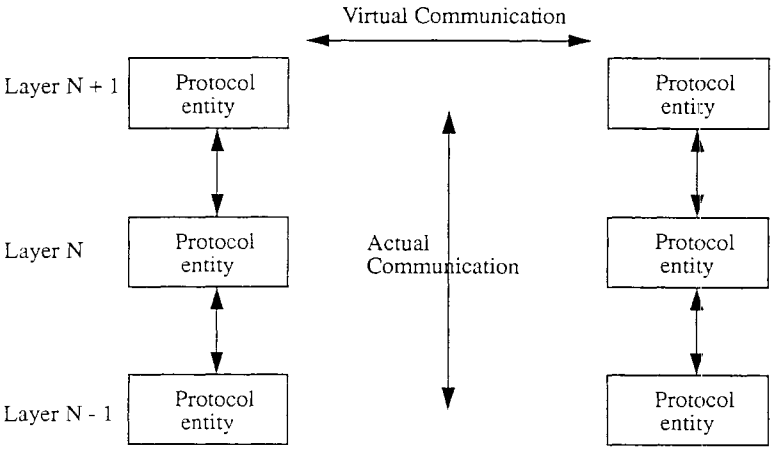


FIG. 3 A layered architecture.

Standard Network Architectures

The most common network architecture is the Open System Interconnection (OSI) specified by the ISO. Other examples of standard architectures are the set of IEEE 802 standards for local networks, the Department of Defense (DoD) Transmission Control Protocol/Internet Protocol (TCP/IP) suite used in the Internet community, and the Manufacturing Automation Protocol (MAP) introduced by General Motors.

The Open System Interconnection Architecture

The OSI Model was developed by the ISO and CCITT in 1984 and was originally a model for computer communications architectures. It now is being extended for use in integrated networks. The OSI Model consists of seven layers and can be divided into two subgroups (see Fig. 4). Layers 1 through 3 are known as the subnet layers and Layers 4 through 7 are referred to as the host layers. Even though communication appears between peers, the transfer of information occurs between adjacent layers on nodes. Thus, Layer N is expected to supply specific services to Layer $N + 1$ (with the exception of the highest layer) and to receive specific services from Layer $N - 1$ (with the exception of the lowest layer).

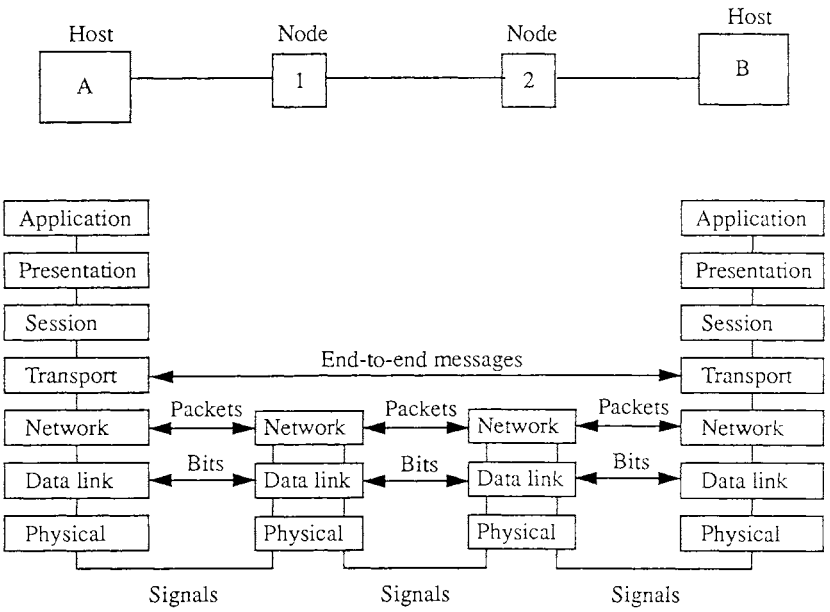


FIG. 4 The Open System Interconnection Model.

The layers of the OSI Model are

- Layer 1, physical layer, for transmission of bits on a link
- Layer 2, data-link layer (DLL), for transmission of frames on a link
- Layer 3, network layer, for transmission of packets across a subnet
- Layer 4, transport layer, for transmission of messages end to end between two hosts
- Layer 5, session layer, for set up and management of an end-to-end communication
- Layer 6, presentation layer, for formatting, encryption, and compression of data
- Layer 7, application layer, for network services (E-mail, file transfer, remote access, etc.)

In the following few paragraphs, we briefly explain the function of each of the OSI layers by the services it provides to the layer above it. (For more details, the reader is referred to Ref. 2.)

Physical Layer. The physical layer provides the data-link layer (DLL) with a means to transmit data over the physical medium. It expects only a bitstream from the DLL, which it converts into the appropriate electrical or optical signals for transmission over a physical medium.

Data-Link Layer. Just as the physical layer concerns itself with the transmission of electrical or optical signals, it is up to the DLL to provide a communication service over a transmission medium to the network layer. The job of the DLL at the transmitting end is to create frames with headers that contain all the relevant error-control and sequencing information. At the receiving end, the DLL is responsible for handling problems caused by packets that are lost, damaged, or duplicated upon arrival. It is worth pointing out that, for broadcast-type networks, the DLL is divided into two subcomponents known as the logical link control (LLC) and the medium access control (MAC). These are covered in more depth in the section on local-area networks (LANs).

Network Layer. The network layer, responsible for end-to-end transmissions across a subnet, provides services concerning the routing of data and congestion control. It hides the details of the network (transmission and switching functions) from the transport layer. This allows technical advancements to be made to the subnet without affecting the operation of the upper layers. Routing and congestion control are covered in detail in separate sections.

Transport Layer. The transport layer concerns itself with the exchange of data between hosts. It does not concern itself with how the data is transferred,

only that it reaches the destination correctly. As such, it is responsible for the establishment and deletion of connections between hosts across the network. The transport layer is truly the first end-to-end layer since it communicates directly with a peer process on another host machine. It provides for a transparent transport system to the upper layers, and incorporates both error-recovery mechanisms and flow control. It also is responsible for multiplexing the data-streams from several connections to the same end point.

Session Layer. The session layer provides the dialogue control that allows users to establish and synchronize connections between applications on different hosts.

Presentation Layer. The presentation layer provides the valuable service of resolving differences in data representations between two application processes. It is concerned with the syntax used and other forms of data representation that allow two different applications the ability to find a common ground over which to communicate.

Application Layer. The final layer, known as the application layer, provides a means for the application processes to access the OSI Model and exchange/share information.

The Department of Defense Architecture

The Department of Defense (DoD) architecture is very similar to the OSI Model with respect to the four lower layers. It uses a different set of protocols for peer-to-peer communication but the functionality is identical. On top of Layer 4 are applications; these applications encompass the functionality defined by Layers 5–7 in the OSI Model. The DoD protocol suite is used in the Internet community and is very common in UNIX®-based workstations.

Institute of Electrical and Electronics Engineers Architecture

The IEEE defined an architecture for local-area networks (LANs). It basically consists of the two lower layers of the OSI Model. As mentioned in the section on the DLL, Layer 2 is subdivided into two layers to handle broadcast-type environments. More details are given in the section on LANs.

Standard Network Protocols

In the sections below, we describe some of the protocols used by the different layers for communication. Examples of standard protocols are given.

The Physical Layer

Specifications for this layer are concerned with the mechanical, electrical, functional, and procedural tasks to be supported. The mechanical specifications deal with the connector's interface, how many pins must exist, and the dimensions of the connector itself. Electrical specifications define signal characteristics, in other words, the pulse duration and amplitude of the signals on the medium. The functional aspect of the physical layer deals with how to define pins on the connector (i.e., control/data pins, VDD, and GND pins, etc.). The last characteristic is the procedural specification; it defines the setup, use, and deactivation of the physical connection.

Standards associated with the physical layer are RS-232-C, RS-449/422/423, CCITT X.21, and the like.

Data-Link Layer

DLL protocols are responsible for implementing error-recovery mechanisms and flow control. We describe some of these schemes here. The two most popular schemes for error control are go back N and selective repeat. For the former, the destination discards all frames that are received out of sequence (erroneous frames are automatically discarded). An acknowledgment is sent to the transmitter of the last frame received correctly and in sequence. Upon its reception, the transmitter retransmits all outstanding frames (those for which no acknowledgment has been received yet). This is opposed to the selective repeat scheme in which the destination indicates exactly the frames that it is missing. The advantage of the go back N is that the buffering scheme at the destination can be fairly simple, but it does waste throughput (frames retransmitted even though they are received uncorrupted).

Another very important function of the DLL is to be able to slow a fast transmitter down so that it does not overwrite data that has been received previously (flow control). The simplest scheme is stop and go, in which, for every frame transmitted, the receiver has to wait until it receives an acknowledgment before it may transmit the next frame. The sliding window scheme allows several frames to be outstanding between the transmitter and receiver. It is like a token mechanism in which up to N tokens maybe used to send packets. Every returning acknowledgment frees up a token again. (Note that the stop-and-go scheme is a special case of the sliding window with $N = 1$). An optimum N can be calculated that will maximize the throughput on the link.

A variety of protocols exist for the DLL and are either character-oriented or bit-oriented protocols. The character-oriented protocols use character sets (either American Standard Code for Information Interchange [ASCII] or Extended Binary Coded Decimal Interchange Code [EBCDIC]) for DLL control; an example is ANSI X3.28 BYSNC. While bit-oriented protocols do not use information-coded characters for control since they perceive communication as a continuous bitstream, they use flags and other bit sequences for control information. Examples of bit-oriented protocols are High-Level Data-Link Control (HDLC), Link Access Protocol-Balanced (LAP-B) (which is part of

CCITT Recommendation X.25), and Advanced Data Communication Control Protocol (ADCCP) (which is part of CCITT Recommendation X.75).

