INTRODUCTION TO COMMUNICATIONS TECHNOLOGIES

A GUIDE FOR NON-ENGINEERS

STEPHAN JONES • RON KOVAC

INTRODUCTION TO COMMUNICATIONS TECHNOLOGIES

A GUIDE FOR NON-ENGINEERS

STEPHAN JONES AND RON KOVACS

AUERBACH PUBLICATIONS

A CRC Press Company

Boca Raton London New York Washington, D.C.

INTRODUCTION TO COMMUNICATIONS TECHNOLOGIES

A GUIDE FOR NON-ENGINEERS

OTHER AUERBACH PUBLICATIONS

The ABCs of IP Addressing
Gilbert Held
ISBN: 0-8493-1144-6

The ABCs of TCP/IP
Gilbert Held
ISBN: 0-8493-1463-1

Building an Information Security Awareness Program
Mark B. Desman
ISBN: 0-8493-0116-5

Building a Wireless Office
Gilbert Held
ISBN: 0-8493-1271-X

The Complete Book of Middleware
Judith Myerson
ISBN: 0-8493-1272-8

Computer Telephony Integration, 2nd Edition
William A. Yarberry, Jr.
ISBN: 0-8493-1438-0

Cyber Crime Investigator's Field Guide
Bruce Middleton
ISBN: 0-8493-1192-6

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes
Albert J. Marcella and Robert S. Greenfield, Editors
ISBN: 0-8493-0955-7

Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages
Andy Jones, Gerald L. Kovacich, and Perry G. Luzwick
ISBN: 0-8493-1114-4

Information Security Architecture
Jan Killmeyer Tudor
ISBN: 0-8493-9988-2

Information Security Management Handbook, 4th Edition, Volume 1
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-9829-0

Information Security Management Handbook, 4th Edition, Volume 2
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-0800-3

Information Security Management Handbook, 4th Edition, Volume 3
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1127-6

Information Security Management Handbook, 4th Edition, Volume 4
Harold F. Tipton and Micki Krause, Editors
ISBN: 0-8493-1518-2

Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management
Thomas R. Peltier
ISBN: 0-8493-1137-3

Information Security Risk Analysis
Thomas R. Peltier
ISBN: 0-8493-0880-1

A Practical Guide to Security Engineering and Information Assurance
Debra Herrmann
ISBN: 0-8493-1163-2

The Privacy Papers: Managing Technology and Consumers, Employee, and Legislative Action
Rebecca Herold
ISBN: 0-8493-1248-5

Secure Internet Practices: Best Practices for Securing Systems in the Internet and e-Business Age
Patrick McBride, Jody Patilla, Craig Robinson, Peter Thermos, and Edward P. Moser
ISBN: 0-8493-1239-6

Securing and Controlling Cisco Routers
Peter T. Davis
ISBN: 0-8493-1290-6

Securing E-Business Applications and Communications
Jonathan S. Held and John R. Bowers
ISBN: 0-8493-0963-8

Securing Windows NT/2000: From Policies to Firewalls
Michael A. Simonyi
ISBN: 0-8493-1261-2

Six Sigma Software Development
Christine B. Tayntor
ISBN: 0-8493-1193-4

A Technical Guide to IPSec Virtual Private Networks
James S. Tiller
ISBN: 0-8493-0876-3

Telecommunications Cost Management
Brian DiMarsico, Thomas Phelps IV, and William A. Yarberry, Jr.
ISBN: 0-8493-1101-2

INTRODUCTION TO COMMUNICATIONS TECHNOLOGIES

A GUIDE FOR NON-ENGINEERS

STEPHAN JONES AND RON KOVACS

AUERBACH PUBLICATIONS
A CRC Press Company
Boca Raton London New York Washington, D.C.

This edition published in the Taylor & Francis e-Library, 2005.

"To purchase your own copy of this or any of Taylor & Francis or Routledge's collection of thousands of eBooks please go to www.eBookstore.tandf.co.uk."

Library of Congress Cataloging-in-Publication Data

Jones, Stephan
Introduction to communications technologies: A guide for non-engineers / Stephan Jones, Ron Kovac.
p. cm.
ISBN 0-8493-1266-3 (alk. paper)
1. Telecommunication. I. Kovac, Ron. II. Title.

TK5101 .J66 2002
621.381--dc21

2002074433

Visit the Auerbach Web site at www.auerbach-publications.com

International Standard Book Number 0-8493-1266-3
Library of Congress Card Number 2002074433

ISBN 0-203-97286-4 Master e-book ISBN

Dedication

To my family — my wife Jan, for a lifelong tolerance of my eccentric behaviors, and to my children, Stephanie, Kelsey, and Luke, for accepting their father as a propellerhead who likes to read non-fiction

Steve Jones

A venture of this sort does not come without its pain. But the pain is usually felt by other people. Accordingly, I thank my family for putting up with me during these times and providing moral support. But I really want to dedicate this book to my parents. Thanks Mom and Dad for making me what I am.

Ron Kovac

This page intentionally left blank

Contents

This page intentionally left blank

Acknowledgments

We would like to thank our outstanding research and graduate assistants who gave their qualified input on the text and for being additional editors of the document:

- Erik Kropa
- Ryan Shaffer
- Frederic Larchier
- Shane Neff
- Matthew Wright

— **Steve Jones**

- Brian Miller
- Wendy Whittern
- Nancy Rim
- Katie Gotshall

— **Ron Kovac**

This page intentionally left blank

Preface

The field of Information Technology is broad and ever-expanding. The technologies that are common today may be obsolete tomorrow. While this book introduces you to concepts central to the field as it stands today, it does not cover everything; it would take volumes of books to teach all that this field encompasses.

This book has been written with the intention of explaining some of the technologies that comprise the IT field. If you are an engineer, this book is not for you. As the name implies, it has been written to give non-engineering professionals a foundation of knowledge that will serve them well as they become managers in the IT field. One need not have a technical background to gain the valuable knowledge that lies within these pages — the book was designed with that in mind.

The material covered within is the same as the material presented in the foundation technology course for the Center for Information and Communication Sciences at Ball State University, one of the most-respected programs of its kind in the country. Students pursuing a Masters of Science in Information and Communication Sciences receive the same instruction in their pursuit of the degree. Students who are graduated from this program continue to become consultants, sales persons, and technical managers in the IT field. They work for companies such as AT&T, Verizon, and Accenture.

You too can glean the knowledge necessary to become a leader of technology professionals. This book willl provide a foundation for your career but it is not all that is required to ensure success. It takes a desire to achieve, and a work ethic to match. You must explore further the topics presented in this book. Read the chapters, research their contents, understand the material within, and you will develop the knowledge necessary to succeed. Keep a binder containing your notes and other materials that correspond with the topics covered within the text. This will not only help you to stay current with industry information, but it will also teach you where to find information that relates to the field.

This page intentionally left blank

Chapter 1

Systems and Models of Communications Technologies: Shannon-Weaver, von Neumann, and the OSI Model

The language, acronyms, and discussions in communications technology (CT) are based on fundamental ideas that can be considered systems. Understanding these fundamental systems allows knowledge of various information technologies to be added, brick by brick, to build on understanding current and developing technologies. One of the primary systems in CT is signaling. Signaling occurs in traditional voice telephone connections, local area networking, and wireless communications ranging from cellular to satellite systems. Each of these areas of signaling usually becomes the domain of an engineer who is focused specifically in this area of expertise. Preparing someone to understand all the intricacies of each of these disciplines is a huge undertaking. However, understanding the basic underlying principles of the signaling process can give the non-engineering professional the ability to converse on the topic intelligently.

The capacity to communicate is determined by a number of factors that influence the quality of the signal. How will the information be sent or transmitted? Will the person or device at the distant end of the communication signal have the ability to receive the transmitted signal? Will the receiving end

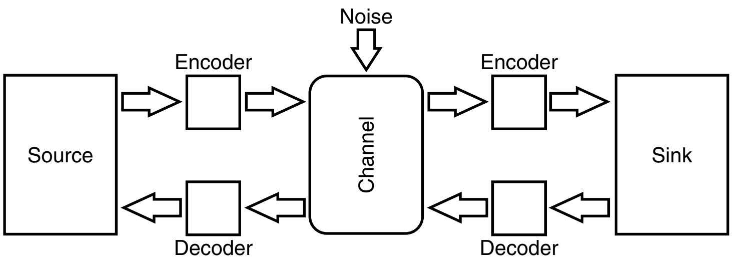


Exhibit 1 Shannon-Weaver model of communication.

need to decipher or decode the signal in any way? What would happen if noise was introduced to the transmitted signal? Would it cause the transmission signal to be corrupted in any way?

Exhibit 1 is a good example of how communications can be understood in a model (or systems format). The source (transmitting side of communications) signaling systems/needs to encode the information to be transmitted to fit onto the medium or channel being used to convey the information. The medium can be a range of possibilities: air, copper wires, or even fiber-optics. When we speak to another human, we determine whether or not the person understands the language we are speaking. As the source, we encode our information in the language and put it on the medium (air) to be delivered to the other person. What if the transmitting person has French as his primary language and the receiving end of the conversation (transmission) does not? The receiving end will need to decode the French language into one that he or she is able to understand. The return signal from the receiving end may ask the transmitting source, "Is this what you are trying to tell me? If it is, then we can discuss this topic further." This type of transmit/receive/confirm format is the basis of human communication and is also employed in data networking transmissions.

Claude Shannon developed a mathematical equation that defines the theoretical limit of the capacity in this model. He theorized (and later proved) that the amount of information being transmitted was based on a number of factors including noise, frequency of the transmission, and the strength of the signals. The formula is:

$$C = B \log_2 (1 + S/N) \qquad (1.1)$$

Do not be concerned about solving the math problem! It is presented to show the relationship between the signal (S) and noise (N) in a given transmission based on the bandwidth (B) or frequency at which the signal is being transmitted. The capacity (C) of information being transmitted is determined by all of these factors. As we move into more-complex topics, we will be able to use this formula to help us understand how much information can be transmitted over a wireless connection for our local area network or how our cell phone can be used to connect to the Internet. This formula tells us that as the noise in a transmission increases, the capacity to send information will

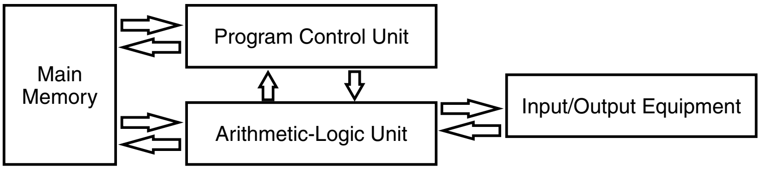


Exhibit 2 Components of the stored-program model.

decrease. As the frequency (or bandwidth) in which we transmit increases, there is a greater capacity for information transfer. We will discuss the topics of frequency and bandwidth in a subsequent chapter.

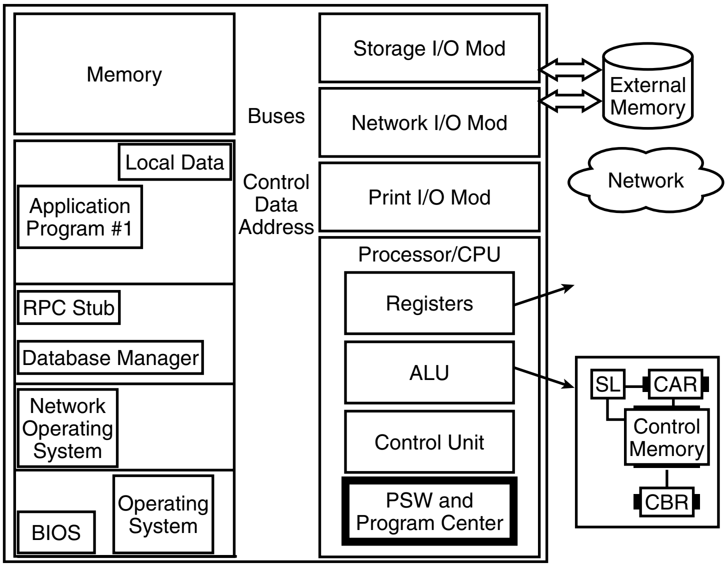
Computing Model

Any device on a communication network can be considered a node. A node can be a computer, telephone, router, server, tandem switch, or any number of devices that receive and transmit information on their respective networks. If every device connected to a network used a different format for collecting, storing, modifying, or transmitting information, the design of networks and the components connected to the networks would be extremely difficult to accomplish. John von Neumann, a mathematician whose theories were incorporated with the development of the first electronic digital computer, proposed a model based on work originally presented by Alan Turing (another mathematician who is famous for leading the group responsible for deciphering the Enigma code during World War II). von Neumann's idea is known as the stored-program concept. Exhibit 2 is a simple block diagram of von Neumann's model.

The general structure of this model is based on four primary components, with a fifth component necessary for interblock signaling. This model can be extrapolated to overlay the definition of how the nodes connected to any communication network operate:

1. *Main memory:* Stores data and instructions.
2. *Arithmetic and Logic Unit:* Performs computational functions on binary data.
3. *Control unit:* Interprets the instructions in the memory and causes them to be executed.
4. *Input/output (I/O) equipment:* Devices operated by the control unit.

The fifth component of this model is the bus structure. The information that needs to be exchanged between these blocks relies on an interconnecting medium referred to as a bus. Bus structures can be found in everything from digital wristwatches to the most sophisticated high-speed computing device. We will look at this model and how it relates to a computer and, using the same model, define how it works with telephone systems, data networking equipment, and other nodal devices.



Courtesy Frank M. Groom, *Movement and Storage of Information,* class notes.

Exhibit 3 von Neumann's architecture in a computing device.

The main memory on the computer is its working area. The program files that are needed to run specific applications are stored in this work area. It can be analogized as a large legal pad of paper. The program that is running on the computer is the top page of the tablet; this area of memory is also called the random access memory (RAM) of a computer. If it needs more information to process a request, the system will look into the pages available on the tablet to see if the date is there. To retrieve more information on a program or to pull a completely new program into the work area, the system needs to retrieve more pages of information (data). Another typical memory storage area is the hard drive, which, according to our model, is viewed as an input/output device.

The process of responding to requests for data is based off a set of instructions that is written in binary language. Most of us have never seen the machine language that runs our digital devices, but it is the tongue of the Information Age. The requests (instructions for information retrieval) printing, accessing a modem, and other functions are acted on by the central processor unit (CPU). The CPU relies on the Arithmetic and Logic Unit (ALU) to crunch the numbers and to be able to feed the information back so it can control the flow data.

Exhibit 3 represents a more-detailed view of the stored-program model. The memory portion of the diagram is now populated with the various pages of information necessary to operate the computer: BIOS, operating system, and application programs. The bus structure that was represented by arrows in Exhibit 2 is blocked in by a larger representation in Exhibit 3, which shows the connection between the memory, the CPU, and the ALU. The I/O modules are connected to external memory (hard drives), networks, or printers. This

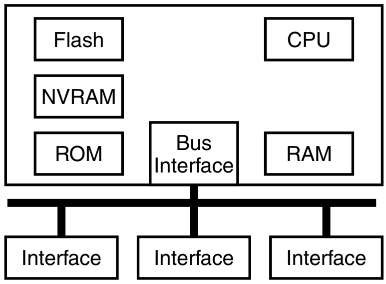


Exhibit 4 Simple router architecture block diagram.

step up in detail can be applied to other network equipment that requires processing and memory management to work.

The model can be used to define how a router, a digital PABX, and data networking switches work (these topics are defined in subsequent chapters). A router is a device used in data networks to forward information from one network to another. They are the workhorses of the Internet, the World Wide Web (the Web), and corporate wide area networks (WANs). With this level of responsibility, the sophistication of the equipment may seem more complex than it really is. A router is required to analyze packetized information received from its I/O module connection in order to decide where the information packet is sent or routed next. This requires an operating system that keeps the organization of the system flowing correctly. A CPU to control requests in conjunction with the ALU is necessary to analyze the binary data. Connecting all of these parts together is a bus structure, that is able to send and receive millions of requests every second!

Exhibit 4 is another example of how the von Neumann architecture works on a different type of computing device. The router has all the components previously defined for a computer, and it works in a similar manner. The operating system and application programs reside in the flash and other nonvolatile memory. RAM is the working area memory in the router just as it is in the computer. A router does not need the same memory capacity that a computer has but requires the same binary process of 1s and 0s to analyze data.

By understanding the von Neumann architecture, you can use it to comprehend how any number of devices will operate on different networks. The foundational work for this model was presented in 1946; 56 years later, it continues to be used to define the works of digital devices.

Open System Interconnect (OSI) Model

The ability to interchange different vendors' products in a network without issues of incompatibility has long been a concern of those who work in the industry. Most strive to make various components talk intelligently to each other on a reliable and consistent basis. The International Standards Organi-

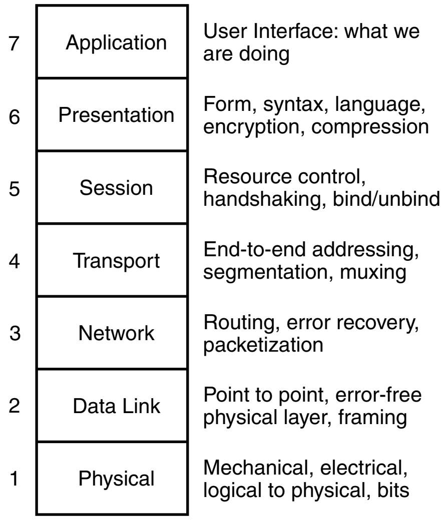


Exhibit 5 OSI seven layers reference.

zation (ISO), which consists of various representatives from countries around the world, has presented an open system interconnect (OSI) model. This protocol model consists of seven layers, each with specific functions and responsibilities within the stacked layers. The OSI, although not used as a *de facto* standard by all companies developing equipment for use in networks today, is used as a guideline to simplify the development and interoperability between vendors. The most consistent adherence to the OSI model exists at its lower levels (1 through 4) and is less well-defined in the higher layers of the stack. Some of this information may not make a great deal of sense to you initially, as we progress through different technologies and relate how they communicate with the OSI model. Technologies such as Ethernet, frame relay, ISDN, ATM, and other confusing acronyms are all compared to the OSI stack when signaling, transmission, encryption, and other functions are discussed. Understanding the basic principles of the model is most important at this point in your reading.

Exhibit 5 shows each layer's responsibility in the model and a brief definition of its function. A more in-depth examination of each layer is required to fully understand the purpose and interrelationships of the layers.

Layer 1 is the physical layer. It is used to describe how data that will be sent out on the network will be transmitted. It defines electrical, optical, or frequency modulation, depending on the type of medium (e.g., copper, fiber, wireless) the network employs. Connections standards such as EIA-232 are defined in this layer. This layer should not be confused with the actual cable that is used for transmitting the data; it is the layer within the OSI model that defines how that connection will be made. Modem connections to the coaxial cable are defined within this layer.

The data link layer is the second layer of the OSI model. The data link layer is concerned with physical (as opposed to logical) addressing. At this layer, a network device (e.g., a computer) has an address assigned to its network interface card (NIC) that uniquely identifies a device. Layer 2 is also concerned with network access (e.g., the NIC), framing of upper layer data for use at the physical layer, and error detection. Layers 1 and 2 are the most universally accepted protocol layers of the OSI model.

The third layer, the network layer, has become an integral cog in the movement of data across the world internetworkings. The logical addressing of a device is located at this layer. Routing of information on the Internet, the Web, and other WANs is based on the logical address found at the network layer. The most widely used and accepted Layer 3 address scheme is the Internet Protocol (IP). (Path or route selection is based on the IP address of a device.) The network layer is also responsible for formatting data from higher layers into packets that are passed down to the data link layer for organization into frames to be delivered to the physical layer.

At this point, it is important to note that the network layer does not interact with the physical layer. Layer 3 does not know what signaling format Layer 1 will use to provide the data to whatever medium is being used to deliver the information. Each layer of the OSI model only has interaction with the layer directly adjacent to it in the stack. Encapsulation, the process of putting received information into another format for delivery, occurs at each layer of the OSI stack. This allows for flexible architecture arrangements and the ability to change Layer 1 and Layer 2 programming to accommodate the connectivity of disparate systems. Think of a letter that is addressed in French to someone on a university's campus. Because the handlers of the mail may not understand French, the letter is put inside another envelope addressed in English so that as it transits the university's postal network it can easily be identified. The English labeled envelope is the encapsulation of the French data. It is this flexibility that allows Apple computers to be networked with Windows-based machines.

The transport layer, the fourth layer of the model, is primarily responsible for end-to-end integrity of communications between two nodes on a network. The transport layer establishes, manages, and terminates the exchange between two devices. End-to-end error correction and the flow control of data transmission are the responsibility of the transport layer. Layer 4 is responsible for the segmentation of upper layer data being sent down for external delivery. The segmented data is passed down to the network layer to be placed in packets. Transport Control Protocol or TCP resides at this layer. TCP is responsible for the integrity of the data delivered with IP. The two protocols — TCP and IP — are the primary carriers of data in the world today. Other delivery protocols live at this layer, and will be discussed when TCP/IP is defined in a subsequent chapter.

The next three layers of the OSI model are generally considered the realm of software design in contrast to the first four layers having a relationship with the hardware configuration of a device. The upper layers have not been developed universally and may not even be defined for some devices or connections, unlike the lower layers.

The session layer, the fifth layer, is responsible for establishing, managing, and terminating communications between two devices. It is also the area in which full-duplex or half-duplex communication is defined. The session layer determines if one device can be interrupted by another device while communicating. If a session connection is lost during data transfer, the session layer is responsible for helping recover the communication.

Layer 6, the presentation layer, is the translator and interpreter for data being sent from the upper application layer and for the data moving up the stack to be acted on by the application layer. The presentation layer is also responsible for encryption defined as the conversion of data into a secure format that can be read only by predefined recipients. Compression formats are also found at this layer. In the recent past, the sixth layer has been the least defined of the model. However, with the advent of new video and voice technologies being offered over the internetworks, this layer is becoming a critical component for communications across the WAN.

The last layer, seven, is the application layer, which is the closest to the user. It is the interface that runs between the network and the application being used on a device. E-mail protocols, HTTP (web language), and other interface applications reside at this layer. Error recovery from data being assembled after transmission also can be the responsibility of the application layer. It provides for a final integrity check for the data transmission being received.

The OSI model has been put to use in developing numerous advanced networking technologies and continues to provide the technical mapping for integration between disparate networks, vendors, and software. This model simplifies the understanding of how a complex set of protocols interact to deliver information across the Internet. One of the most widely used protocols based on this model is the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. Analogizing the delivery of information over the Internet to how a letter is written, addressed, routed, and eventually delivered with comparisons to the OSI model is helpful in understanding how both TCP/IP and the OSI work.

When writing a letter, a medium for delivery is considered. A blank sheet of paper is used to formulate information into a written language that is understandable to the reader. When the letter is completed, it is placed in an envelope and addressed; the postal service routes the letter to its destination. In looking at the analogy in reference to the TCP/IP protocol, data is created in the upper layers of the OSI model (blank sheet of paper) and prepared for sending. It is encapsulated (the envelope) as it passes through Layers 4 and 3. At Layer 3, the data is given a logical address that is understood by the delivery system (postal service). When the data is pushed out to the network, the address is used to route (deliver) the information to its destination. The addressing scheme associated with TCP/IP is a simple format similar to a home address, but sophisticated enough to provide millions of addresses understood all over the world. A more-detailed look at this addressing scheme is explored in the chapter on Wide Area Networks.

Summary

The key to understanding complex systems is in learning the fundamental platforms on which they are built. Using these models as a template to figuring out difficult technology interactions is a functional form of problem solving for the novice as well as the journeyman technologist. Shannon's communication model defines how much information can be processed, given the parameters of the environment in which the data is to be transferred. This model can be employed in wireline as well as wireless delivery schemes. It also can be used to define how humans communicate in various settings.

von Neumann's stored-program model gives us an idea of how the majority of computing devices have been configured since the mid-1940s. The model can be used to understand how other nodal components of networks function, such as routers, switches, and newer integrating devices that combine voice, data, and multimedia into a single network. The five basic components of the model exist in different capacities and functions in all these devices.

The open systems interconnect model is the most widely used generic protocol stack for communications over various networks. The OSI Model was developed by an international group that wanted to create interoperability across disparate networks, manufacturers, and vendors. The TCP/IP suite of protocols is modeled from this stack. It is the primary delivery mechanism for information over the Internet. Its addressing scheme is understood worldwide and continues to evolve as newer technologies are emerging.

Questions for Review

Multiple Choice

1. According to the capacitance theorem, as the noise in a transmission increases:
   a. The capacity to send information increases
   b. The capacity to send information decreases
   c. The capacity to send information is not affected
   d. None of the above
2. All of the following are components of the von Neumann stored-program concept, except:
   a. Main memory
   b. Program control unit
   c. ALU
   d. OSI
3. The OSI model consists of how many layers?
   a. 4
   b. 5
   c. 6
   d. 7

4. A node is:
   a. Any device on a communication network
   b. A computer
   c. A printer or a computer
   d. A printer
5. According to the von Neumann model, a hard drive is:
   a. A part of the main memory
   b. A part of the ALU
   c. An input/output device
   d. A part of the bus structure
6. Encapsulation is:
   a. Something that occurs at Layer 5 only
   b. The process of putting information into another format for delivery
   c. Something that occurs at each layer of the OSI model
   d. Both b and c
7. Internet Protocol (IP) resides at what level of the OSI model?
   a. The transport layer
   b. The network layer
   c. Layer 2
   d. The data link layer
8. All of the following are components of the Shannon-Weaver model of communication, except:
   a. Encode/decode
   b. Message
   c. Capacity
   d. Noise
9. The OSI model was created by:
   a. Shannon
   b. von Neumann
   c. The International Standards Organization (ISO)
   d. The Institute of Electrical and Electronic Engineers (IEEE)
10. In the OSI model, each layer:
    a. Interacts with all other layers
    b. Only interacts with the layers directly above or below it
    c. Does not interact with any other layers
    d. Only interacts with layers that are higher than it

Matching Questions

Match the following terms with the best answer.

1. $C = B \log_2 (1 + S/N)$
2. Noise
3. Data link layer
4. ALU
5. Transport layer
6. Packetization
7. von Neumann
8. OSI
9. I/O
10. Encapsulation

a. A component of the Shannon-Weaver model
b. A model containing seven layers
c. TCP
d. Frames
e. Developed the stored-program concept
f. Occurs at all levels of the OSI model
g. Capacitance theorem
h. Occurs in Layer 3 of the OSI model
i. Performs computational functions on binary data
j. Operated by the control unit in the von Neumann model

Short Essay Questions

1. Explain the communication process in terms of the Shannon-Weaver model.
2. Why is it necessary to have a standard model in which to discuss networks or computers?
3. List and define each component of the von Neumann stored-program concept.
4. List and explain what occurs at each layer of the OSI model.
5. Explain the impact that the von Neumann model has had in terms of digital devices.
6. Using examples, explain each step of the communication process in terms of the Shannon-Weaver model of communication.
7. Define the fifth component of the stored-program concept, and explain how it is used.
8. Explain, in words, the capacitance theorem.
9. Develop a situation where you think that knowledge of the systems presented in this chapter would be helpful in your career.
10. Explain why it is important for a non-engineering professional to understand the material presented in this chapter.

This page intentionally left blank

Chapter 2

Basic Concepts of Electricity

An appreciation and understanding of communications technologies is attainable without ever delving into hard-core engineering topics of physics and calculus. An understanding of the applied nature of the components of electricity, however, will give nonengineering professionals greater comprehension of the topics covered in this book. Explaining the associated terminology with examples of their use in networking environments will help make the connection between theoretical and practical science.

> Electricity: Basic concepts of electrical systems in telecommunications. Functions associated with components (e.g., resistor, capacitor) and their effect on signaling (e.g., resistance, capacitance).

Common Units of Technical Measurement

Conversations between technically oriented people inevitably touch on terminology that sounds (and sometimes is) foreign to those who do not understand the nomenclature of various measures used in communications technology. When the throughput of a specific circuit is said to have 1.5 megabits per second, it is helpful to know that mega is equivalent to the number (in this case 1.5) times 1,000,000 or 10^6. Understanding these units is important when comparing different service offerings, evaluating mean time between failures of various components, or reading the calculated aggregation of network throughput necessary for purchasing a circuit for a corporate office. Exhibit 1 gives a brief example of the prefixes and their associated values.

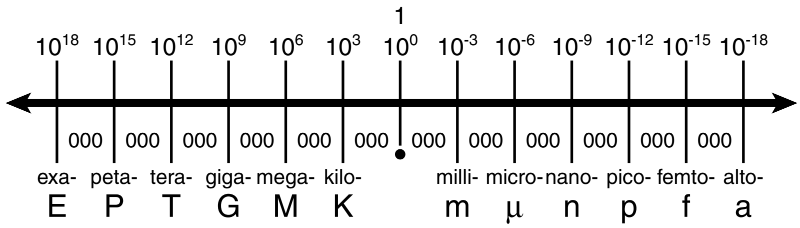


Exhibit 1 Scientific notation chart.

Exhibit 2 Common Uses of Scientific Notation

Prefix	*Frequency*	*Data*	*Voltage*	*Resistance*	*Power*
Tera	Terahertz (THz)	Terabit (Tb)			
Giga	Gigahertz (GHz)	Gigabit (Gb)			
Mega	Megahertz (MHz)	Megabit (Mb)	Megavolt	Megohm	Megawatt
Kilo	Kilohertz (kHz)	Kilobit (kb)	Kilovolt	Kilohm	Kilowatt
Milli			Millivolt	Milliohm	Milliwatt
Micro			Microvolt	Microhm	Microwatt

Exhibit 1 also provides a reference for the various names and values associated with the power of 10 (10^n). Each place is given three zeros to be added or subtracted from the number being discussed, depending on the direction away from one the value is moving. The most common uses of the prefixes are listed in Exhibit 2.

These terms will be used throughout this book without further explanation of their meaning. The exhibits will make excellent reference tools for further reading in communications technologies.

Signals

The delivery of information across the voice and data networks requires somewhere along the continuum a signal from a sender to a receiver to either establish the circuit in which the information is to travel or to verify information has been sent and received. Exhibit 3 shows a block diagram of a voice circuit. The signal process is necessary to establish a connection between the sending party and the receiving party (remember Shannon's law?). The signals are generated in traditional wireline (as opposed to wireless) by signals or frequencies being sent from the dial pad on the telephone.

The signals are propagated over the copper wire infrastructure to the Central Office (CO; the telephone company switching gear closest to your premises). From there, the analog signal is converted to a digital transmission and it is sent out over fiber-optic connections to the various tandem switches, toll offices, ISPs, and other entities that use the existing infrastructure for

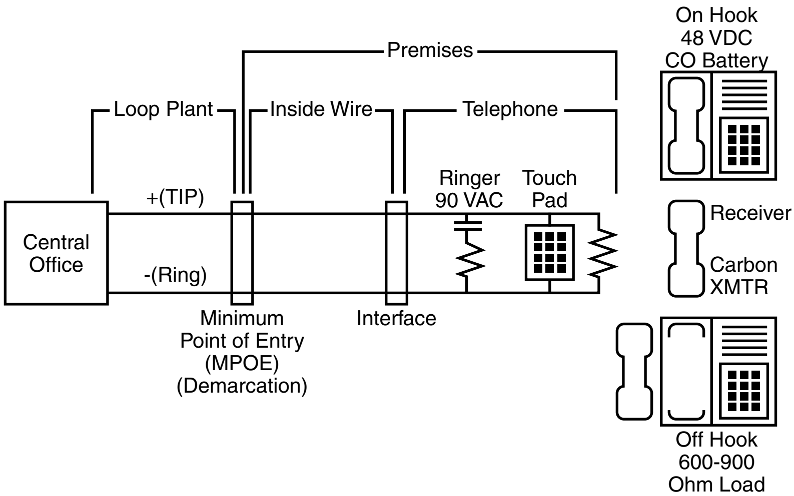


Exhibit 3 Components of a wireline circuit.

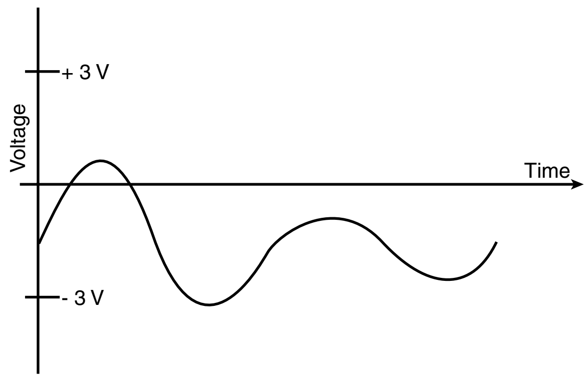


Exhibit 4 Simple waveform.

access. Over the course of this book, we will progress our way through the basic signaling system: the creation of the electrical portion, the traditional analog to digital conversion scheme, the layout of the telephone network and how it is connected, and finally, the steps involved in transmitting through the network.

A signal is typically defined by a waveform, a picture produced by an oscilloscope that shows the highs and lows of the voltage or current associated with the signal. The waveforms vary in intensity, shape, duration, and complexity. Exhibit 4 gives an example of a simple waveform that is graphed over a period of time in reference to its voltage output. Note that the signal is gradually diminishing in its height or peak, attenuating (or losing) its intensity over time. The variation and repetition of a waveform over a specific period of time is referred to as the waveform's cycle. The cycle is usually measured

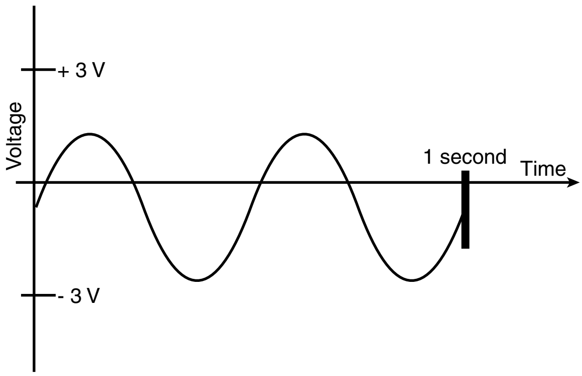


Exhibit 5 Repeating waveform.

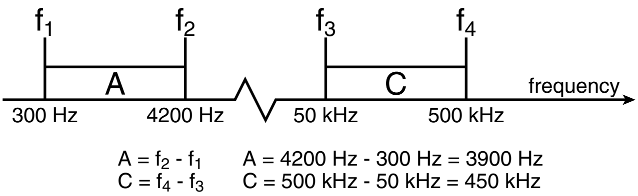


Exhibit 6 Bandwidth representation.

by how many times per second the waveform replicates itself on the graph. This measure is called cycles per second or, in more current terms, Hertz (Hz). If a waveform completes one cycle every second, it is said to be operating at 1 Hz; if a waveform is replicating itself a thousand times every second, it is said to operating at 1 kilohertz (kHz). Electricity in the United States, when measured at an electrical outlet, operates at 60 Hz.

Exhibit 5 shows a signal replicating itself twice over a one-second time period. It is said to be operating at 2 Hz or two cycles per second. The frequency of a signal is defined as the number of cycles divided by the time in which they occur. The period is the time it takes a waveform to complete one complete cycle. These waveforms are characteristic of various signals in the public switched telephone network, wireless communications, and data networks.

Taking this principle one more step, we can discuss bandwidth. Bandwidth is a range of frequencies a communication channel is defined within for specific signaling functions. It is incorrect to refer to throughput (bits of information usually measured by number per second, e.g., kilobits per second) and bandwidth interchangeably. Exhibit 6 is a visual definition of bandwidth. The values discovered for the areas defined by subtracting the lower frequency from the higher frequency gives the bandwidth for a particular band; in this case, that which is associated with bandwidth *A* and bandwidth *C*.

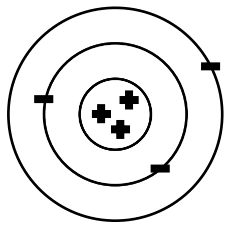


Exhibit 7 Simple atom structure.

Current

One of the most feared and avoided courses in high school and college is physics. Physics, however, is the scientific discipline that explains how things work in our universe. Applying the principles of physics to communications technologies for non-engineers can be done from a level of understanding that eliminates the formulas and calculus that have caused the avoidance of the subject in the first place. A simplistic definition of the building blocks of matter and how they relate is important in our discussion of how information is transmitted from a source to a receiver.

All matter in the universe is comprised of microscopic components called molecules. These molecules are the smallest definable piece of a material. Molecules can be broken down into even smaller building blocks called atoms. Atoms consist of even smaller structures that hold different types of electrical charges: protons (positively charged particles), neutrons (no electrical charge), and electrons (negatively charged particles). Protons and neutrons make up the center of the atom, its nucleus. Orbiting around the nucleus are the electrons, usually in equal numbers in relation to the protons in the nucleus. A basic principle of physics states that the protons and neutrons are bound together by a force that is directly proportional to the size of the particle and its distance from other particles of similar and opposing electrical charges. At the outer edges of the atom, the forces that hold the electrons in orbit around the nucleus are not as strong as those closer to the center of the nucleus; these loosely held electrons are referred to as free electrons because they can be moved out of their orbit. It is the movement of free electrons that causes electric current to exist. Exhibit 7 is a block diagram of what an atom with three protons and three electrons looks like underneath a high-powered electron microscope. Note that the outer orbiting electron is the most susceptible to becoming a free electron.

Forcing the atoms to lose and gain electrons creates an electrical charge that can be harnessed to make all the various components of communications technologies function. Some materials can be caused to move electrons between atoms at a more excited rate than other materials. A conductor is a material, such as copper, gold, or silver, that has a very high excitability and can carry electrical current freely. An insulator is a material that does not allow its electrons to break away from their nucleus easily. Plastic, rubber, and glass are considered good insulators.

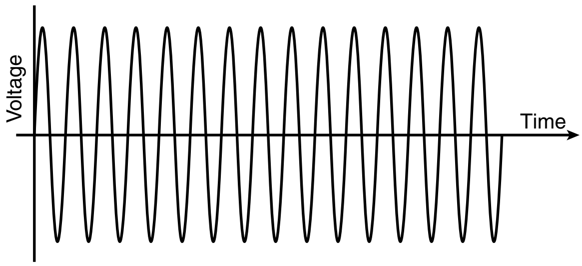


Exhibit 8 Alternating current over a 0.25-second time period.

The rapid change of free electrons in a conductor causes current to flow. One atom changing followed by another, then another in sequence is not how electrons move in a conductor. A by-product of this rapid movement of electrons is heat generation. If a device or conductor is not capable of handling high current pull, the cable will feel warm to the touch (and sometimes burn through). Heat dissipation is an important component of designing electronic circuitry because of the current flow through the various parts in the device.

Current flow is the movement of the free electrons in the same direction in a conductor. The unit of measure used to describe current flow is the ampere, or amp. The letter I is used to represent current in electronic schematic drawings and equations.

Alternating current (AC) is the type of electrical power available at wall outlets. It is one of the two types of current flow; the other is direct current. The charge of the current passing through the conductor changes from a positive to a negative value over a period of time. In the United States, the value alternates 60 times per second; in Europe, 50 cycles per second. At this rate, a light bulb switches on and off 120 times per second — too fast for the human eye to detect. Exhibit 8 shows the rate change of an AC signal. AC can be thought of as changing direction as it goes from its positive to its negative position. This process is continuous until the power source is eliminated.

Direct current (DC) is used primarily in electronic components in computers, cellular phones, the public switched telephone network (PSTN), and data networks. It is capable of doing more work than AC; however, it does not travel as well, meaning it is not distributed over long distances as efficiently as AC. DC can be considered a continuous flow of current in contrast to the periodic condition of AC. Exhibit 9 gives a comparison of DC current to AC current.

Resistance

Resistance is the force that opposes the flow of electrons in a material. Resistance is represented by the letter R in mathematical equations and by the symbol Ω (ohm) in graphical drawings or on components that need to have their resistive values noted. Every material has some form of resistance to electron flow, some more than others. These values of resistance are directly

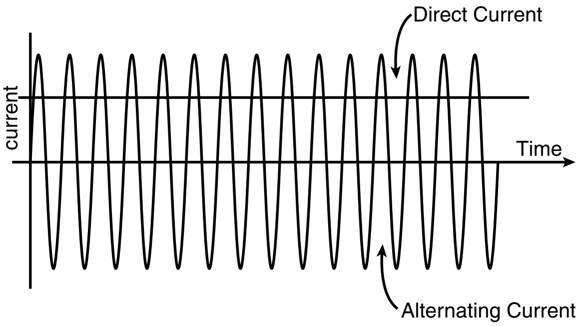


Exhibit 9 Direct current versus alternating current.

related to the previous discussion about conductors and insulators. Different values of resistance are used to vary the current flow to various components in a device. By manipulating a single source of current to service a wide variety of functions using inexpensive resistors (and other electronic devices), the cost of a device is greatly reduced. The cost of a device increases proportionately as power and current requirements become more complex.

Voltage

The ability to perform work or the energy potential of the electrical charges described previously is called a volt, which is represented by the letters V or E in diagrams and equations. There is a direct relationship between current and voltage. The greater the work to be accomplished, the more current is required. Most circuitry is designed to work within specific engineering requirements with current and voltage established at maximum and minimum values. Exceeding either end of the scale will either cause the equipment to fail for lack of power, or overheat and become damaged from overloading the circuitry. Most electronic equipment today works at relatively low voltages that are converted from the standard 120 V AC to ±3 or 5 V DC within the equipment.

Voltage is generated from a number of sources. It is obtained by chemical reactions within a battery, from various forms of power generating plants (e.g., coal, nuclear, hydro), and from alternative sources such as the sun and wind. The amount of voltage available for use from a source is directly related to current and resistance.

As current increases through a resistive material, the amount of force has increased, and the ability to do work has increased as well. The volt represents this value in a simple formula:

$$\text{Resistance} \times \text{Current} = \text{Voltage}$$

This is the basic relationship that is defined by Ohm's law. This law applied to any resistive circuit with one of the values unknown allows the discovery of the unknown value. The importance of this law is evident when evaluating electrical demands for a communications room. Each device in a business environment — PBX, server, router, switch — has a specific voltage and current requirement listed on its specifications sheet. What would happen if the current requirements on the circuit feeding the communications room exceeded the value rating of the current in the electrical panel? Overload! An overload causes the circuit breaker to stop current flow to the circuit, as it is designed to do. By knowing the values and their relationship to each other, proper planning for system upgrades can be adequately accomplished. This knowledge allows you to understand the electrician when discussing physical plant requirements for your facilities.

Ohm's law is always calculated using amps for current, volts for voltage, and ohms for resistance. Because these values can vary depending on the appliance or circuit — megavolts, milliamps, kilohms — they must be converted to satisfy the basic form of the value. By using the scientific notation chart in Exhibit 1, the conversion is simplified.

Capacitance

The ability of an electrical conductor to hold a charge is considered its capacitance. There are components in electronic equipment, called capacitors, that are designed to take and give back electrical charges. They act as batteries within the circuitry, maintaining specific levels of voltage across designated components. When two oppositely charged conductors are placed in close proximity to each other, they create and hold an electrical charge until the power source of their charge is removed. The closer the proximity of the conductors, the greater the ability of the conductors to hold the charge. Capacitors take advantage of this property by separating two conductive elements with dielectric material that controls the charge–discharge rate. All wires within a cable bundle possess the ability to create conductance because of their close proximity to other cable pairs that are transmitting signals (which generates electrical charges). The insulating sheath of the wires helps reduce any adverse conductance from occurring. However, if higher frequencies or power demands are pushed through the wires, the charge rate of the wires is significantly affected. Capacitance is directly related to frequency: as the frequency increases, the capacitance decreases, giving the circuit in which a coupling capacitor is situated an open condition to DC voltage. Exhibit 10 gives a basic graph of the relationship between frequency and capacitance.

Inductance

Wrapping wire around a core and passing current through the wire creates an inductor. The core can consist of numerous materials; however, magnetic material helps create an electromagnetic field around the core. The more wraps of wire and the strength of the core material magnetically increase the resistance of the inductor to return to its precharged state. This property of

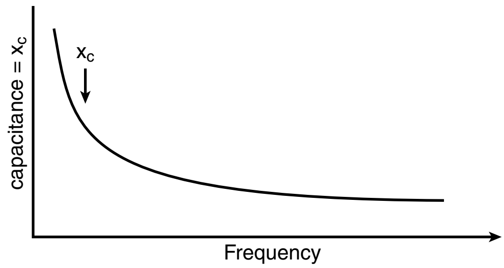


Exhibit 10 Capacitance in relationship to frequency.

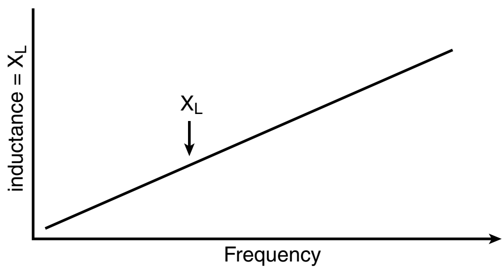


Exhibit 11 The relationship between inductance and frequency.

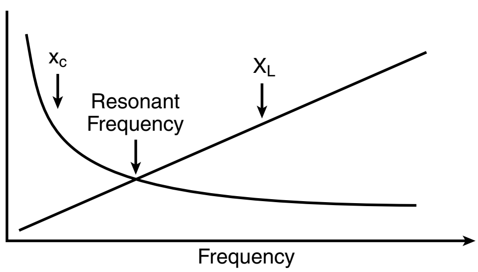


Exhibit 12 Resonant frequency.

an inductor is important in a number of components. Transformers, both step-up and step-down types, are built on the inductor principle. Coils, the devices used to send telephone signals greater distances through the network, are designed as inductors. Inductance is the resistance of a conductor to allow current to change direction. There is a small amount of inductance associated with cable pairs bundled together in a sheathed environment. It is negligible in most conditions; however, with increased frequency transmission through a pair of conductors, the inductive reactance can easily increase. Inductors act as filters to AC values while imposing little effect on DC signals. Exhibit 11 shows the relationship between frequency and inductance in a circuit.

The difference between capacitance and inductance and their relationship to frequency is shown in Exhibit 12. The point at which the two resistive values meet is known as the resonant frequency of the components. Electrical circuit design engineers use the resonant frequency point to create filters that eliminate everything but the resonant frequency. The filtering process is used in finding a radio or television station and cleaning up an analog circuit from extraneous noise from higher frequencies before it is converted into a digital format.

Power

When electrons are forced to move between points of potential difference (e.g., positive and negative terminals on a battery), work is being accomplished. The measure of the rate at which work can be accomplished is called power (P). The unit of measure used to define power is called the watt. One amp of current is flowing and one volt is being applied to create one watt of power. The direct relationship of current, voltage, and power is:

$$\text{Current} \times \text{Voltage} = \text{Power}$$

As current increases, the amount of work that can be done also increases. The same holds true with an increase in voltage. However, simply increasing a voltage source to try and gain more work out of an electrical motor results in disaster. Each electrical device manufactured has a specific rating that dictates the maximum voltage and current draw for that device. Most equipment is fused to disallow an overdraw on either voltage or current, which causes the device to shut down. Electrical wires, connectors, and components are built to tolerate certain levels of power. It is too cost-prohibitive to build devices that can work across all voltage and current values. Power is expressed in terms such as watts, kilowatts, and megawatts.

AC to DC Conversion

DC voltage is a better workforce than AC voltage. However, the delivery of DC voltage over long distances, such as the grid that supports residential, commercial, and industrial power needs, is not feasible. On the other hand, AC is well-suited to be transported at high voltages and stepped down to accommodate the multiple use requirements that it serves. Electronic devices, such as computers, televisions, routers, PBX, fax machines, and servers, work internally with DC voltage. Each device must convert the outlet 120 V AC supply to a DC value to make it operational for the myriad of chips, transistors, and other components running the device.

DC is derived from AC by a device known as a rectifier, which uses special components to control the flow of AC current and bring the negative or alternating side of the signal together with the positive side of the signal. These devices, called diodes, allow current to flow through them in one direction only. There are numerous types of diodes, and they all perform a

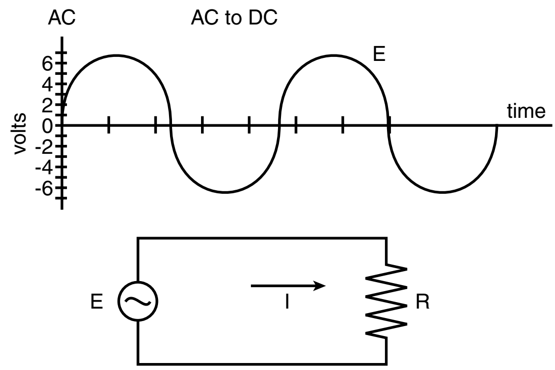


Exhibit 13 AC sine wave.

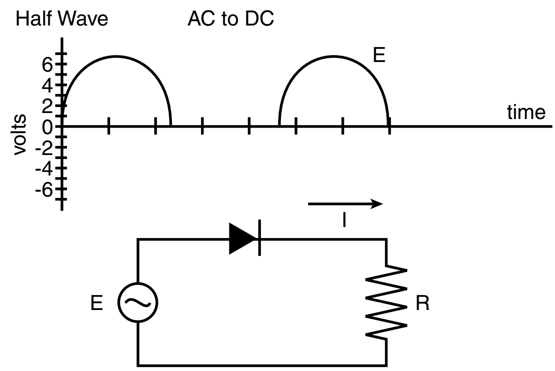


Exhibit 14 Diode eliminating negative current flow.

similar function that varies with voltage and current. The diode acts like a switch to current. Coupled with a capacitor, diodes can create a constant current flow for components within electronic equipment. Exhibit 13 depicts the first step in this conversion process, the normal sine wave signal from an AC source. The direction of the current flow is also shown. Exhibits 13 through 19 show a step-by-step conversion of AC to DC.

A diode is put in place to stop the reverse current flow from occurring. Exhibit 14 shows this first step.

Exhibit 15 shows how a capacitor, when inserted into the circuit, keeps the voltage from dropping back to zero. Remember that the capacitor acts like a battery in the circuit and discharges as the current is reversed in the circuit. This discharge process gives back into the circuit voltage to power the circuit.

We now need to bring the voltage to a more constant rate and eliminate the drop that occurs prior to the charge sequence. This is accomplished by creating a full wave rectifier, which pulls the negative current flow to a positive condition with the aid of diodes and a capacitor. By charging and discharging the capacitor at a higher rate of speed, the attenuation of the voltage becomes negligible. Exhibit 16 shows how the sine wave is pulled from the negative

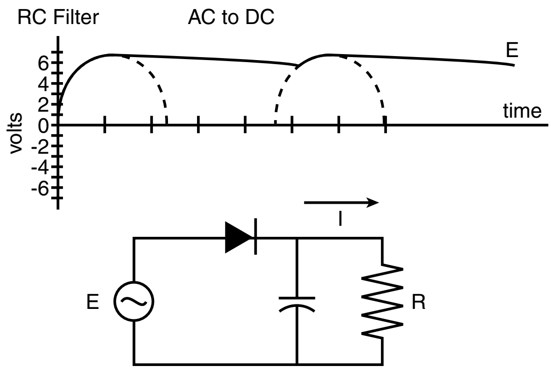


Exhibit 15 Capacitor added to the AC/DC conversion process.

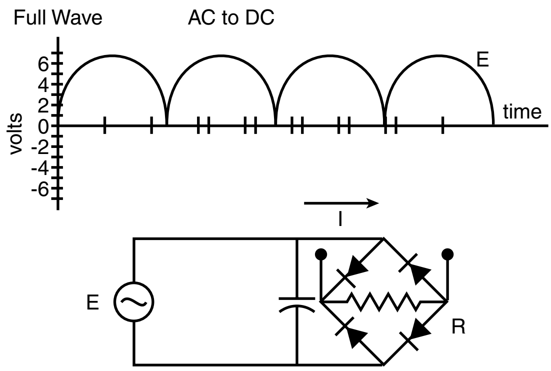


Exhibit 16 Full wave rectified AC signal.

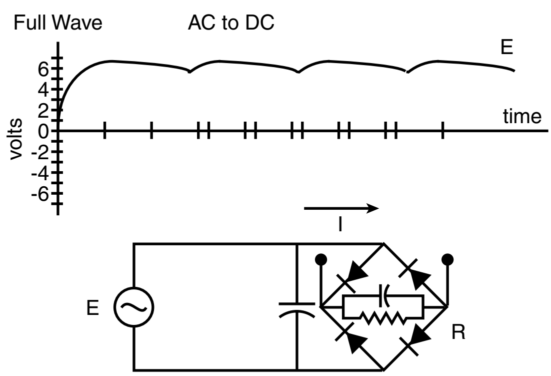


Exhibit 17 Full wave rectifier with capacitor.

side of the circuit by using the rectifying diodes. Exhibit 17 shows how the capacitor charges and discharges to hold the voltage to a more-consistent rate. The voltage reading is done at the two nodes on the rectifier.

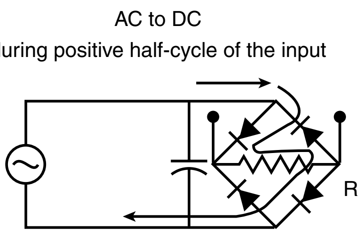


Exhibit 18 Positive cycle of full wave rectifier.

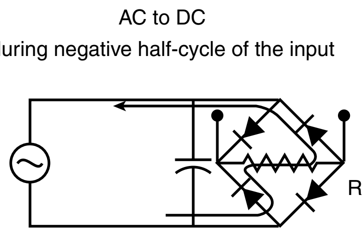


Exhibit 19 Negative cycle of full wave rectifier.

Exhibit 20 Case Study: The Electric Chair

Developed as an alternative to hanging in the 1880s, the electric chair has killed more than 4300 people. The electric circuit is rather simple: the condemned person's body is connected to a high-voltage circuit, becoming a resistance load. The electrodes are usually attached at the head and at the ankles. They are terminated by a sponge soaked in a saline solution to decrease the resistance in the circuit, the human body not being a good conductor in general. There is no standard protocol for the voltage; however, if it is too low, it takes too long, and if it is too high, it burns the body. Nowadays, the voltage is usually set between 2000 and 2200 volts for a current set between 7 and 12 amps. Although in theory the victim's nerves are immediately paralyzed, stopping all sensation of pain, the few who have survived execution said the pain was unbearable.

Exhibits 18 and 19 show how the current flows through the rectifier during the positive and negative cycles. Again, the reading for the voltage is accomplished at the nodes on either side of the rectifier.

Now that you understand the importance of DC voltage conversion, take a look inside of your computer and follow the power lead from the external 120 V AC source through the unit. It is converted to DC immediately upon entry into the unit (see Exhibit 20).

Summary

A basic knowledge of electricity is critical to understanding how the signaling process occurs across voice, data, and video networks. The correct nomenclature and scientific notation is important to understanding all aspects of measurement and throughput discussed in communications technologies.

The atom and its electrical properties were explored to give a better understanding of how current is created in an electrical circuit. Current, resistance, and voltage were explored as the three key components of electricity. Ohm's law is the basic principle that shows the relationship that these three properties have with each other.

Power, inductance, and capacitance were discussed. Power is the measure in which work is performed within a circuit. Its representation as watts is pervasive throughout all disciplines that require electricity to operate. Capacitance and inductance were discussed briefly as to their effect on electrical circuits and their ability to be coupled together to create a filter at specific frequencies.

The conversion from AC to DC was examined. The importance of this conversion is resident inside every electronic piece of gear that needs to be plugged into an electrical outlet to either have a source of power or charge the batteries that provide the DC voltage for the circuitry to work.

Questions for Review

Multiple Choice

1. What is the voltage provided by the Central Office (CO) to the telephone?
   a. 120 V AC
   b. 120 V DC
   c. 48 V AC
   d. 48 V DC
   e. None of the above
2. The waveforms vary in:
   a. Intensity
   b. Shape
   c. Duration
   d. Complexity
   e. All of the above
3. A signal is considered to be attenuating when:
   a. It is losing its intensity over time
   b. It is losing its period over time
   c. It is gaining its period over time
   d. It is gaining its intensity over time
   e. None of the above
4. A range of frequencies is called:
   a. Throughput
   b. Period
   c. Bandwidth
   d. Passband
   e. All of the above

5. What is Ohm's law?
   a. Resistance × Voltage = Current
   b. Voltage × Current = Power
   c. Current × Resistance = Voltage
   d. Current/Voltage = Resistance
   e. None of the above
6. As frequency increases:
   a. Capacitance increases and inductance increases
   b. Capacitance increases and inductance decreases
   c. Capacitance decreases and inductance decreases
   d. Capacitance decreases and inductance increases
   e. None of the above
7. The resonant frequency point is used to create filters that will eliminate:
   a. The resonant frequency
   b. All but the resonant frequency
   c. All frequencies higher than the resonant frequency
   d. All frequencies lower than the resonant frequency
   e. All of the above
8. What is the relationship between current, voltage, and power?
   a. Current × Voltage = Power
   b. Voltage/Current = Power
   c. Power × Current = Voltage
   d. Voltage × Power = Current
   e. None of the above
9. AC:
   a. A worse workforce than DC
   b. Well-suited for transport over long distances and at high voltages
   c. Delivered at the wall outlet
   d. Must be converted to DC to serve electronic devices
   e. All of the above
10. A filtered full wave rectifier is composed of:
   a. 1 diode and 1 capacitor
   b. 1 diode and 1 inductor
   c. 4 diodes and 1 inductor
   d. 4 diodes and 1 capacitor
   e. None of the above

Matching Questions

Match the following terms with the best answer.

Match the different values:

1. 1 V	a. 1000 V
2. 1 mV	b. 1000 mV
3. 1 µV	c. 0.001 mV
4. 1 kV	d. 0.000001 kV

Match the different values:

1. 280 Hz	a. 2,800 kHz
2. 2.8 MHz	b. 28,000 Hz
3. 28 kHz	c. 0.28 kHz
4. 0.28 GHz	d. 280 MHz

Match the units:

1. Voltage	a. Ohm (Ω)
2. Current	b. Ampere (A)
3. Resistance	c. Watt (W)
4. Power	d. Volt (V)

Match the units:

1. Frequency	a. Second (s)
2. Period	b. Bit per second (bps)
3. Bandwidth	c. Hertz (Hz)
4. Throughput	d. Hertz (Hz)

Match the definitions:

1. Molecules	a. Do not possess an electrical charge
2. Protons	b. Are composed of atoms
3. Neutrons	c. Are negatively charged particles
4. Electrons	d. Are positively charged particles

Match the characteristics:

1. Copper	a. Conductor
2. Glass	b. Conductor
3. Plastic	c. Insulator
4. Gold	d. Insulator

Considering a simple electrical circuit (battery, wires, load), match the values:

1. 10 V, 2 A	a. 5 Ω
2. 2 kV, 5 A	b. 25 kΩ
3. 0.5 kV, 20 mA	c. 5 kΩ
4. 25 mV, 5 μA	d. 400 Ω

Match the values:

1. 10 V, 2 A	a. 10 W
2. 2 kV, 5 μA	b. 10 mW
3. 0.5 kV, 20 mA	c. 200 mW
4. 25 mV, 8 A	d. 20 W

Match the definitions:

1. Voltage
2. Current
3. Power
4. Frequency

a. The number of cycles divided by the time in which they occur
b. The ability to do work
c. The movement in the same direction in a conductor of the free electrons
d. The measure of the rate at which work can be accomplished

Match the definitions:

1. Resistance
2. Capacitance
3. Inductance
4. Diode

a. The ability of an electrical conductor to hold a charge
b. The force that opposes the flow of electrons in a material
c. Allows current to flow only in one direction through it
d. The resistance of a conductor to allow current to change direction

Short Essay Questions

1. Define a waveform and name its four characteristics.
2. Define frequency and period, and name their respective units.
3. Define bandwidth and give an example.
4. Define current flow and name its unit. What are the differences between the two types of current?
5. Define resistance and name its unit.
6. Define voltage and name its unit.
7. Define capacitance.
8. Define inductance.
9. Define power and name its unit.
10. Describe briefly the AC to DC conversion.

This page intentionally left blank

Chapter 3

Modulation and Multiplexing

The first two chapters of this book have given you the fundamentals necessary to understand more-complex topics associated with communications technologies. Modulation and multiplexing are the principles of moving information in progressively more efficient methods. We will use the knowledge gained in the previous chapters to help us understand specific information transfer methods. We will examine the radio frequency spectrum, the modulation schemes that are used to maximize the limited resources of the spectrum, and new and emerging techniques of multiplexing that allow us to put more information into a limited space on the spectrum. This examination will give us the information necessary to understand how radio stations broadcast and how cellular phones communicate through the airwaves.

Spectrum

Spectrum is the radio frequency available for personal, commercial, and military use. Specific portions of the spectrum are allocated for aircraft communications and navigation, commercial radio stations, broadcast television, military communications, and cellular telephony. The radio frequency spectrum is a limited resource; there are only so many available licenses that can be issued for use of the spectrum. The recent auctions (and re-auctions) by the Federal Communications Commission (FCC), the federal regulatory body responsible for spectrum allocation in the United States, is an indication of how highly valued the available spectrum is. Some companies have bid so high for the licensing rights to specific spectrum that they were bankrupt from those costs before they were able to implement the infrastructure for service delivery. Exhibit 1 gives a reference to various bandwidths of frequency and the service they are currently assigned to provide.

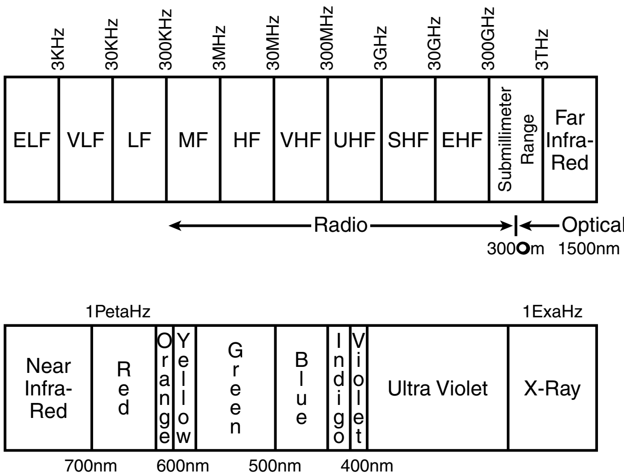


Exhibit 1 Radio frequency bandwidths.

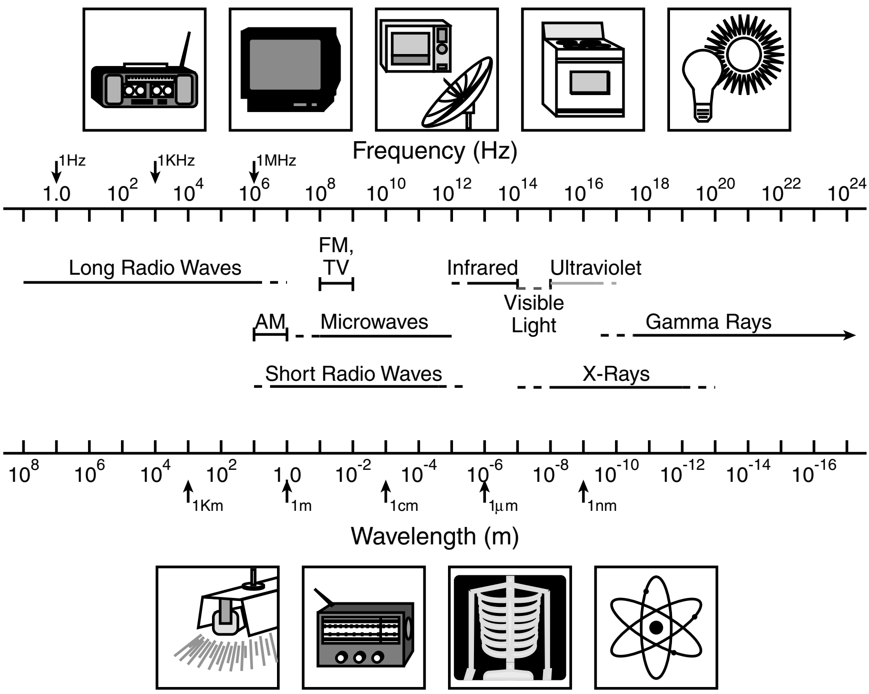


Exhibit 2 Devices and the associated spectrum.

This spectrum covers every device that emits a radio frequency from its structure, such as microwave ovens, AM/FM radios, fluorescent lights, televisions, wireless local area networks, and microwave signal towers. Exhibit 2 shows a broad example of all the devices related to the spectrum and where on the spectrum they can be found.

The use of spectrum is controlled by each national governing body. The International Telecommunications Union (ITU) defines international standards, regulates international radio frequency, and facilitates the development of communications technologies worldwide. Within the ITU, the World Administrative Radio Conference (WARC) sets international frequencies. Because there is a limited amount of spectrum available for commercial use, this global governing body serves an important role in harmonizing the various demands put on the spectrum.

Spectrum in the United States is allocated in three categories: government, licensed, and unlicensed. Government spectrum allocation covers military, navigation, and secure communications, and aviation and public safety frequencies. Licensed spectrum includes cellular technologies, wireless local loop, satellites, and radio and television stations. Unlicensed spectrum that are available for use in the United States are from 902 to 928 MHz, 2.4 GHz, and 5.8 GHz. These bands are also known as the industrial, scientific and medical (ISM) frequencies. The FCC's Web site provides a full listing of every spectrum allocation currently distributed (http://www.ntia.doc.gov/osmhome/allochrt.pdf).

As we move up the spectrum, radio waves become light waves. This gives us an indication that as wavelengths become smaller, they become susceptible to conditions that affect the transmission of light. Frequencies below 6 GHz are not greatly affected by line-of-sight issues or obstructions blocking the signals. Beyond 6 GHz, we are bound by the limitations associated with the curvature of the earth, atmospheric conditions such as fog and rain, and buildings and other structures that impede the signal's transmission path. We will discuss more of these issues as we delve into the specific wireless technologies in this and subsequent chapters.

The goal of information transfer is to get the greatest possible throughput within the bandwidth allocated for that specific service. Increasing the throughput either requires an increase in bandwidth, which results in obtaining more portions of the limited spectrum, or requires more information on the existing bandwidth using modulation schemes. Exhibit 3 gives an example of the bandwidth required for different communications technologies that use radio waves to deliver information.

Amplitude Modulation

In amplitude modulation (AM) frequencies, the carrier signal adds to an information signal to create a joint effort to deliver the original signal as far and as efficiently as possible. Exhibit 4 shows a theoretical perspective of what an information signal and carrier signal may look like.

The cycles per second graphical comparison in Exhibit 4 shows the difference in frequency between a signal and carrier. In AM frequencies, the signal is used to excite or modulate the carrier, and controls the amplitude of the signal, etching the information onto the carrier signal in an additive type of process. Exhibit 5 shows another perspective on the spectrum continuum of the difference between the baseband (signal) frequency and the carrier.

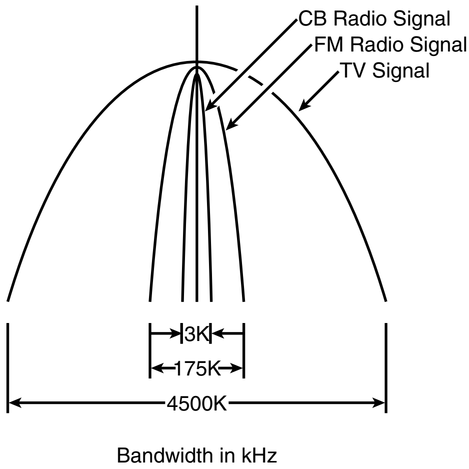


Exhibit 3 Throughput considerations for communications technologies.

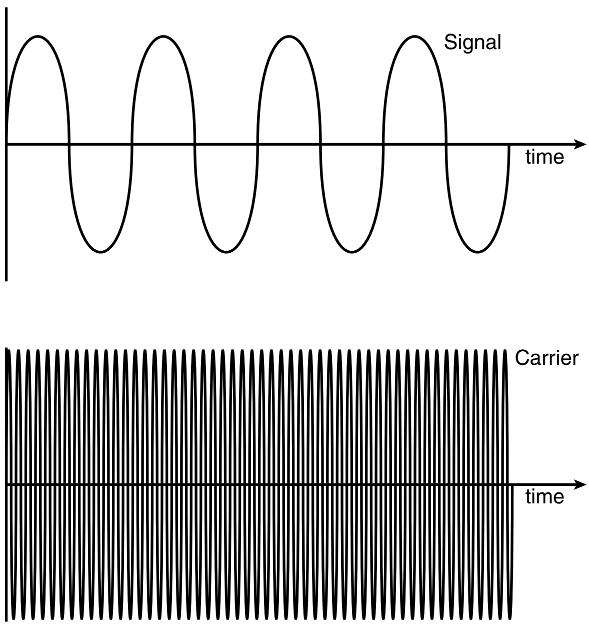


Exhibit 4 Comparison of signal and carrier waveforms.

By placing the signal onto the carrier (added in a nonlinear method), we have the ability to move information with electromagnetic waves (radio waves) over incredible distances. Exhibit 6 shows a more-accurate perspective of what a voice signal may look like prior to modulating an associated carrier frequency. Exhibit 7 is the result of the carrier frequency being modulated by the signal, creating an information signal based on the amplitude of the carrier frequency. The carrier frequency reaches a maximum value corresponding to

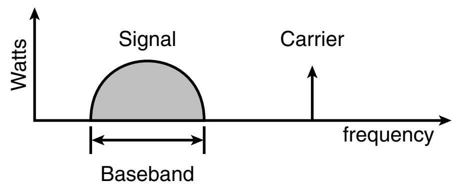


Exhibit 5 Perspective of signal and carrier differences in relation to frequency.

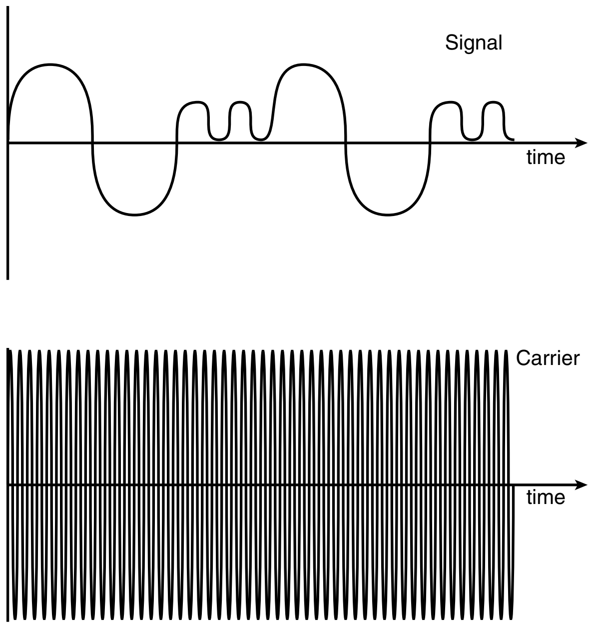


Exhibit 6 Representative signal and carrier frequencies prior to modulation.