Network Layer

The network layer provides two types of service to the upper layers: connection oriented (CO) or connectionless (CL). CO service emulates a circuit-switched connection between the two end points. The difference lies in the fact that no physical channels are reserved for the connection, it is only a logical channel, and the link is shared by many connections. For CL service, there is no designated path between the source and the destination and the information is segmented and can be sent over different links.

The most common CO protocol is CCITT Recommendation X.25, which is used primarily in public data networks (see "Homogeneous Networks"). Within OSI, there is no example of a CL protocol. The Interface Protocol (IP) utilized by the Internet community is a good example of a CL protocol. IP is used for communication by most UNIX workstations.

Transport Layer

Just as for the network layer, the transport layer can provide either a CO or CL communication service to the upper layers. The ISO and CCITT have defined TP4 (Transport Protocol—Class 4) as the transport-layer standard. The "4" stands for Classes 0–4 (TP0, TP1, TP2, TP3, and TP4), each class defining a different set of services that includes multiplexing, error detection and recovery, and flow-control capabilities. It provides a CO service.

The Transport Control Protocol (TCP) of the DoD standard is also a CO service and, just as IP, it is used for communication between hosts in the Internet community (it is supported by most UNIX workstations). User Datagram Protocol (UDP) is an example of a CL service and is used by some of the applications defined in the DoD architecture (e.g., E-mail).

Session Layer

Session-Layer protocols are responsible for the setup and teardown of connections between two hosts and the synchronization of data transfer between them. Dialogues can take the form of two-way simultaneous (full duplex) and two-way alternate (half duplex), with the latter requiring some type of token management. Token management is simply a method in half-duplex mode that guarantees that only the host holding the token can perform a critical operation without worrying about the other host accessing the channel.

There are no good examples of session-layer protocols. Most applications have them built in (e.g., the DoD architecture). OSI has defined a specification but it is not used.

Presentation Layer

Similar to the session layer, there are no standard protocols for the presentation layer (they are built into current applications). Data compression and encryption are two prime functions that will be included in any specification.

Application Layer

Several application-layer protocols exist; these include those defined by the DoD architecture (which includes session and presentation layers). Common protocols seen within the application layer include the File Transfer, Access, and Management (FTAM) Protocol, which is used widely in public networks, and the CCITT X.400 standard, also known as Message Handling System (MHS) or E-mail. The protocols used in the Internet include File Transport Protocol (FTP), Telnet (a virtual terminal protocol for connecting to remote hosts), Simple Mail Transfer Protocol (SMTP) (used for E-mail), and the three UNIX-based commands: rsh (remote execution of commands), rlogin (a virtual terminal with log-in facilities), and rcp (remote copying of files).

Local-Area Networks

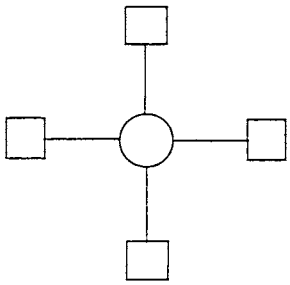
Local-area networks (LANs) are networks that span short distances and provide local connectivity. They were introduced in the early 1970s to meet the demands of the information age—the proliferation of personal computers and electronic document systems. The main features of LANs may be summarized as follows:

- They typically consist of a common shared resource.
- They provide point-to-point and multipoint communication.
- They are characterized by high bit rates and inexpensive interfaces.

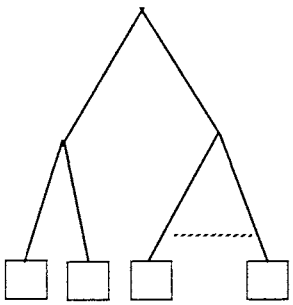
LANs epitomize the modern era of computing. The electronic office came into being because of LANs, they allowed printers and file servers to be shared, and they are the main vehicle for electronic mail. Below, we describe some of the popular LAN topologies and access protocols. Also, a brief outline of wireless LANs, a new and upcoming development in the field, is given.

Topologies

There are four widely used configurations: star, ring, tree, and bus. Figure 2 shows the bus and ring topologies and Fig. 5 illustrates the tree and star topologies. For each one, we can enumerate a list of advantages and disadvantages.



Star



Tree

FIG. 5 Star and tree topologies, two of four widely used local-area network topologies.

Their performance is highly dependent on the access protocol used. We discuss these issues when we describe each configuration in some detail.

Star

In a star topology (Fig. 5), all the nodes are directly connected to a central switch via point-to-point links. Each link is bidirectional. The switch is responsible for relaying signals between the different nodes. The simplest switch configuration will just broadcast to all the nodes. A more-intelligent system will select the appropriate outgoing link on which to transmit the signal. Throughput of the network will increase if data can be buffered at the switch during periods of congestion. As to reliability, the network is down when the switch is down.

Ring Topology

Ring networks (Fig. 2) consist of nodes connected via point-to-point links in a closed loop. The links can be uni- or bidirectional. Some topologies consist of a

dual-ring topology for reliability and higher throughput. The most common configuration consists of a single unidirectional ring. All nodes on a ring network are active, that is, they act as repeaters. The signal is received by each node, amplified, and then sent out again. There is therefore no physical limitation to the size of these networks. However, because of this repeater characteristic, the signal incurs some delay at each node, thereby affecting the throughput/delay characteristics of the network. This may be overcome at the data-link layer through a choice of more complex protocols. In regard to reliability, there is a single point of failure for the single ring; any node or link failure will bring down the network. The dual topologies can be reconfigured to provide connectivity in case of a single failure.

Bus and Tree Topologies

Both bus and tree topologies are characterized by the use of a multipoint medium. The medium can be either uni- or bidirectional. For the unidirectional medium, to provide the desired connectivity, the topology has to be a dual tree or dual bus. Nodes are generally passive. In case of the tree topology, the nodes constitute the leaves. Each branch of the tree is controlled by what is referred to as a hub. Hubs act as repeaters, receiving the signal and broadcasting it over the links. Through use of more intelligent hubs, the throughput of the network may be increased by selective broadcasting. As to reliability, for the bus network, only a link failure will affect it. In the tree network, the failure of a hub will isolate a branch of the tree, thereby limiting the connectivity of the system.

Media Access Protocols

Compared to the OSI Reference Model, LANs only span the lower two levels. However, in LANs we find that the data-link layer is split into two distinct sublayers: the media access control (MAC) and the logical link control (LLC). The MAC regulates the access to the channel shared by the nodes and the LLC supervises the transmission of frames. The IEEE has played an important role in the specification and standardization of LANs. The IEEE 802 Standard covers most commercial LANs, with some exceptions (e.g., Appletalk™). The IEEE 802.3–9 Standards specify the physical layer and the MAC, each one representing a different LAN (see Fig. 6). The IEEE 802.2 Standard specifies the LLC; it is a common interface for all of the IEEE 802.3-9 standards. Below, we describe some of the most popular LANs in terms of their topology and their MAC.

Examples of Local-Area Networks

Networks Based on Carrier Sense Multiple Access with Collision Detection

The IEEE 802.3 standard specifies a bus network that uses a MAC protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

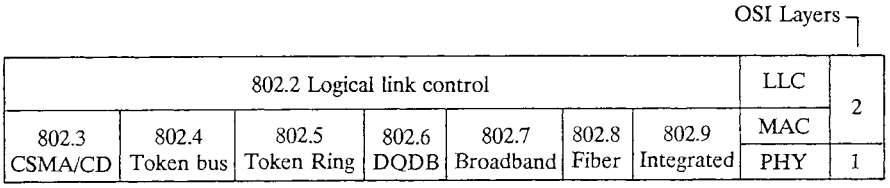


FIG. 6 The Institute of Electrical and Electronics Engineers architecture.

There are five versions of IEEE 802.3; they all differ (medium, coding, topology) at the physical layer. All the 802.3 networks use broadcasting of information with collision detection; however, each version uses its own technique for sensing the channel and detecting collisions (highly dependent on the physical layer).

Ethernet is very similar to one of the IEEE 802.3 versions (10BASE5 network); they both use the same MAC. The difference lies in the structure of the frame. Next, we describe the Ethernet network in some detail.

The Ethernet network consists of the following:

- Nodes that contain a network interface card
- Transceiver cable that connects the interface card to the transceiver
- Transceivers that connect to the network via a tap

As to the operation of Ethernet, when a node has a packet to transmit, it copies it into a buffer on the interface card. The interface card waits for the transceiver to indicate when the cable is idle. It then sends the Manchester-encoded bits comprising the packet to the transceiver for transmission on the cable. While transmitting, the transceiver monitors the cable to detect a collision. When one occurs, it stops transmitting and informs the interface board. The interface board then transmits a random sequence of bits (32–48 bits) that constitute a jam signal to inform the rest of the network that a collision has occurred. The interface card waits a random amount of time before retransmitting (using a backoff algorithm). The interface card gives up after 16 successive collisions.

The backoff algorithim used is the binary exponential backoff algorithm. If a packet has collided n successive times, where $n < 16$, then the node chooses a random number K with equal probability from the set $(0, 1, 2, 3, \ldots, 2^m - 1)$, where $m = \min(10,n)$. The node then waits $K \times 512$ bit times (512 bit times are less than the propagation delay on the network). Nodes not transmitting also can detect a collision because the frame size of a collided packet does not exceed 500 bits. Minimum frame size is 544. Maximum specified collision detection time is 450 bit times ($< 2\times$ end-to-end propagation delay).