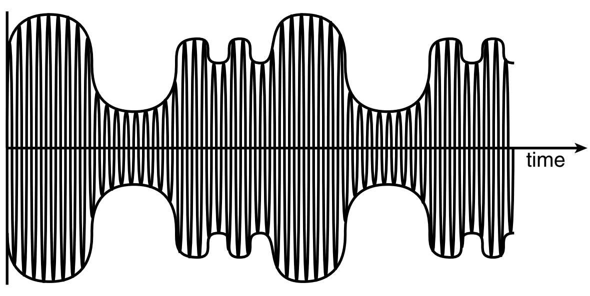


Exhibit 7 Amplitude modulated carrier frequency.

the highest positive value of the information signal. The carrier also reaches its minimum value when the information signal is at its lowest negative level.

We can see the original information signal traced on the amplitude of the carrier frequency. We can also see a mirror image of the information signal

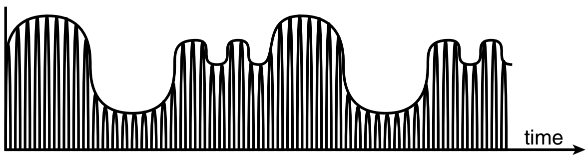


Exhibit 8 Single sideband carrier frequency.

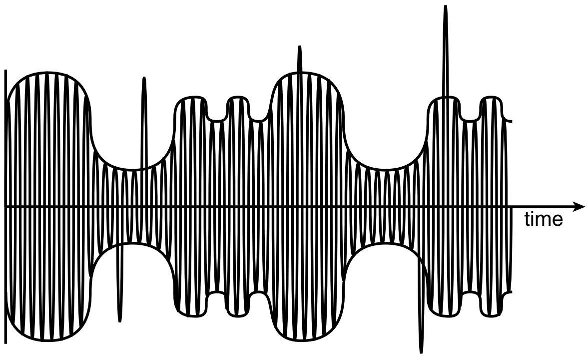


Exhibit 9 Electromagnetic noise and an AM signal.

on the negative side of the carrier signal. This envelope of information can be reduced to a single side of information by filtering out the lower side of the signal. This process creates greater bandwidth usage and is called a singlesideband carrier (SSB). Exhibit 8 is an example of an SSB signal.

Amplitude modulation is highly susceptible to noise. Any high-power electromagnetic interference that is present in the atmosphere can add to the AM signal. This added power raises the amplitude of the signal beyond a recognizable range; it is the reason that we hear the static condition at the receiving end of the transmission when listening to an AM radio station during electrical storms. Exhibit 9 represents noise added to an AM signal. Note the spikes of power above and below the signal envelope. These power surges are detected as noise by the receiving end of the signal. The efficiency and simplicity of an AM transmission make it possible to implement it throughout the country in stationary and mobile configurations. Though surpassed by other modulation techniques for quality of sound applications, AM continues to be a viable technology for delivering information. A simple block diagram provided in Exhibit 10 helps us understand how the basic flow of information travels, modulates the carrier, and reaches the antenna for broadcasting.

Frequency Modulation

In frequency modulation (FM) frequencies, the information signal causes the carrier signal to increase or decrease its frequency based on the waveform of the information signal. The rate and amount of frequency change are

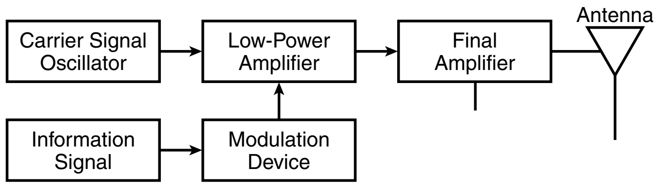


Exhibit 10 Simple block diagram of amplitude modulation.

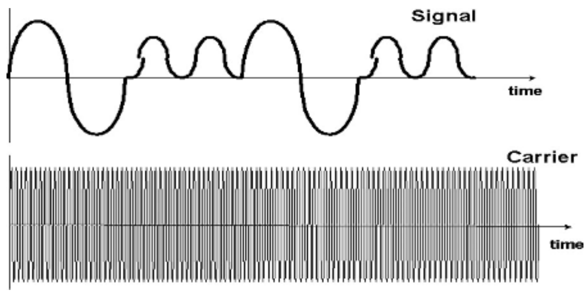


Exhibit 11 Information signal and carrier frequency for frequency modulation.

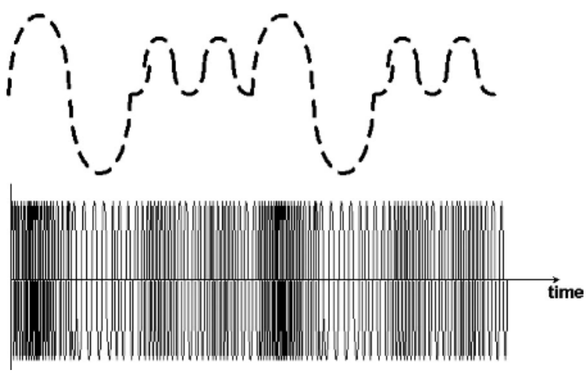


Exhibit 12 Frequency modulated carrier signal.

related to the frequency and amplitude of the input signal. Exhibit 11 gives an example of how the information signal would cause the carrier frequency to behave.

The signal frequency's amplitude will define the amount that the carrier frequency will deviate from its' original frequency and will also determine the speed of carrier deviation. Exhibit 12 shows how the carrier frequency is affected by the information signal.

As the diagram shows, at the peaks of power from the signal, the carrier frequency is increased to its' maximum rate, which is depicted by the closer widths of the cycles. As the amplitude swings to a lower power, the frequency decreases in speed.

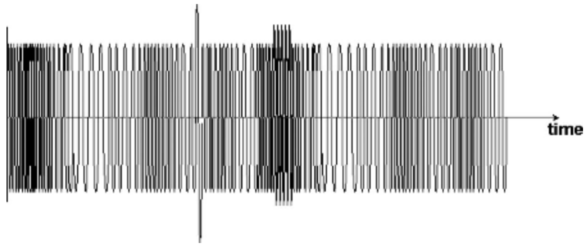


Exhibit 13 FM signal noise.

FM signaling has its' greatest advantage over AM in that it is less susceptible to noise. Because the amplitude of the FM signal is not affected by the signal source that modulates the carrier, adverse amplitude changes provided little impact on the transmission quality. Any spikes added to the amplitude of the FM signal are filtered off on the receiving end of the transmission. Exhibit 13 represents noise added to an FM signal.

The downside of an FM transmission is that it does not have the same range as an AM transmission. FM carrier frequencies are three orders of magnitude higher than those of AM carriers (kilohertz for AM as opposed to megahertz for FM). As we move up the frequency spectrum, signals start to exhibit characteristics of light waves. Though FM frequencies are still a distance away from actual light frequencies, issues such as curvature of the earth and geographic obstructions still affect them.

Phase Modulation

When an information signal is examined, it looks similar to a sine wave from trigonometric functions. Because a sine wave is defined by degrees ranging from 0 to 360, we can think of the sine wave as a complete circle; the cycle of a wave is defined by when it repeats its' form over a specific period of time. If we could start an information signal of the same amplitude and frequency at differing phases, audit could be detected by the receiving equipment based on the starting phase shift, we could incorporate more information within the same frequency spectrum. Exhibit 14 shows how the information signal can be shift by 90° angles.

New information could be started on our depicted signal at the 0°, 90°, 180°, and the 270° phase shifts. There are various forms of coding associated with the phase modulation. Phase shift keying (PSK) is used in modems, voice coders, and other transmission equipment that is limited to the frequency spectrum but has a need for increased throughput. By using these creative methods of maximizing allocated frequency, or frequency capacity limited by Shannon's law, we can increase the throughput of numerous technologies.

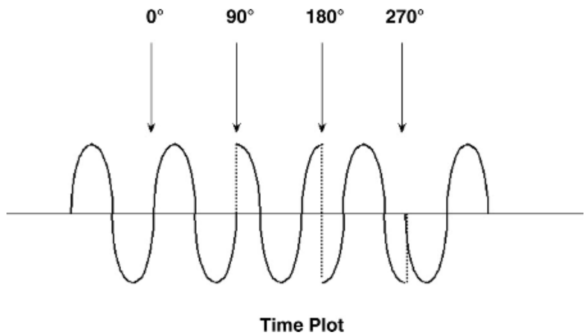


Exhibit 14 Phase modulation with a 90° phase shift.

Pulse Amplitude Modulation

Pulse Amplitude Modulation (PAM) is the first step in converting analog waveforms into digital signals for transmission. PAM was used extensively in the all-electronic generation of telephone switching gear. Sampling the signal waveform and ascribing a voltage value to the point on the wave where it was sampled defines PAM. Exhibit 15 depicts a signal being sampled (vertical lines) at very small rate. Exhibit 16 shows what the resulting voltage amplitudes would look like once analog information is defined in electronic form.

The sampling rate of the analog wave defines the quality of the signal. Increased sampling helps replicate the signal closer to its' original form. The *Nyquist Theorem* dictates that sampling should occur at a rate that is twice

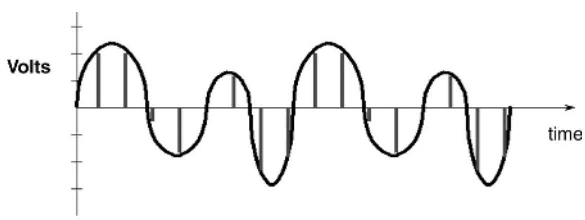


Exhibit 15 Analog waveform sampling.

Exhibit 16 Pulse amplitude signal.

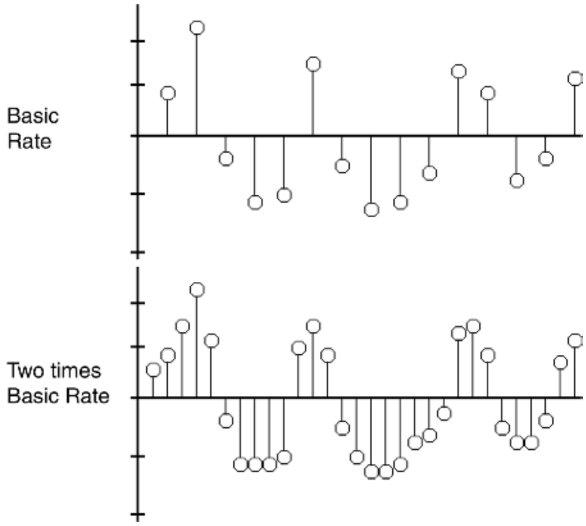


Exhibit 17 Nyquist sampling examples.

the highest frequency being sampled. Human voice travels a range from approximately 30 Hz to 24000 Hz. However, the predominant amount of information being transmitted resides in the range from roughly 300 Hz to 3700 Hz. Engineers created a filtering process that would allow the sampling of a bandwidth of 4000 hertz (4kHz), which would encompass the frequencies defined. The sampling rate, needing to be twice the highest frequency being sampled (4kHz) would result in an 8000 sampling rate per second. To attempt to image sampling something at such a high rate in a very short period of time always leaves me in awe of how digital systems were original designed. Exhibit 17 compares a basic rate to twice the basic sampling rate and the resulting replicated waveforms.

The figure showing twice the basic rate can be seen as having a greater replication of the original waveform based on the points of each pulse. Defining those pulses and their associated voltage values in a binary format is the next step in moving to digital transmission technologies.

Pulse Code Modulation

Because we have defined the process in which we sample an analog signal, and how we need to provide for a high rate of sampling per second to provide for a close facsimile of the original signal, we can move on to defining how we digitize this electronic information. *Pulse code modulation* (PCM) provides a process in which each PAM signal is converted into an eight-bit binary character. The binary format of using just ones and zeros creates a condition of either on or off, voltage or no voltage, and light or darkness. Because we can represent any number in the decimal system with a binary format, we can use just two signals to deliver any combination of numbers.

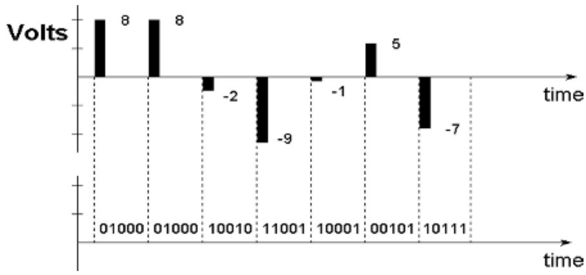


Exhibit 18 Converting from PAM to PCM.

This condition of sending just two different conditions in various configurations to represent an infinite possibility of numbers is the underpinning of digital transmission. By providing an eight-bit (1 byte) for each PAM signal, we now need to create a way in which this information is delivered in an orderly fashion, to keep all the ones and zeros from running into each other. Exhibit 18 is an example of the conversion from PAM to PCM.

The binary numbers chosen here are arbitrary but represent a factual conversion of the PAM signal. A more sophisticated process occurs in *quantizing* the information. Quantizing is the systematic method of providing standard binary numbering to PAM samples for PCM conversion. Nested within quantizing is the procedure called *companding*.

Companding is the process where there is a greater number of samples provided at lower power conditions of the signal waveform, rather than at the higher power portions of the same waveform. This is done to reduce the signal to noise ratio (Shannon's capacity law, again) at points along the signal where the ratio is such that noise may have a greater impact on the quality of the signal. The word companding is a sum of the words *compress* and *expand*. Networking equipment will compress the sending end signal as described above, while the receiving equipment will expand the compressed information back into a recognizable waveform. Exhibit 19 depicts the assigning of more values on the lower power sections of the information signal.

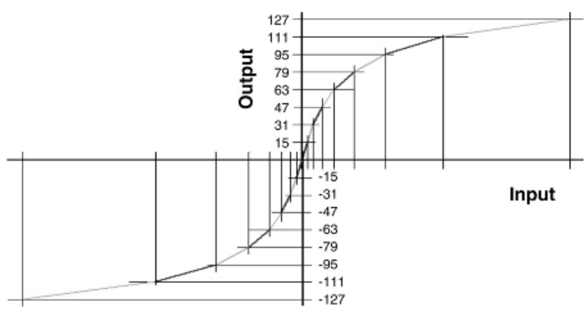


Exhibit 19 Companding.

Note that at both the positive and negative portions of the waveform at the low power areas there are more values assigned for ascribing values to PAM samples.

After this portion of the digitization process is completed, the binary values are encoded into a format that is recognizable at the receiving end of the digital signal. How all of these ones and zeros stay organized is a process known as *multiplexing,* which we will cover in a subsequent chapter.

Summary

Modulation schemes for delivering information from a source to a receiver have evolved from simplistic delivery systems to extremely complex and sophisticated methods. The foundational material presented in this chapter should provide the reader with the tools to understand how information is moved across various mediums and the positive and negative attributes associated with each scheme.

Amplitude and frequency modulation have been used for numerous delivery systems ranging from radio station broadcasts to cellular technologies. Phase modulation contributes a more sophisticated way to bring additional information onto the existing frequency without increasing the bandwidth that has been allocated.

Pulse amplitude modulation was the first step in converting analog signals into the digital environment. From PAM we moved into pulse code modulation. The sophistication of PCM is evident by the complexity of the Nyquist sampling process, quantizing, companding, and encoding. A greater understanding of how PCM is placed out into the networks so various technologies can talk to each other will be covered in a subsequent section on multiplexing.

Questions For Review

Multiple Choice

1. Multiplexing is the process of:
   a. Using technological methods to put more information into limited bandwidth
   b. Using a carrier signal to deliver information transfer more efficiently
   c. Assigning frequencies to various organizations to achieve information transfer
2. The international regulating body concerned with frequency allocation:
   a. Federal Communications Commission (FCC)
   b. World Administrative Radio Conference (WARC)
   c. International Telecommunications Union (ITU)

3. Government allocated spectrum:
   a. Television, radio, and satellite
   b. WLANs, cordless phones, and microwave ovens
   c. Military, aviation, navigation, and secure communications
4. Licensed spectrum allocation:
   a. Military, aviation, navigation, and secure communications
   b. WLANs, cordless phones, and microwave ovens
   c. Television, radio, and satellite
5. Unlicensed spectrum allocation:
   a. WLANs, cordless phones, and microwave ovens
   b. Television, radio, and satellite
   c. Military, aviation, navigation, and secure communications
6. Transmitting signals above the 6-GHz range can be limited by:
   a. Interference caused by power spikes
   b. Interference caused by household appliances and cordless phones
   c. Curvature of the earth, atmospheric conditions such as fog and rain, or buildings that might block the path of transmission
7. What is modulated in AM?
   a. Frequency
   b. Power
   c. Amplitude
8. The information carrier in AM reaches its minimum value when the information signal is at its:
   a. Highest value
   b. Lowest value
   c. Average value
9. AM radio is very susceptible to noise; this is caused by:
   a. High-powered electromagnetic interference which raises the amplitude of the information signal to an unacceptable level
   b. The single sideband carrier is unable to create the envelope of information which filters the lower side of the signal
   c. As the distance increases from transmission, power lines carry a similar frequency, which interferes with information transfer
10. Frequency modulation (FM):
    a. The information signal causes the carrier signal to increase or decrease its amplitude.
    b. The information signal causes the carrier signal to increase or decrease its frequency based on the waveform of the signal.
    c. The information signal causes a power increase on the carrier signal based on the waveform of the signal.

Matching Questions

Match the acronym or value on the left with the statement that best describes it on the right.

1. Single sideband carrier (SSB)
2. Frequency modulation (FM)
3. TV signal
4. Unlicensed spectrum allocation
5. AM radio signal
6. CB radio signal
7. Licensed spectrum
8. 6-GHz frequency range
9. Government allocated spectrum
10. FM radio signal

a. Cellular phone technology, satellites, radio, and television
b. 4500 kHz
c. The point in which frequency transmission is dependent on line-of-sight
d. 375 kHz
e. 902 to 928 MHz, 2.4 and 5.8 GHz
f. Highly susceptible to noise
g. Envelope filtering of the negative side portion of the signal
h. Military, navigation, and aviation
i. 3 kHz bandwidth
j. The information signal causes the carrier signal to increase or decrease based on the waveform of the information signal

Short Essay Questions

1. What is the name of the governing body that controls international frequency allocation and regulation?
2. What is the name of the branch of the executive government in the United States that regulates frequency allocation and usage?
3. Frequency spectrum in the United States can be broken into three categories; what are they, and provide an example of each.
4. What is the significance of the 6-GHz frequency range?
5. When transmitting frequencies above the 6-GHz range, signal propagation is limited by special design constraints; name three of these special considerations.
6. Provide two ways that information throughput can be increased.
7. Explain how amplitude modulation works to deliver a radio signal over a longer distance.
8. Why is AM radio frequency more susceptible to noise or interference than FM?
9. Explain the relationship between frequency and wavelength.
10. Describe the difference between AM and FM modulation techniques.

Chapter 4

Signaling Formats, Multiplexing, and Digital Transmissions

The conversion of analog signals to a digital format, as discussed in Chapter 3, gave the telecommunications world a new delivery mechanism that opened the door to new and far-reaching technologies. These new technologies could not have been imagined when 1s and 0s started pulsing down copper wires. From cellular data and telephony applications to packets of data moving across the Internet, all have their roots in digital signaling applications.

Understanding the process of conversion previously discussed helps you to understand the process of delivering the data from one location to another. The term *data* is used in a broad sense because all voice conversations through core networks as well as traditional data transmissions are represented by the same type of symbol format: 1s and 0s. This chapter will discuss the various formats used to send binary signals along an information path and connect to common digital circuits used in commercial applications today.

Digital Formats

There are a number of different methods for transmitting electrical pulses through a medium to represent data. Exhibit 1 shows the primary formats used in the communications industry. The most popular, bipolar return to zero, or alternate mark inversion (AMI), and its relationship to digital information transfer will be discussed at length.

There are two primary ways of delivering this information over a selected medium: half-duplex and full-duplex. Half-duplex is the ability of a communications circuit to transmit information in both directions (sender and

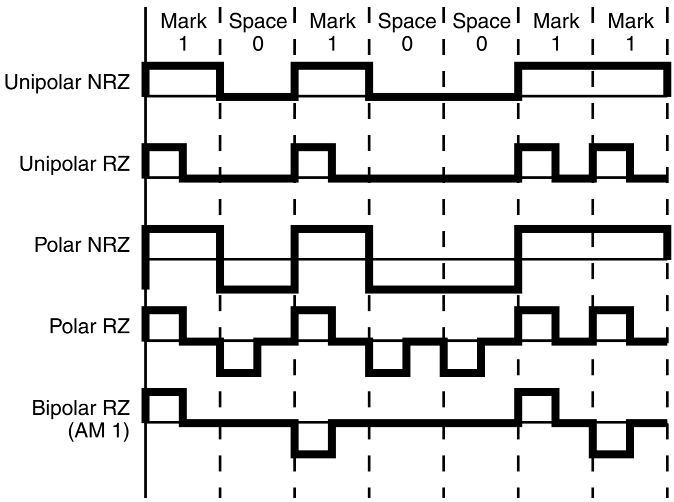


Exhibit 1 Binary signaling formats.

receiver); however, only one direction of information flow can be accommodated at one time. This requires a system that will help the information acknowledge information transfer and delivery and act as the gatekeeper that allows the return information flow from receiver to sender. Early data transmission circuits relied on this format to allow the passage of information and the confirmation of received data over unreliable, noise circuits.

Full-duplex allows the transmission of information simultaneously in both directions from sender and receiver. Most data connections today rely on bidirectional data flow to handle the increased throughput demands. The basic local area network technology, Ethernet, has expanded its technical offerings over the years to include full-duplex transmission as the demand for higher data throughput increases.

These forms of transmission come in one of the binary formats shown in Exhibit 1. Unipolar nonreturn to zero (NRZ) defines its unipolar signaling by keeping the voltage polarity (positive or negative) the same throughout the transmission. The send and receive equipment is designed to recognize and detect only the signal polarity defined by the hardware configuration. The nonreturn to zero aspect of the signal indicates that the mark or the indication of a binary 1 is held high or "on" for a specific time period during the transmission. The time period that the mark is held on is dictated by the technology being used. The signal does not return to the neutral or nonvoltage condition unless a bit defined as a 0 is transmitted.

Unipolar return to zero (RZ) is an improvement over its nonreturn predecessor because it requires less power to drive the signal, the required mark on time is reduced and it sets the idle condition of the line signal in a nonvoltage condition. Polar NRZ uses both positive and negative voltage indications to reference the binary signals. Any negative voltage condition can be viewed as a 0 data bit and any positive voltages can be viewed as a 1 data bit. The progression to Polar RZ is evident in Exhibit 1.

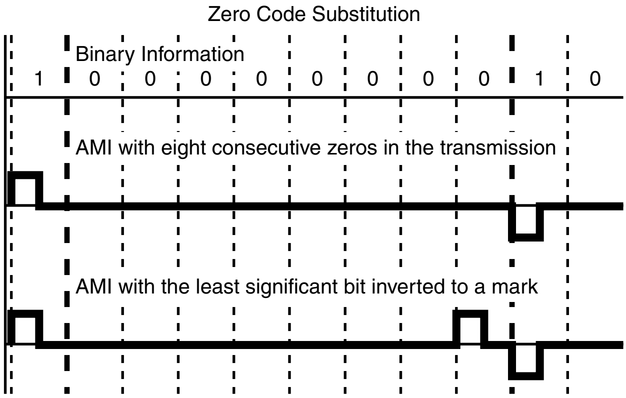


Exhibit 2 Alternate mark inversion on a data transmission.

The final mutation of the information transmission methods is the bipolar RZ. This method changes voltage indication for every mark that occurs in the transmission. This process is used because of power requirements necessary for transmission and the ability to detect errors in the signal stream more effectively. If two marks appear consecutively in the data stream as positive (or negative) marks, there has been an error in transmission. One of the keys to digital transmission is the synchronization of the data bit stream from sender to receiver in a circuit switched environment. Recognizing this fact, the transmission equipment looks to the signal stream for timing information. If no information is being transmitted, which translates into 0s or no voltage pulsing down the circuit, timing problems may occur. The most popular ways currently used to notify the receiving equipment that the transmitting equipment is “still alive” is by using either the zero code substitution (ZCS) method or the bipolar 8 zeros substitution (B8ZS) method.

ZCS simply inverts the least-significant bit in a stream of 0s to indicate a mark. Exhibit 2 shows how the before and after condition is represented in a transmission. ZCS goes by a number of other acronyms and names: AMI is used interchangeably with ZCS to define the 0 code replacement process. Another term used is Bit7, which also refers to the eighth bit being changed from a 0 to a 1 to keep the signal active. In voice traffic, the insignificance of this data bit being given an improper value has little effect on the conversation quality of the signal.

B8ZS uses a different technique to solve the same problem. When it recognizes the same string of 0s, it substitutes a known violation of bits in place of the 0s, which is detected on the receiving end, recognized for the violation, and discarded as a replacement package for the 0 string. Exhibit 3 is an example of how B8ZS behaves in a signal transmission; note how B8ZS violates the polarity of the next mark that is inserted into the string of consecutive 0s at slot four. It follows with the first half of a dual violation in the fifth data slot, and another violation inserted into the seventh slot. The eighth slot is also marked and is in correct bipolar indication to the next mark. As previously mentioned, this is the preferred format for keep-alive signaling

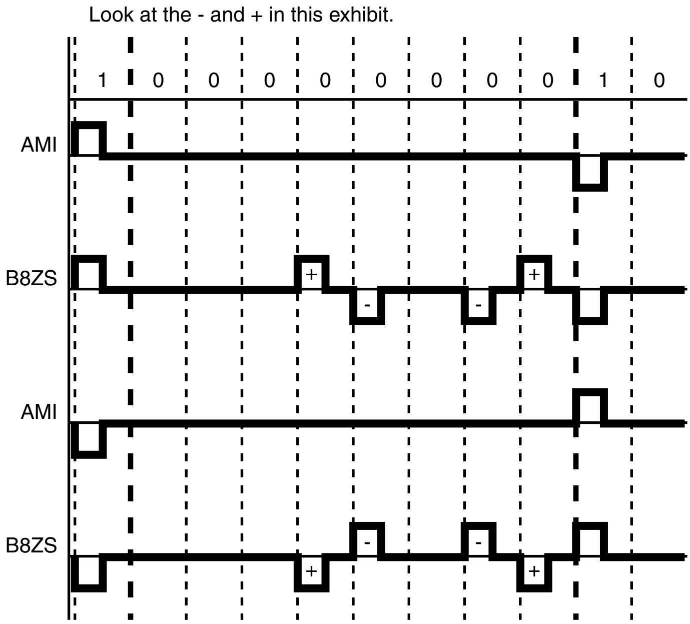


Exhibit 3 Bipolar 8 zero code substitution.

on digital circuit transmissions. This function is achieved with hardware connecting the transmitting equipment to the wide area network.

The channel service unit (CSU) or the digital service unit (DSU) are devices used to interface between transmitting equipment and the external circuit in the wide area network that carries the information. These devices were once part of the network owned by the telephone companies; however, since divestiture they have become the responsibility of the companies using the circuits. The CSU/DSU device is used to convert the signal from the transmitting equipment from a unipolar condition to a bipolar 1 and to detect incoming violations and give alarm indications of the errors. The CSU/DSU also is used for loopback testing on the circuit. The device can recognize a predefined bit stream and loopback to the sender transmitted data. This process is used to check the integrity of the circuit and to troubleshoot areas of failure on the connection. Knowing how to loop back a data circuit to the CSU/DSU and having established benchmarks as to its normal operating condition is critical in maintaining a quality data connection.

The importance of this information is grounded in the fact that all connections to the wide area network rely on the proper formatting and correction process. If a digital circuit is ordered with ZCS keep-alive signaling while the carrier provides B8ZS, alarms, faulty operation, and flaky problems start appearing in relation to the circuit. If the system is looking for ZCS and a packet of 1s and 0s comes down the line as B8ZS, the system tries to analyze the data bits as information. Because there is an intentional bipolar violation in B8ZS, the receiving system signals alarms because it is not expecting to see those violations in the data stream. Obviously, coordinating and double-checking all network and system programming is critical to network management.

Multiplexing

The two primary forms of multiplexing currently used across both voice and data networks are frequency division multiplexing and time division multiplexing. These two methods have been employed to gain the most throughput on a given circuit with respect to frequency for information transmission.

Frequency Division Multiplexing

Frequency division multiplexing was originally developed to provide a way to deliver more voice circuits over a limited amount of copper wires carrying the circuits across the network. FDM divided the available bandwidth into 3000-Hz subchannels to carry voice conversations. These channels were bound by 500-Hz guard channels, frequency spacing on the low and high end of the subchannel, and brought together in a multiplexer to be delivered over the common medium. (A multiplexer is a device that combines more than one frequency or circuit in a time or bandwidth-specific manner to be delivered over a shared medium.) In FDM, the separation is based on the frequencies used for the channel transmission.

FDM has had a number of important uses ranging from increasing the capacity of voice trunks in the core network to providing the format for microwave transmission applications. However, FDM has been replaced in most applications by time division multiplexing (TDM) because FDM has a number of drawbacks. The primary drawback is found when a signal is regenerated for extended transmission: noise is amplified along with the original information. Quality issues come into play as the signal is amplified too many times over longer distances, thus increasing the amount of noise sent with the original amplified signal.

Nevertheless, FDM is applicable today with improvements in solid-state technologies used in the amplification process. Digital subscriber line (DSL) is based on an FDM application over twisted pair copper cable running to the residential environment. DSL is a high-speed network access technology that provides T-1 rates over an existing copper infrastructure.

Time Division Multiplexing

Time division multiplexing is currently the most common form of multiplexing used in North America. Similar to FDM, it combines a number of circuits together to be delivered over a single transport medium. However, unlike FDM and its use of frequency for the allocated separation, TDM uses specifically allocated time slots to deliver the information.

The synchronization of the TDM signal is critical to the delivery of information. Each time slot requires special framing and coordination bits that tell the receiving end where each information slot starts and stops. TDM is based on digital signaling from end-to-end. Each channel is allocated a specific time slot to deliver information to the receiving end. If no information is available for transfer, no data (0s) are entered. This can be a waste of available throughput capability that has been addressed with a more complex method of TDM called statistical time division multiplexing (STDM), which uses all available time slots to send significant amounts of information and handles inbound data on a first-come, first-served basis. TDM, however, continues to be the primary methodology of delivering information over digital circuits.

Digital Circuits

The most widely used digital circuit in North America is currently the T-1. Variations of this circuit, DS-0 and fractional T-1, are the cornerstones of the digital hierarchy of the communications network. The fiber-optic core network infrastructure is designed to load and transfer the T-1 circuit across the network.

The basic building block of all digital circuits is the digital signal 0 (DS-0), which is equivalent to one 64 kbps circuit used for either voice or data communications. This discussion looks at the process associated with voice signaling, because it is more complicated and the transfer of knowledge to the data communication applications is easier to make. In Chapter 3, we discussed the Nyquist theorem, which states that samples should be taken at twice the highest frequency for fidelity. If a voice circuit carries the bulk of information in a bandwidth of 4000 Hz, we would sample the voice circuit at a rate of 8000 times each second. Each one of the 8000 samples is represented by a binary number 8 bits (one byte) in length. If we multiply the 8000 samples times 8 bits, we get the number of bits per second — 64,000 — that are transferred in a single DS-0.

The DS-0 is the building block of the DS-1 or T-1 (these terms can be used interchangeably). The DS-1 consists of 24 DS-0s. The throughput of the circuit is based on multiplying 64 kbps 24 times, resulting in 1.536 Mbps. The actual throughput of a DS-1 is 1.544 Mbps because there are 8000 framing bits added to the data stream to separate each segment appropriately.

Questions for Review

Multiple Choice

1. Which of the following is used for error detection?
   a. B8ZS
   b. AMI
   c. ZCS
   d. All of the above

2. Which of the following throughputs is the rate of the actual data in a T-1 circuit?
   a. 1.544 Mbps
   b. 1.864 Mbps
   c. 1.544 kbps
   d. 1.536 Mbps
3. Which binary format is the most efficient and most used?
   a. Unipolar NRZ
   b. Bipolar RZ
   c. Polar NRZ
   d. None of the above
4. What are the CSU/DSU devices not used for?
   a. Detection of incoming violations
   b. Determining the number of trunks needed for information transmission
   c. Interfacing the transmitting equipment and the external circuit
   d. Carrying information in a WAN environment
5. Frequency division multiplexing (FDM) has the following characteristics:
   a. Divides bandwidth by frequency to send more information
   b. Sends more information than TDM
   c. Labels the individual packets with a time stamp
   d. All of the above
6. Time division multiplexing (TDM) has the following characteristics:
   a. If a particular channel has no information to send, TDM wastes the channel
   b. Sends more information than FDM
   c. The most common form of multiplexing in North America
   d. All of the above
7. If the highest frequency in a voice circuit is 3500 Hz, how many samples will there be?
   a. 5000
   b. 6000
   c. 7000
   d. 8000
8. If a DS-0 has the throughput of 64 kbps, what is the total throughput of a single phone line?
   a. 56 kbps
   b. 80 kbps
   c. 64 kbps
   d. 128 kbps
9. If a DS-0 has the throughput of 64 kbps, what is the actual throughput of a single phone line? (Hint: similar to the modem.)
   a. 56 kbps
   b. 80 kbps
   c. 64 kbps
   d. 128 kbps

10. Which bit stream would best represent B8ZS?
    a. 0 0 0 0 0 0 0 –
    b. 0 0 0 + – 0 + –
    c. 0 0 0 + – 0 – +
    d. + 0 0 0 0 0 0 0

Matching Questions

Match the acronym or value on the left with the statement that best describes it on the right.

1. ZCS	a. The actual throughput of a T-1
2. TDM	b. The equivalent of a T-1 over the PSTN
3. CSU/DSU	c. The equivalent of a telephone line
4. DS-0	d. Changing the last bit to keep the signal alive
5. 1.544 Mbps	e. For detection of error based on a polar violation
6. AMI	f. Bandwidth of a voice circuit
7. FDM	g. Dividing a specified frequency to send more information
8. 1.536 Mbps	h. Ensures the transmission across a WAN
9. DSL	i. The total throughput of a DS-1
10. 4000 Hz	j. Using time slots to send more than channel of information over a single line

Short Essay Questions

1. Explain the differences between half- and full-duplex, and why one transmission method might be chosen over another.
2. Excluding AMI, what would be possible advantages and disadvantages for the remaining four binary formats that are all seemingly doing the same thing?
3. Why has bipolar RZ (AMI) been designated as the most widely used binary signaling format?
4. What do ZCS and B8ZS have in common, and how do these signals work?
5. What, if anything, is the difference between AMI, ZCS, and B8ZS?
6. What is the correlation between the CSU/DSU and AMI, ZCS, and B8ZS?
7. What is a major problem with a digital circuit using ZCS as a keep-alive signal and that signal's carrier using B8ZS signaling?
8. What are the differences between FDM and TDM, which multiplexing method would be more effective, and why?
9. What might be a major disadvantage of TDM?
10. Explain how we arrive at 1.544 Mbps as the throughput for a T-1 line.

Chapter 5

PSTN to CPE

The public switched telephone network (PSTN) has been a part of our daily existence for over one hundred years. The historical significance of Alexander Graham Bell's invention, or possibly his ability to patent his idea only moments before his competitor Elisha Gray, has been the cornerstone of communications technology from the late 1800s through the 1990s. The reliability of the telephone services provided has been defined by the term *five nines,* which refers to the availability of dial tone 99.999 percent of the time. Understanding the basic delivery mechanism of the PSTN (the hierarchical configuration of the switching offices), the customer premise equipment (CPE) that connects to the network, and the basis of circuit switched technology allows you to become fluent in a language spoken, until a few decades ago in this country, by only members of the Bell family.