Token-Ring-Based Networks

The token ring was developed by IBM. Several different token-ring networks exist; IEEE 802.5 specifies one such standard. Token-ring networks differ primarily in the frame structure and their token-release mechanism.

A token-ring network works on the premise of a token circulating around a ring. The token is used as a permit to transmit. A node that wants to transmit has to wait for the token to come by. It then grabs the token and replaces it with another bit pattern signifying beginning of frame (start of frame delimiter, SFD). The frame is appended to the SFD. Depending on the token-release mechanism implemented, the station either

- Releases the token after the frame is transmitted (release after transmission, RAT), or
- Releases the token only after the source S has received the transmitted frame again (release after reception, RAR).

The advantage of the first scheme is that it is more efficient; the stations do not have to wait for a full rotation time. However, the second scheme simplifies acknowledgments. The destination station indicates in a special field in the trailer of the frame if it received the frame, if it was in error, and so on.

To increase the efficiency of the token ring, a counter called the token-holding timer (THT) is used. Stations that have more than one frame in their buffer may transmit several consecutive frames until the expiration of the THT.

For token-ring networks, access delay (i.e., the access time to the ring) is of concern, in particular, for control information or synchronous services (3). We specify MMAT (maximum media access time) for nodes using THT:

- Assume Node 1 gets a control packet to transmit just as it is transmitting the last frame before expiration of its THT.
- Every node is loaded and transmits for THT.
- Then MMAT can be calculated as follows:

$$MMAT_{RAT} = DP + NxTT + TP + (N - 1)THT$$

or

$$MMAT_{RAR} = (N + 1)DP + NxTT + TP + (N - 1)THT$$

where

N = number of nodes
DP = ring latency
TT = token transmission time
TP = frame transmission time

Token Bus Networks

Token bus networks are bus networks that use a token-passing MAC. IEEE 802.4 specifies the only commercially available token bus network. It is used by the MAP protocol suite for factory communication (as it guarantees bounded time delays). Its operation can be summarized as follows.

The token is passed from one station to the next in cyclic order. The address in the token indicates the next user. If a station has nothing to transmit, it addresses the token to the next node. For the operation of the MAC Protocol, each node needs to know its successor. So, if a node is removed from the bus, its predecessor must be informed. Because of this, every node on the network has to be active (i.e., has to read the token and pass it on). If a node does not want to participate, it must remove itself from the bus.

The process of adding and deleting nodes from the bus can be automated as follows:

- Periodically, an active node issues a SAS (solicit a successor) frame.
- An idle node can become active by responding to this SAS message.
- The SAS contains the address of the originator and the address of its successor.
- The reply to the SAS message from an incoming node includes its address.
- The incoming node knows its predecessor and successor from information in the SAS frame. The originator of the SAS frame knows its new successor from the reply.
- If several nodes want to become active at the same time, we have a collision. It is resolved using a binary tree resolution method that uses the nodes' addresses as keys.
- If a node wants to become idle, it sends out a message "I want out." It includes predecessor and successor addresses.
- Its predecessor then knows where to send the token after the node leaves the network.

A token bus network also includes mechanisms for recovery from node failures:

- If a node fails, it will not respond to its token.
- The predecessor will observe the nonresponse and send out a message "Who follows *X*."
- The next node will respond and receive the token. The predecessor and successor tables of the two nodes neighboring the failed node are updated.

Performance Comparison

Comparing the performance of Ethernet to that of token rings and token buses, we find that the efficiency can be much higher for the token schemes but

Ethernet is more reliable. It is a passive network, makes no use of tokens that may be lost or corrupted, and has no active network components that could impair the performance of the whole network if faulty. For an analytical comparison, the reader is referred to Ref. 4. For all of the three networks, the throughput is very much a function of the frame length and network size in terms of number of nodes and length of the cable.

The Logical Link Layer

As mentioned in the discussion of media access protocols, the LLC is responsible for the transmission of frames between two nodes on the network. As such, its basic functions are error control, frame multiplexing, and controlling the data flow. The third function is not always implemented at the LLC level; it is often left to higher layers in the hierarchy to regulate.

There are three basic LLC frames: data frames, test frames, and XID (exchange identification) frames. Test frames are used to test a connection to another node. LLC frames also can specify a service class in the form of a priority that is used with the IEEE 802.4–6 networks. XID frames are used to find the members of a group.

Three types of service are specified by the LLC: connectionless, acknowledged connectionless, and connection oriented. Connectionless service is a purely datagram-type transmission with no guarantees that the frame is received or that it has no errors. A flow-control mechanism can be superimposed to limit the number of packets transmitted within a certain period. It will have to be implemented at a higher level. Acknowledged connectionless service refers to a datagram service in which a frame may be transmitted only after an acknowledgment has been received for the previous frame (i.e., built-in flow control, stop and go). For the connection-oriented service, the LLC goes through a call setup phase, then a data-transmission phase, and terminates with a call teardown phase.

Wireless Local-Area Networks

Computer communication is as important in mobile environments as in static ones. Personal computers are becoming much more mobile, some locations do not allow for cabling, and, in some instances, the flexibility to set up a communication environment quickly, take it down, and reset it again, are dictating wireless communication. While in the past wireless LANs used proprietary protocols and operated at capacities of only 1 megabit per second (Mb/s), several companies are today developing products compatible with the Ethernet and token-ring networks and providing 10-Mb/s communication. In this section, we therefore do not dwell on the MAC protocols described above, but instead focus on the salient features of wireless indoor communication (5).

One of the challenges today is in regard to the technology needed to obtain such mobility. Infrared technology has been adopted by several vendors to develop wireless LAN systems compatible with the IEEE 802.3 Ethernet stan-

dard. Infrared light is not visible to the human eye; it uses frequencies lower than those of red light. However, its frequency is high enough, greater than 1000 gigahertz (GHz), so that it can be reflected off solid objects. Thus, walls in particular can be used to reflect the signals; in this way, all transmitters or receivers do not need to be in line of sight of each other, but also can use reflected signals to communicate.

Radio frequencies (RFs) also can be used as a transmission medium. Some of the issues involved with RF are bandwidth availability, signal reflections, interference, and Federal Communications Commission (FCC) regulations. To deal with these issues, two main approaches have been developed. One, the narrowband solution, transmits raw data directly on a given center frequency. In this case, the main difficulty for an indoor LAN is the multipath interference, as signals are reflected off various objects and arrive at the receiver at different times. Thus, smart antennas must be used to overcome this obstacle. Such a solution requires, however, that channels be clear, that is, that no other noise or signals will be present. As a consequence, every transmitter location must be licensed by the FCC.

The second solution to the use of RFs as a transmission medium is based on using the ISM (industrial, scientific and medical) bands, allowed by the FCC for wireless communications. As long as the safety power standards are not exceeded, anyone can transmit in these bands. Spread-spectrum technology is used operating in CDMA (code division multiple access) mode. Both direct sequence and frequency hopping are used by different designers today. Spread spectrum can deal effectively with multipath and noise interference problems.

To build a wireless radio (or light) LAN, two topologies are possible. One allows direct communication between any two users (a peer system) and the other is based on a central controller. A peer communication system is a naturally less-expensive, entry-level solution as no controller overhead is incurred. In this case, however, the near–far problem can be a limiting factor since transmissions between stations near each other can prevent far stations from accessing their neighbors located nearby. Furthermore, there is no way to adjust the output power of the stations so that these types of conflicts are avoided. While the entry-level cost of a central-controller-based system is higher, it eliminates the near–far problem since each station needs only to reach the single central-controller point. The existence of a central controller also facilitates network management, access control, and can be used to implement functions such as a LAN-to-WAN (wide-area network) interface.

The development of IEEE 802.11 formal specifications for wireless LANs, and the proliferation of portable computing elements and falling equipment costs, harbor a good potential for these systems.

Metropolitan-Area Networks

Metropolitan-area networks (MANs) are networks that span longer distances than LANs and provide local interconnectivity. MANs were introduced when it

was considered important to provide local businesses with a means of interconnecting their LANs over wider distances. As such, they provide higher bit rates than LANs and are characterized by more expensive interfaces. Currently, MANs are used either as local backbones to interconnect many LANs at a site or as high-speed LANs. MANs, like LANs, have regular topologies and, similar to LANs, the data-link layer is split into an LLC and an MAC that provide the same functionality.

Though many MANs have been proposed over the years, only two MAN standards have been accepted. One is the fiber distributed data interface (FDDI) specified by ANSI (also referred to these days as a high-speed LAN standard). The other is the distributed queueing dual bus (DQDB) specified by IEEE (802.6). We describe these below, providing details as to the topology and the operation of the MAC sublayer.

Examples of Metropolitan-Area Networks

Fiber Distributed Data Interface

The FDDI is a dual-ring network that was proposed as a MAN by ANSI (6). Figure 7 shows the topology. Currently, there are two FDDIs specified by the standard, FDDI-I and FDDI-II. The former was proposed for nonisochronous services; the latter is a new specification that allows the support of isochronous services.