PSTN

The PSTN is based on the creation of a direct connection from the sender to the receiver over an extremely sophisticated delivery network comprised of copper, fiber-optics, satellites, fixed wireless, and mobile wireless circuits. The network is comprised of five basic components (with numerous subsets): the telephone, network access, central offices, trunks and special circuits, and CPE. Each of these categories (and its subsets) is an area of expertise completely understood only after years of experience and knowledge. It is difficult to maintain fluency in just one of these areas, let alone trying to be knowledgeable across all topical areas. The purpose of this section is to provide a firm understanding of the basic components of PSTN.

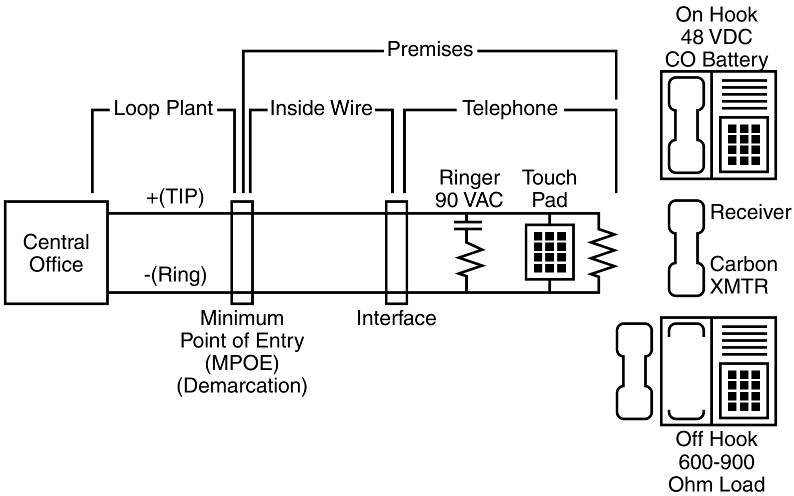


Exhibit 1 Subscriber loop.

The Telephone

The local loop or subscriber loop is the equipment used to connect residential and commercial service to the telephone company's Central Office (CO). This connection consists primarily of copper twisted pair cabling. Exhibit 1 shows a block diagram of the subscriber loop.

The telephone that we have become accustomed to as an everyday commodity of service acts much the same as a light switch. To toggle the dial tone "on," the switch is thrown by lifting the handset, which is commonly referred to as *going off-hook*. Within the inner workings of the telephone, a switch is closed that provides current from the CO to the electronic components of the telephone. The circuit consists of two wires or a pair of copper wires ranging from 18 to 24 AWG (American wire gauge). The tip side of the line when measured with a voltmeter to an earth ground reads zero voltage, the ring side of the cable pair reads –48 volt direct current (DC). The –48 V DC connection provided by the copper wires strung to your location from the telephone company is delivered with negative voltage because it provides for greater resistance in the ionization of the materials in the copper cable. This helps reduce the corrosion of the wire. The two terms, *tip* and *ring,* originated from the component parts on the plugs used by the early telephone operators that connected one party to another.

The transmitter acts like a microphone, converting analog wave signals that excite a diaphragm which vibrates carbon chips to create electrical signals that are transmitted over the telephone cable pair. Modern electronic subsets (telephones) use a similar method of generating a signal with more-sophisticated electronic components. The receiver's responsibility is to replicate the transmitted electrical vibrations back into a decipherable, audible signal. Today's network primarily starts in an analog environment (the exception is

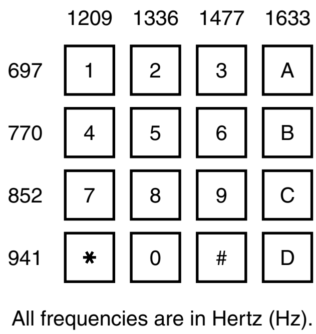


Exhibit 2 Dual tone multifrequency dial pad. All frequencies are in Hertz.

where digital trunks are terminated with digital subsets or other digitally oriented CPE) that converts the transmission from the analog signal at the CO to a digital transmission that is sent over the network to the receiving party's CO. Finally, the signal is returned to an analog format and is sent to the receiver's subset. This "last mile," or the connection from the CO to the end user, is the bottleneck for delivery of high-speed services. The copper environment was engineered to provide reliable service for voice-grade transmissions within a 4000-Hz bandwidth. Various components and configurations (e.g., coils and taps) have caused considerable problems in trying to deliver high-speed data connections to customers.

The signaling to the CO from the subset that is carrying the information to route the call is based on two methods: dual tone multifrequency (DTMF) and rotary (or pulse) dialing. DTMF or Touch-Tone™ provides two distinct frequencies for each key that is pressed on the dialpad. These frequencies are collected at the CO and used to define the called party. Exhibit 2 shows the different frequencies and their alphanumeric association.

The second format (which has all but disappeared from the network in North America) is the rotary or pulse dialing signal. Rotary dials relied on a make-break condition of a set of relays on the dial to open and close the circuit to the CO. The ratio of connection to disconnection (make:break) was 60:40. The on/off pulse of the subscriber loop signaled the CO equipment to indicate the number dialed. The pulse period is 100 ms (millisecond) in duration, one pulse for each digit and ten pulses for the digit zero. Exhibit 3 graphs the pulse signal and the make:break ratio.

The signal notice to the receiving end is processed as an alternating current (AC) signal of 65 to 105 V AC. This low amperage signal activates the ringing device inside the subset that is separated from the DC circuitry of the phone by a relay, which opens when the handset is taken off-hook.

When the signal is received in either DTMF or pulse configuration, the CO pulls the signal from the circuit and passes it along to an overarching signaling network that coordinates all the setup and teardown of calls in North America: Signaling System Seven (SS7). SS7 is an out-of-band method of transferring the information sent by the calling party to set up a call to a receiving station. Out-of-band is defined by the use of a network other than the one in which

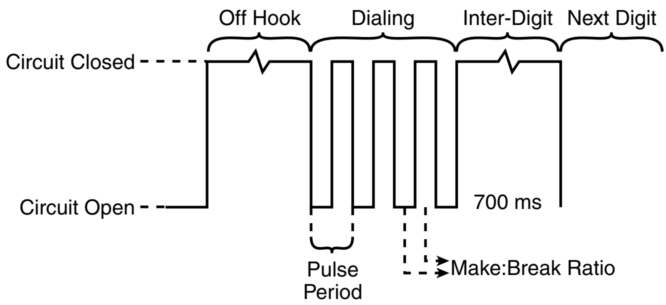


Exhibit 3 Pulse dialing.

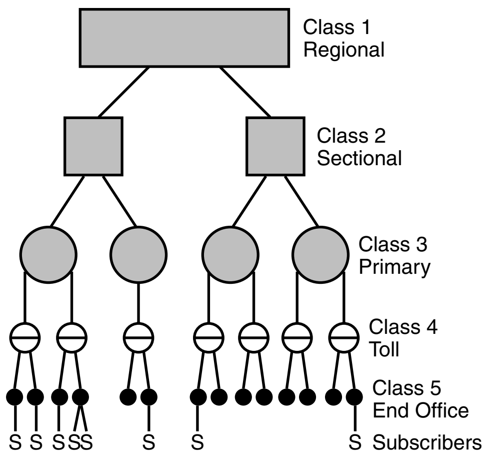


Exhibit 4 PSTN tiered offices.

the voice conversation travels over to secure a circuit. Along with the dialed number, other features such as caller identification (CLID) are controlled by SS7. This is done for two reasons: (1) to enhance the services offered to the end user (CLID, call forwarding, public service access point [PSAP] information), and (2) to eliminate fraud from attempts to emulate the signals in band that bypass toll charges. The path of the conversation is based on a hierarchical network that works on a hub-and-spoke configuration. (A more in-depth understanding of SS7 is important for companies wanting to use the associated database information for routing calls within the corporation or between corporate locations.)

Network Access

The original AT&T network was designed on a five-tiered central office environment. Exhibit 4 shows the progression from the end office to the switching center that directly services the residential and business circuits, up to the regional offices that connect major portions of North America. AT&T has approximately twelve regional offices located around the country.

Since the advent of digital switching in the network, this hierarchy has become flatter, with the sectional and primary layers bypassed in more-advanced network configurations. The toll office also represents a tandem switch that acts as a trunk aggregator between end offices. A tandem switch does not provide dial tone to an end user; rather it acts as a switching point between end offices. It is used to eliminate mesh networking between end offices in large metropolitan areas.

Network access is defined by a number of participants ranging from what is left of the Regional Bell Operating Companies (RBOCs), other independent local exchange carriers, interexchange carriers, cellular operators, and competitive local exchange carriers. After the 1984 breakup of the Bell system, seven regional companies were formed to continue providing the local loop dial tone to their respective market areas. Over the past 18 years, this configuration has been modified considerably by an act of Congress (Telecommunications Act of 1996), which has left in its wake an unrecognizable picture of the previous landscape of the industry. There are volumes of legal proceedings, texts, and Congressional records that have attempted to describe everything that has resulted in this open market approach to telecommunications services. The desired result was to create a more-competitive environment for consumer services, and to encourage innovation in creating new technologies for end users. However, only some of this has transpired. However, the plethora of players involved has caused considerable consternation with the general public. The causes of these frustrations begin with issues ranging from long distance carrier service being changed without customer consent to disastrous finger-pointing battles over dead-circuit resolution. Trying to sort out who provides which portion of your service and how you should be correctly billed requires a full-time staff member at a minimum for some larger corporations.

Sorting out the acronym soup associated with the service providers is a good starting point in understanding the differences between the players. The local exchange carrier (LEC) is the entity that provides the last mile of service from the CO to a residence or business. This is true of the service provided in Cottonwood, Idaho, to Miami, Florida. The monopoly granted to the Bell Company at the turn of the twentieth century helped ensure service to an extremely large segment of the population. Other legislation such as the Rural Electrification Act (REA) provided resources for rural LECs to connect users scattered in less concentrated areas.

The LECs have had control over the provisioning of dial tone until the Telecommunications Act of 1996 forced the market open to other competitive local exchange carriers (CLECs). One of the major reasons for the huge increase in the technology market sector was based on the buildout of networks by the CLECs. One of the reasons for the rapid decline of the technology markets in early 2000 was also based on these companies. Their rapid rise and subsequent demise was based on a number of political, competitive, and hardware and software issues. There are a few companies remaining competing with the LECs to provide dial tone to major metropolitan areas. However, the CLEC industry has failed to provide a national competitive alternative to the existing LECs. Hopefully, as companies sort out restructuring and acquisitions over the next few years, combined with the infusion of new and improved access technologies (e.g., wireless local loop), the consumer will be given an actual choice in local service.

With wireless local loop (WLL) or fixed wireless access (FWA), companies have tried to bypass the use of LEC infrastructure by using broadband wireless connections between their points of presence (POP) and customer locations. The technology falls into two major categories and additional subcategories. The licensed band services of local multipoint distribution services (LMDS) range from the 24 to 31 GHz portion of the spectrum. Multichannel multipoint distribution services (MMDS) work in the 2.5- to 2.686-GHz range. The unlicensed industrial, scientific, and manufacturing (ISM) band of 2.4 GHz also is populated by a number of technologies vying for broadband wireless market share. These technologies will be explored in more depth in a subsequent chapter on wireless technology.

LMDS and MMDS license holders were primarily focused on delivering bundled services voice, data, Internet, and multimedia access to metropolitan customers. The principle of using this technology was sound; however, combinations of equipment malfunctions, antenna deployment, and property management resistance to wholesale services made the penetration necessary for profitability difficult. The higher the speed (the more Hertz per second), the more line-of-sight (LOS) is necessary for delivery of the signal. Weather, physical obstructions, and municipal restrictions on antenna placement have slowed the growth of this part of the network.

The interexchange carrier (IXC) is also known as your long distance provider. AT&T, WorldCom, Qwest, Global Crossing, Sprint, and other players have completely changed this market segment from a single provider of services only 20 years ago to one that provides profitability to numerous companies at a lower cost to consumers. Equal access to providing toll services has allowed numerous companies to enter this segment of the business. Many companies were formed in makeshift offices with bundled services purchased from AT&T routed through their switching gear to the long distance network. This segment of the industry also suffered from a severe shakeout resulting in fewer players competing for a diminishing profit margin on long distance services. The promise of service from advertisers at less than five cents per minute is a considerable drop in profit margin from ten cents just a few years ago. Long distance service is becoming a commodity that is being bundled into other services as a "no charge" offering (e.g., cell phone services). Variations of simply one cent between carriers can mean a huge profit margin difference for a company that may take or make thousands of voice calls every day. The smaller players in this market have either been absorbed by the larger ones or have taken over their larger rivals (e.g., WorldCom acquiring MCI).

IXCs can either locate their POP in the end office or more strategically in tandem offices where they can serve more than one CO. A major advantage for newcomers in this market is that their networks have been built from scratch.

The newness of the equipment allows for modern switching gear, more-sophisticated infrastructure cabling (e.g., fiber-optics and dense wave division multiplexing), and less human-resource overhead to maintain an intelligent network. This is one aspect of competition that has benefited the consumer.

Cellular providers have also become an integral piece of the network access puzzle. With the advent of digital wireless services for voice and data connections, cellular providers have been able to get early technology adaptors to "cut the cord" with wireline LEC services. The progression to even more advanced technology is anticipated with third generation wireless (3G). Offerings will further encourage more mobile communications access to the network. A greater examination of these technologies will be covered in the chapter on wireless technology.

Trunks and Lines

The Central Office's main function is to provide a connection from the end user, residential or business, to the switched network. Knowledge of the different types of available circuits and their functions will help the consumer in provisioning services for their personal use or business application.

Loop Start

Loop start lines are the basis of all residential and small- to medium-size business services provided today. Loop start lines have immediate dial tone. The circuit is ready to be dialed out on 24 hours a day, 7 days a week, all year long. When we go off-hook with the handset of our telephone, we open the switch to allow the dial tone carrying voltage to be sent to the receiver. Small- to medium-size businesses use these circuits on key systems that present more than one outside line to the user. Key system function will be discussed later. Loop start lines are generally less expensive and engineered for quicker deployment than other types of circuits. A loop start circuit is monitored based on its DC current status for signals, and on- and off-hook conditions.

Ground Start

Ground start trunks are used for private automatic branch exchange (PABX or PBX) connections to the CO. These circuits are associated with medium- to large-size businesses. The circuit pair does not have the immediate dial tone that is associated with the loop start trunk. Instead, the CO waits for the PABX to send a signal (ground) to close a relay at the CO that allows the dial tone to be sent to the end user. The purpose of this type of trunk is to keep glare, or collisions, from occurring between outbound callers on PABX and inbound callers to the business. Most business environments rely on dialing a code (usually the digit "9") from a subset to access an outside line. If the trunk was always hot, as in the case of loop start trunks, it would allow inbound traffic to collide with outbound access. In most states, the public regulatory commissions dictate the use of ground start trunks on PABX based on the Federal Communications Commission's (FCC) registration number filed in compliance with ordering circuits from the LEC. Ground start circuits (and other business-defined circuits) cost more than the residential service.

Direct Inward Dial (DID) Trunks

DID trunks are used with PABX or some of the more-advanced hybrid systems available on the market today. These technologies will discussed later. The purpose of DID trunks is to allow a large block of numbers to be assigned to users on the customer side of PABX from the CO, while connection between PABX and the CO is much smaller than the numbers assigned. A trunk circuit that gains its power from PABX (instead of the CO) "looks" at the number that the CO forwards to it. After this, the number is compared to a table that defines the call's internal station destination. The circuit connection ratio to the amount of numbers assigned can range from a 4-to-1 structure down to a 2-to-1 configuration, depending on the level of inbound traffic. These trunks are designed to give external callers direct access to individuals or departments within large corporations.

E&M Trunks

"Ear and mouth" (E&M) trunks were originally designed to connect multiple PABXs separated in wide area conditions. The E&M circuit is designed to seize dial tone from the remote site and allow the calling party to have a remote station dial tone from the distant PABX to reduce the toll traffic within a corporation by using the always-on E&M circuit. The advent of lower priced long distance services and direct connect T-1 carrier services has eliminated the major demand for E&M circuits. The cost of the E&M was based on wire mile distance between the locations and could be very expensive if the circuit spans a great distance (e.g., state-to-state). Some carriers continue to define the connection of their digital trunks with E&M parameters (e.g., AT&T) because the circuit is a switch-to-switch connection.

Centrex

Centrex is more of an extension of the CO than an actual trunk. Its features act similar to those of PABX, except the features reside in the CO switch rather than in hardware located on the customer premises. This type of circuit was originally designed for companies that had scattered locations across a metropolitan area needing a common dialing plan. Centrex callers dial four or five digits to call within their dial plan. For example, a police substation can call another substation or the main jail by dialing a four-digit station number. Dialing out of the network requires an access code (e.g., "9") to be routed outside of the dial plan. Historically, Centrex configured in this manner has been an expensive proposition with limited numbers of lines. In large system configurations, there is a definite advantage to the Centrex service over PABX installation, especially if the company is scattered across a wide geographic area.

Centrex has also been marketed to small- to medium-size businesses by the LECs under various plans that ensured that the customer stayed "connected" to the LEC. The PABX features of the Centrex service can be advantageous to these businesses; transferring inbound calls back out to another location or a mobile user, conference calling, and station dialing features to an associated business location.

The trunks and their properties have been discussed in relation to their analog configurations. However, all of these services can be provided in a digital format if the customer has the equipment capable of handling the transmission. There are other circuits, more specific and narrow in their application (e.g., ringdown circuit used for hot lines, or "hoot and holler" audio circuits for the used auto parts business) that were not discussed but are available (for a price) from the LEC.

Customer Premise Equipment (CPE)

CPE is a relatively entrenched portion of the industry, becoming active after the Carterfone Act of 1968. The act forced the Bell system monopoly to allow competition for connection to the telephone company's lines within the customer's premises. The business system environment had been a major source of revenue for the telephone company. But the act changed the entire landscape of the industry and was the impetus for deregulation of other areas of the telecommunications industry and the eventual breakup of the Bell system. With the incursion of numerous competitors known as interconnects, the percentage of LEC ownership of customer equipment rapidly diminished.

Various components currently make up the CPE landscape. Small- to medium-size businesses today use digital key systems to handle multiple inbound and outbound trunks, while the larger corporations rely on PABX to handle the larger traffic demands that their companies generate. Wedged between these two entities is the hybrid system that has the simplicity of the key system and the feature-rich environment of the PABX.

Private Automatic Branch Exchanges (PABX)

PABX, also known as private branch exchanges (PBX), in its simplest configuration can be viewed as specialized computers that are used to connect inbound voice traffic with the appropriate destination, route outbound calls to available trunks, and allow station-to-station communication. PABX is characterized by feature-rich offerings that process voice calls. They are used to consolidate numerous internal users to a reduced set of trunks connected to the PSTN. Peripheral and system-supported services such as voice processing, station message detailed recording, automatic call distribution, and least cost routing have been created to handle and record call traffic in a highly efficient manner.

PABX subsets can be either economical, single-line analog or highly specialized, digital multibutton subsets. The practicality of putting a durable analog phone on a production line in a manufacturing facility is the same reasoning that the Bell system applied when installing similar types of devices in the residential environment.

Today's PABX can connect to analog as well as digital trunks from the LEC or IXC. The collection of information on how outside trunk traffic is handled, duration of calls made, the number of calls made, and other important traffic considerations are generated by station message detailed recording (SMDR). It is important at this point to note that you should understand that acronyms vary with product manufacturer. Lucent uses different terminology than Nortel, which is different than Panasonic. Various software programs are used to pull out information on single-user activity, and corporate-wide traffic can message SMDR output. Busy hour, busy day, busy time of year, and other management staffing considerations, along with monitoring for internal toll abuse are important aspects of SMDR.

Automatic call distribution (ACD) is a system capability that allocates incoming trunk calls among agents in a programmed group in a way that each agent receives an equitable share of the load. ACD is the cornerstone of the call-center industry. If you have ever called L.L. Bean or another catalog company, or have dialed into a customer service center, your call has been processed by an ACD system. There are highly specialized stand-alone ACD systems (e.g., Interactive Intelligence, Aspect) which are designed specifically for the call-center environment. Many higher quality PABX include ACD software in their standard software configuration to handle varying levels of inbound traffic.

The ACD can be configured to work as a subset of the PABX-served users. An example of this is to create a customer service center within a corporation for external clients with the ACD, while the rest of the corporation works from a traditional configuration on the system. There are uses within companies today where call traffic must be processed in a queued fashion in order to efficiently handle large volumes of traffic. For example, short-staffed human resources offices become inundated with calls after a change has occurred with a monthly payroll deduction. Handling the calls in a timely, orderly manner is the hallmark of ACD.

Exhibit 5 shows a logic flow of how a call is analyzed and processed within an ACD program. The flow of the call after it rings into the group to which it is routed is depicted by the flow diagram in Exhibit 6.

Information that is generated from the ACD traffic reports is much more detailed than those of ordinary SMDR output. It can track agent productivity, which allows the business to assign human resources to different call centers located around the country (or world), based on traffic patterns and agent performance. ACD has spawned a separate industry and the supporting cast from its ability to manage traffic in an efficient and cost-effective manner.

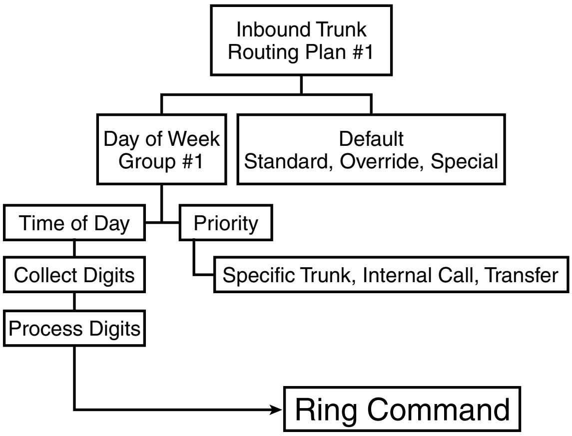


Exhibit 5 ACD programming flow.

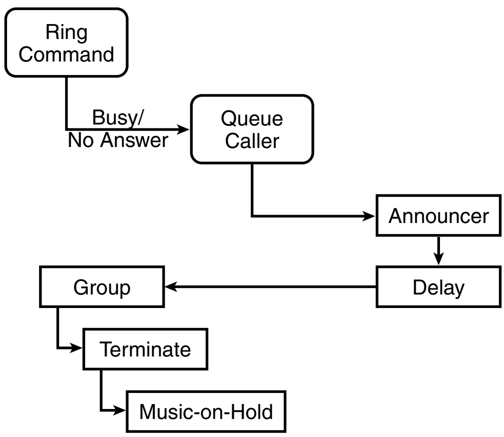


Exhibit 6 ACD call flow after ringing into an assigned group.

Least cost routing (LCR) or automatic route selection (ARS) is the automatic selection of the most economically available route for each outgoing trunk call. Route selection can be based on numerous factors including time of day, day of week, destination area code, class of service of caller and trunk, and status of the trunk. LCR can be used to absorb dialed digits, modify the outbound digit stream by inserting predefined numbers, and select the trunk based on a wide variety of variables. The tables that define the routing sequence of calls in PABX are similar to those used by SS7 to route PSTN calls through the network.

The advent of digital PABX gave business users sophisticated features years before the COs were upgraded to fully digital systems. Features such as call forwarding and call waiting were in place on PABX in the late 1970s while most of the same class of service features did not appear in residential service until the mid- to late 1980s. PABX is currently going through another generational change to a platform that is termed *softswitch*. The softswitch is more user-defined in its configuration and has peripheral software and hardware that has compatibility with different manufacturers. The next generation of switches will be capable of full Internet Protocol (IP) packet switching of voice traffic, as well as delivering data network information over shared wide area connections.

Digital Key Systems and Hybrids

The original analog 1A2 key systems were configured to have one trunk position under each button on the subset. When the line was seized, the light appeared on all the telephones connected to the system. A held call activated a relay system that caused the light to flash at a rate different than that of an inbound ringing call. Intercom, or station-to-station calling, was connected to one of the buttons and was designed to call individual stations from either the receptionist position or from another station. The cable necessary to deliver these features to a standard six- or ten-button analog key set had 25 pairs of wires bundled together in a cable that was at least one half inch thick! Today, the same basic features plus PABX features are available through a single pair of wires to each subset, and a reduction in the size of the main distribution frame (MDF) area is a whole order-of-magnitude!

Digital key systems come in various configurations but they are consistently defined by the number of trunks and stations the control unit can support. A system term, *8/24,* has the capacity for eight PSTN trunk connections and can provide access to twenty-four subsets. The control units of these systems are sealed units, which can be repaired either by the manufacturer or an authorized repair agent. The reliability of these units is extremely high, with mean time between failure (MTBF) rates comparable to CO equipment. However, when the system does go down, components cannot be easily replaced in the field, resulting in the *entire* control unit being replaced. The trade-off is a reduced cost for functionality over component-level replacement of hardware.

Hybrid systems can be configured as either key systems with each inbound trunk available under a button on the subsets or they can replicate the functionality of PABX with single line subsets for the majority of users and a console at a main reception location. These systems have component-level configurations and are port-defined in their capacity. For example, a system that has 144 ports can have a maximum configuration of 128 stations and 16 trunks. The same system can be configured with numerous variations and combinations of trunks and stations, depending on the application demands. These systems have evolved to replicate all the PABX features including ACD, LCR, digital trunk interfacing, and other advanced system and station features.

This market segment is also migrating toward a “soft” environment where the end user provides all the intelligence the system requires on an open system platform. These systems are configured on a non-proprietary operating system and have major components (e.g., power supplies) that are available from numerous suppliers. They have been based on PC platforms and have received negative publicity because of the lack of reliability or uptime compared to traditional telephone equipment. However, these new systems will eventually replace existing systems because they will be driven by end-user programming and not restricted to proprietary controls on processor upgrades or closed system architectures to peripheral devices.

Voice Processing

Voice processing can fall under an umbrella definition for two basic systems: auto attendant and voice mail. The initial market representation of voice processing was characterized by those who held a strong disdain for interaction with a machine and those who enjoyed the increased productivity that the technology provided. Over the last decade and a half, voice processing has migrated to a highly technical process that can route and handle calls as efficiently as any human has in years past. Auto attendant has allowed the traditional receptionist to take on tasks other than being permanently connected to the main inbound call location. The ability of inbound callers to be routed directly to a designated department or individual with the auto attendant's assistance has changed the nature of call processing even for small businesses.

Voice mail (VM) has as many supporters as it does detractors. The ability to save and organize messages without trying to decipher cryptic handwritten messages from a harried receptionist was a great leap forward in customer service. On the negative side, the same technology can be used to hide behind, as in cases where the called party never answers the phone, always allowing VM to screen all inbound traffic. The users (and abusers) of VM have transformed it into a commodity that we now enjoy with residential as well as cellular services. VM has rapidly migrated down from being available only on larger PABX configurations to being fully compatible with small 3/8 digital key systems. A fully integrated connection, one that shares processor information between the voice processing device and the telephone system, should be the only type of device installed for business applications. Without the "shared intelligence," the system compatibility is questionable at best. Systems manufactured by or for telephone system manufacturers usually have minimal compatibility issues and are supported by a single source provider, which leaves little leeway for blame if the system fails.

Summary

The PSTN has provided over one hundred years of reliable service to the North American population. Divestiture of the Bell system caused various technology markets to explode in the last quarter century. Competitive environments ranging from long distance to CPE have caused the industry to expand exponentially. Expansion, contraction, consolidation, and reemergence of players within the industry have kept it innovating for years.

CPE is a relatively new portion of the telephony industry, coming into existence after the 1968 Carterfone Act. The connection of a smorgasbord of products to the PSTN has launched many subspecialties in the industry ranging from fax machines to heating, ventilation, and air conditioning (HVAC) monitoring systems. The business telephone market has provided technology advances that have set the pace for the competitive nature of the industry. Future systems will converge with data networks where the connection to the wide area will be indefinable between voice or data function.

Questions for Review

Multiple Choice

1. What does the term *five nines* refer to?
   a. The voltage sent over the ring
   b. The response time waiting for dial tone
   c. The quality of service needed from telephone service
2. The tip side of the cable pair, when read with a multimeter, will read:
   a. –48 V DC
   b. Zero voltage
   c. –48 V AC
3. Why is negative voltage used in residential telephone wiring?
   a. It provides a cleaner current that does not fluctuate.
   b. It enables the phone company to use diesel-powered generators to supply power to the telephone line.
   c. It prevents corrosion of the lines.
4. What is an interexchange carrier (ICX)?
   a. The company that provides the last mile of service to a home or business.
   b. A technology that requires line-of-sight.
   c. The company that provides long distance service to a home or business (AT&T, MCI, Sprint).
5. Voice-grade circuit transmissions fall within:
   a. GHz bandwidth
   b. GHz bandwidth
   c. Hz bandwidth
6. What is the difference between a subscriber loop and a local loop?
   a. The subscriber loop refers to the connection of end customer equipment to the CO; the local loop refers to the connection of the CO to the nationwide network.
   b. No difference, they both refer to the equipment used to connect residential and commercial equipment to the CO.
   c. The local loop refers to the equipment on the end user's property; the subscriber loop refers to the LEC's equipment.

7. If a customer presses the 9 on a Touch-Tone phone, what two numbers are sent as frequencies to the CO?
   a. 852; 1477
   b. 770; 1477
   c. 697; 1209
8. Signaling System 7 (SS7) refers to
   a. The method used to transmit the ring tone to the end subscriber.
   b. An out-of-band method of transferring call setup information to the receiving station
   c. The method used to obtain an instant dial tone when the CPE is taken off-hook
9. A tandem switch acts as:
   a. The switch used at the CO to connect the end subscriber
   b. One of the layers in the original AT&T five-tiered Central Office hierarchy
   c. A switch that connects two Central Offices together
10. Loop start trunks are:
    a. Trunks that provide immediate dial tone to the end user
    b. Trunks that depend on the premise equipment being taken "off-hook" to provide the ground necessary to send a dial tone from the CO to the end user
    c. Designed to connect two distantly placed PABX

Matching Questions

Match the acronym or value on the left with the statement that best describes it on the right.

1. The last mile
2. LMDS
3. CPE
4. Loop start
5. ISM (industrial, scientific, and manufacturing) band
6. Ground start
7. DTMF
8. Tandem switch
9. Centrex
10. MMDS

a. Aggregates trunks connecting two central offices
b. 2.5 to 2.686 GHz
c. Prevents glare or collisions between incoming and outgoing calls
d. Acts like PABX except hardware is located at CO and not at the customer's site
e. Only came into existence after the 1958 Carterphone Act
f. The connection from CO to end user
g. Used in Touch-Tone dialing, where two numbers are sent as frequencies to the CO
h. 24 to 31 GHz
i. Immediate dial tone
j. 2.4 GHz

Short Essay Questions

1. What does the term digital key system refer to?
2. Describe least cost routing and automatic route selection.
3. What is automatic call distribution (ACD)?
4. What is PABX, and why does an organization choose to implement one?
5. Explain the difference between Centrex and PABX.
6. Loop start and ground start are two types of trunks. Describe them.
7. What is an IXC?
8. Define Signaling System 7 (SS7).
9. What is dual tone multifrequency (DTMF)?
10. Explain tip and ring.

Chapter 6

Circuit Switching, ISDN, ATM, and SS7

The two main types of connecting points of communication across wide area networks are circuit switching and packet switching. The purpose of this chapter is to help you understand what a circuit switched environment entails, the advantages and disadvantages compared to a packet switched environment, and a brief examination of asynchronous transfer mode and how it emulates a circuit switched connection. The overlaying control mechanism of the public switched telephone network and System Signaling Seven is explained also.

Circuit Switching

Circuit switching establishes a dedicated connection between the sending point and the receiving point that is not shared with any other signaled information. This methodology is how the public switched telephone network (PSTN) works. Circuit switching is highly reliable, provides a secure communication link, and is ideal for the distribution of data with a quality of service related to the throughput. More recent technologies such as Integrated Services Digital Network are based on a circuit switched environment.

When the PSTN was first constructed, every phone user was connected to every other phone user within a particular area. This became impossible to maintain as the number of users increased. This "permanent" connection can be considered a permanent virtual circuit (PVC). Exhibit 1 illustrates what this dedicated network looks like. The need to share media between locations led to the development of a switch — a device that allows more than one signaling point to transfer information to an endpoint over a dedicated connection.

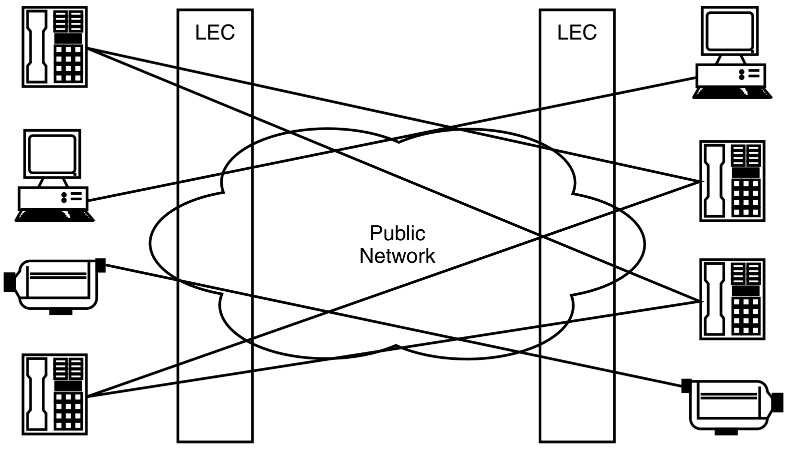


Exhibit 1 Dedicated network.

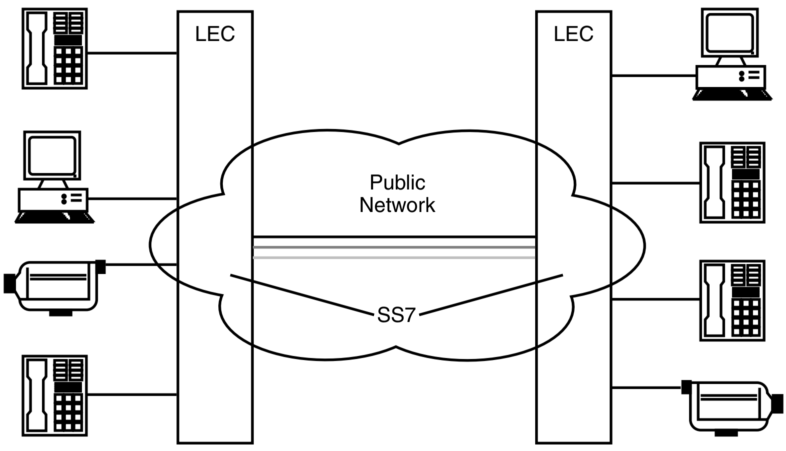


Exhibit 2 Circuit switched network.

When the transfer of information was complete, the connection between the sending and receiving point was disconnected, allowing for another transmission from a different source. Circuit switching creates the ability for any point to communicate with another endpoint anywhere in the network in a dedicated connection. This environment, however, does not allow for multiple connections to a single point at the same time for simultaneous information delivery. Exhibit 2 illustrates the connections associated with a circuit switched network.

The setting up and tearing down of connections that are not permanent to the endpoints are termed switched virtual circuits (SVC). The process of setting up the communication link between the endpoints requires the establishment of connection prior to information transfer. Exhibits 3 through 6 illustrate the setup process.

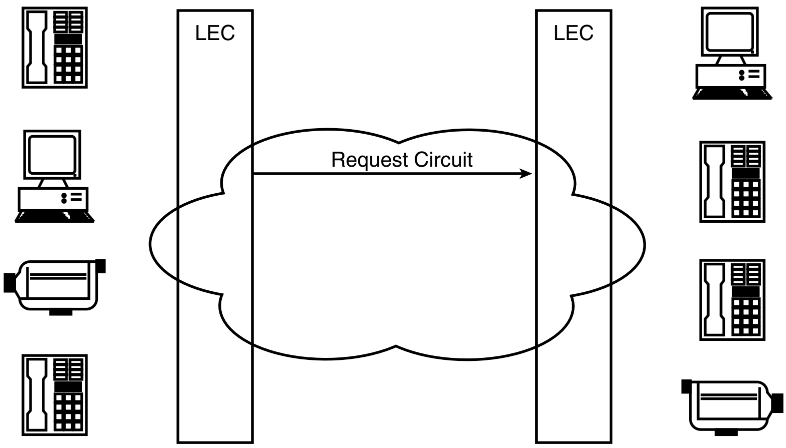


Exhibit 3 Circuit switch request.

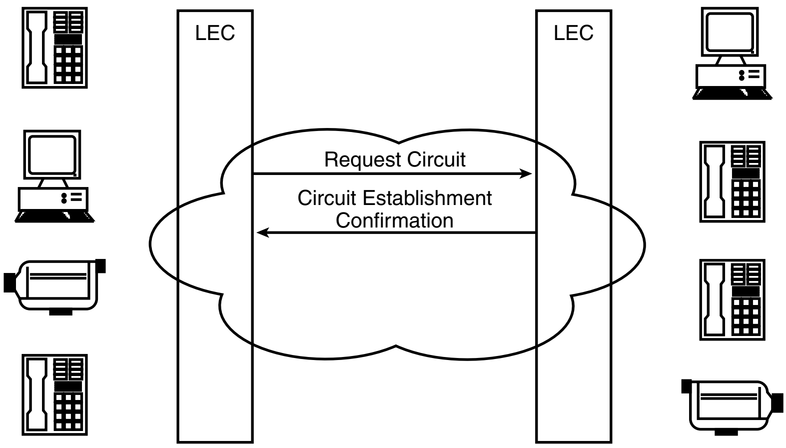


Exhibit 4 Circuit switch confirmation.

System Signaling Seven (SS7)

SS7 was developed and implemented in the late 1970s and early 1980s to provide the connection management for an all-digital network. The eventual migration to SS7 created an out-of-band signaling method for the PSTN. Out-of-band refers to the fact that all the information for circuit acquisition, setup, and teardown exists in a frequency band (in this example, a network) different than the path taken by the information. Prior to SS7, all the information about the circuit connection was passed in-band or within the band of frequency that the information was being sent. This posed a problem in that the information to direct and charge for toll calls could be fraudulently injected into a signal. This faked signal allowed the caller to bypass long distance telephone charges.

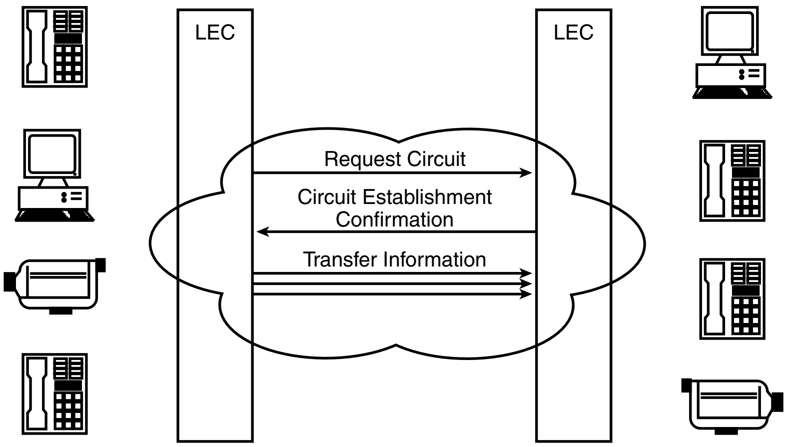


Exhibit 5 Circuit switch connection.

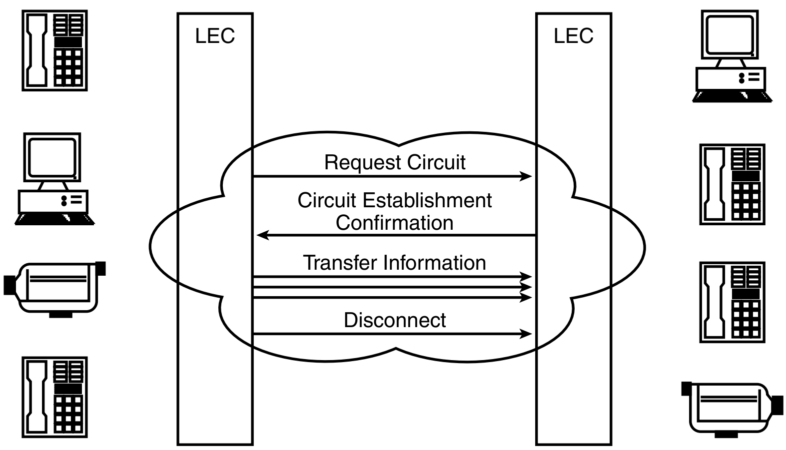


Exhibit 6 Circuit switch disconnect.

SS7 provides supervision, address signaling, call progress information, and alerting notification across the network. Its only function is to provide signaling between switches on the PSTN. There are three primary points affiliated with the SS7 network:

1. Service switching points (SSP)
2. Service transfer points (STP)
3. Service control points (SCP)

SSPs are the locations closest to the user. They are points at the central office (CO) or tandem switch on the PSTN at which the initial information about a call is collected and passed along the network. In some cases with newer technologies (e.g., Interactive Intelligence Call Center Switch), this switching point can be directly accessible from the customer premise equipment (CPE).

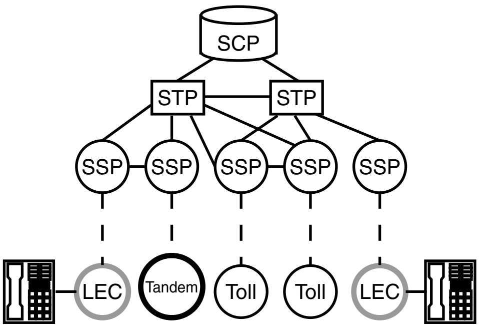


Exhibit 7 SS7 block diagram.

STPs can be considered points on the SS7 network that transfer link information to the next switch to help establish the circuit. STPs are established in a redundant configuration to ensure the reliability of the network. If an STP fails, at least one redundant STP steps in and performs the connection management in place of the failed STP. The STP gets its guidance information about the call from the switch control points.

SCPs can be visualized as databases containing all the addressing information about a particular area of the country. These databases can be maintained either by the telephone companies or private enterprises providing services to the PSTN (e.g., Intrado Corporation, Boulder, Colorado). SCPs provide the information that makes emergency 911 calling, caller identification, and other network-related features possible. The most important idea to remember about SS7 is that it is an out-of-band, stand-alone network used to set up, monitor, and tear down switched circuits on another network. Exhibit 7 illustrates a simple layout of the SS7. Note that each point is connected with more than one link for redundancy purposes.

SS7 has recently become extremely taxed because of the increased demands on the network. The implementation of new wireless (cellular) connections and new regulatory edicts requiring position location for mobile emergency dialing has forced some upgrades to the network. The links between the points are being expanded from 64 kbps connections to T-1 connections. As Integrated Services Digital Network technology has finally become more prevalent in the network, SS7 is necessary to transfer all information from endpoint to endpoint.

Integrated Services Digital Network (ISDN)

ISDN is a digital transport circuit that can provide voice, data, and video (multimedia) services over a PSTN connection. ISDN relies on SS7 to carry its connection information from source to destination in approximately two seconds across the North American network. The all-digital nature of ISDN allows the signal to stay in its digital form without the need to change from analog to digital then back to analog again. The initial rollout of ISDN by the

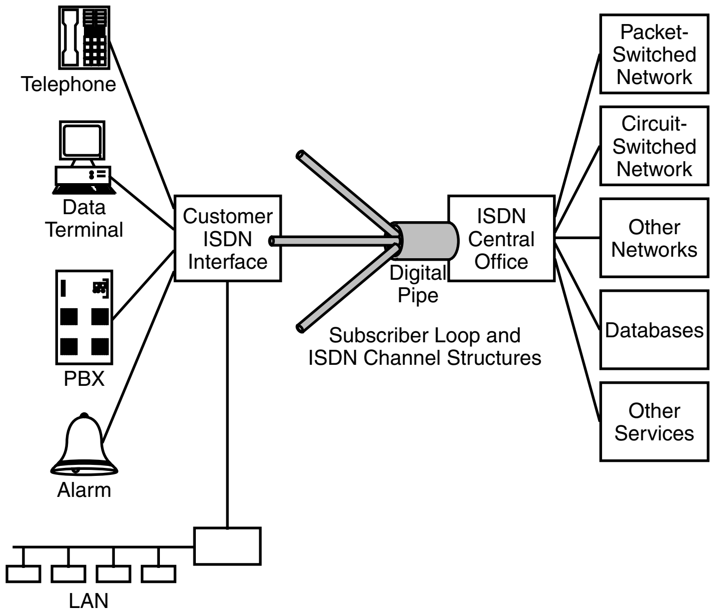


Exhibit 8 ISDN applications.

telephone companies was met with a great deal of skepticism. It was not until the need for high-speed connections to the Internet in the mid- to late 1990s that ISDN began penetrating the market. In order to connect the ISDN circuit to a residential home, one had to wait between 45 to 60 days for the circuit to be engineered. Though other high-speed data connections have surpassed ISDN for throughput capacities, it remains used as an excellent backup direct dial connection for data networks because it is part of the PSTN.

ISDN Configurations

There are two types of ISDN predominantly in use today: basic rate interface (BRI) and primary rate interference (PRI).

BRI consists of two bearer (B) channels of 64,000 bits per second (64 kbps) throughput. The two channels are managed by one 16,000 bits per second (16 kbps) data (D) channel. The BRI circuit is also referred to as a 2B+1D channel, a two-bearer-channel and one-data-channel configuration. The standard throughput for a BRI ISDN circuit is that of the two B channels or 128 kbps. There are applications that can take the D channel throughput and maximize it for other services and overhead bits used to manage the circuit (e.g., 144 kbps total) but when considering applications, the 128 kbps should be considered.

Bonding, also called *H-channels,* is the use of multiple BRI circuits together to provide greater throughput. A 384-kbps configuration, which is the use of three BRI circuits (or six B channels) where the ISDN circuits are used parallel to each other, is common with videoconferencing applications. There are other

H-channel configurations available from fractionalizing (smaller segments) of the larger ISDN circuit or PRI.

PRI is a 24-channel, 1.544 Mbps circuit in North America used in large-scale applications for PBXs, high-demand data networks, or other high throughput applications. (The European version is a 2.048 Mbps circuit similar to the European E-1 rates.) The B channel capacity is the same as on the BRI circuit, with 64 kbps for each channel, and the D channel is a 64-kbps capacity. The PRI circuit has 23 channels that can be used for the defined application, with the 24th channel being used as the D channel to control framing, signaling, timing, supervision, and other circuit control issues for the other 23 channels. Multiple PRIs can be configured, depending on the CO equipment to run multiple PRI circuits (6 to 8) with one D channel used to manage all the B channels. A redundant D channel can be specified in the engineering configuration as a backup to a circuit failure if the system is configured in this manner.

The switched nature of PRI has helped eliminate the need for point-to-point T-1 circuits in many networks. The PRI connection is treated as a long distance telephone call for connections made out of the source's local access transport area (LATA). PRI circuits can be designed to have portions of the service used for the data network, some for the voice needs, and still other channels defined for videoconferencing services. The channels can be configured to be used on-demand by a system administrator who may have a specific occasion where more data throughput or video services are needed. Exhibit 9 gives a representation of the two ISDN channel configurations.

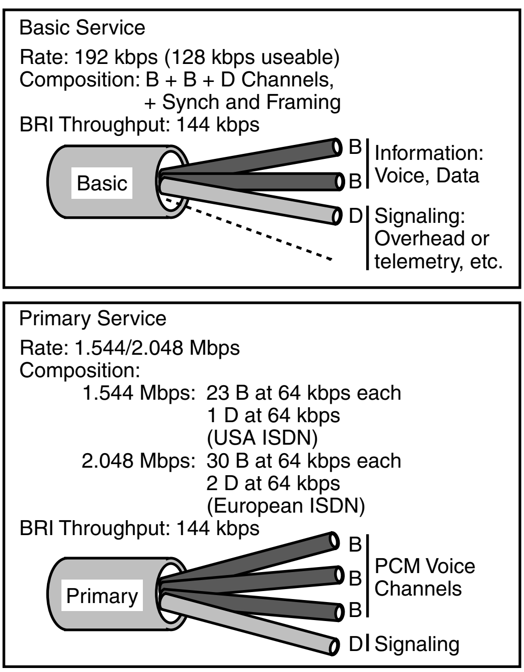


Exhibit 9 ISDN configurations.

ISDN Network Interface Configurations

ISDN requires specific termination equipment, depending on the type of connection required. Network termination (NT) equipment comes in different configurations and is responsible for physical layer and electronic connectivity between the user and the CO. The NT is also responsible for the conversion from two-wire to four-wire service at the CPE, for synchronization, and for management and monitoring of the circuit. The two demarcation types of NT equipment are termed NT-1 and NT-2. NT-2 has the same features listed previously but is associated with PBX terminations, which may be directly imbedded in the interface card of the system.

Terminal equipment (TE) can either be directly compatible (TE-1) with an ISDN circuit or can require conversion from its current configuration to make it compatible with the ISDN circuit. The terminal adapter (TA) is responsible for this conversion. There are four primary points of network demarcation that are defined for various purposes and characterized by an alpha code:

- *R:* Link between non-ISDN gear and an ISDN TA
- *S:* Connects ISDN devices to NT-1, NT-2, and N-2 devices
- *T:* Connects NT-1 to an NT-2 device
- *U:* Connects network termination equipment to the PSTN

It is important to make sure that equipment purchased to connect ISDN services together is compatible with the CO. Different manufacturers (e.g., Lucent, Nortel, Siemens) have been known for quirky connection issues in their ISDN circuits.

Asynchronous Transfer Mode (ATM)

ATM is a cell-based, asynchronous delivery technology designed to carry voice, data, and multimedia services over the same link at the same time. It can emulate a traditional voice network and provide synchronous delivery of a voice conversation or it can be used to deliver bursty asynchronous data traffic over the wide area. ATM can be configured from desktop to desktop across the wide area network (WAN). It is known for its high quality of service and flexibility, and is currently the switching method of choice in the major carriers' long haul networks. ATM is capable of providing connection-oriented services (e.g., voice) and connectionless services (e.g., local area network [LAN] emulation) over the same network.

ATM Architecture

ATM exists as a compromise between circuit switching and packet switching technologies. It bases the cell structure of data on a 53-byte or octet configuration. Each cell that is put out on the network is 53 octets in length: 5 octets for the header information and 48 octets for the payload, or actual data. ATM establishes a connection between source and destination similar to a traditional telephone voice call before it transmits information. However, by defining its throughput on specific cell sizes, ATM resembles a packet network (e.g., Ethernet). ATM cells define their own route through a network but they are defined by a connection-oriented condition.

The ability of ATM to work with both voice and data has made its use applicable in numerous environments. Converting data to ATM cells can occur at a number of points along the transmission path. It can be converted to a cell format at the workstation or computer. The network interface card (NIC) can be installed as an ATM NIC, giving the network a LAN ATM environment. An internal network switch can also convert packet data into the ATM cell-based protocol. An edge router connecting the internal network to the WAN can be the site of conversion to ATM cells. The CO or the carrier switch can convert data into an ATM cell structure. Its adaptability within and between networks has made ATM a flexible technology for network design.

ATM is the primary choice of technologies for a number of applications when quality of service is required for the data throughput. It can be used for workstation-to-workstation computer-aided design (CAD) and computer-aided manufacturing (CAM) where large files of graphical information must be transferred from one engineering site to another. ATM is used in the backbone of campus networks to deliver multimedia to the desktop and to handle heavy client/server traffic. It can be implemented in the metropolitan area network (MAN) to connect different locations of the same enterprise with high-speed, high-bandwidth, and high-quality service. It is also implemented in the carrier network backbone for reliable switching performance on the long distance network.

ATM is delivered at different speeds to the end user's location. The list in Exhibit 10 includes some speeds that were specifically designed for IBM-based networks in which speed conversions were not desirable. ATM can also be configured to emulate local area network throughput protocols. Exhibit 10 lists some of these configurations.

ATM Cell Structure

As mentioned previously, the ATM cell is based on a 53-octet configuration. Exhibit 11 gives a basic definition of the cell structure with the 5 octet header and 48 octet payload. Exhibit 12 breaks the cell down into its component parts.

ATM Structure Defined

Each compartmental segment of the simplified cell has a specific task associated with the delivery of the ATM cell. The compartments or fields were designed for maximum flexibility, depending on the demand or adaptive layer configuration. The adaptive layer allows the ATM circuit to be configured to meet various types of media requirements, such as voice and video requiring zero delay and synchronous delivery while data has the luxury of being sent

Exhibit 10 ATM Speeds of Transport

ATM Speeds
25 Mbps IBM 4B/5B
51 Mbps SONET
100 Mbps TAXI 4B/5B
155 Mbps SONET
622 Mbps SONET
2.4 Gbps SONET

Net Interface Speeds
Circuit Emulation
1.5 Mbps
45 Mbps

LANE Interface Speeds
10/100 Mbps Ethernet
16 Mbps Token Ring

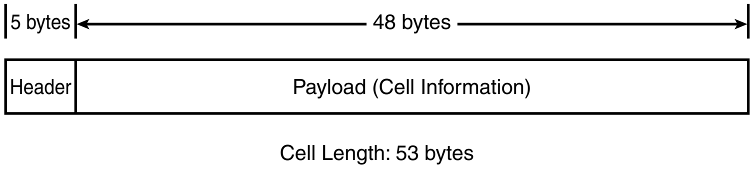


Exhibit 11 ATM basic cell diagram.

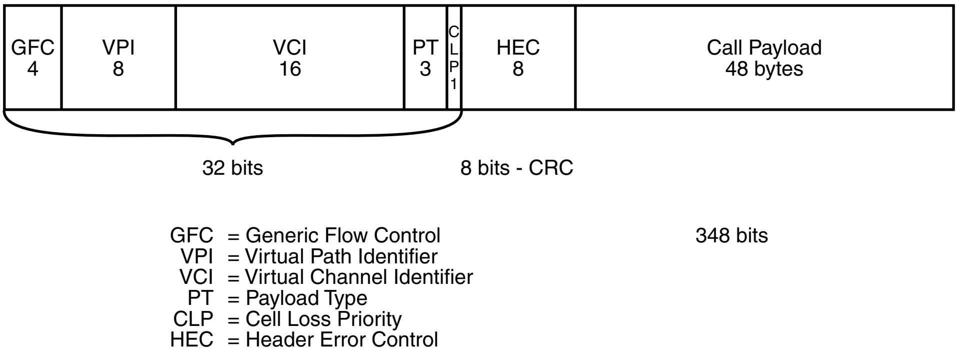


Exhibit 12 ATM cell structure.

in bursty asynchronous patterns. Defining the fields for the ATM cell helps with the basic delivery mechanism of the protocol.

Generic flow control (GFC) allows a handshake control with customer-provided equipment such as a multiplexer to regulate the ATM device. This field is eliminated (overwritten) when the cell is transferred out to the network.

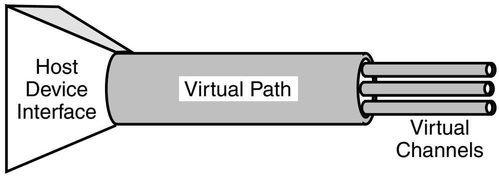


Exhibit 13 ATM channels.

Virtual path and virtual channel identifier (VPI/VCI) are logical connections between endpoints. A physical circuit (e.g., a fiber-optic cable connecting two devices on the network) can have one or more virtual paths (VP) contained within it. A VP can have one or more virtual channels logically located within it. The ATM multiplexing is based on these two levels. Exhibit 13 shows how these paths relate. The switching that occurs in the network is based off the VPI. A VPI can be considered a dedicated, private line that maintains a constant throughput capacity that may change the network paths used to deliver the payload.

Payload type defines which ATM adaptive layer is assigned to the cell and whether or not the cell is being used as an information cell related to the management of the network.

Cell loss priority defines cell discard priority during congestion on the network. There are two settings: high and low. The high priority setting tells the network that the cell should not be considered for discarding.

Header error control provides an error check on the header only. If there is an error located within the header, it can be defined for either correction or rejection by the network.

Payload is what ATM is all about. Whether it is data, voice, or multimedia, it resides in this field segmented into a 48-byte chunk of information that is reassembled on the receiving end of the circuit.

Although emerging technologies have been touted as replacing ATM in the network (e.g., Gigabit Ethernet), ATM has quality of service that cannot be matched by other technologies and its ability to deliver different services over the same circuit is unique.

Summary

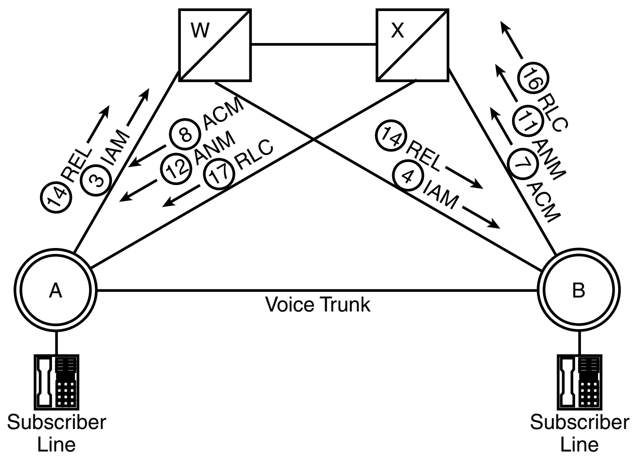
Circuit switching has been the basis of information delivery for over one hundred years. Variations on the original theme have defined newer digital technologies that can carry voice, data, and multimedia (e.g., video) services in a virtually dedicated path that emulates the original circuit switched environment.

Integrated Services Digital Network (ISDN) has led the broadband digital connection from the Central Office to residential services. It has since been eclipsed in the residential market by other technologies, but continues to serve as a viable means of reliable digital connectivity for commercial services. ISDN was designed as the delivery mechanism into asynchronous transfer mode

(ATM) networks. ATM is a broadband technology and service that can go from desktop to desktop across the WAN. It can be found as the central switching mechanism in most backbone networks.

System Signaling Seven (SS7) is an overlay network responsible for making the connections from endpoint to endpoint within the PSTN. SS7 also provides database information about the calling party and has the functionality to pass other features throughout the network. It is an out-of-band signaling system that controls the traffic for all telephony services in North America (Exhibit 14).

Exhibit 14 Case Study: Call Setup



To add value to the architectural structure of the SS7 environment, it is important to understand exactly how a call is originated and completed over a SS7-enhanced network. Suppose you are making a call to speak to your mother on a holiday. In this example, you are located on switch A, and you place your call to your mom, who is located on switch B.

You dial your mother's number on your DTMF phone.

Switch A analyzes the dialed digits and determines that the call needs to be sent to switch B.

Switch A selects an idle trunk between itself and switch B and formulates an initial address message (IAM), the basic message necessary to initiate a call. The IAM is addressed to switch B. It identifies four main topics: the initiating switch (switch A), the destination switch (switch B), the trunk selected, and the calling and called numbers.

Switch A picks one of its A links (e.g. AW) and transmits the message over the AW link for routing to switch B.

STP W receives the message, then inspects the routing label and determines that it needs to be routed to switch B. STP W transmits the message on link BW.

Switch B receives the message, analyzes it, and determines that it serves the called number and that the called number is idle (not being used).

Exhibit 14 Case Study: Call Setup (Continued)

Switch B formulates an address complete message (ACM), which indicates that the IAM has reached the correct destination. The ACM identifies the sending switch (B), the receiving switch (A), and the selected trunk.

Switch B picks one of its links (e.g. BX) and transmits the ACM over the link for routing to switch A. At the same time, it completes the call path in the backward direction (toward switch A), sends a ringing tone over that trunk toward switch A, and rings the line of the called subscriber.

STP X receives the message, inspects the routing label, and makes the determination that it is to be routed to switch A on link AX.

On receiving the ACM, switch A connects the calling subscriber line (you) to the selected trunk in the backward direction (so you can hear the ringing sent by switch B).

When your mom picks up the phone, switch B formulates an answer message (ANM), identifying the intended recipient switch (A), the sending switch (B), and the selected trunk.

Switch B selects the same A link it used to transmit the ACM (link BX) and sends an ANM. By this time, the trunk must also be connected to the called line in both directions (to allow conversation).

STP X recognizes that the ANM is addressed to switch A and forwards it over link AX.

Switch A ensures that the calling subscriber is connected to the outgoing trunk (in both directions) so your conversation with mom can take place.

If you hang up first (following the conversation), switch A generates a release message (REL) addressed to switch B, identifying the trunk associated with the call. It sends the message on link AW.

STP W receives the REL, determines that it is addressed to switch B, and forwards it over link WB.

Switch B receives the REL, disconnects the trunk from the subscriber line, returns your trunk to idle status, generates a release complete message (RLC) addressed back to switch A, and transmits it on link BX. The RLC identifies the trunk used to carry the call.

STP X receives the RLC, determines that it is addressed to switch A, and forwards it over link AX.

On receiving the RLC, switch A idles the identified trunk. Both trunks are now open for another conversation to be connected.

Questions For Review

Multiple Choice

1. In a dedicated network, which of the following is not true?
   a. The connected points maintain their connection even though the call has ended.
   b. The connection must be established each time a call is placed.
   c. The number of lines needed to maintain this environment is too great.
   d. The time to set up a connection is very short.
2. A circuit switched environment has all of the following benefits, except:
   a. Greater accessibility to various points on the network
   b. Allows for multiple connections to a single point
   c. Circuit is no longer used upon call completion
   d. Users do not use a circuit they do not need
3. Which of the following is not associated with SS7?
   a. Service routing points (SRP)
   b. Service control points (SCP)
   c. Service switching points (SSP)
   d. Service transfer points (STP)
4. SCPs make which of the following possible?
   a. Call holding
   b. Call forwarding
   c. Endpoint dialing
   d. Call identification
5. ISDN has which of the following benefits?
   a. ISDN is faster than T-1 line
   b. Always contains more data channels for routing efficiency
   c. Serves as a good redundancy line
   d. All of the above
6. PRI stands for:
   a. Primary return interface
   b. Primary rate insert
   c. Primary ratio of an ISDN line
   d. Primary rate interface
7. The NT equipment is responsible for:
   a. Synchronization
   b. Conversion from two-wire to four-wire service
   c. Electronic connectivity between the user and the CO
   d. All of the above
8. ISDN circuit is made compatible with the use of:
   a. TA
   b. CO
   c. NT-2
   d. TE

9. ATM is efficient because:
   a. There is no strict cell structure.
   b. It uses octets rather than individual bytes.
   c. It has a specific cell size and composition.
   d. The conversion of data into an ATM cell happens within the operating system.
10. The _____ defines how easily the ATM cell can be discarded.
    a. CLP
    b. HEC
    c. CPT
    d. VPI

Matching Questions

Match the acronym or value on the left with the statement that best describes it on the right.

1. ISDN	a. Acts as a call router
2. 64,000 kbps	b. Checks for errors in the ATM cell
3. STP	c. The total throughput of a BRI circuit
4. 911	d. Amount of data sent in an ATM cell
5. 1.544 Mbps	e. Can convert data into an ATM cell
6. 144 kbps	f. Calls made possible with SCPs
7. TA	g. Data services over the PSTN
8. 384 bits	h. Responsible for ISDN conversion
9. NIC	i. The total throughput of a PRI circuit
10. HEC	j. The capacity of a PRI D channel

Short Essay Questions

1. Explain the differences between PVC and SVC.
2. Explain the process of setting up and tearing down a connection between two endpoints.
3. Give a definition and example of out-of-band signaling.
4. Identify and describe the points that a call may hit in transmission.
5. What are the two most common forms of ISDN, and what might each form be used for?
6. List the actual versus the data throughputs of the two forms of ISDN, and list the number of B and D channels in each.
7. Explain the differences between NT, TE, and TA.
8. What might be a reason for choosing ATM?
9. Where might the ATM conversions take place?
10. Briefly describe the function of each portion of the ATM cell.

This page intentionally left blank

Chapter 7

Wireless Technologies: AMPS, GSM, TDMA, CDMA, Satellites, and Microwave Systems

Wireless technologies are rapidly becoming the main delivery tool of information throughout the world. The penetration of cellular services in Europe is at 75% of the population and is moving toward total market penetration. In many European countries, a student without a cell phone attached to his ear or not sending text messages to a friend across the classroom is atypical. Though voice service is the major source of revenue for the cellular service providers, data applications are quickly becoming the driving force for technological change in the industry.

Three generations of wireless technologies have evolved over the past 20 years. Because the industry is in constant flux as it is either moving to or coming from a network upgrade or software change, understanding the basic fundamentals of wireless technology and services will allow the reader to adapt with the industry as the next generation evolves.

Advanced Mobile Phone Service (AMPS)

AMPS was created and tested in the early 1980s. The first test area in the United States was in the Chicago metropolitan area. From its inception, this technology has been referred to as cellular service because of the configuration of the antenna propagation field.

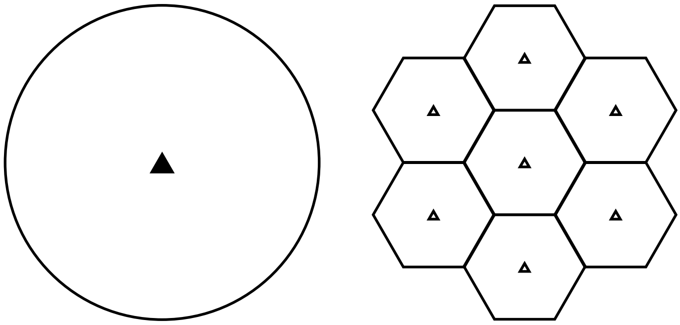


Exhibit 1 Cell site engineering configuration.

Though theoretically shaped like honeycomb cells on the engineering layout, the cell sites provide a way to reduce power, increase access, and reuse frequencies in the limited bandwidth allotments for cellular services. Exhibit 1 shows two sector layouts. The large cell site on the left has a high power output and a wide area of coverage with minimum access available. In the configuration on the right with multiple sites and different frequencies being used in each cell, the access is increased, the power of each antenna is reduced, and a similar area is being covered for service.

Because of the interrelated nature of power, antenna placement (and height), and cell radius, a radio frequency (RF) engineer must be attentive to the number of users who may need access to the network. Early configurations of the AMPS network did not anticipate the dynamic growth of the market, which left users with busy signals in large metropolitan areas more often than their gaining access to the network.

Cutting the cells into even smaller areas, reusing the frequencies in tighter configurations, and providing for more user access addressed this issue. The reuse of seven rule, which states that no cell can use a frequency from an adjacent cell, forced diversity in frequency placement in the network. The bandwidth that is available to cellular providers is limited. Exhibit 2 shows the bands allocated to the wireless providers. Because there is a scarcity of frequency for cellular service, new and creative methods have been invented to maximize the frequencies that are available.

Multiple Access Technologies

The original cellular multiple access technology is known as frequency division multiple access (FDMA). FDMA is a multiple access technique in which users are allocated specific frequency bands. The user has singular right of using the frequency band for the entire call period. Exhibit 3 is a graphical representation of FDMA.

Though functional and easy to define frequency use, FDMA was not an efficient use of the spectrum. Because a single user captures the frequency

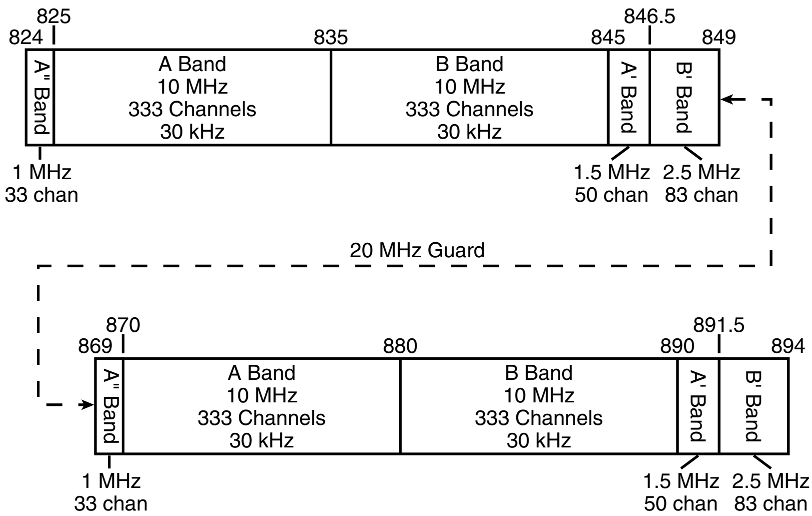


Exhibit 2 Wireless frequencies.

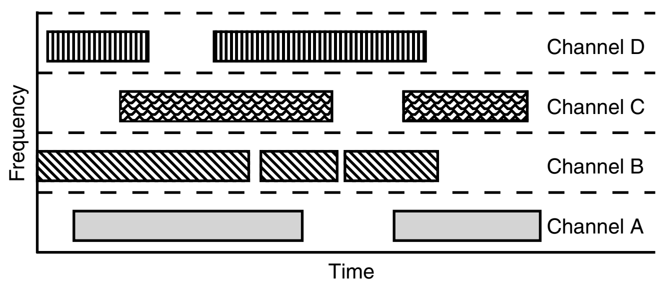


Exhibit 3 Frequency division multiple access.

channel until the call is completed, the maximum use of bandwidth was not realized. FDMA has been replaced in the network with time division multiple access (TDMA) for greater frequency use. FDMA continues to be a viable technology used in microwave and satellite transmissions, which will be covered later in this chapter.

TDMA is an assigned frequency band shared between a few users; however, each user is allowed to transmit in predetermined time slots. Hence, channelization of users in the same band is achieved through separation in time. Quiet time or unused time slots in TDMA can be maximized by inserting a user into the time slot. This method is similar to time division multiplexing used in wireline transmissions. Exhibit 4 provides an example of a TDMA configuration.

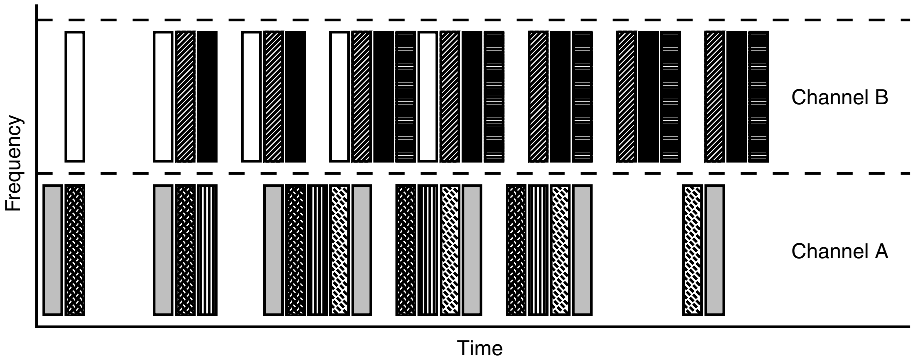


Exhibit 4 Time division multiple access.