FDDI specifies two types of stations, one that can connect to both rings and one that connects to one ring only. The physical layer of FDDI is composed of

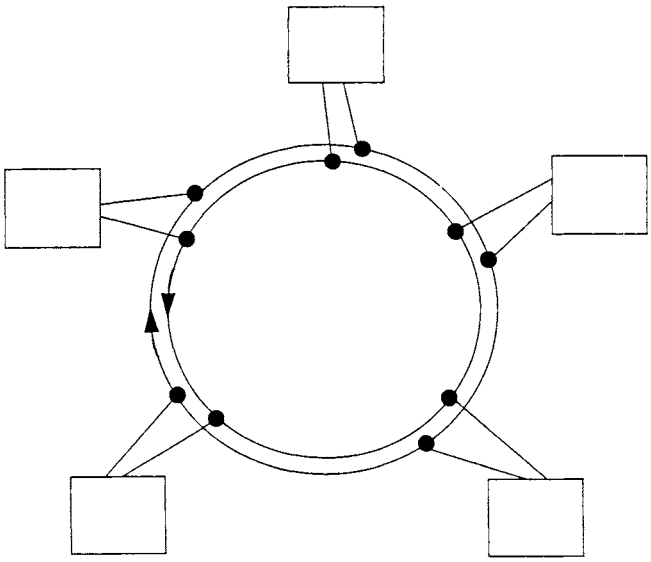


FIG. 7 Fiber distributed data interface topology.

two sublayers: (1) the physical layer medium dependent (PMD) sublayer, which specifies the medium, the receivers and transmitters, and so on; and (2) the physical (PHY) sublayer, which specifies the signal rate, the coding and modulation methods, preamble, and so on.

The data-link layer consists of the MAC and LLC. The MAC layer is responsible for obtaining access to the ring. Traffic on FDDI is split into synchronous traffic and asynchronous traffic. The MAC Protocol uses a timed-token protocol to guarantee access to the ring for synchronous traffic within a maximum bound specified at ring initialization. It also uses RAR, that is, the sender removes the frame from the ring. The destination indicates frame reception by setting bits in the ACK (acknowledge) field. All stations on the ring are active; therefore, to increase reliability, bypass switches are used.

To summarize the MAC operation,

- The nodes at initialization agree on a target token rotation time (TTRT). The minimum bid is the one used. All bids for synchronous traffic cannot exceed the total bandwidth (BW) of the channel. Leftover BW is used by asynchronous traffic.
- Each station stores the TTRT time in a TRT (token rotation timer) counter.
- A station that has synchronous traffic to transmit may do so whenever it receives the token. A station may not exceed its requested BW.
- For asynchronous transmission, a station may transmit data only when it gets the token before the TRT counter has expired. Whenever the TRT counter expires and the station has not seen the token, a second counter called Late-Ct is set to 1. The TRT is set to TTRT again. If the TRT expires a second time, the station assumes a ring failure and reinitializes the ring.
- A station may transmit asynchronous data only when Late-Ct = 0 and the TRT has not expired. It may transmit data until the TRT expires. When the counter expires, it does not abort the transmission; it continues transmitting the frame until it is completed (there is a maximum frame size on the ring).

Using this protocol, FDDI can guarantee access to the ring for synchronous traffic at least every 2 × TTRT units of time. For the efficiency of FDDI, let η denote the efficiency of the system (3), then

$$\eta = [TTRT - Nx(D + TT) - DP]/TTRT$$

where

N = number of stations on the network
D = delay in each station (active nodes, read all bits on ring)
TT = token transmission time
DP = the ring latency

We see that the performance of FDDI improves with large TTRT and deteriorates with DP. In other words, the longer the ring, the poorer the performance will be. Finally, it is worthwhile observing that an FDDI network also can be considered as a local-area solution.

Distributed Queueing Dual Bus

DQDB is a dual-bus-based network (see Fig. 8). All nodes are attached to both buses. Transmission is unidirectional on each bus. It operates as a distributed first-come, first-served (FCFS) queue. Time on the bus is broken into small units called *slots*. The role of the MAC is to decide the transmitter of information in each time slot.

DQDB was proposed first by a group in Australia under the name QPSX (queued packet and synchronous exchange) (7). The IEEE standardized it under the 802 series (802.6). It also was adopted by the Regional Bell Operating Companies (RBOCs) as their MAN standard. It forms the basis for their switched multimegabit data service (SMDS) offering.

As opposed to FDDI, the physical medium and related signal processing are not specified for DQDB. The 802.6 Standard only covers the MAC layer. To summarize the MAC operation,

- A head-end station is responsible for generating 53-byte slots (9 header and 44 data).
- Two bits are used in each slot for gaining access to the bus, a B (busy) bit and an R (request) bit.
- The busy bit indicates if the slot is occupied. The request bit is used by a station to send a request for a slot. It is sent on the bus in the reverse direction of transmission.
- Two counters are used by the MAC protocol: the request counter (RC) and the countdown (CD) counter. The former keeps track of outstanding requests on the buses for slots. The second keeps track of the station's position in the queue.
- The RC counter is incremented for every R bit and decremented for every empty slot. RC keeps track of those in the queue at all times.
- When a station has a frame to transmit, it sends out a request. It then sets CD equal to RC. Every empty slot that comes by decrements RC. When CD expires, the station may transmit in the next available slot. CD indicates the position of the station in the queue at the time it sends the request. RC keeps

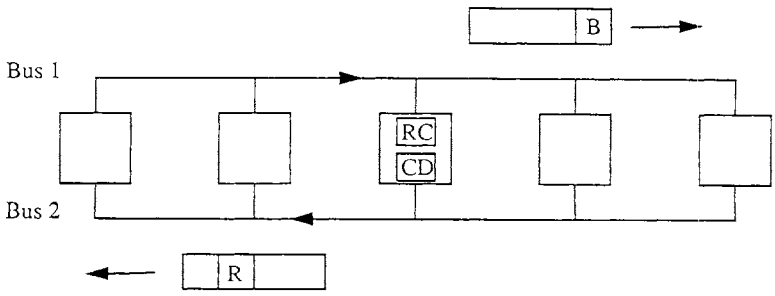


FIG. 8 Distributed queueing dual bus topology.

track of those in the queue at all times. Note that stations are passive; information is written onto the bus only by the stations.

The DQDB can achieve full channel utilization, that is, its efficiency η is 100% (no slots are wasted). The original DQDB Protocol is unfair though, with a station's throughput being dictated by its position on the bus. Several proposals were put forward to amend this situation. The one described in Ref. 8 was adopted. Its operation can be summarized as follows. Every F frames, a station is required to let an empty slot go by. F is decided by the network manager. A large F increases efficiency but slows convergence to the fair state.

A further improvement to the performance of DQDB can be obtained by the use of erasure nodes. These are stations that have the ability to delete information in a slot and make it available for use by stations further down the bus. This increases the throughput of the network. An erasure node must be an active station as it not only reads all the slots but deletes those that are addressed to stations above it on the bus.

Like FDDI, DQDB supports synchronous service. The slots are put in a frame by the head-end station; the first X slots are reserved for synchronous traffic. X changes, depending on the total BW required by the synchronous load. The frame repeats every 125 microseconds (μsec).

Wide-Area Networks

Networks that span more than 50 kilometers (km) are generally referred to as wide-area networks (WANs). They are communication networks that consist of switching nodes and transmission links and span large geographical areas. In the early days of computer networks, the host and user terminals would attach directly via a communication processor or multiplexer to the network. Now, the communication environment is more hierarchical in structure. File servers and workstations are served by LANs, which are internetworked and are connected to a wide-area backbone network via a gateway.

Switching

Without switching, we would have point-to-point communication. To achieve full connectivity would be impossible or very expensive. Switching allows the sharing of communication resources among many users without having to provide for a direct link between them. There are two types of switched networks: circuit switched (CS) and packet switched (PS). Although the basic premise is the same for both (i.e., they provide a communication channel between two or more communicating entities), they do not share the same philosophy. Below we briefly discuss both.

Circuit Switched Networks

In CS networks, the communicating entities are given the use of a channel for the duration of the connection. When all the links are full, incoming calls are blocked until a circuit is freed. The channel is of a constant bit rate, and provides a continuous flow of information. Telephone networks traditionally have been CS; each telephone call is a given a fixed 4-kilohertz (kHz) or 64-kilobits-per-second (kb/s) channel.

Packet Switched Networks

Because computers send bursts of information, it was recognized early that it would be much more efficient to have several end users share a communication channel instead of dedicating one to each user. The notion of statistical multiplexing was used; information would be collected into small units called packets and these packets would be placed in a queue for transmission over a link. At the switching nodes in the network, the packets of several users would be queued awaiting transmission. The heavier the load, the longer the queues would be and therefore the longer the delays would be. This type of transmission often is referred to as *store and forward,* and does result in an interrupted flow. However, it can have error-detection/correction capabilities built into it. Individual packets can be flagged and retransmitted.

There are two types of PS techniques:

1. Virtual circuit (VC) (see Fig. 9-*a*), which provides a logical end-to-end connection between a source and its destination. All packets associated with the connection carry a virtual circuit identifier in the header. At each node, an incoming virtual circuit is mapped onto an outgoing virtual circuit, thereby creating a complete path end to end. Note that no resources are dedicated to the VC.
2. Datagram (see Fig. 9-*b*), in which all packets are treated as independent units, no paths are set up between source and destination. Each packet is transmitted with the destination address in its header and packets belonging to a source destination pair could follow different paths in the network.

To compare virtual circuits and datagrams,

- There is a tradeoff between node memory and network bandwidth: VCs use up memory in nodes to maintain VC tables; datagrams use up more space in headers as addresses tend to be longer than VC numbers.
- VCs go through a setup phase and teardown phase; this process takes up time and bandwidth and may not be justified for short connections.
- VCs are vulnerable to nodal crashes; all tables could be wiped out, forcing connections to be reestablished. For datagrams, only those at the node that crashed will be lost, others are rerouted around the failure.