Each individual pattern in Exhibit 4 represents a different user at a different time in the same channel. Because there are two frequency channels allocated, there is a three- to fivefold increase of user data over FDMA. Emerging compression techniques that compress voice bytes into less throughput requirements has increased the number of users with TDMA.

TDMA was developed in the United States but it used Global System for Mobile communications (GSM), found in Europe and the rest of the world, as its template for development. The methodologies are similar; however, because GSM was "not invented here" (NIH syndrome), U.S. companies were resistant to accepting the technology when networks were originally being developed. Although the United States did not accept GSM, it has the highest technology. The ability for European users to go from one country to another (roam) without disruption of cellular service is a testament to its market dominance. Because there is a singular platform for cellular services in Europe, more peripheral applications have been developed for GSM. The United States has a number of competing technologies, which makes it difficult for third-party vendors to create applications to work across all networks. This particular issue has caused development of new wireless applications to lag behind Europe by a minimum of 24 months!

The most advanced and sophisticated method of multiple access currently on the market was developed by Qualcomm and is called code division multiple access (CDMA). CDMA was designed to be used by the military for secure battlefield communications. The method is highly resistant to any type of frequency jamming and electronic eavesdropping. The civilian application of the technology has boosted the capacity of the allocated bandwidth to an estimated five to seven times greater than that of TDMA-based technology.

CDMA has been analogized in the following scenario: within a room filled with people, only two people speak the same language. Each pair of conversationalists needs to be able to talk to each other above the chatter caused by conversations in different tongues. If everyone else in the room maintains the same volume level, conversation between the two parties is possible, and all other conversation sounds like noise to them. In CDMA, the base station of the cellular network defines a specific code in which to encrypt the signal

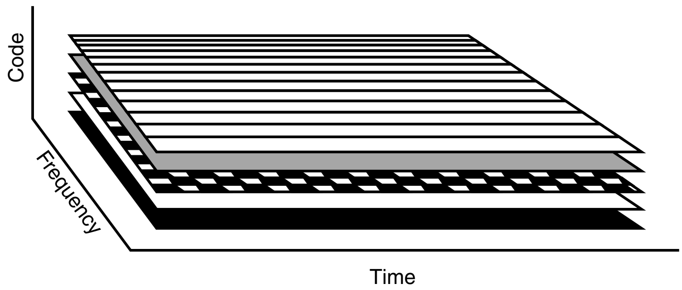


Exhibit 5 Code division multiple access.

to mobile phone. The signal is then sent out within a 1.25-MHz bandwidth along with coded information from other conversations. The other conversations, although within the same frequency band as our define call, are detected as noise by the receiving party and rejected. A good definition for CDMA is that it is a technique in which users engage the same time and frequency segment, and are channelized by unique assigned codes. The signals are divided at the receiver by using a correlator that accepts only signal energy from the desired channel. Undesired signals contribute only to noise.

CDMA accomplishes this delivery by using Walsh codes to provide a few million unique codes to define the signal before transmission. This level of sophistication should signal to you that a high level of signal timing, manageability, and resilience would be mandatory. CDMA also replicates the converted analog signal/digital output multiple times, and spreads or interleaves the data across the entire bandwidth allocated for transmission. Along with the weaving process, the transmission randomly skips to different frequencies for brief periods of time to send the information. This bobbing and weaving process provides redundancy and security that helps deliver the information, regardless of transmission interruptions. The normal encrypted nature of CDMA technology has made it resistant to hackers who may try to steal transmissions or information relating to the identification of the handset. Exhibit 5 provides a visual representation of the different conversations that can occur simultaneously on the same frequency with CDMA. Each layer of the exhibit can be visualized as a different conversation.

CDMA has the ability to deliver ten to twenty times the capacity of FDMA for the same bandwidth. CDMA also has a capacity advantage over TDMA by five to seven times. This claim is challenged by the manufacturers and resellers of GSM and TDMA technology-based services; however, it is an evolving technology that can provide the wireless data needs for the third generation of wireless services.

Mobile Switching

The transfer of any wireless system from a mobile unit to a landline or another wireless device involves a complex path of wireless and wireline connections.

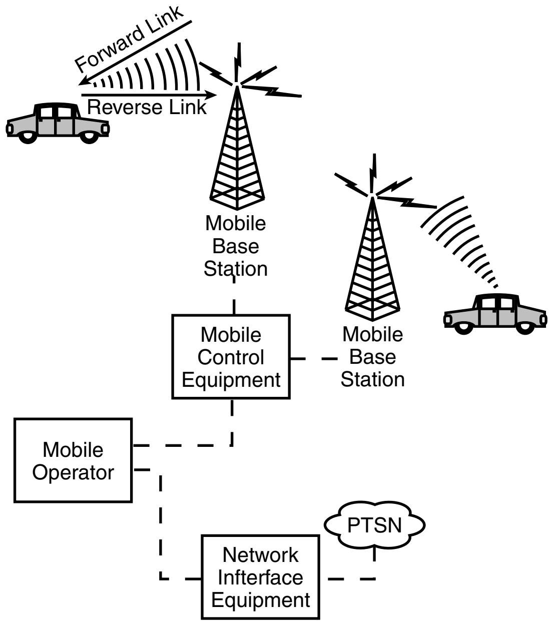


Exhibit 6 Mobile wireless switching.

Exhibit 6 shows some of the major components in the network that will be discussed.

The mobile switching center (MSC), which is known by a number of different names including mobile telephone switching office (MTSO), is the heart of the mobile network. The MSC provides the system control for the mobile base stations (MBS) and connections back to the public switched telephone network (PSTN). The MSC is in constant communication with the MBS to coordinate handoffs (or switching) between cell sites and connections to the landlines, and to provide database information about home and visiting users on the network. The MSC acts much the same as a landline Central Office, except that it interfaces with the wireless component of the network also.

The MBS is the first point of contact with the mobile user. The mobile user's cellular device while active is constantly searching for a signal that will help it orient to a particular MBS. The MBS is responsible for allocating available frequencies (in the case of GSM and TDMA networks) to users who travel through the cell's footprint. As the user traverses the cell, the signal strength from the MBS weakens at the perimeter of the coverage area. The user's cellular device has already been looking for another signal to switch to and has relayed that information back to the MSC through its current connection. The MSC coordinates the switch from one MBS to another with a stronger reception signal for the mobile user. Exhibit 7 shows how a cellular user is switched in the wireless mobile network.

Networks using CDMA technology do not look for other frequencies to pass the weakening signal to as it enters another sector. Because CDMA relies

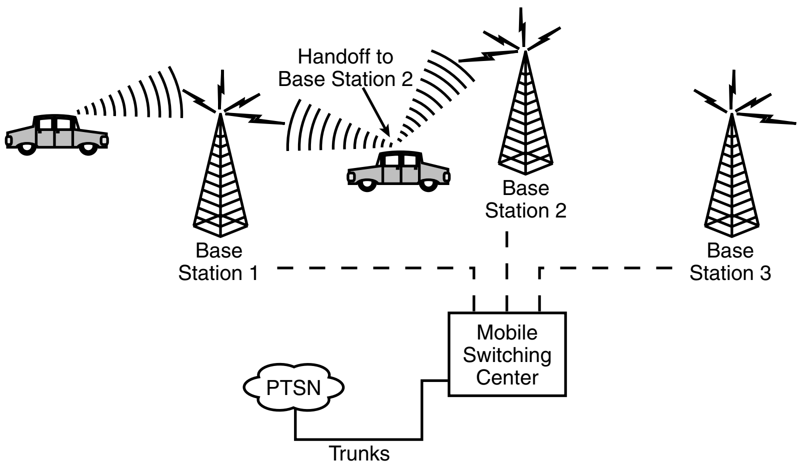


Exhibit 7 Mobile cellular handoff.

on coded signals that are broadcast on the same frequency, the handoff in this environment is directed to the stronger signal strength of the appropriate MBS. This type off handoff is termed a soft handoff in contrast to that which is performed by switching frequencies in the GSM or TDMA networks' hard handoff. There are other control channels that are involved in keeping a call active (e.g., paging channel, pilot channel) but their purpose and definition are beyond the scope of this text.

Antennas

The antenna is an integral part of the cellular environment. An antenna is a circuit element that provides a changeover from a signal on a transmission line to a radio wave and for the gathering of electromagnetic energy (i.e., incoming signals). An antenna is a passive device in the network, which means that the antenna is a receiver and transmitter of electromagnetic energy but is not responsible for amplifying the signal. Other components on the network are charged with the responsibility of making sure the signal is strong enough to be broadcast according to engineering and Federal Communications Commission (FCC) guidelines. In transmit systems, the RF signal is generated, amplified, modulated, and applied to the antenna. In receive systems, the antenna collects electromagnetic waves that are "cutting" through the antenna, and brings on alternating currents that are used by the receiver. Antenna characteristics are essentially the same regardless of whether an antenna is sending or receiving electromagnetic energy.

Microwave and satellite transmissions depend on the same antenna theory to send their signals. Knowing some unique properties of antennas will help your knowledge of multiple wireless technologies other than mobile cellular services.

Exhibit 8 Wavelength Formula

λ = c/f = 186,000 miles/second

frequency of the signal

where
c = speed of light
λ = wavelength of the signal
λ use 3×10^8 when dealing in meters for the speed of light

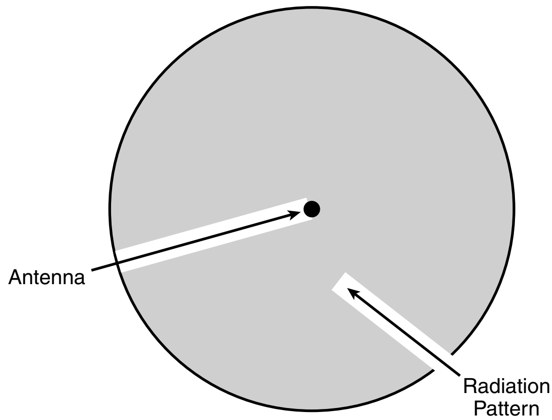


Exhibit 9 Omnidirectional antenna-radiated power pattern.

- *Reciprocity:* An antenna characteristic that essentially states that the antenna is the same regardless of whether it is sending or receiving electromagnetic energy.
- *Polarization:* The direction of the electric field, the same as the physical attitude of the antenna (e.g., a vertical antenna transmits a vertically polarized wave). The receive and transmit antennas must have the same polarization.
- *Radiation field:* The RF field that is created around the antenna and has specific properties that affect the signal transmission.
- *Antenna gain:* The measure in decibels of how much more power an antenna will radiate in a certain direction with respect to that which would be radiated by a reference antenna.

Antennas come in various sizes and shapes and have specific functions based on the RF signal reception characteristics. Antennas are designed primarily on wavelength of the signal to be transmitted and received. Half-wave ($2/\lambda$) and quarter-wave ($4/\lambda$) antennas use a simple formula that defines their size in meters or in feet (Exhibit 8).

The radiated pattern of the antenna depends on a number of factors. Antennas can be designed to meet specific broadcast requirements and focus the radiated beam of RF energy in a narrow pattern rather than being sent in an omnidirectional pattern (Exhibit 9). Directional antennas are used to direct

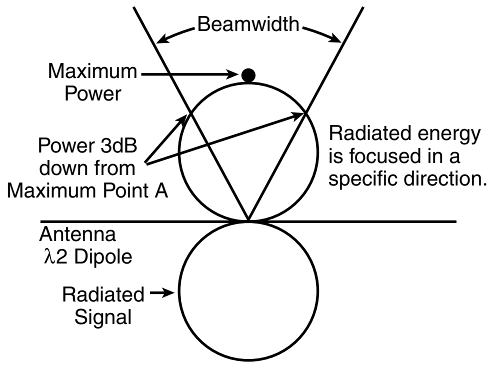


Exhibit 10 Beamwidth.

the RF energy toward a specific geographic region. The power of the signal drops off at a fairly rapid rate away from the centerline of the signal. The power of the transmission drops in half (–3 dB) at points on either side of the main focus of the signal. The width between these two power drop points is called the beamwidth (see Exhibit 10).

Smart Antennas

Smart antennas are base station antennas with a pattern that is not fixed but adapts to the current radio conditions. Smart antennas offer the possibility of a large increase in capacity. In fact, increases of three times for TDMA systems and five times for CDMA systems have been reported. Major drawbacks and cost factors associated with smart antennas include increased transceiver complexity and more-complex radio resource management.

The idea of smart antennas is to use base station antenna patterns that are not fixed but adapt to the current radio conditions. This can be visualized as the antenna directing a beam toward the communication link only. Smart antennas add a new way of separating users, namely by space, through space division multiple access (SDMA). By maximizing the antenna gain in the desired direction and simultaneously placing a minimal radiation pattern in the direction of the interferers, the quality of the communication link can be significantly improved. SDMA implies that more than one user can be allocated to the same physical communications channel simultaneously in the same cell, only separated by angles. In a TDMA system, two users will be allocated to the same time slot and carrier frequency at the same time and in the same cell. In systems providing full SDMA, there will be many more intracell handovers than in conventional TDMA or CDMA systems, and more monitoring by the network will be necessary.

There are a number of different types of smart or intelligent antennas that are being readied to enter the market. The first is the switched lobe (SL), also called switched beam. It is the simplest smart antenna technique, and contains only a basic switching operation between separate directive antennas or predefined beams of an array. The setting that gives the best performance, usually in terms of received power, is chosen for signal delivery.

The second type of smart antenna is the dynamically phased array (PA). By including a direction of arrival (DoA) algorithm for the signal received from the user, continuous tracking can be accomplished and it can be regarded as an extension of the switched lobe concept.

The last type of smart antenna developed for commercial use is the adaptive array (AA). In this case, a DoA algorithm for determining the direction toward interference sources (e.g., other users) is added. The radiation pattern can then be adjusted to void out the interferers. In addition, by using special algorithms and space diversity techniques, the radiation pattern can be modified to receive multipath signals that can be combined. These techniques will take full advantage of the signal to interference ratio (SIR) for better transmission quality.

Microwave Signals

The knowledge of RF signal propagation which was discussed in the chapter on modulation coupled with the information on antennas within this chapter are the fundamental building blocks necessary to understand how microwave signals are transmitted and received. Microwave signals continue to be used today in land-based systems, and are the medium of choice when communicating with satellites. The range for microwave signals is from 1 to 40 GHz. To understand how much information can be transmitted within this huge bandwidth, consider that all the AM and FM radio, broadcast television, aviation communication, public safety (e.g., police radio), and most mobile cellular channels reside *under* the 1-GHz frequency! A bandwidth of 1 GHz represents a huge space in which information can be transferred, while microwave is *40 times* that amount.

Microwave transmissions were developed during World War II, and were converted to civilian use as long-haul carriers for frequency division multiplexed trunks across the United States. Fiber-optic cable infrastructure has replaced most of this service because fiber has a higher quality of service (QoS), thanks to a lower bit error rate (BER), which means the number of pieces of information corrupted or lost during transmission is better with fiber-optic versus microwave transmission. Microwave continues to be a viable means of signal transmission for right-of-way issues, geographic obstruction problems, and wireless local loop considerations. Impairments to microwave signal transmission include:

- Equipment, antenna, and waveguide failures
- Fading and distortion from multipath reflections
- Absorption from rain, fog, and other atmospheric conditions
- Interference from other frequencies

These issues will be discussed in more detail later in this chapter. The impairment questions need to be asked during any engineering configuration for a microwave transmission facility. These issues include:

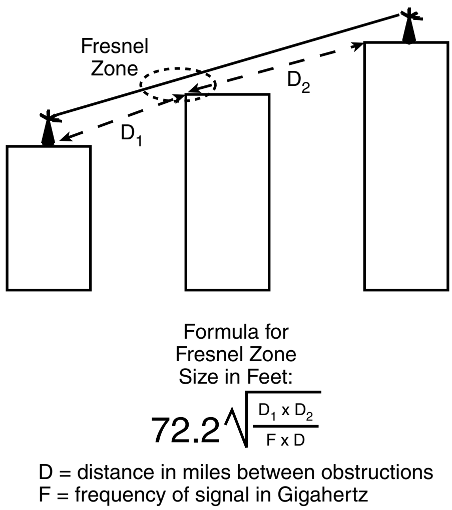


Exhibit 11 Fresnel zone considerations.

- Free space and atmospheric attenuation are defined by the loss of signal traveling through the atmosphere. Changes in air density and absorption by atmospheric particles are principal reasons for affecting the microwave signal in a free air space.
- Reflections cause multipath conditions and can occur as the microwave signal traverses a body of water or fog bank.
- Diffraction is the result of variations in the terrain the signal crosses.
- Rain attenuation or raindrop absorption is the scattering of the microwave signal, which can cause signal loss in transmissions.
- Skin effect is the concept that high frequency energy travels only on the outside skin of a conductor and does not penetrate into it any great distance. It determines the properties of microwave signals.
- Line-of-sight (LOS) is defined by the Fresnel zone. Fresnel zone clearance is the minimum clearance over obstacles that the signal needs to be sent. Reflection or path bending occurs if the clearance is not sufficient (Exhibit 11).
- Fading is caused by multipath signals and heavy rains, which can cause signal disruption. Exhibit 12 is a depiction of how the microwave normal and faded signals are viewed. High frequencies are repeated and received at or below one mile. Lower frequencies can travel up to 100 miles but 25 to 30 miles is the typical placement for signal repeaters.
- Range is the distance a signal travels. Its increase in frequency and its extended range are inversely proportional repeaters. Back-to-back antennas and reflectors are used to extend the reach of microwave signals.
- Interference is as the name implies. There are two types of interference to be considered. The first, adjacent channel interference, is caused by signal transmissions of frequencies too close in proximity. With the

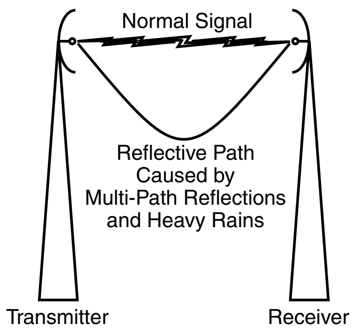


Exhibit 12 Fading.

advent of analog-to-digital signal conversion, digital is not greatly affected by adjacent channel interference. The second type of interference is overreach. Overreach is caused by a signal feeding past a repeater (or receive antenna) to the receiving antenna at the next station in the route. This condition is eliminated by zigzag path alignment or alternate frequency use between adjacent stations.

Each of these specific considerations must be assessed prior to system installation or addressed by your RF vendor to satisfy QoS considerations prior to adopting a microwave transmission solution.

The components of a microwave system are comprised of three basic elements: the digital modem, the RF unit, and the antenna. The RF unit is based off properties similar to other radio signal modulation schemes. You can start to visualize the building blocks of the previous technologies discussed, helping to prepare you to understand this technology.

The digital modem modulates the information signal (intermediate frequency or IF) into the RF unit. From there, the RF unit pushes the signal through to the antenna. A direct connection to the antenna is preferred. The RF unit connects to the antenna with either coaxial cable or a waveguide, a hollow channel made of a low-loss material used to guide the RF signal to the antenna for broadcasting. The primary methods used today for modulating the signal for transmission are AM and FM signaling.

Engineering Issues for Microwave Signaling

Because radio frequencies begin to behave in a manner similar to a beam of light as the frequency increases (moves up the spectrum), there are some specific issues that must be addressed when planning microwave transmission links. The first consideration is the allowable BER for the transmission. The BER is a performance measure of microwave signaling throughput. A count of more than 10^{-6} (one error per million transmitted bits of information) is usually considered an acceptable bottom threshold for data transmissions. If

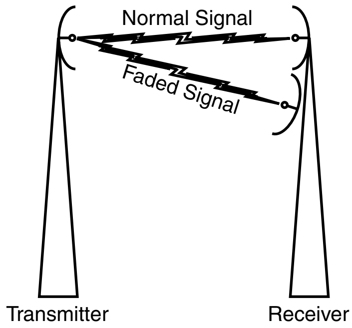


Exhibit 13 Space diversity.

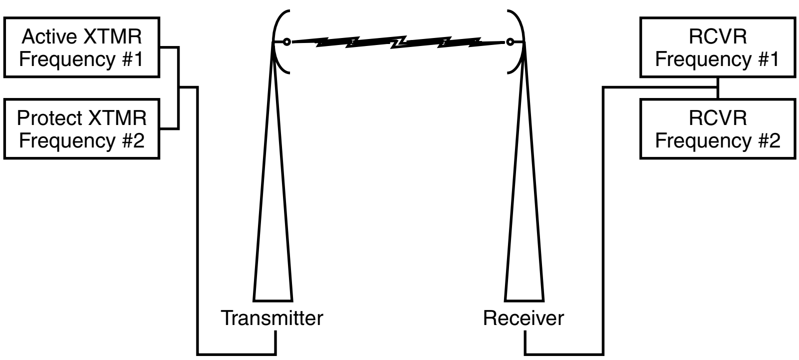


Exhibit 14 Frequency diversity.

the data failover is at 10^{-3} (one error per one thousand transmitted bits of information), voice traffic can withstand this higher error rate.

There are four primary diversity issues that must be considered with microwave placement: space diversity, frequency diversity, hot standby, and the use of a PRI connection for a failover. Space diversity protects against multipath fading by automatically switching over to another antenna placed below the primary antenna on the receive site. This is done at the BER failure point or signal strength attenuation point to the secondary antenna that is receiving the transmitted signal at a stronger power rating (Exhibit 13).

Frequency diversity uses separate frequencies (dual transmit and receive systems); it monitors the primary signal transmission for failover at a specific BER and switches to the standby or redundant frequency. Interference usually affects only one range of frequencies, so switching from the primary to secondary signal usually resolves the interference problem. This type of diversity is not allowed in noncarrier applications because of spectrum scarceness (Exhibit 14).

Hot standby is designed for equipment failure only. This method provides a complete redundant set of transmission and reception gear for the site. This is an expensive but necessary proposition if there is a critical nature associated

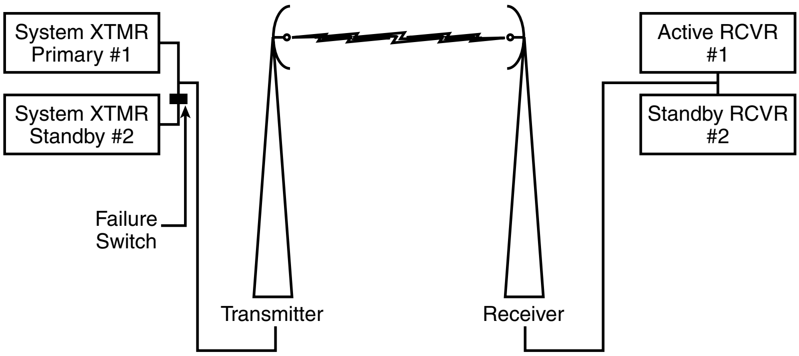


Exhibit 15 Hot standby.

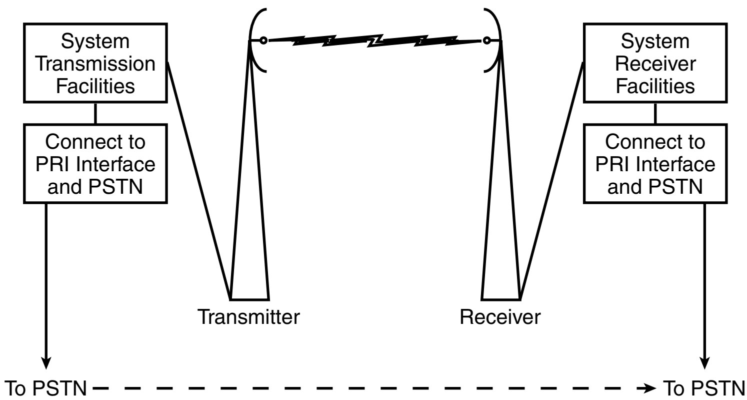


Exhibit 16 PRI failover.

Exhibit 17 Availability Formula

Percent availability = 1 – (outage hours/8760 hours per year)

Private microwaves have 99.99% availability

with the link. Exhibit 15 gives a block diagram of what a hot standby microwave transmission link contains.

Using an ISDN PRI circuit as a failover for exceeding the BER for a particular signal transmission is a cost-effective method of providing a redundant path for the transmission. Though the PRI circuit cannot handle the same throughput as the microwave signal, it would provide for a minimal redundant connection, while the primary connection regains an acceptable BER, or in the case of equipment failure, until the defective parts can be replaced (Exhibit 16).

Exhibit 18 Case Study: Wireless Local Loop

A widely developed application of the wireless technologies is the wireless local loop (WLL). WLL is a system that substitutes the copper cable that connects the subscriber's premises to the public switched telephone network by radio signals. The WLL market already counts million of users. It is developed in Third World countries as a substitute to the plain old telephone system (POTS) because it is usually cheaper to install mobile base stations rather than connect every premise with copper cable. It is also developed to promote broadband in rural areas.

WLL can be implemented on different analog and digital cellular networks. Analog cellular, such as AMPS, is limited in terms of capacity and functionality; however, it is expected to be a major platform in the short-term because of its widespread implementation. As digital cellular replaces analog cellular for mobile services, digital cellular (GSM, TDMA, and CDMA) is the emerging standard for WLL, especially CDMA, which offers the highest capacity and a high level of privacy thanks to spread-spectrum modulation. Personal communications networks also have their role to play by allowing the user to be connected to the telephone network regardless of its location.

The technology exists to implement WLL intensively, and the deployment of a new network is a matter of months; however, deploying these systems are costly and profits are not guaranteed, especially in competitive environments.

A final consideration that is constructive in planning a wireless broadband connection is to estimate the mean time between failures (MTBF) of the equipment being used. All electronic equipment will fail eventually. The manufacturer provides an estimated time frame in hours for the durability of the equipment. A simple formula is used that can help calculate quickly from the engineering specifications sheet how reliable the equipment will be for the particular application. Exhibit 17 gives the basic mathematical computation for the availability formula.

Summary

Wireless technologies are capable of providing new and ever-changing applications for the business environment. The migration from the original AMPS technology for mobile cellular service to FDMA, TDMA, GSM, and CDMA has created greater opportunities with the available bandwidth allocated to service providers.

Antennas are a critical part of any wireless network. Their purpose in the system is to transmit and receive the signal in various formats. Next-generation smart antennas are being developed to provide additional use of the limited frequencies between and within particular cells. SDMA is emerging as a unique form of multiple access for antenna frequency reuse.

Microwave technologies have been around since World War II. They were developed into the primary long-haul mechanism for telephone services. Although they have been replaced by fiber-optic trunking for this service today, they have developed niche services for wireless local loop, telephone company bypass, and short-haul connectivity in metropolitan environments (Exhibit 18).

Questions for Review

Multiple Choice

1. What is the advantage of cell site engineering?
   a. Reduce power
   b. Increase access
   c. Reuse bandwidth
   d. All of the above
2. What is an advantage of GSM over TDMA?
   a. It was invented in Europe
   b. It is technically better than TDMA
   c. It has a higher technology penetration in the world
   d. All of the above
3. What is the wavelength formula?
   a. $\lambda = c * f$
   b. $\lambda = f/c$
   c. $\lambda = c/f$
   d. None of the above
4. What is the availability formula? Percents availability equals:
   a. 1 – (outage hours * 8760)
   b. 1 – (outage hours/8760)
   c. 1 + (outage hours/8760)
   d. None of the above
5. In which type of handoff is the user assigned a new frequency?
   a. Soft handoff
   b. Medium handoff
   c. Hard handoff
   d. All of the above
6. The power of the transmission drops in half (–3 dB) at points on either side of the main focus of the signal. What is the width between these two power drop points called?
   a. Beamwidth
   b. Radiation pattern
   c. Wavelength
   d. None of the above
7. Impairments to microwave signal transmission include:
   a. Fading and distortion from multipath reflections
   b. Absorption from rain, fog, and other atmospheric conditions
   c. Interference from other frequencies
   d. All of the above
8. What are the two types of interference for a microwave signal?
   a. Adjacent channel interference
   b. Reflection
   c. Overreach
   d. Diffraction

9. Which of these components is part of a microwave system?
   a. Digital modem
   b. Analog amplifier
   c. Laser unit
   d. Waveguide or coaxial cable
10. What is the bit error rate (BER)?
   a. The threshold under which a mobile user is disconnected from the network
   b. A performance measure of microwave signaling throughput
   c. Indicates a hacker corrupts the transmission channel
   d. All of the above

Matching Questions

Match the following terms with the best answer.
Match the wireless frequencies:

1. A band uplink	a. 880 to 890 Mhz
2. A band downlink	b. 825 to 835 Mhz
3. B band uplink	c. 835 to 845 Mhz
4. B band downlink	d. 870 to 880 Mhz

Match the definition:

1. FDMA	a. Users engage the same time and frequency segment, and are channelized by unique assigned codes.
2. TDMA	b. Users can be allocated to the same physical communications channel simultaneously in the same cell, only separated by angle.
3. CDMA	c. Assigned frequency band shared among a few users.
4. SDMA	d. Users are allocated specific frequency bands.

Match the increase of users:

1. TDMA	a. 5 to 7 times over TDMA
2. CDMA	b. Depends on the type of antenna
3. CDMA	c. 3 to 5 times over FDMA
4. SDMA	d. 10 to 20 times over FDMA

Match the definition:

1. Reciprocity	a. The antenna is the same regardless of whether it is sending or receiving electromagnetic energy.
2. Polarization	b. The measure in decibels of how much more power an antenna will radiate in a certain direction with respect to that which would be radiated by a reference antenna.
3. Radiation field	c. The direction of the electric field, the same as the physical attitude of the antenna.
4. Antenna gain	d. The RF field that is created around the antenna and has specific properties that affect the signal transmission.

Match the antenna length by using the wavelength formula:

1. f = 1 MHz, antenna length = $\lambda/4$	a. $15 * 10^{-3}$ m
2. f = 100 MHz, antenna length = $\lambda/2$	b. $75 * 10^{-3}$ m
3. f = 1 GHz, antenna length = $\lambda/4$	c. $1.5 * 10^{-3}$ km
4. f = 10 GHz, antenna length = $\lambda/2$	d. $46.5 * 10^{-3}$ miles

Match the definition:

1. Switched lobe antenna	a. Continuous tracking can be accomplished
2. Phased array antenna	b. The radiation pattern can then be adjusted to void out interference
3. Omnidirectional antenna	c. Contains only a basic switching operation between separate directive antennas or predefined beams of an array
4. Adaptive array antenna	d. Not a smart antenna

Match the definition:

1. Atmospheric attenuation	a. The scattering of the microwave signal
2. Reflections	b. Defined by the loss the signal undergoes traveling through the atmosphere
3. Diffraction	c. Can occur as the microwave signal traverses a body of water or fog bank
4. Raindrop absorption	d. The result of variations in the terrain the signal crosses

Match the definition:

1. Skin affect	a. Caused by multipath signals and heavy rains
2. Line-of-sight	b. Defined by the Fresnel zone
3. Fading	c. The distance a signal travels
4. Range	d. The concept that high frequency energy travels only on the outside skin of a conductor and does not penetrate into it any great distance

Match the definition:

1. Space diversity	a. Protects against multipath fading by automatically switching over to another antenna placed below the primary antenna on the receive site
2. Frequency diversity	b. Transmission is a cost-effective method of providing a redundant path for the transmission
3. Hot standby	c. Monitors the primary signal transmission for failover at a specific BER and switches to the standby or redundant frequency
4. PRI connection	d. Provides a complete redundant set of transmissions and reception gear for the site

Match the definition:

1. BER $> 10^{-3}$	a. Acceptable for both voice and data
2. BER $< 10^{-3}$	b. Not acceptable for both voice and data
3. BER $< 10^{-6}$	c. Acceptable for voice only

Short Essay Questions

1. Define AMPS and explain the reuse of seven rule.
2. Define FDMA.
3. Define TDMA.
4. Define CDMA.
5. Define MSC and explain the two different types of handoffs.
6. Define antenna and name its four unique properties.
7. Define smart antenna and name three types of smart antennas.
8. Define SDMA.
9. Define microwave signals and give their range of frequencies.
10. Define BER, the four types of diversities, and MTBF.

This page intentionally left blank

Chapter 8

Packet Switching and Local Area Network Technology

In the previous chapters, we looked at the use of circuit switched networks. In circuit switched networks, a dedicated path is carved out of a larger network to form a communications path. This path or circuit is set up by signaling, created when you want to communicate and terminated when the communication is ended. During this time, the path is exclusively yours. A telephone call is a good example of a larger network. The public switched telephone network (PSTN) allocates a path for your call. When you hang up the phone, the circuit is terminated and put back in the pool for the next caller to use.

The circuit switched network is very effective but also very inefficient. During your phone call, the circuit is dedicated for your use even when no one is speaking. This waste of resources is similar to allocating a lane on the highway for your use with no one else allowed to use the lane until you have reached your destination.

An alternative to circuit switching is packet switching. In packet switching technology, the path or circuit is shared by many users at once (similar to today's highway system). Packet switching allows an extremely efficient use of resources and, if properly done, is an effective mechanism for communication. Each packet, similar to a car on a highway, carries information that is destined for different locations.

A local area network (LAN) is an excellent example of packet switching technology. A LAN is a privately owned network that provides communication to a local environment (typically less than two kilometers). The network can support interfloor, interbuilding, and even intercampus communication, and can be used to connect local devices to a larger network. Another characteristic of the LAN is the packet switching or shared environment. At any one point in time, different packets are present, each made up of different users and destined for different locations.

The Business and Human Factors

Whether in a social or professional setting, people have a need to communicate with each other. In a business situation, this is not only a human need but also a business imperative. For work to be accomplished, people need to work together to solve problems and create resources for the company. LANs do two essential things: (1) allow for information sharing, and (2) provide resource sharing. These benefit the organization by allowing for improved decision-making and therefore increased competitiveness.

During the 1980s when personal computers (in significant numbers) were implemented in the working world, there were islands of information that were connected only to a human operator. Increased data and information were generated but without an efficient and effective means to share the information, it was usually lost within the bounds of a department. In the 1990s, the LAN connected the islands together, thus creating bridges (network) between users. The most common applications used with information sharing are electronic mail, calendaring, and file transfer.

Another popular use of LANs is resource sharing. Essentially this is many people sharing one device. For example, each user with a personal computer usually has a need to print files every so often. A printer can be secured for each person, or a common printer (resource) can be shared among departmental personnel. The same concept of sharing a printer can be applied to many hardware devices (scanner, fax machine) as well as software. Rather than install a copy of a word processing package on each of the department PCs, a single copy can be placed on a centralized resource, a server, to be used by many people. Resource sharing, although a bit more complicated in implementation and delivery, leads to centralized management and support, decreases cost, and increases effectiveness of resources.

The use of LANs within an office environment has become a common and crucial element for information sharing and resource sharing, thus producing an increased effectiveness at decreased cost. LANs are also becoming prevalent in the home and in small remote offices. Often clumped into one category, SOHO (small office/home office) has the same purpose as office LANs but they are smaller in size and lower in cost. For example, each of the PCs in your home can share a common printer (located, of course, in the kitchen), and your family can keep up a common calendar (sharing information that all can view and modify as needed). In a small remote office where personnel come in only when they need a connection to the corporate office, a LAN allows access to corporate information (such as pricing, vacation accrual, etc.) and to shared printer and fax services.

The Costs of a LAN

The benefits of the LAN are obvious to those implementing it, but the costs are less obvious. When considering the cost of a LAN (or any type of network), the total cost of ownership (TCO) should be considered and factored in. Two broad categories of TCO are:

- Initial one-time costs
- Ongoing costs

Initial Costs

The majority of the initial costs of a LAN include the hardware and software required to create the network. These include:

- End-user devices (personal computers, etc.)
- Wiring
  - Cable costs
  - Installation costs
  - Termination costs
- Network equipment
  - Hubs, switches, routers
- Network operating system (NOS)
- Shared devices
  - Servers
  - Printers
  - Fax machines

Depending on the numbers of users, the complexity of the applications, the distances, and the corporate standards in place, the costs can range from thousands to hundreds of thousands of dollars. One particular item in the list that should not be taken lightly is wiring installation. This element includes running the wires from each computer to centralized equipment (usually in a closet or basement). If the building is old (contains asbestos) or has hard obstacles (concrete floors), this one-time cost item can be extremely high. On the other hand, if the building is under construction and the walls are not yet in place, the installation is relatively easy and low in cost. These elements are discussed in detail in the technical section of this chapter.

Ongoing Costs

The other category of costs, the most often forgotten category, is the ongoing cost of ownership. In no way is the subject of cost brought forward to scare you away from networks. LANs are an essential part of the way business is conducted these days, and part of the cost of doing business. You should approach them with eyes wide open and be aware of them (Exhibit 1). The items to consider are:

- Personnel to maintain the network
- Equipment maintenance, upgrades, and repair contracts
- Moves, adds, and changes
- Outside links
- Software licensing

Exhibit 1 TCO of a LAN

Item	*Number*	*Cost*	*Total*	
Initial Costs				
Personal computers	10	$1,000	$10,000	
Network equipment				
Hubs	2	$500	$1,000	
Router	1	$1,500	$1,500	
Wiring	10 rooms	$400	$4,000	
Network operating system				
Shared devices				
Printer	1	$750	$750	
Fax	1	$300	$300	
Initial cost				$16,850
Ongoing Costs				
Personnel	¼ FTE	$7,000	$7,000	
Equipment maintenance		$2,000	$2,000	
Media access control address		$1,000	$1,000	
Outside line	$500/month	$6,000	$6,000	
Software license		$1,500	$1,500	
Ongoing cost				$17,500
Total cost, first year				**$34,350**

Personnel

Just as we would never construct a building without factoring in the costs of cleaning and maintaining it, we should never consider constructing a network without also considering the costs of personnel to monitor, operate, and upgrade it. These personnel, usually highly trained and fairly costly, provide for the daily and yearly care and feeding of the network. The size of the network dictates the size of the support team (network administrators, or NAs). A small remote-office environment can survive using one person as the NA, designating one fourth of their time spent on the network (after training); a 100-person office environment would require a full-time NA being assigned to this role and function.

Equipment Maintenance, Upgrades, and Repairs

All equipment is prone to break down, and replacement should be considered. Two strategies are prevalent: (1) obtain a maintenance contract that provides for replacement if something fails, or (2) take the risk and purchase a replacement in the event a unit fails. The criticality of your network and data usually dictates the strategy you select. If you want the network to be operational 24/7 with a 99.999 percent uptime, a maintenance contract is appropriate; if you can accept downtime of a few days, the second strategy is acceptable.

A positive note for consideration of the first strategy is support and upgrades. When getting a maintenance contract, vendors usually provide not only replacement of equipment in case of failure but access to further support and upgrades for software. These two factors can have a critical effect on your network uptime.

Moves, Adds, and Changes (MACs)

No matter how stable you think you are, moves, adds, and changes (MACs) occur. When a new office is partitioned from a large office, a new network connection needs to be added. Mr. Jones moves upstairs and his connectivity needs to be moved and modified. Ms. Smith has been promoted and her access to network resources has been changed. Each of these elements has a personnel and a hardware cost. Depending on the fluidity of your organization, a sizeable budget may need to be set aside for these MACs.

Outside Links

Usually, a LAN provides access to the Internet, to another corporation, or to headquarters. This connection of the LAN to the outside almost always carries ongoing costs with it. These costs can be significant ($5000 per month), depending on the speed, distance, and protocol used.

Software Licensing

The software used on the LAN is usually licensed (leased) to you for use on your network. Software includes computer operating systems (Windows, NT), applications (Word, Excel, Lotus), network operating systems (Novell), and server operating systems. The costs for software are sometimes a one-time experience but if you want to upgrade the current version of the software, the costs are recurring. Depending on the number of users and the complexity of the software used, costs can be significant.

The Technical Factors

The Working Parts of a LAN

A LAN has four essential components (Exhibit 2):

- End-user devices
- Physical media
- Networking equipment
- Network operating system

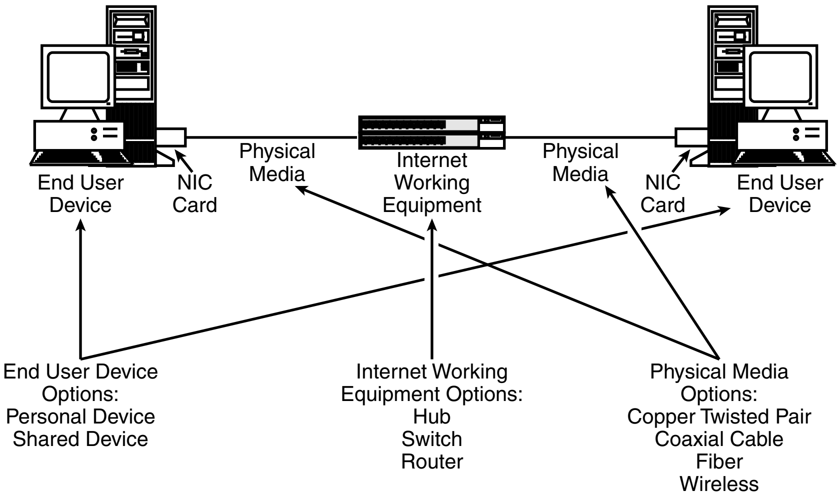


Exhibit 2 Parts of a local area network.

End-User Devices

The most visible parts of a LAN, the end-user devices (personal computers, printers, modems, and servers), are what the users see and what they interface with but are not really part of the LAN. However, without these devices the network would not be useful to the users at the end. End-user devices are the transmitters and receivers of the information and the bridge between humans and the digital world.

Most end-user devices are personal in nature, meaning they are assigned to a single person. A desktop computer provided to an employee is a perfect example of a personal end-user device. But there also are shared end-user devices, typically printers, fax machines, and scanners, that serve a department or a unit within an organization.

Physical Media

The second network element is the physical media or wiring that connect the end-user devices to the network, allowing communication to occur. Although not necessarily visible to the user, this is an essential component of the LAN. The physical media can come in many shapes and sizes (Exhibit 3), the selection of which is dependent on either what is currently existent in the building or the characteristics of the organization. The options include twisted pair cable (i.e., Category 3, shielded twisted pair or Category 5, unshielded twisted pair), coaxial wire (thicknet or thinnet) or fiber-optic cable. Twisted pair cable is the most prevalent in today's LANs and the most effective way to accomplish building wiring. The signal tends to propagate down the wire in an efficient manner and, due to the limited use of copper, is a very cost effective medium.

Exhibit 3 Types of Physical Media

Name	Type	Data Rate (Mbps)	Distance (meters)	Often Used by	Cost ($ per foot)
Category 1	UTP	1	90	Modem	0.10
Category 2	UTP	4	90	Token Ring	0.05
Category 3	UTP/STP	10	100	10BaseT Ethernet	0.13
Category 4	UTP/STP	16	100	Token Ring-16	0.18
Category 5	UTP/STP	100	200	100BaseT Ethernet	0.25
RG-58	Coaxial cable	10	185	10Base2 Ethernet	0.30
RG-8	Coaxial cable	10	500	10Base5 Ethernet	0.85
X3T95	Fiber	100	2,000	FDDI	1.00

Exhibit 4 Picture of a network interface card.

Coaxial cable is difficult to work with and higher in cost. Although still present in networking, it appears to be used less and less. Fiber-optic cable, although a bit more expensive to purchase and install, has the advantage of being almost totally immune to noise and interference from the outside (lighting, motors, etc.) and, due to its higher speed and lower security risk, is being used more and more in the LAN environment.

Networking Equipment

The third component of a LAN is the networking equipment: hubs, switches, routers, and network interface cards. Often unseen by the user, hidden in

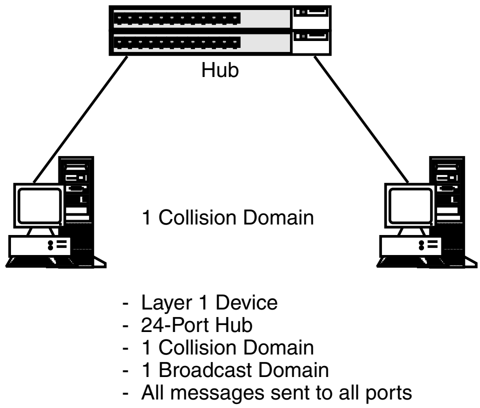


Exhibit 5 Hub operation.

closets and basements, this equipment forms the heart and brains of the network, sending information to the proper destination. Each of these devices performs the functions of getting the data from its source to its destination. Because they operate differently, a little discussion on each is appropriate.

Hubs

Hubs serve two major purposes:

1. To provide a physical access point to the network
2. To amplify and repeat the signal

With regard to physical connectivity, a hub provides a place to plug in a computer, or many computers, for network access. Similar to a three-pronged extension for a wall outlet, a hub typically provides multiple ports (2, 8, 16, and up to 96) for computer access. Hubs, like the NICs, must be compatible with the physical media being used and the speed of the network (i.e., Category 5 cable at 10 Mbps; see Exhibit 5).

The second purpose of the hub is to amplify and repeat signals. Hubs are mostly dumb devices that operate at Layer 1 of the OSI model. When a hub receives a signal on one port, it amplifies and repeats the signal out on all of the ports. Without regard to the message or its destination, the hub broadcasts to everyone, leaving the intended receiver to pick up the message.

Hubs can also go beyond these two basic purposes and do other things. Some hubs are "smart" and report when they are not feeling well or when the network is very crowded. This capability can help greatly in finding and solving network problems. Others hubs can translate between different physical media and speeds. For example, a single hub can have Category 5 UTP at 10 Mbps, coaxial thinnet, and fiber-optic cable connected to it. These hubs are a blessing when diverse physical media are used in the workplace.

Exhibit 6 Picture of a switch.

Switches

Although similar to hubs in providing physical connectivity, switches (Exhibit 6) act differently in the core function of repeating and amplifying the signal. Switches provide a common physical access point and multiple ports for the physical connection of end-user devices. Similar to hubs, they come in 4-, 8-, and 16-port varieties, and selection is determined by the physical media used.

Switches act differently with regard to receiving and transmitting the packets (Exhibit 7). Switches act at Layer 2 of the OSI model, and transmit packets based on the media access control (MAC) address. A MAC address is a physical address permanently stamped in a device, in the NIC, and cannot easily be changed, much like your mailing address (unless you move).

The MAC address is learned by the switch through ARP (Address Resolution Protocol) requests. When the switch is turned on, it sends out ARPs to all devices connected, asking “who is there?” Each device dutifully responds with its MAC address, and the switch then creates a map of who lives at each port.

On receiving a message, the switch looks to see where the packet is going, checks its map to see at which port the destination exists, and then repeats that packet out to the proper port. By sending the packet to the MAC address and not broadcasting to every port, network traffic is considerably reduced and performance is enhanced.

Switches, like hubs, can be smart and translate between different physical media. They tend to be a bit more expensive than hubs; but considering the positive effects on network performance, the cost is well worth it. Most corporations are doing away with hubs and replacing them with switches.

Routers

Although performing the same two core functions as hubs and switches (physical connectivity and message forwarding), routers are smarter and more

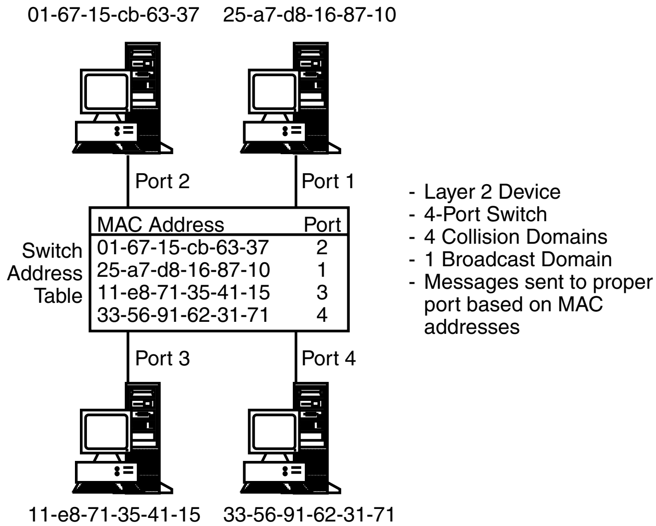


Exhibit 7 Switch operation.

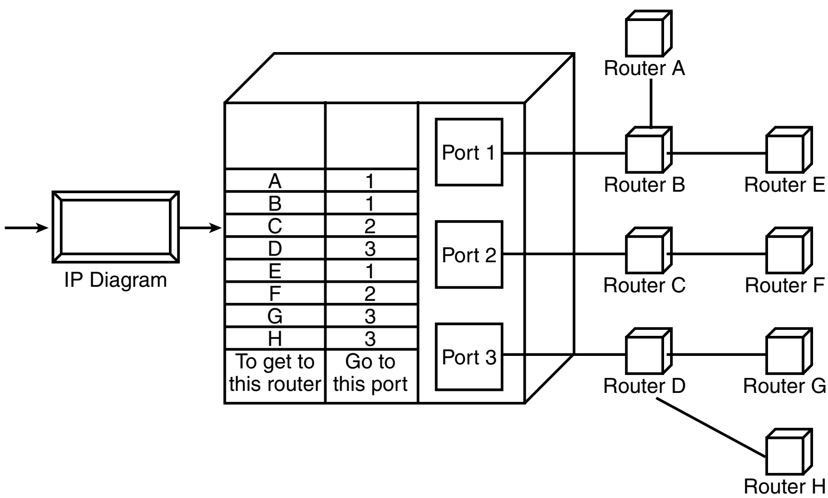


Exhibit 8 Router operation.

effective in a network. Routers (Exhibit 8) operate at Layer 3 of the OSI model (the network layer) and route packets to their proper destination address based on the network address rather than the physical address. Recalling the street address analogy, a network address is a moniker given to a computer (based on protocol) similar to a family surname. Currently, the dominant network protocols, TCP/IP and IPX (discussed in depth in a later chapter), provide the PC a logical address (similar to a surname). Just as a family with a surname lives at a physical address, a TCP/IP address exists at a network MAC address.

Routers route packets to their destination based on the network address rather than the MAC address. What is the benefit? Every time you get a piece of mail addressed to the wrong person or a previous occupant at your house (physical address), you see the benefit: logical addresses are smarter and can find the correct location very quickly based on the network address.

Routers learn addresses in ways similar to switches. Each router has a network address and knows where its neighbors are, therefore it is much more capable of getting the packet to the right place. Needless to say, the benefit for this more-effective routing of packets is speed and cost. Because a router has more to do, it takes longer to accomplish a task and can slow network performance. If used inappropriately, a router can slow a network down appreciably. Routers also tend to cost more than switches or hubs and are usually used at the edge of a LAN (where the LAN needs to connect to the outside world). The expression today is *"switch first and route if you must,"* which means use switches in a network first and routers only if you have to.

Although similar in appearance, hubs, switches, and routers forward packets in vastly different ways. To confuse things even more, there are many other offshoots of these: bridges, Brouters, and Layer 3 switches are but a few of the marketing labels put on devices that forward packets within LANs.

Network Interface Cards (NICs)

Network interface cards (NICs) are the beach-heads between the end-user device and the network (Exhibit 4). They perform the translation and encoding necessary for a PC to talk through the network.

Personal computers have different internal structures, called bus structures, which vary depending on the manufacturer and the type of PC. One must know the internal bus structure and find the correct NIC to fit it. For example, a laptop computer uses a PCMCIA bus structure while desktop machines have bus structures such as PCI and ISA, which dictate the type of NIC that must be installed in order to gain network connectivity.

Additionally, the NIC must be compatible with the network it is being connected to. Two criteria are important here: (1) physical media used, and (2) speed. If the network you are to connect to uses coaxial cable, a physical connection must be made to that cable and the NIC must be compatible with that connection. If you are using the more popular Category 5 cable, the NIC must use that connector type. Speed is also important. If you are connecting to a Category 5 cable that runs at 100 Mbps, the NIC must be capable of that connection speed.

Other important criteria should be considered in the purchase decision for the NIC, including management functions, protocols supported, reliability, and intended structure. Based on predominant use in the marketplace, the most popular NICs are PCI bus with a network connection for Category 5 cable at 10/100 Mbps (these NICs can autonegotiate their speed for either 10 or 100 Mbps). The prices range from $49 to $200 per card, and new computers are delivered with the NICs already installed, attesting to the increased popularity of LANs in the workplace and at home.

Network Operating Systems (NOSs)

In order to make the network equipment operate together, software is needed. The software is called a network operating system (NOS) and it controls the order of communication between end-user devices (both personal and shared). Unlike a PC operating system which controls an individual piece of equipment, the NOS controls communication between these devices. Popular NOSs are Novell Netware, Microsoft's LAN Manager, Artifort's LanTastic, and IBM's Lan Server.

Common LAN Flavors

There are as many LAN flavors as there are flavors of ice cream. This variety exists to meet the varying needs of the user base. Although there are many flavors, three bubble to the top as the most common. These three account for about 95 percent of the market share.

Ethernet (802.3)

Over 60 percent of the LANs worldwide use Ethernet. The Ethernet standard, developed by DEC, Xerox, and Intel, has become a *de facto* standard developed by the Institute of Electrical and Electronic Engineers (IEEE) 802.3 Standard Committee. The Ethernet LAN uses a logical bus topology. In a bus topology, all information is sent to a common core (the bus) where it is pulled off and listened to by all the computers. The computer to which the message is addressed hears its name and processes the message. Similar to calling out someone's name in a crowded hallway, the target computer (the person whose name you call) hears and processes the message. As its advantage, the logical bus is efficient from a wide perspective and, without a single point of failure, is less prone to fail. From a negative standpoint, the common logical bus may attract excessive traffic and may be a security concern.

From a physical standpoint, an Ethernet LAN is usually a star topology (Exhibit 9). All the connecting devices go into a hub or switch, where they are internally connected to a bus. When conceptually thinking about networks, we think of them in their logical format; when we actually hook up the wires, we find, for convenience sake, a physical star. Simply put, Ethernet topology is a logical bus and a physical star.

Several end-user devices share this same logical bus, so it is important to control access to the bus. If two computers want to communicate at the same time, their packets collide on the network and become jumbled. In order to stop these collisions, a control access method must be used. Ethernet uses a control access method called Collision Sense Multiple Access/Collision Detection (CSMA/CD). With CSMA/CD, computers listen until they hear nothing

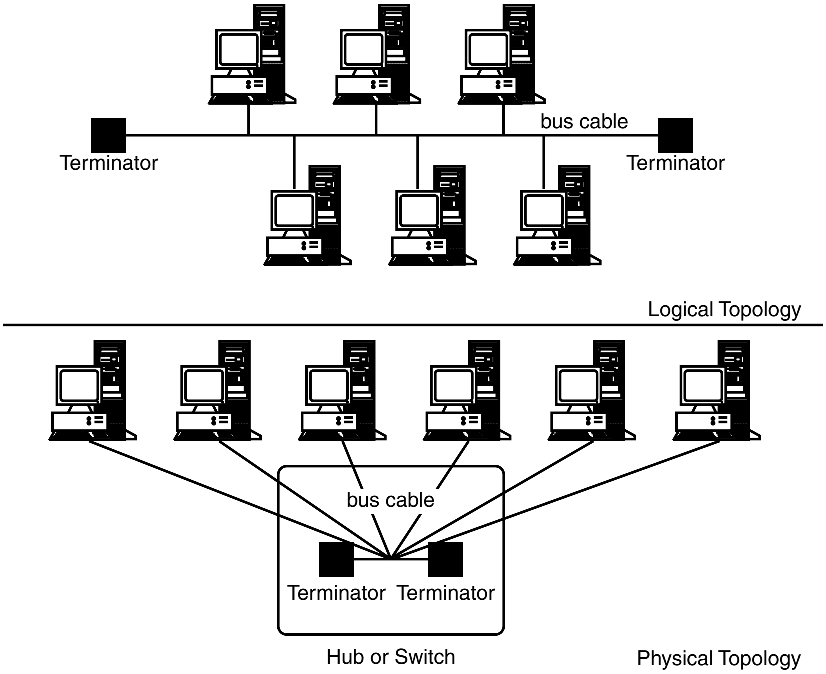


Exhibit 9 Ethernet logical and physical topology.

(meaning the bus is clear), and then they put their packets on the bus (the CSMA part). If the bus is busy, the computer waits until the bus is clear before it transmits.

Suppose two computers want to communicate. They both listen to the bus and note that it is clear. Both put their packets on the bus at the same time. In this case, a collision occurs. This is where the collision detection (ICD) comes in. After putting the packets on the bus, the computer continues to listen and if it hears a collision (packets other than its own on the bus), it immediately stops transmission. Both computers then wait a random amount of time before transmission begins again. Because the computers are waiting random periods of time, it is very unlikely that the two will start transmission again at the same time, causing more collisions.

Ethernet is a baseband type of transmission, meaning that only one signal is on the bus at a given time. The most common physical media used with Ethernet is twisted pair (Category 5), although, as noted before, coaxial cable and fiber-optic cable are used also.

Although originally specified at 10 Mbps, Ethernet is now commonly used at 100 Mbps, with 1 Gbps being implemented, and specifications for 10 Gbps completed. Generally as the speed of the network increases, the distance limitation between the end-user devices and the network equipment (hub, switch, and router) decreases. This is often a critical factor in assuring communication to all people in a building, so this must be assessed carefully.

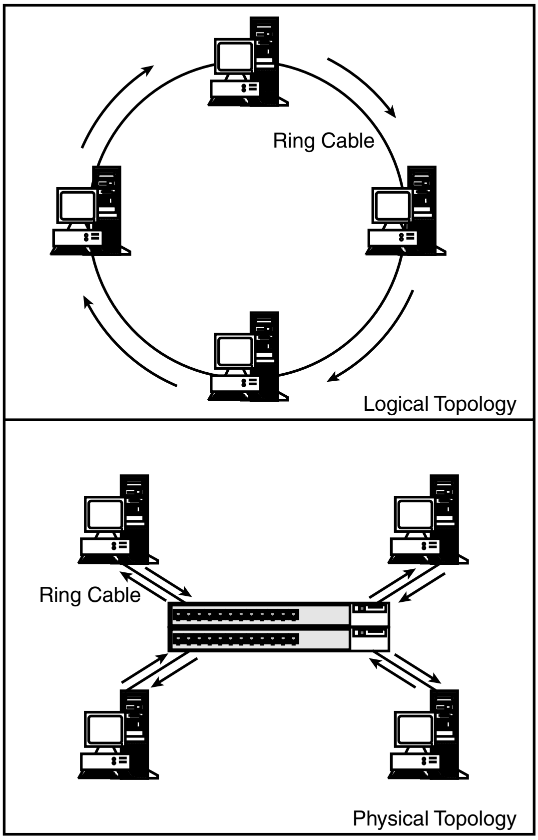


Exhibit 10 Token Ring logical and physical topology.

Token Ring (802.5)

Token Ring, the second most popular flavor of LAN, was developed by IBM. Although originally developed as a proprietary system, it has been accepted by IEEE under the 802.5 standard.

Instead of the logical bus used in Ethernet, the Token Ring LAN uses a logical ring. In a ring topology, all computers are connected to each other in a closed loop with each computer passing the packets on to its neighbor. In its physical appearance, Token Ring is a star topology in which all computers are connected to a hub or a multiple access unit (MAU). Although physically similar to Ethernet from an outside perspective, the internal logic of Token Ring is vastly different (Exhibit 10).

Unlike the control access method of CSMA/CD used in Ethernet, a different access method was developed for the logical ring topology. As the name implies, a token is used for access control. One token goes around the ring, and when a computer gets the token it is allowed to transmit packets (assuming it has packets to transmit). If the computer gets the token but has nothing to say, it passes the token to the next computer in the ring; if the computer has packets to transmit, it keeps the free token so that no one else transmits.

When its transmission is completed, the computer puts the free token back onto the ring and another computer can use it to transmit its packets.

Two problems can exist with this access method: a lost token and a captured token. If a token is corrupted or lost in the ring, no computer gets the token, thus no computer is able to transmit. A captured token can be caused either by a computer that has so much data to transmit, it hogs the network and never gives up the free token, or the computer crashes while holding the token. In either of these cases, the network cannot transmit data and is disabled.

To prevent either of these conditions from happening, one of the computers in the ring is assigned as the "token monitor" which then monitors the network to assure the free token is passed around and that no computer hogs the network.

Token Ring was developed to run at 4 Mbps over Category 3 cable but has been upgraded to operate at 16 Mbps over higher quality cable. Although this is a massive improvement, it is still a long way from the current 100 Mbps standard for Ethernet, and there are currently no plans to upgrade its speed to allow it to compete with Ethernet.

AppleTalk

AppleTalk was developed as a proprietary network system to connect Macintosh computers together. Although nonstandardized, it performs most of the same functions as Ethernet and Token Ring, and works with a cable system known as LocalTalk. AppleTalk works at 230 kbps, making it much slower than Ethernet or Token Ring. However, it is extremely simple to use, and comes as a plug-and-play feature of Macintosh. Currently, most Macintoshes use Ethernet also, attesting to the *de facto* standard of Ethernet and LANs.

The Regulatory and Legal Factors

The Use and Function of Standards

Standards — hard to live with them, impossible to live without them. Standards are a set of guidelines or rules that people and corporations agree to follow in order to make the world an easier place to live and work. Imagine if tire sizes were not standardized and we had to go to the manufacturer of our car for new tires. Imagine if lamps used unique-sized light bulbs and only the lamp manufacturers carried the specific bulb.

Without standards, each company can be extremely unique, creating products that it thinks are best for you. With standards, companies are often limited in their creativity and uniqueness, but as consumers we get:

- *Lower costs:* Competition for the same market often provides lower cost.
- *Flexibility:* A network can have equipment from multiple vendors, therefore users are not locked into a specific vendor.
- *Compatibility of equipment.*

Unless there is a unique and critical need, and if money is no object for your company, or if your company is on the cutting edge of its industry, you will be using standardized equipment, and rightfully so. Standards make the operation of a system and organization go much more smoothly and give you flexibility in your actions.

The Process of Standardization

There are essentially two types of standards: *de facto* and formal. *De facto* standards are agreements that have no official or legal meaning. For example, the Windows operating system is a *de facto* standard that companies other than Microsoft write programs and applications for. Because of Microsoft's position, there is a plethora of programs available for our computer (which is great) and prices are dropping daily. Most corporations purchase computers with Microsoft products on them, strengthening the *de facto* standard. On the other hand, a formal standard is one developed by an official industry or government entity. The process of creating a formal standard is threefold:

- *Specification:* The entity identifies the problem to be addressed, the issue involved, and the terminology to be used.
- *Alternative identification:* The different alternatives are identified, and the pros and cons of each are brought out
- *Acceptance:* The group agrees on the best solution and garners support from leaders in the field.

A lot of fame and fortune can be gleaned from this process and the resultant standard, so it is not without its problems and hidden agendas which, along with the myriad of issues, complexities, and human considerations, often make the standard-setting process very lengthy. It often takes three to five years to start and complete a formal standard. With technology changing so rapidly, by the time a standard is set it may no longer be needed.

Standard-Making Bodies

There are numerous standard-setting bodies; due to the nature of the field, most of them are international. The more visible ones are:

- International Organization for Standardization (ISO): Because the abbreviation comes from the French version of the name, it is ISO and not IOS. Based in Geneva, Switzerland, and international in nature, ISO members come from the national standards organizations for each member country. Its task as part of the ITU (discussed next) is to make recommendations about data communications interfaces and telephone and telegraph systems on an international basis.

- International Telecommunications Union (ITU): This body is the standards-setting arm of the United Nations International Telecommunications Union. Formerly known as CCITT (Consultative Committee on International Telegraph and Telephone), it has representatives in more than 160 countries. ITU formulates recommendations for use by the telephone and telegraph industry, common carriers, and hardware and software vendors.
- American National Standards Institute (ANSI): Comprised of over 900 vendors, it is the coordinating arm for the United States system of standards. Its role is to coordinate development of national standards and to interact with international standards bodies so that they are aligned with each other.
- Electronic Industries Association (EIA): EIA is a body that determines equipment and hardware standards. The common RS232 cable connection standard is a result of EIA. Its members come from telecommunications vendors.
- Institute of Electrical and Electronic Engineers (IEEE): A professional society based in the United States that focuses on LAN standards.

The Legal Aspects

Although these bodies set standards, they do not make laws. In other words, the standards are not legally enforceable in any country. They are formal agreements that make the world an easier place to operate but they do not have to be followed. Vendors follow them in order to sell their products; consumers buy standardized products because of the benefits.

Summary

In this chapter, we explored the packet switching technology of networks, specifically local area networks (LANs). We first looked at why LANs are used in business and what benefit they provide to business and private users. Next, we explored the costs of a LAN, and defined the total cost of ownership.

We then delved into the technical factors associated with a LAN. We looked in depth at the four parts of a LAN (end-user devices, physical media, networking equipment, and network operating system) and at the various flavors of LANs. Both logical and physical layout of Ethernet and Token Ring LANs were discussed.

Finally, we discussed the reasons that standards are important, and we reviewed the process of setting standards. We also listed the various standards-making bodies that exist in the world today.

Exhibit 11 describes a case study that applies to the technology discussed in this chapter.

In the following chapter, we will delve further into networks, exploring the language and routing protocols that get your message to the intended receiver.

Exhibit 11 Case Study: 10 Gigabit Ethernet Put to the Test at NetWorld+Interop[a]

Eighteen vendors of 10G Ethernet products contributed their wares for a demonstration of the technology at NetWorld+Interop 2001 in Atlanta in an effort to show the network industry that prestandard 10G technology can successfully communicate.

The product test fest was hosted by the 10 Gigabit Ethernet Alliance (10GEA) industry group and was billed as more of a general product demonstration than a proving ground to show whose products worked and whose did not, so results on vendor-to-vendor interoperability were not released. Even so, demo organizers say the showing of 10G products proves to enterprise and carrier users that 10G bit/sec Ethernet is ready for deployment and that the technology's hefty price tag could drop soon, thanks to advancements being made in optical interface and 10G chip technologies.

Major Gigabit Ethernet switch vendors that participated in the demo included Avaya, Cisco, Extreme Networks, Foundry Networks, and Nortel. All of these switch vendors have announced 10G products that are supposed to ship by year-end, except for Extreme, which has not yet specified a shipping date or price for its product. Component and testing equipment makers represented at the demonstration included Agilent Technologies, Broadcom, and PMC-Sierra.

"The focus was getting the vendors to play together and to get traffic flowing," over 10G connections, says Bob Grow, chair of the 10GEA and an Intel engineer.

Instead of just connecting all the vendors' 10G switches together in one large 10G bit/sec mesh, the switches were set up in a mixture of topologies, with some switches aggregating multiple gigabit connections and a few connecting to each other over 10G links.

Five of the seven vendors' switches in the demonstration were able to talk to each other over 10G links, according to Grow.

[a] Phil Hochmuth, *Network World*, 9/17/01.

Questions for Review

True/False

1. LANs are inefficient for resource sharing.
2. The total cost of ownership should take into account initial costs and ongoing costs.
3. If you are in a stable organization, you should not have to make moves, adds, or changes to your network configuration.
4. Coaxial cable is no longer used as a networking medium.
5. NICs are the connections between the end-user device and the network.
6. Hubs route packets based on MAC addresses.
7. Switches can be replaced by hubs.
8. Ethernet uses a logical bus and a physical star topology.
9. Token Ring uses a logical bus and a physical ring topology.
10. AppleTalk is identified as the IEEE 802.3 Standard.

Multiple Choice

1. MAC stands for:
   a. Media access control
   b. Moves, adds, and changes
   c. All of the above
   d. None of the above
2. Ethernet usually uses which of the following topologies?
   a. Physical bus
   b. Logical bus
   c. Physical ring
   d. Logical ring
3. Token Ring uses which of the following topologies?
   a. Physical bus
   b. Logical bus
   c. Physical ring
   d. Logical ring
4. Which of the following technologies uses CSMA/CD?
   a. Token Ring
   b. Ethernet
   c. Frame relay
   d. All of the above
5. What is not a characteristic of a LAN?
   a. Uses circuit switching technology
   b. Is a privately owned network
   c. Provides communication to a local environment
   d. Is used for resource sharing
6. IEEE Standard 802.5 refers to:
   a. Ethernet
   b. Token Ring
   c. AppleTalk
   d. None of the above
7. A MAC address is:
   a. Configured by the network administrator
   b. Found on the computer's network interface card
   c. Assigned by the internet provider
   d. Found on the computer's hard drive
8. Token Ring was developed to run at:
   a. 4 Mbps
   b. 16 Mbps
   c. 100 Mbps
   d. 56 kbps
9. Which of the following is not an ongoing cost of network ownership?
   a. Installation cost
   b. Personnel to maintain the network
   c. Equipment maintenance and upgrades
   d. Software licensing

10. Which of the following is not a consideration in the selection of the NIC?
    a. The physical media being used
    b. Network speed
    c. The type of network it is being connected to
    d. The type of computer being used

Short Essay Questions

1. What is CSMA/CD? How does it work, and what technology does it work with?
2. Name and describe the four components of a LAN.
3. Describe packet switching. Compare and contrast it to circuit switching.
4. Name and describe two considerations for network costs.
5. Describe a problem that exists with the Token Ring access method.

Chapter 9

The Language of the Internet: TCP/IP

This chapter explores the language and functions used in data communication and the Internet. Data communication, the Internet specifically, has a language all its own. The language of the Internet, Transmission Control Protocol/ Internet Protocol (TCP/IP), was developed as a universal language that would be as standard as possible to avoid all the pitfalls of picking any one proprietary system.

Be aware that there are many languages for data communication. TCP/IP is certainly not the only one, or the best one, but it is the language of the Internet (a very popular tool in today's culture). We will look at this language in depth in this chapter, and will introduce you to a few other languages that are used. With the information from the previous chapters, you will garner a better and deeper understanding of the way data communications operate within a business environment.

The Business and Human Factors

Humans have a need to communicate and we often meet this need through our technology. By providing mechanisms, standards, and connections, we allow machines and humans to communicate.

One of the fastest-growing mechanisms for communication today is electronic mail or e-mail. E-mail allows fast and cheap communication between people. The biggest advantage of e-mail is its asynchronous nature, allowing communication that is not real-time. We have all had the need to contact someone, and we pick up the phone and dial the number, only to be met either by a busy signal or no answer at all. E-mail allows us to send a message to a person and have that message responded to when the recipient is available.

E-mail is certainly not the panacea of communication, and not for all types of communication such as urgent messages. It is just another tool that can, if used effectively, round out our repertoire of communication methods and meet our need to get and give information.