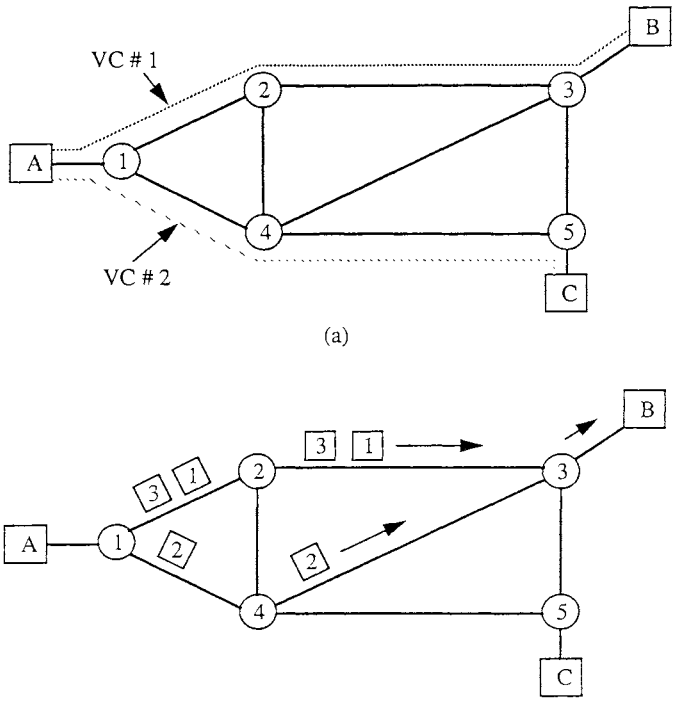


FIG. 9 Packet-switching techniques: *a*, virtual circuits; *b*, datagrams.

Routing

Routing is one of the main functions of the WAN. The routing algorithm is responsible for choosing a path from the source to the destination to deliver the transmitted data. In general, a path between a communication pair will involve several hops. The question of where the routing decision is made and on what information it is based is what distinguishes between different routing schemes implemented in networks. Below, we summarize some of the options available when writing the algorithm (9).

- The decision can be made (1) for each packet (datagram routing), (2) for each message (message routing) (several packets), (3) for each connection (VC routing) (several messages).
- The algorithm can be adaptive or nonadaptive.
- Adaptive algorithms can use periodic or aperiodic updates.
- Adaptive algorithms can be centralized or decentralized.
- In its decision making, the algorithm can use (1) local information, (2) global information, (3) local and global information.

When designing a routing algorithm, several things should be kept in mind: it must be correct, it must be simple (i.e., not use up too many network resources), it must be robust to survive failures and temporary overloads, it must be stable (i.e., avoid oscillations due to routing decisions), it must be fair (i.e., all users get a fair share of the network resources), and, finally, it should be efficient in its use of the network links. Generally, the goal of a routing algorithm is to optimize

- Some performance parameter (e.g., average delay or average throughput); generally, minimize average delay subject to a throughput constraint or maximize average throughput subject to a delay constraint
- Use of network resources (e.g., trunk bandwidth nodal buffers)

The following nine sections provide some examples of routing algorithms.

Shortest-Path Routing

By shortest path, we mean the minimum sum of a chosen metric over the path. The routing algorithm chooses the path that is considered to be the shortest at the time the decision is made. Five examples of how the path length could be measured are (1) in number of hops, (2) in geographic distance (km or miles), (3) in average delay (sec), (4) in cost (dollars), (5) in traffic flow (trunk utilization). Several algorithms exist to calculate the shortest path; the Bellman–Ford algorithm is the most popular (10).

Multipath Routing

Multipath routing also is referred to as bifurcated or proportional routing. The algorithm chooses a certain path from a set of eligible paths with a certain probability. The probabilities may be determined ahead of time, and they could depend on the number of hops, cost of link, average delay, and so on. If the algorithm is dynamic, then the probabilities must be recalculated at specified intervals to reflect changing network conditions. This algorithm only works for networks that have multiple paths between source–destination (S-D) pairs. It is reliable when there is more than one disjoint path between two end nodes. It also can be designed such that it distributes the load evenly throughout the network.

Centralized Routing

The centralized routing scheme, as its name suggests, uses a routing center (RC) to determine the paths to be taken for every connection. Network nodes send updated information to the RC (periodically or aperiodically). The RC then uses this information to compute the most optimal paths. The routes then are

sent in the form of routing tables to be used by the nodes for local path assignment. In some cases, connection requests are sent to the RC by the source node, which will respond with the full path information. The centralized approach has one distinct advantage: the RC has global knowledge of the network and therefore can make optimum choices. However, there are several disadvantages:

1. The time to compute paths may take longer than the transient conditions in network. Also, the distribution of routing tables is not instantaneous.
2. It represents a single point of failure.
3. It generates a lot of overhead traffic, in particular in the neighborhood of the RC. Links to the RC could get clogged with updates and routing requests.

Isolated Routing

Isolated routing is a decentralized routing algorithm that uses local information at the nodes for making routing decisions. Each node compiles its own local statistics; no routing information is exchanged within the network. Several algorithms fall in this class; they are well suited for datagram networks.

- Random routing, by which a packet is transmitted over a link that is chosen randomly from the set of outgoing links; no information is used in making the decision.
- Hot-potato routing, for which the underlying premise is to get rid of incoming packets as fast as possible, in other words, to join the shortest queue. The algorithm could be improved by having the node scan an ordered list of links to each destination and use the first link on the list with a queue level that is below a given threshold.
- Backward learning, for which each packet is required to have the source address and a hop counter in its header. These are used by the nodes to create their local routing tables as follows. Each node the packet passes through increments the hop counter. By looking at the source address and the hop counter, each node on the path can figure out how far the source is away from it via that incoming link. It uses that information to create its own routing table. For every incoming packet, the table is scanned to find the best path (minimum hop count) to the destination. To make sure that no old information is used, nodes need to forget their tables periodically and recreate them from scratch to ensure their validity.

Delta Routing

The delta routing algorithm is a combination of centralized and isolated routing. Local information is collected by the nodes and sent to an RC. The RC computes all paths with different initial links for each node using the information

obtained. All the paths for a node are tested against the "best" one, c_{ij}^{B}, as follows:

$$c_{ij}^{n} - c_{ij}^{B} < \delta \qquad \text{for all } n \text{ initial links}$$

If this holds, path c_{ij}^{n} is considered equivalent to best path c_{ij}^{B}. All the equivalent paths are sent to the respective node by the RC. Nodes choose one of the equivalent paths based upon local information (e.g., shortest queue) or at random.

Note that when $\delta = 0$, RC makes the choice as there is only one best path. When $\delta = \infty$, each node makes its own decisions, as all paths are equivalent. The value of δ determines the degree of autonomy of the network nodes; it must be properly adjusted for optimum performance.

Flooding

Flooding is the most robust of the routing algorithms; an incoming packet at a node is sent out via every outgoing link. However, it does generate a tremendous amount of overhead. The algorithm must contain a rule to stop the flooding at some point. Several possible techniques can be used: (1) There can be a hop counter in the header that is decremented by each node traversed; when it reaches zero, the packet is destroyed by the transit node. To guarantee that packets get to their destination, the counter must be set to the maximum network dimension; (2) Nodes keep track of packet sequence numbers for each source. Repeats encountered within a certain period are killed.

Delay-Based Distributed Routing

The delay-based distributed routing algorithm was used first in the old ARPANET (Advanced Research Projects Agency Network) (11), but was abandoned when found to be too unstable (the time to converge was too long compared with the network transients). Nodes were required to exchange delay vectors periodically with their immediate neighbors. As each node received a delay vector, it updated its own routing tables and it in turn broadcasted its updated delay vector.

Flow-Based Routing

The flow-based routing algorithm can be used to calculate fixed routing tables for single-path routing based on long-term traffic flows between all the S-D pairs in the network. If the traffic load between each S-D pair is known, then, via mathematical formulations, one can calculate the traffic flows over all the network links given a particular network topology. One then can calculate the average delays in the network as follows:

$$T_i = 1/(\mu_i C_i - \lambda_i)$$

where

λ_i = total flow over link i
C_i = capacity of link i
μ_i = packet size in bits

To minimize total average delay, one can formulate an optimization problem that will assign flows to paths within the capacity constraints. If multiple-path routing is possible, then T_i calculation becomes much more complicated. The problem must be formulated as a multicommodity flow problem. The calculated flows will give the appropriate proportions for the multipath routing algorithm.

Hierarchical Routing

Hierarchical routing is used in networks that are very large to minimize the size of the routing tables and decrease the complexity of route calculations. The network is divided into regions, subregions, subsubregions, and so on. All nodes belonging to a particular region are aware of the full topology of that region. Some nodes, such as gateway nodes, belong to two or more regions; they are responsible for linking the regions together. When a node encounters a packet that is addressed to a destination outside its region, it forwards the packet to the local gateway. If hierarchical addressing is used, it further simplifies the routing. Whole regions can then be mapped on the outgoing links.

Congestion Control

Congestion in networks results from having too many packets in transit. This can result in degradation of the performance; time delays increase as packets are queued at the nodes (12). Congestion also feeds on itself; when it occurs, excessive time delays will cause time-outs at nodes and retransmission of packets, thereby increasing the load on the network. It therefore is imperative that some control actions be taken either to prevent congestion from occurring (preventive control schemes) or to react accordingly when it has occurred (reactive control schemes).

Preventive controls can be put in place to try to avoid congestion; however, there are no guarantees that they will work. They do waste resources under normal network operating conditions. Reactive controls are activated after the onset of congestion in the network. They could take a while to have effect and in the meantime information can be lost. They also require that the network recognize that congestion has occurred, which in itself is not an easy operation. Below we describe some of the more common congestion-control techniques.

Preallocation of Buffers

Preallocation of buffers is obviously a preventive control technique. For every connection in the network, buffers are reserved at each node along the path to

hold its packets. It is a true store-and-forward scheme; a packet is passed along from one node to another only when a buffer for the connection is available at the next node. It does avoid network congestion in most cases; however, it is wasteful of nodal resources.

Isarithmic Control

Isarithmic control is another preventive control scheme. It limits the total number of packets in the network through use of tokens or permits. Packets are admitted to the network when the source node is in possession of a token. Again, under most circumstances, it does prevent network congestion; however, hot spots can develop in the network, and there is no way of controlling the migration of tokens to the heavily loaded regions on the network. This can then result in local congestion. Another drawback of the scheme is the time it could take to obtain a token at a source node. Tokens also are susceptible to being destroyed or damaged, thereby reducing the overall network capacity.

Window Flow Control

Window flow control is a form of isarithmic control in which a limit is set on the number of packets that may be in transit in the network for each S-D pair. Again, this is a preventive technique. The goal is to find the appropriate window size for each S-D pair. One possibility is to maximize the throughput under an average time-delay constraint. Window sizes can be reduced should congestion occur (this scheme, like those mentioned above, does not guarantee the prevention of congestion).

Packet Discarding at Nodes

Packet discarding at nodes is a reactive scheme; if a node receives a packet and it has no space in its buffers, it discards it. Some intelligence should be used when discarding packets to improve the performance of the network as every discarded packet time-outs and is retransmitted, wasting bandwidth and not relieving the network load. One possibility is to reserve a buffer for packets nearly home. Another is to maintain a hop counter in the packet header that indicates how far the packet has traveled. If the packet has traversed a large number of hops, it is accepted; drop only those that have come from nearby. Intelligent use of buffer space also can improve performance. For shared buffer pools, do not allow any one output link to hog all the buffer space; keep some in reserve for the other links. Also, do not preallocate all the buffers; always keep some in a shared buffer pool that can be allocated on demand.

Choke Packets

The second reactive scheme, the use of choke packets requires that the nodes keep track of the utilization on the outgoing links. When a threshold is exceeded

on a link (the threshold could be different for each link), choke packets are sent back to the sources utilizing that link. This is an indication that they should slow down. If utilization increases beyond a certain critical level, packets are discarded. Utilization values for the links are updated as follows:

$$u_{new} = au_{old} + (1 - a)f$$

where f is measured utilization and a is a constant $0 < a < 1$ that gives the old values some weight, preventing the system from overreacting to sudden traffic surges.

Types of Wide-Area Networks

WANs can be classified into two classes, homogeneous networks or heterogeneous networks. The first networks that were designed for computer communication were of the homogeneous category. Now, most networks fall into the heterogeneous class because of the proliferation of information systems. We describe each one briefly below.

Homogeneous Networks

The first public data networks to be developed were all homogeneous networks. They basically consisted of a backbone network of packet switches surrounded by concentrators and/or terminals. The nodes all were supplied by one vendor and, in many cases, so were the concentrators. One gained access to the network via dial-up service or direct connections. The networks could be hierarchical in structure with gateway nodes connecting regions to a backbone. Examples of such networks are Telenet, TYMNET, DEC's DECnet, IBM's System Network Architecture (SNA), Datapac, Transpac, and so on. They all provided X.25 service, except for SNA and DECnet, which had their own proprietary protocols. For more details on these networks, the reader is referred to Refs. 13 and 14.

Heterogeneous Networks

The current trend in networking is moving toward heterogeneous networks (15). It is a natural development resulting from the proliferation of LANs.

Heterogeneous networks are hierarchical in nature. LANs form the lowest level. These are interconnected to form clusters that in turn are interconnected to form sections or regions. Backbone networks are used to interconnect the various components.

There are many different types of devices that are used for internetworking. Repeaters are used to extend LANs, whereas bridges are used to interconnect LANs. The former operate at the physical level and the latter at the MAC level. Routers or gateways are more sophisticated devices that are responsible for

connecting LANs to backbone networks. They are capable of protocol conversion so that different types of subnets can be traversed. The Internet is an excellent example of a heterogeneous network. Designed to interconnect all the major universities and government laboratories, it consists of a backbone called the NSFnet (National Science Foundation Network) that connects several regions. Each region consists of a network that interconnects local communities.

In the public domain, we find that the carriers are providing frame relay service to their customers (16). The virtual network is a new concept that carriers are selling (17). It consists of setting up a network service for customers that gives them access to high-speed communication links without having to buy the equipment.

Future Developments

Computing applications in all sectors now are dependent upon computer networks to convey massive amounts of data routinely, accurately, and rapidly from one network-connected device to another. Kilobit rates are a thing of the past, 10-Mb/s Ethernet is commonplace, massive use of the 100-Mb/s FDDI is on the horizon, and networks supporting gigabit media rates are emerging. Enterprises of all kinds have become dependent upon networks or networked-computing applications. The reasons for enterprise dependence on networks are well known. Automation as a tool for increasing productivity is pervasive. Automation implies intelligent (computing) devices. Myriad intelligent devices resulted in distributed computing and distributed computing required communication (i.e., networking). This shift in paradigm from terminal to central computer, to a federation of peers cooperating in a computational environment caused the shift from hierarchical- (terminal) based network topologies to the peer-to-peer-oriented (flat) bus and ring network topologies commonplace today. The continued shift in the computing paradigm from distributed computing to network computing with network servers and remote procedure calls, together with rapid increases in the power of intelligent devices to be networked, is causing further alterations in (the) networking (model) and, at least in part, precipitating the need for higher-speed networks in the future.

In parallel, we are witnessing a continuing improvement in optical carrier technology, significant gains in reducing the cost of terminating high-speed links, and the emergence of efficient switching techniques for wide-area communications. Fiber-optic carriers are now the preferred transmission medium for the long-haul communications market due to their very high intrinsic capacity, low noise and interference, and the ever-increasing distance between repeaters.

New long-haul applications such as video conferencing are becoming widespread and existing voice and data communication volumes continue to increase. The need for multimedia services, as well as LAN and MAN interconnection, is further motivating developments in high-speed long-haul systems.

This combination of available technology, declining costs, and a plethora of applications also has resulted in the development of new standards for WANs.

At the physical layer for fiber-optic transmission, the Synchronous Optical Network (SONET), operating at multiple megabits per second has become the widely accepted standard (18). Broadband ISDN (BISDN) is a newly emerging standard that defines the higher layers and the corresponding signaling system (19). Two modes of operation have been defined for BISDN: synchronous transfer mode (STM) and asynchronous transfer mode (ATM). ATM seems to be the more popular choice for the immediate future; it is a form of packet switching that uses fixed-size packets called *cells* (20).

In conjunction with the advances in both the transmission and the protocol sides of things, strides are being made in the switching arena. Fast packet switches are being proposed and developed at some of the major telecommunications companies worldwide (21,22). These switches together with SONET will form the basis for BISDN-based networks of the future.

In the next several years, ripening optical frequency division multiplexing (FDM) and wavelength division multiplexing (WDM) technologies will continue to raise the bandwidth available for both short- and long-haul communications (15). In the short haul, rates of several dozens of gigabits per second have been experimented with successfully and are expected to be out of the labs in the near future. By the mid-1990s, 2.2-Gb/s long-haul links also are expected to become commercially available (23,24). The subsequent gradual shift toward even higher speeds is contributing to the ongoing efforts for developing all-optical, lightwave networking. Progress in mobile computing, the proliferation of portable equipment, and ripening cellular and radio communications networks also will significantly affect the way networks operate as well as the patterns of use. Taken together, the new generation of emerging networks can be expected to induce significant changes in hardware and communication software, providing the bandwidth needed for integrating voice-, data-, and video-based applications, and introducing novel network and protocol design challenges.

Acknowledgments: UNIX is a registered trademark of AT&T Bell Laboratories. Appletalk is a registered trademark of Apple Computer, Inc.

Bibliography

Portable Communications, *IEEE Commun. Mag.*, 27(7) (1989).

Trends in Cordless and Cellular Communications, *IEEE Commun. Mag.*, 29(6) (1991).

Wireless Indoor Communication, *IEEE Network Mag.*, 5(6) (1991).

PCS: The Second Generation, *IEEE Commun. Mag.*, 30(12) (1992).

Bertsekas, D., and Gallager, R., *Data Networks*, Prentice-Hall, Englewood Cliffs, NJ, 1987.

Boggs, D. R., Measured Capacity of an Ethernet: Myths and Realities, *Proc. SIGCOMM*, 222–233 (1988).

Chlamtac, I., and Fumagalli, A., A Solution to Packet Switching in Optical Transmission Networks, *Computer Networks and ISDN Systems*, 26(6–8) (March 1994).

Chlamtac, I., Ruszczyk, C., and Szabo, C., *Integrating Voice and Data in Telecommunication Networks*, Prentice-Hall, Englewood Cliffs, NJ, 1994.

Franta, W. R., and Chlamtac, I., *Local Networks*, 3d ed., Lexington Books, Lexington, MA, 1983.
Klessig, R. W., Overview of Metropolitan Area Networks, *IEEE Commun. Mag.*, 24:9-15 (January 1986).
Martini, P., The DQDB Protocol—What About Fairness? *Proc. Intl. Conf. Communications*, 298-302 (1989).
Morreale, P. A., and Campbell, G. M., Metropolitan Area Networks, *IEEE Spectrum*, 40-42 (May 1990).
Rodrigues, M. A., Evaluating Performance of High-Speed Multiaccess Networks, *IEEE Network*, 36-41 (May 1990).
Rose, M., *The Open Book, A Practical Perspective on OSI*, Prentice-Hall, Englewood Cliffs, NJ, 1990.
Sevcik, K. C., and Johnson, M. J., Cycle Time Properties of the FDDI Token Ring Protocol, *IEEE Trans. Software Eng.*, 13:376-385 (1987).
Spragins, J. D., *Telecommunications Protocols and Design*, Addison-Wesley, Reading, MA, 1991.
Walrand, J., *Communication Networks: A First Course*, Aksen Associates, Boston, MA, 1991.

References

1. Sherif, M. H., and Sparell, D. K., Standards and Innovation in Telecommunications, *IEEE Commun. Mag.*, 30(7) (July 1992).
2. Znati, T. F., Communication Protocols for Computer Networks: Fundamentals. In *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 3 (F. E. Froehlich and A. Kent, eds.), Marcel Dekker, New York, 1992, pp. 323-393.
3. Bux, W., Local Area Networks: A Performance Comparison, *IEEE Trans. Commun.*, 29(10):1465-1473 (1981).
4. Rosenbaum, R., The Technology Behind Wireless LANs, *LAN Times*, 8(13) (1991).
5. Ross, F. E., FDDI—A Tutorial, *IEEE Commun. Mag.*, 24:10-17 (May 1986).
6. Newman, R. M., Budrikis, Z. L., and Hullet, J. L., The QPSX MAN, *IEEE Commun. Mag.*, 26:20-28 (April 1988).
7. Hahne, E. L., Choudhary, A. K., and Maxemchuck, N. F., Improving the Fairness of Distributed-Queue-Dual-Bus Networks, *Proc. IEEE INFOCOM*, 175-184 (1990).
8. Maxemchuk, N. F., and El Zarki, M., Routing and Flow Control in High-Speed Wide-Area Networks, *Proc. IEEE*, 78(1):204-220 (1990).
9. Bertsekas, D., and Gallager, R., *Data Networks*, Prentice-Hall, Englewood Cliffs, NJ, 1987.
10. McKenzie, A. A., and Walden, D. C., ARPANET, the Defense Data Network, and Internet. In *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 1 (F. E. Froehlich and A. Kent, eds.), Marcel Dekker, New York, 1990, pp. 341-376.
11. Gerla, M., and Kleinrock, L., Flow Control: A Comparative Survey, *IEEE Trans. Commun.*, COM-28(4):553-574 (1980).
12. Schwartz, M., *Telecommunication Networks: Protocols, Modeling and Analysis*, Addison-Wesley, Reading, MA, 1987.
13. Tanenbaum, A. S., *Computer Networks*, John Wiley, Chichester, 1988.

14. Chlamtac, I., and Franta, W. R., Rationale, Directions and Issues Surrounding High Speed Computer Networks, *Proc. IEEE*, 78(1):94–120 (1990).

15. Lai, W. S., Frame Relaying Service—An Overview, *Proc. IEEE INFOCOM*, 668–673 (1989).

16. Briere, D. D., *Virtual Networks: A Buyers Guide*, Arthec House, Boston, 1990.

17. Ballart, R., and Ching, Y.-C., SONET: Now It's the Standard Optical Networks, *IEEE Commun. Mag.*, 27(3):8–15 (1989).

18. Minzer, S. E., Broadband ISDN and Asynchronous Transfer Mode (ATM), *IEEE Commun. Mag.*, 27(9):17–24 (1989).

19. Coudreuse, J. P., Communications Using the Asynchronous Transfer Mode (ATM). In *The Froehlich/Kent Encyclopedia of Telecommunications*, Vol. 4 (F. E. Froehlich and A. Kent, eds.), Marcel Dekker, New York, 1992, pp. 123–164.

20. Ahmadi, H., and Denzel, W. E., A Survey of Modern High Performance Switching Techniques, *IEEE J. Sel. Areas Commun.*, 7(7):1091–1103 (1989).

21. Tobagi, F. A., Fast Packet Switch Architectures for Broadband ISDN, *Proc. IEEE*, 78(1):133–167 (1990).

22. Lyles, J. B., and Swinehart, D. C., The Emerging Gigabit Environment and the Role of Local ATM, *IEEE Commun. Mag.*, 30:52–58 (April 1992).

23. Cheung, N. K., The Infrastructure for Gigabit Computer Networks, *IEEE Commun. Mag.*, 30:60–68 (April 1992).

IMRICH CHLAMTAC
MAGDA EL ZARKI

Introduction to Packet-Switched Technology

Introduction and Definitions

Packet switching deals with the transport of digital information between stations in a network. The information is in the form of *packets*, which are labeled sets of information bits. The *label* or *header* identifies the packet with regard to determining its destination and other appropriate treatment during forwarding through the network. *Stations* are the various kinds of communication devices in the network, such as computers, terminals, telephone sets, and so on, that are capable of transmitting and receiving packetized information. With the classical distinction between switching and transmission in telephony, packet switching really combines aspects of switching and transmission, and it therefore would be more appropriate to talk about packet technology, but the following treatment follows dominant practice and uses the term packet switching.

Switching is the process of selecting a means to reach the desired destination, that is, ascertaining that the appropriate receiving party and nobody else gets the information. In general, this involves the selection of a route or path through a network, which in itself can be within a piece of equipment or span a large geographical area. Sometimes, switching is contrasted with *broadcasting* techniques by which the information is transmitted to every participant, but the receivers perform a filtering function and pass on only the information destined for the attached station. We refer to both techniques here as packet-switching technology.

As a function, switching may refer to point-to-point or multipoint connections. In contrast to broadcasting, which targets every participant, subsets of subscribers can be designated in what is called *multicasting* or *group casting*.

Networks are collections of stations that are connected by switches or shared transmission media. A shared transmission medium can be free space (the "ether," a hypothetical substance which classical 19th-century physics assumed to fill all space, in reference to the ancients' concept of the ether filling the upper regions of celestial space) or a guided medium, such as cables or wires or optical fibers in various topologies (e.g., buses, trees, stars, or rings).

Switches are multiport devices that provide connections on demand between pairs or groups of ports. In the case of packets, the connection can be for the duration of the packet only. In computer networking, such devices have traditionally been called *routers*. Switches in a stricter sense imply that a port can request connection (and disconnection) to another port. If ports are connected, usually on a long-term basis, to other ports by a third party (the service provisioner), then one speaks of *cross-connection* rather than switching.

Digital switches may be circuit switches or packet switches. *Circuit switches* deal with continuous streams of bits, usually bidirectional and going to as-

signed, fixed destinations. In contrast, *packet switches* forward discontinuous sequences of packets, and each packet may go to a different destination. Hence, there is an inherent multiplexing capability for each port, that is, each port can be simultaneously connected to several other (changing) ports.

The *store-and-forward* operation is germane to packet switching. This may be the cause of queuing and hence entail variable delays. Different methods of error detection and correction can be applied, depending on the demands of the attached stations.

Packet switching can be offered as a service or it may merely be used as a technology that is transparent to the using stations. *Packet-switching service* implies a standard network access definition and a type of contractual agreement defining the performance to be offered by the network. The service may be *public*, such as the services based on the international standard known as X.25, or *private*, such as offered on local-area networks (LANs). *Packet technology* is used, for example, inside computers to interconnect various architectural components (e.g., peripherals). The technology also is used widely to handle the internal signaling in telephone networks between switches.

The term *packet* is used here in a wider sense, denoting any group of bits with a label. At different levels of the protocol hierarchy (see the section, "Protocols," below) or in different architectures, one may actually use different terms. For example, applications may deal with *messages*; on a point-to-point link, one usually speaks of *frames*; and in Broadband Integrated Services Digital Network (BISDN) (discussed in a separate section), the fixed-size packets are called *cells*.

Packet boundaries can be indicated in different ways. *Fixed-length packets* require the recognition of and synchronization with the packet boundaries, which can be achieved with various means. One can use synchronizing packets, try to find a checksum, or embed the packet in a larger frame structure (e.g., Synchronous Optical Network/Synchronous Digital Hierarchy [SONET/SDH]). *Variable-length packets* usually employ a distinct bit pattern known as a *flag* to indicate the start and end of a packet. This pattern must be suppressed inside the customer-supplied information to avoid false packet boundaries. The technique employed to accomplish this escaping of unintentional flag patterns is known as *bit stuffing*. Alternatively, a four-out-of-five-bit encoding scheme can be used (fiber distributed data interface, FDDI), in which the fifth bit serves various control functions, one of which is delimiting.

The label in a packet can contain different kinds of information. Not only are there the obvious source and destination addresses, but also control fields for acknowledgment, sequence numbers, and checksums for error detection. Often, one employs a "logical" identifier for a connection or session.

Connections in packet switching are known as *virtual circuits* (see the section, "Protocols"). These may be set up and taken down frequently and on demand and then are called *switched virtual circuits*, in contrast to *permanent virtual circuits*, which are provisioned for extended periods corresponding to leased private lines and which are, in contrast to switched virtual circuits, automatically reestablished after network or subscriber outages. For connectionless communication, the datagram (see "Datagram Service") is used (1,2).

History

The invention of packet switching originated with Paul Baran (3), who in 1964 proposed a network connecting computers in institutions involved in government-financed research. The network was to use leased telephone lines from common carriers and special-purpose computers as packet switches. The Advanced Research Project Agency (ARPA) of the U.S. Defense Department eventually sponsored such a project, which became known as ARPANET (4). The network never ceased to exist and today is known as Internet, which consists of several regional networks connected by a backbone known as NSFnet (National Science Foundation Network) (1). It has several international links, such that today several million computers worldwide are interconnected. The ARPANET sponsorship funded the primary research and development for many of the early technological achievements in packet switching. The first ARPANET packet switches were computers from Honeywell, followed by switches designed and built by Bolt, Beranek, and Newman of Cambridge, Massachusetts.

After early attempts to establish a commercial packet-switching service failed, the first such successful service was Telenet in the United States (5), later acquired by the Sprint Corporation and today operating as Sprintnet. During the early 1970s, international standardization efforts under the aegis of the International Telegraph and Telephone Consultative Committee (CCITT) (see the section, "Evolution of Packet-Switching Standards") resulted in the definition of a public packet-switching service interface standard known as Recommendation X.25, which appeared first in 1976 and was subsequently updated in 1980 and 1984. Telenet adopted this standard, and soon such services appeared in many countries, notably Transpac in France and Datapac in Canada.

In parallel with this wide-area packet-switching network evolution, the introduction of packet switching in the local area occurred with the invention of Ethernet at Xerox Palo Alto Research Center (PARC). Ethernet uses packet switching on a shared bus, initially a coaxial cable operating at 1- or 10-megahertz (MHz) baseband frequency. Soon, other approaches for local-area networks appeared, such as the IBM token ring and the token bus. The concept of token access to a shared medium goes back to a paper by Farmer and Newhall of Bell Laboratories (6), but the original token patent is held by Cederström.

While packet switching was conceived as a data-networking technology, there were early efforts to include (interactive) voice. Bayer and Nutt of Bell Laboratories proved the feasibility in the laboratory of running telephony over Ethernet. The technology required to handle interactive voice on a larger scale in addition to data became known as *fast packet switching*. In 1985–1986, AT&T conducted a large-scale field experiment in California to explore the suitability of fast packet switching for telephony, with encouraging results. Variable-length packets were used in 1.544-MHz (T1) technology (7).

Meanwhile, packet switching was introduced inside the telephone network between the digital switches in the toll and access network. For example, in the United States, the Bell System introduced Common Channel Interoffice Signal-

ing (8), which made use of a separate packet-switching network using the standard Signaling System No. 6. Signaling System No. 6 in this decade is being replaced by the CCITT international standard Signaling System No. 7. This use of packet switching within the telephone network is totally transparent to the network user (9).

In contrast, international standardization efforts since the early 1970s have had the objective of providing digital end-to-end connectivity to all telephone users (i.e., replacing the current analog telephone set with a digital station with vastly increased capabilities). This new network, the worldwide introduction of which started in the late 1980s, is known as the Integrated Services Digital Network (ISDN). In its elementary form, the ISDN Basic Rate Interface (BRI) incorporates access to a public packet-switched service in accordance with the X.25 standard (10–13).

Further evolution of ISDN envisions two steps. Introduction of an intermediate step known as frame relay service started in 1992 in various parts of the United States. It uses fast packet switching technology in the T1/E-1 range (1 to 2 megabits per second [Mb/s]) for data only, and may be considered a simplified and faster version of X.25 since it uses a very similar variable-length packet format. The second and currently final step is known as BISDN and uses a technique called the asynchronous transfer mode (ATM), with fixed-size cells of 53 octets at about 150-Mb/s access speed (14–15). Its introduction is underway, but no substantial deployment is expected before the mid-1990s. Both frame relay as well as ATM rely on fast packet switching technology. BISDN would bring packet-switched access at the rate of 155 Mb/s or 622 Mb/s to the end user.

Beyond these already substantial data rates, there are efforts underway to introduce gigabit-per-second networking to the academic and research community in the United States. The strategy is modeled after the very successful introduction of packet networking pioneered by the ARPANET effort discussed above. Currently, active research includes work on fast packet protocols known as lightweight protocols (16).

Packet switching for data in the local area has expanded in speed and scope and includes now the category of metropolitan-area networks (MANs). A technology known as fiber distributed data interface (FDDI) now is widely available (17,18), offering variable-length packet service on a private network basis over duplex token rings running at 100 Mb/s. In order to provide an evolution path that includes voice as well and is compatible with BISDN, another MAN standard has been worked out, Institute of Electrical and Electronics Engineers (IEEE) 802.6 (see the section on the IEEE 802 standards) or distributed queueing dual bus (DQDB). Initial service offerings by various common carriers of a connectionless packet-switched service based on this technology occurred in 1992. The service offered on this architecture as defined by Bellcore (Bell Communications Research) is known as switched multimegabit data service (SMDS) (21).

Finally, the last few years have seen an explosive growth in voice and data services using wireless access, spanning from the cordless residential telephone set to cellular systems offering "personal" communication worldwide. Such services increasingly use fast packet switching technology, at least for their signaling functions.

Technology

Packet switching is the transfer of information in packetized form. A distinction can be made between control and data; in packet switching, both are communicated in the form of packets. In contrast, in other systems, such as in those employing circuit switching, data may be in nonpacketized form such as a stream of bits, whereas the control information is packetized. An example is the ISDN Basic Rate Interface (BRI), which carries data as bit streams on 64-kilobits-per-second (kb/s) transparent bearer (B) channels, while control is over a separate, packetized D channel (the D channel was initially conceived as a small incremental "delta" channel to carry the signaling; hence the name). As an aside, the ISDN BRI has the option of providing packet-switching service following the X.25 Protocol standard on the packetized D channel intermingled with signaling information. Thus, the ISDN subscriber has immediate access to packet-switching service.

Packet switching is one of three store-and-forward switching methods; message switching and cell switching are the others. In *message switching*, the application's message is accepted by the network in its entirety and then forwarded as a unit. For practical reasons, a size limit must be imposed on the message; hence, the user must break up larger messages into segments fitting this size, which, when chosen too large, causes undesirable delays for shorter messages. Hence, one tries to compromise by selecting a packet size that just fits most short messages, which leads to packet switching. Using very short, fixed-size packets leads to a concept called *cell switching*.

While digital circuit service enjoys a relatively short and fixed delay, packet-switching services suffer from a longer and variable delay, but they can add error detection and correction to make the channel appear more reliable by compensating for noise. Moreover, packet service allows intrinsic statistical multiplexing, which is needed for services like multimedia. The multiplexing aspect, on the other hand, necessitates introduction of some flow-control measures to avoid stations receiving more information than they can handle.

While microelectronics and computer technology have been the enabling technologies for packet switching, there are several other subject areas with strong bearing on packet switching. Among them are protocols, network performance, routing algorithms, and packet switch architecture.

Protocols

A *protocol* is a set of rules that governs the interaction of concurrent processes in distributed systems (22,23). Since an extensive treatment of protocols is given in another article in this encyclopedia (24), this article concentrates on elements relevant to packet switching. The reader should recall the International Organization for Standardization (ISO) Open System Interconnection (OSI) Reference Model for protocols, which defines a seven-layer structure, ranging from Layer 1 (the physical layer) at the bottom, to Layer 7 (the application layer) at the top.

Notice that the OSI Model is a reference model only, that is, it can be and actually is violated by real-world implementations.

One can distinguish five elements of a protocol (22,23):

1. The service to be provided
2. The assumptions about the environment of the protocol
3. The protocol's message vocabulary
4. The encoding format of the messages
5. The procedure rules for the consistency of message exchanges

The focus in packet switching is on Layer 2, the data-link layer, and on Layer 3, the network layer. The service provided by a packet-switching network is usually a network-layer service. One distinguishes two fundamental types of service: virtual-circuit service and datagram service.

Virtual-circuit service also is known as connection-oriented service since it consists of three phases: (1) the connection setup phase, which establishes the virtual circuit; (2) the message-exchange or communication phase; and (3) the disconnect phase. Since the notion of virtual circuit is central to packet switching, we should contrast it with a "real circuit." In a digital communication system, a (real) circuit designates transmission of uninterrupted streams of bits, usually in both directions, analogous to the analog circuit, which implies galvanically connected stations. Just as in other uses of virtuality such as in computer memory, a virtual circuit "fakes" the presence of a real circuit when needed, that is, whenever there are data present to be transmitted, the virtual circuit performs this task, but when no data are present, the actual hardware channel can be used for other purposes. Thus, the data are transferred in packetized sequence. In operation, the setup request from a calling station includes the address of the called station. The network will forward the request to the called station. If accepted, the virtual circuit is established by giving each station a virtual-circuit identifier (not necessarily the same for each partner) that is used for the duration of the connection (i.e., until either party requests disconnection). The nodes or switches in the path involved in communication keep the state information for the life of the circuit, which abbreviates the task of switching for future packets on this circuit. Since the key attribute is the setting up of a path followed by all packets, one also talks of virtual-circuit routing (25).

Datagram service is also known as connectionless service. All datagrams contain the destination address, and the nodes or switches in the network decide anew for each datagram what route to take. Thus, subsequent datagrams may take different paths, arrive out of sequence, or get lost. The network can react more easily to link and node failures or overload situations. The delay incurred by the setup phase is avoided, but the network must be prepared to take a lot of data at any time without a warning. Since a datagram service offers less functionality than virtual-circuit service, providing a virtual-circuit service as a layer on top of datagrams is not uncommon as, for example, in the most widely used Transmission Control Protocol/Internet Protocol (TCP/IP) (1,26).

Packet-switching service brings a new way of charging for service. Whereas