The growth and popularity of the Internet has been due to many things, but certainly e-mail is the greatest part of its growth and the Internet's most popular application. Whether you measure by the availability or by the number of users, e-mail is the killer application of the Internet.

One of the key reasons for the success of e-mail is the ability to send mail to almost anyone anywhere in the world for a minimal amount of money. Added to that is the ease of putting together an e-mail and the quick travel time. It is now common upon meeting someone to ask their telephone number and e-mail address.

What once was a medium for "techno-savvy" people only is now as important as the telephone; in fact, e-mail may be even more important than the telephone. In today's business environment of international corporations, where time zones become a severe hindrance, the asynchronous nature of e-mail allows people to communicate at their convenience. Recently, the American Management Association found that more than 57 percent of business executives in America rely on e-mail for their work.

Corporations also find that e-mail is cheaper than local mail, and companies want to leverage their investment in Internet technologies. When companies want to extend their customer support base and improve management communication and interaction with customers and suppliers, e-mail seems to fit the bill well.

From a human perspective, e-mail use has also changed. What was once the domain of well-educated, affluent men is being discovered by females, people without college education, and those with modest incomes. These newcomers are coming online for predominantly personal reasons: to keep up communication with friends and family around the world.

Some characteristics that are intriguing are:

- The average size of an e-mail message is increasing, with the growth attributed to attachments.
- There are approximately 440 million e-mail addresses worldwide.
- By the end of 2001, the average number of messages received was 35 per person per day.
- In 1999, 200 billion pieces of mail were delivered by the U.S. postal system. E-mail has outpaced regular mail volume with 560 billion messages being delivered per year.
- An estimated 20 percent of all e-mail received was commercially driven. This is probably less than the junk mail we receive in the postal mailbox.
- Despite challenges from instant message services and virtual workspaces, e-mail is still the clear winner in Internet use.

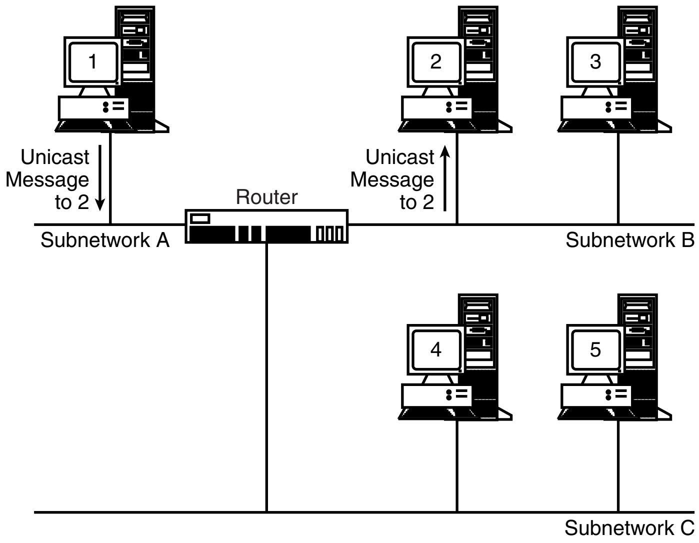


Exhibit 1 Unicast transmission.

E-mail is clearly not the panacea for all communication flow. It is not effective for sensitive conversations or for information that is needed instantly. However, e-mail is another helpful tool when passing information is key and where time differences and working styles are different.

The Technical Factors

Message Casting

Messages sent on a network are categorized by the number of recipients they are directed to. The three basic categories of messages are unicast, multicast, and broadcast.

Unicasting

With unicasting, the sender transmits the message in the form of packets addressed to a single destination (Exhibit 1). A unicast message is intended to go from one computer to another computer. It is similar to a person in a crowded room calling out a particular name (which tells an intended party who the message is addressed to).

Multicasting

With multicasting, a message is transmitted to people in a distinct group or classification (Exhibit 2). If you called out for all females to listen to you, each of them, knowing their group or classification membership, would then listen to the message.

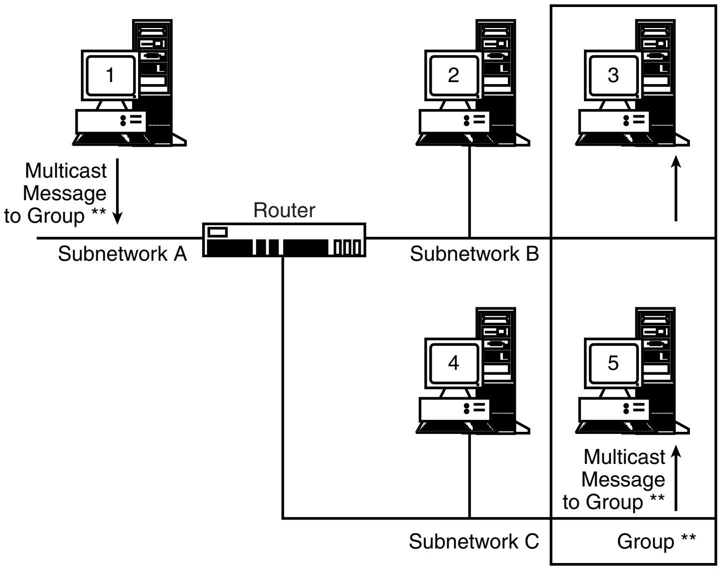


Exhibit 2 Multicast transmission.

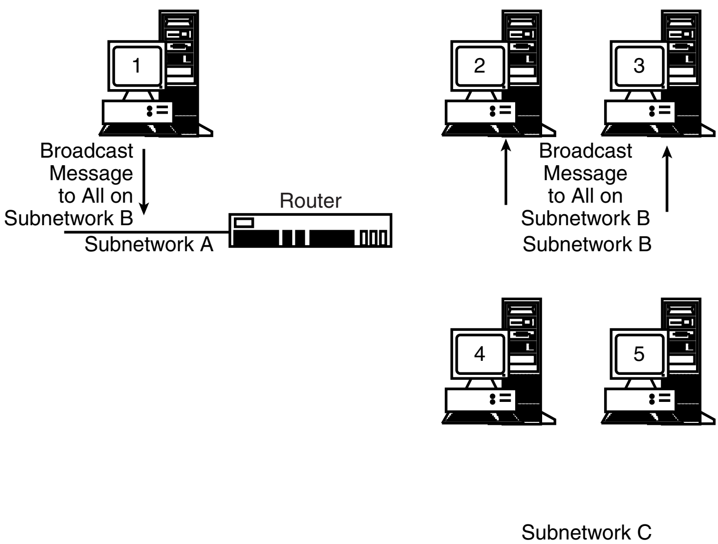


Exhibit 3 Broadcast transmission.

Broadcasting

With broadcasting (Exhibit 3), a message is transmitted to an entire group bound together by a physical restriction. If you called out to an entire room, "everybody listen," everyone in the room would respectfully do so. Broadcasting on a network means that every computer or server on the network or network segment receives and processes the message.

For each of these conditions to exist, the intended sender and receiver must know certain information about each other. For example, in our analogy each person must know their name, their gender, and what room they are in. The sender also must know the same information for communication to occur. Obviously, some mechanism or standard must be agreed to so that all people can communicate effectively. These standards or agreements in method must exist and are part of Layer 3 of the OSI model, the network layer. At Layer 3, schemes for message addressing all network devices is agreed to and subsequently used for communication to happen effectively.

Message Addressing

For effective message transmission, whether unicasting, multicasting, or broadcasting, each device on the network must have a distinct and unique global address, and the address must be understood by each member on the network.

TCP/IP is one of the most predominant of the network languages (routed protocols), thus, it has a unique naming/addressing scheme. Each routed protocol has a different naming/addressing scheme, but we will look only at TCP/IP.

In the case of TCP/IP, addresses are broken down in two separate parts: network ID and host ID. The network ID is similar to city and state in a mailing address. This information tells the post office the general location of your street, but it is not exact enough to pinpoint your house. The host ID portion of a TCP/IP address gives the specific location of your computer on your network (similar to your house number on your street) and therefore assures a unique address.

IP addresses are written in numerical form, similar to a telephone number, but in four distinct parts. Each of the parts is designated as either part of the network ID or the host ID. Each of these parts is called an octet, and is separated by a period or dot:

```
Part1.Part2.Part3.Part4
```

In reality, each part is a number between 0 and 254. So an address can be as follows:

```
127.52.16.4
```

Now the question arises, which of the parts or octets are part of the network ID and which are part of the host ID? Our example of the street address shows some similarities:

Street address	**TCP/IP address**
John Doe	127.52.16.14
123 Main Street	
Whitestone, New York	

Exhibit 4 Classes of TCP/IP Addresses

Class	*Number of Addresses in Host Portion*	*Number Range*	*Breakdown*
A	16,777,214	1.0.0.0–127.0.0.0	N.H.H.H
B	65,534	128.1.0.0–191.259.225.225	N.N.H.H
C	254	192.0.0.0–223.255.255.755	N.N.N.H

Note: N = network, H = host.

In a street address, the city and state are always on the bottom line. This information can be thought of as the network address. The network address, and the city and state, provide the general location but not the exact address of your house. The street address and the name (lines 1 and 2) provide the exact location. The host portion of the IP address provides this exact information; but with a TCP/IP address, the octets vary by the class of address it is. There are three common classes of TCP/IP addresses, as shown in Exhibit 4.

Class A licenses are for large organizations, and provide large numbers of octets or host IDs for local use. Class B licenses are for medium-sized organizations, and allow for two of the octets for host IDs. Class C licenses are used for small organizations, and allow for only the last octet to be used for host addresses. Referring to the breakdown portion of Exhibit 4, we see the number of octet labels for either the network (N) or the host (H) portion.

Depending on the size and intentions of an organization, a particular class of license is allocated; the license then defines which of the four octets are the network ID portion and which are the host ID portion of the address (Exhibit 5).

Network Routing

To understand how addresses work, you must first understand how the messages route through the network to get to their destination. Routing is the process for delivery that packets take from the sender's computer to the receiver's computer through the network.

For many of the LAN technologies and topologies we have looked at, the routing is simple. The message goes to all devices on an Ethernet bus or to each individual device in a Token Ring, and the receiver hears its address and processes the message. However, the Internet is complex, and routing is a difficult mechanism that is critical to getting the message to the right place (Exhibit 6). There are essentially two categories of routing: centralized and decentralized.

Centralized Routing

In centralized routing (Exhibit 7), all decisions about the path a packet is going to take are made by a central device. In star topology, all packets are routed to the central device where decisions are then made on how to forward

Exhibit 5 Case Study: State University

State University is a mid-sized university in the Midwest. It has approximately 20,000 students divided over seven colleges. When State University applied to the InterNIC (an organization that is charged with registering domain names and IP addresses as well as distributing information about the Internet), it was given a Class B license based on its current size and projection of growth: 136.15.0.0. With a B license, the first two octets define the network ID portion of the address (136.15). These octets define and differentiate State University from all other colleges, commercial firms, and organizations in the world. The last two octets are left to State University to use as host ID addresses.

State University is an organized and methodical place; it has decided to separate the host addresses for each college and each computer. Thus, the addresses for each computer look like this:

College of Arts and Sciences

136.15.1.1.— Joe Dean's computer
136.15.1.2.— Sally Secretary's computer
...
136.15.1.254.— Tom Teacher's computer

College of Fine Arts

136.15.2.1.— Frank Dean's computer
136.15.2.2.— Sam Receptionist's computer
...
136.15.2.254.— Kristen Teacher's computer

The internetworking equipment reads the addresses and determines which class of license it is (from the number in the first octet), which network it is, where the network is, and finally, which computer of that network the message goes to.

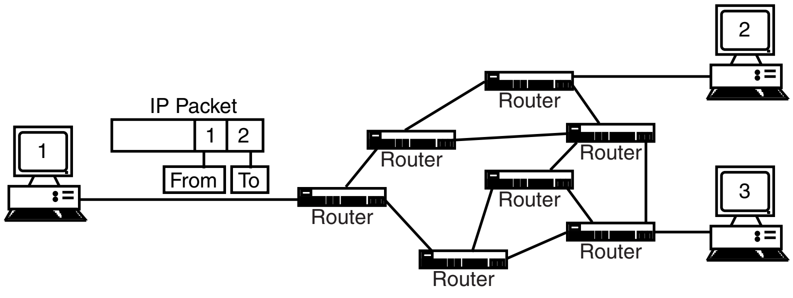


Exhibit 6 Message routing.

the packet to its destination. The central device, a telephone switch or a router, learns which devices are connected to it and then creates a table to keep track of the address and location of each device. The table is used to look up each connected device to determine the path it must take. Even in a complex topology, a central device can maintain an effective routing table and route the packet to its intended destination.

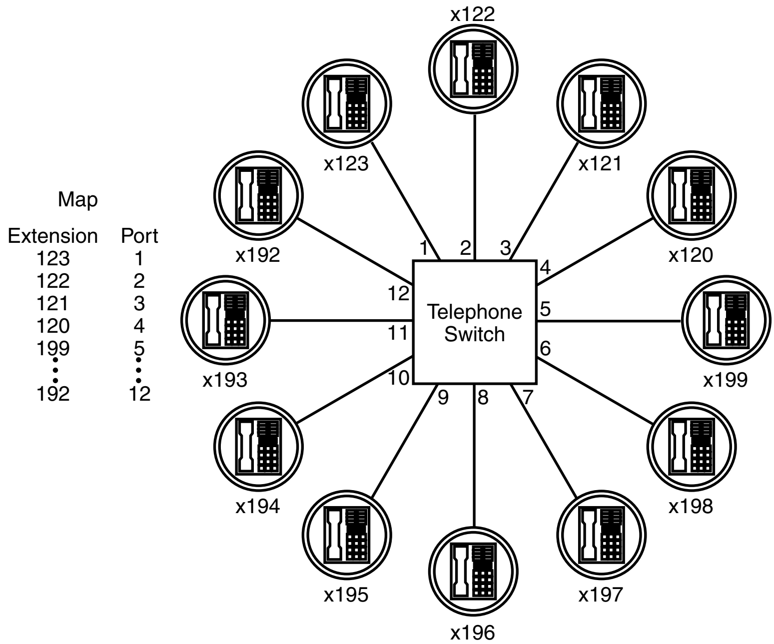


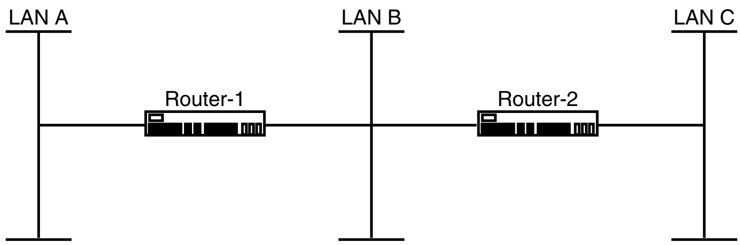
Exhibit 7 Centralized routing.

However, the primary advantage of centralized routing is its network efficiency. One routing table that keeps track of the whole network is maintained, and thus computer resources and precious network capacity are managed by focusing all the work on one device. This primary advantage is also its biggest disadvantage. If the central device fails, the network fails. Without a brain to tell the packets where to go, they will wander aimlessly around the network until they finally die. Another disadvantage of centralized routing is scalability. As the network grows and more devices are connected to it, the central routing table can become very large and unmanageable. These disadvantages and the need for networks that always work have led to the advent of decentralized routing.

Decentralized Routing

In a decentralized routing scheme, no one device maintains the routing table (Exhibit 8), but many devices maintain parts of it. This may seem chaotic (too many cooks spoil the broth) and inefficient (many machines doing the same thing), but in reality it works very effectively.

The key to this effective operation is a set of rules called routing protocols. Routing protocols are rules that govern how each device works within the whole network and how the whole network operates as a system. For example, in an office one person is responsible for sorting the mail, another is responsible for delivering the mail, another is responsible for filing the mail. *In toto,* they are each part of a large system that assures that the mail system operates effectively.



Router-1

Destination	Distance	Next Hop
LAN A	0	
LAN B	0	
LAN C	1	Router 2

Router-2

Destination	Distance	Next Hop
LAN A	1	Router 1
LAN B	0	
LAN C	0	

Exhibit 8 Decentralized routing, routing table.

Exhibit 9 Routing Protocol Selection

	LANs	*WANs*
Small	RIP	OSPF
	IGRP (proprietary)	
Large	OSPF	OSPF
	EIGRP (proprietary)	BGP-4

There is no best routing protocol and there are various flavors of rules to choose from; however, each rule is a set of procedures that makes the system work, if all the members in the network follow the rules.

These routing protocols have been accepted by the industry and have been standardized in their operation so they can be used across different vendor platforms. Basically, the routing protocol is selected by the type and size of the network (Exhibit 9).

Some of the routing protocols are proprietary, which means they work only with a specific vendor's equipment. If you have this certain vendor's equipment, it is appropriate to select the proprietary routing protocol; if you have a multivendor environment, or use a different vendor's equipment, you must select other routing protocols, e.g., RIP, OSPF, or BGP. These routing protocols are standardized and run across different platforms and systems.

The Language of the Network: Routed Protocols

We have described how packets are routed using routing protocols along a path to their correct destinations but not how these packets are arranged (routed protocols). The packets must be arranged in a specific form according to a set of rules in order to be understood. Similar to language, these routed protocols have rules, i.e., there must be a verb in each sentence, words must match in tense, etc.

Exhibit 10 IP Packet Structure (IP Version Four)

Version	Type of service	Total length	Flags	Hop limit	Protocol	Source address	Destination address	Data

These network languages operate predominantly at the network layer (Layer 3) of the OSI model and form the information we wish to communicate. The languages have become standardized so they can be understood by many different vendors and computers. Although there is a plethora of standardized and proprietary languages, we will look at three of the most common: TCP/IP, IPX/SPX, and SNA. Although each language operates differently, there are many similarities between them, and you are encouraged to understand these similarities.

TCP/IP

The language of the Internet, Transmission Control Protocol/Internet Protocol (TCP/IP), is the most common and the oldest standardized routed protocol. Because it can use a variety of data link protocols (Ethernet, Token Ring, ATM, frame relay), it is a very popular and effective protocol. Coupled with its ability to transmit messages without errors (or at least to correct its errors), it is the language most networks and equipment speak.

As you may suspect, TCP/IP is made up of two separate parts: TCP and IP. The Internet Protocol (IP) was developed in the 1970s as a way of packetizing and sending messages across what was then called the Advanced Research Project Agency (ARPA) network. Operating at the network layer of the OSI model, the main function of IP is the addressing and routing of packets. Because IP functions on all the networking devices, the network can route the packet using the IP addresses and IP routing protocols (RIP, OSPF, etc.) This function provides the method for getting a packet or a message from the sender to the receiver.

Exhibit 10 shows the detailed breakdown of an IP packet (Version 4). Each of the parts (think of them as verbs, nouns, adjectives) serves a specific purpose:

- Version number: Shows the version of the IP language. Version 4 is the most common one used today.
- Type of service: A field that can be used to identify the type of packet (voice, data, video message) and allow for prioritization or quality of service (QoS, discussed later).
- Hop limit: To stop lost packets from forever traveling across a network, a limit is put on the number of hops or transmissions from one router to another. This field essentially controls the life of the packet in the network.
- Source address: The IP address from which the message originated.
- Destination address: The IP address to which the packet is destined.

Exhibit 11 TCP Packet

Source port	Destination port	Sequence #	ACK #	Length	Flow control	Options	Data

- User data: This is where your message (an e-mail, a word processing file, or a phone call) is actually placed. The other parts of IP are all business overhead but essential. The user data field can vary from 8 bytes to 1428 bytes in length.

The other portion of TCP/IP is the Transmission Control Protocol. TCP performs a few essential functions and couples well with the IP portion of TCP/IP. Its main functions are:

- Packs and unpacks the data: Sometimes a message cannot fit into one packet, so it must be broken down into many packets and reassembled at the other end. TCP performs this function but must be operating at both ends of the network in order to break up and reassemble the data.
- Ensures reliability: IP by itself is similar to the postal system; you send the message and pray that it gets to its intended recipient. Combining TCP and IP is like sending mail "guaranteed," return receipt requested. TCP waits to hear from the receiver that it got the message. If the message is lost or corrupted during its travels, TCP resends the packets. A typical TCP packet is shown in Exhibit 11.

A TCP packet is a bit different from an IP packet. You can see the fields that are provided for successful packing and unpacking (Sequence #) and to ensure reliability (ACK [acknowledgment] #). The sequence number lists the part of the total this packet is from (for example, 2 out of 3). The acknowledgment section is received after the receiver confirms its receipt.

IPX/SPX

IPX was developed by Xerox in the late 1970s and became a proprietary packet protocol used with Novell Netware. Because Novell has a fairly large market share, the language is common on networks, and probably will not disappear in our lifetime. (However, Novell has recently introduced its new network product that uses TCP/IP instead of IPX/SPX for encapsulation.)

As the name implies, IPX/SPX is made up of two essential pieces (Exhibit 12). The SPX portion behaves in much the same manner as TCP and has the same function to perform (ensuring reliability, and packing and unpacking the data). The IPX portion of the protocol behaves very much like the IP portion of TCP/IP. The major difference is in the addressing: as part of the address, IPX incorporates the MAC address of the devices, thus the address of an IPX device has both the Layer 2 and Layer 3 information required for communication to occur.

Exhibit 12 IPX Packet Structure

Checksum	*Lensil*	*Control*	*Destination Address*	*Destination Network Address*	*Destination Socket*	*Source Address*	*Source Network Address*	*Source Socket*	*User Data*
2 bytes	2 bytes	1 byte	6 bytes	4 bytes	2 bytes	6 bytes	4 bytes	2 bytes	Varies

SNA

IBM developed a proprietary network protocol called Systems Network Architecture (SNA) in the late 1970s. The protocol is very effective on IBM machines. SNA is not just a routing protocol or a routed protocol, but a full telecommunications architecture.

A bit of history might help here. IBM was one of the forerunners in computers. Developing the mainframe and personal computers, IBM rose to prominence and even dominance in the field. Understanding that people need to communicate over distances, and recognizing the lack of a routing language, IBM developed SNA as a protocol for networking.

In the late 1980s, a philosophic shift away from proprietary architecture toward an open system and mixed vendor networks took hold in both computing and networking. TCP/IP was embraced as the panacea; anything proprietary was discounted. As a company, IBM suffered many losses in the early 1990s. Many reputable sources predicted its mainframe and architecture would wither away by the twenty-first century.

Both IBM and its mainframe are still around; in fact, both are doing amazingly well. Despite many projections, there is a need for mainframe computing power and reliability. Many of its architectures still exist, and SNA is certainly one that will be encountered in the workplace; therefore, it is necessary for you to have a minimal understanding.

In SNA parlance, the end-user terminals are designated logical units (LUs). These LUs are endpoints to the SNA network, and their code is programmed into the device. LUs talk to each other via sessions. The controlling network software, upon a request from an LU, sets up a session with another LU (another terminal, a mainframe computer, or a microcomputer). Before the session actually begins, rules (amount of data to be sent, frame size, etc.) are specified by the two LU devices. Each LU having a coded number (similar to a MAC address) also is assigned a network name which allows LUs to talk to another name regardless of its location (the network makes the translation between name and coded number). As the session progresses, the packets move along in a Synchronous Data Link Control (SDLC) frame. The session is ended when one of the LUs sends a deactivate request (Exhibit 13).

Besides LUs as SNA-addressable devices, there are also physical units (PUs) and system service control ports (SSCPs) (Exhibit 14). PUs can be the end terminals and microcomputers, and they also can be a terminal control or a computer front end. These PUs have an intelligent role to play in the large-scale

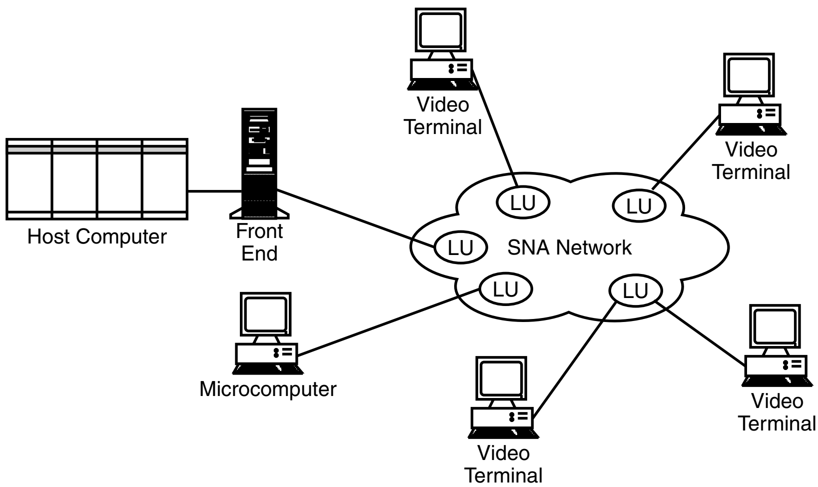


Exhibit 13 Synchronous Data Link Control framing session.

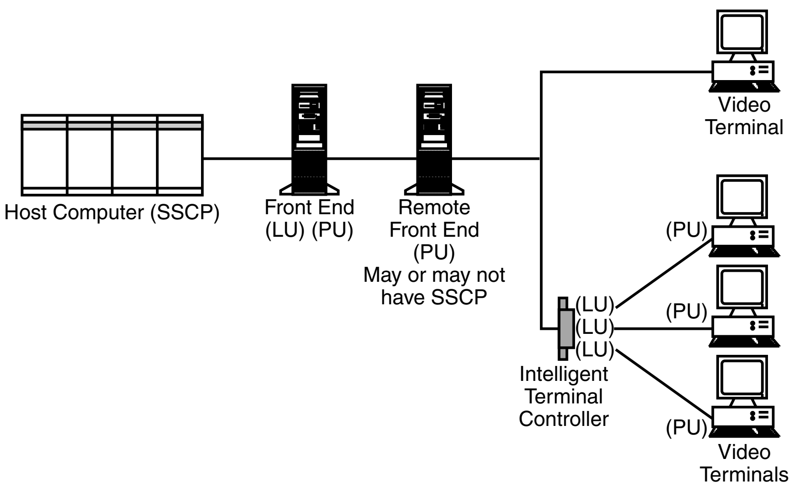


Exhibit 14 System Network Architecture devices.

SNA network. The SSCP, a set of SNA components, manages the entire SNA network or a part of the SNA network (called a domain).

Another part of the SNA world, besides the network-addressable units discussed previously, is the path control network. The path control network provides the routing and flow control necessary when moving data in the network. The path control mechanism handles:

- Prioritization of traffic
- Error detection and recovery
- Network monitoring and alerting

SNA Access Programs

Besides the previously mentioned hardware and software necessary for SNA, a telecommunications access program must be used to complete the network operation. There are essentially four access programs available:

1. Telecommunications Access Method (TCAM): Provides the basic functions needed for controlling circuits. It has its own commands and can schedule traffic, handling operations while also providing status reporting and recovery from network failure.
2. Virtual Telecommunications Access Method (VTAM): Newer and more robust than TCAM, VTAM manages a structured SNA network.
3. Network Control Program (NCP): IBM's effort to move the telecommunications access method from the mainframe computer and distribute it to the front-end processor.
4. Customer Information Control System (CICS): A telecommunications access method that truly relieves the host computer operating system of the many tasks of telecommunications. It is the world's most widely used mainframe teleprocessing monitor, and even the competition admits its robustness and stability. Security and message logging are also done very well.

IBM is also changing to meet the demands of the current generation. A newer SNA architecture and advanced peer-to-peer networks (APPNs) have been released. Both support industry-standard network and common data link protocols, overcoming many of the incompatibility issues in traditional SNA.

IPv6

We previously discussed TCP/IP is one of the routed protocols of networks. The IP that we discussed was Version 4, the most commonly used version of the protocol; however, there are other versions.

Although IPv4 is the most commonly used version of the Internet protocol, it is not without its flaws. During the growth of the Internet in the early 1990s, there were many issues that IPv4 could not handle well:

- Address space: Although designed to have adequate address space for each device, when the worldwide nature of the Internet and the commercial vendors coming onboard the Internet were factored in, available addresses were rapidly being depleted.
- Security: We all want our e-mail and other transfers of information to be secure so that it cannot be intercepted. IPv4 does not have built-in security and is subject to being easily intercepted and stolen.
- Quality of Service (QoS): Some messages are more important and timely than others. If we hope to use the Internet for voice and video transmission, a way must be provided to assure these packets are transmitted with a higher priority than e-mail (which could be minutes

late without any major disruption). QoS allows for different packets to be "tagged" with codes that indicate their priority for moving through the network.

These major issues and many other minor issues led to the formation of a committee to develop IP for the next generation (IPng). Requirements were drawn up for IPng, including solutions for address space, security, and Qos issues mentioned previously. However, there were more requirements laid down. IPng must:

- Be compatible and not require more-robust and complicated hardware.
- Have a smooth transition plan to move from IPv4 to IPv6.
- Be as easy and as fast to route as IPv4.

These are tall orders given that the protocol must do much more with the same resources. Many proposals were submitted and eventually IPv6 was accepted and ratified in the mid-1990s. Why is IPv6 not being used fully now? A fair question; following are just two of the answers:

- Scope of change: Every PC, networking device, and end-user device must be changed from IPv4 to IPv6. This scope of change is tremendous, causing corporations to shy away from it.
- Quick fixes: Much was done to and around IPv4 that allowed it to overcome most of the major issues identified previously. For example, the built-in security of IPv6 was stolen, named IPsec, and included as an add-on to IPv4.

Eventually, the switch will have to be made from IPv4 to a newer and more-robust version. Will it be IPv6? It's hard to say. What may happen is that the IT professionals will pull out IPng and start implementing it when the public cries for more (usually after a critical event stops things from working).

The Regulatory and Legal Factors

Throughout this chapter and others, we have seen the reference to the 802.x standard (x being typically a 3 or a 5). In this section, we will explore exactly what this is.

Formally, the standard is the 802–1990 IEEE standard, put together by the Institute of Electrical and Electronic Engineers, and ratified in May 1990 (hence the –1990). In text form, the 802–1990 standard is referred to as the "IEEE Standard for Local and Metropolitan Area Networks." The standard was also recognized and approved by the American National Standards Institute (ANSI) in November 1990.

IEEE standards are developed by its technical committees. Members of the committees serve voluntarily and without pay, and are not necessarily members

Exhibit 15 802.X Family and the OSI Model

OSI Model	*802 Family*			
Application				
Presentation				
Session				
Transport				
Network	802.2 Logical link			
Data link		802.3	802.5	802.11
Physical	802.1 Bridging	Medium access	Medium access	Medium access
Medium				

of IEEE. The standard presented represents a consensus of the experts on the subject, and use of the standard is totally voluntary. IEEE standards are subject to review at least every five years.

The 802–1990 standard is actually a family of standards for local and metropolitan area networks. The scope of the 802–1990 family and its relationship to the OSI reference model is shown in Exhibit 15. There are other members of the 802.x family but only the most important ones are shown.

- The 802.2 part of the family describes the logical link control (LLC) medium that forms the communication link between the data link layer and the network layer.
- The 802.3 part of the family describes the CSMA/CD access method and physical layer specifications for Ethernet.
- The 802.5 part of the family describes the Token Ring access method and physical layer specifications for wireless local area network.

Other parts of the family have specifications and standards for security (802.10), voice and data access networks (802.9), and metropolitan area network access and physical layer specifications (802.6).

The actual description of the standard is beyond the scope of this book; suffice it to say the standard is fairly complex and detailed, but it provides guidance to engineers for the development of products which can work together.

Summary

In this chapter, we have discussed in depth the subject of networks. Specifically, we have looked at the way messages get routed in a network from the origination point to the intended destination. In so doing, we have studied the requisite pieces and products that the network needs.

We have looked at the types of messages that networks send: unicast, multicast, and broadcast messages. We have studied the requisite addressing needed to send these messages, specifically the addressing used with TCP/IP.

Exhibit 16 Case Study: Metro Ethernet Gains Momentum[a]

Metro-area Ethernet is becoming a popular way to reach LAN speeds across a city campus and beyond. The services market is expected to grow by about 37 percent during the next five years, with revenue increasing to $740 million in 2006 from $155.2 million this year [2001], according to market research firm IDC.

Now service providers and corporate users are looking to use metro Ethernet for applications other than basic connectivity. Recently, metro provider Telseon and storage switch company Nishan Systems introduced technology to carry Fibre Channel over Gigabit Ethernet, thereby letting customers extend storage area networks to the metropolitan area. Yipes Communications Inc. in June launched a partnership with Wire One Technologies Inc. to accelerate the rollout of videoconferencing to enterprises.

These and other applications — including storage backup, IPTV, live video feeds, disaster recovery, and data retrieval — are high-bandwidth applications well-suited to a fiber-based Gigabit Ethernet. Indeed, enterprise managers are thinking of what types of services may be of value down the road.

"Disaster recovery is something we would use in the future but our data is too sensitive for offsite storage," said Ray Melnik, a system engineer at Fish & Neave, a New York law firm that ships large legal files using metro Ethernet. "Now if they had a secure tunnel into our own server that no one else could access, that would be viable."

Jaros Baum & Bolles, a Newark, New Jersey, consulting and engineering firm, is testing IPTV services from Fiber City Networks, also in Newark. Jay Conti, the firm's IS manager, said the quality is "just like watching a video."

"I can see a financial company involved in the stock market using this to run CNBC all day," he said.

Metro-area Ethernet is expected to be popular for a few reasons. First and foremost, it breaks the infamous last-mile bottleneck. Customers can get from 1-Mbps to 1-Gbps Ethernet service for a fraction of what they would pay for traditional carrier circuits. A customer can replace a 1.544-Mbps T-1 connection at about $1500 with a 100-Mbps connection that can be purchased for as low as $1000 a month. Another break for customers is eliminating the long provisioning times associated with ordering circuits from an incumbent carrier.

For the largest customers, an OC-3 (155.5 Mbps) or OC-12 (622 Mbps) can be replaced by metro Ethernet services ranging from 50 Mbps to 1 Gbps. A gigabit will typically cost a fraction of its Sonet equivalent, according to Vesna Swartz, executive vice president of marketing at Telseon, an Englewood, Colorado, service provider.

Metro Ethernet is still an emerging technology, but urban users already have a few choices of where they can buy these services, according to Ron Kaplan, an IDC analyst. A few incumbent carriers sell what is called a transparent LAN service, but perhaps the best source of metro Ethernet (though they are all geographically limited today) is from among the spate of start-up and comparatively young companies, led by Cogent, Fiber City Networks, Telseon, Time Warner Telecom, Yipes Communications Inc., and others. Within the latter group, not every service provider is interested in expanding beyond simple access services.

Cogent, for example, is making its name as a low-cost service provider, offering 100 Mbps at $1000 per month. Yipes and Fiber City are layering on other services, like storage, TV, and security, according to Yankee Group analyst Nick Maynard. Yipes and Telseon also give users the ability to provision their own services using a graphical user interface.

[a] Margie Semilof

TCP/IP uses three classes of licenses (Class A, B, and C) for addressing, and incorporates host ID and network ID portions of the address.

We explained the way messages move around a network through routing protocols. There are many different types of routing protocols, and their selection is dependent on the type of network and the equipment it uses.

We discussed the languages of the Internet, further exploring the structure of TCP/IP and other languages such as IPX/SPX and SNA. We ended the technical factors section of this chapter exploring the future of IP through IPv6.

Finally, we looked at how standards are formed and why they are needed. (See Exhibit 16 for a case study of these lessons.)

Questions for Review

True/False

1. In unicast messages, a message is transmitted in packets.
2. In broadcasting, a message is transmitted with *no* physical restrictions.
3. IP addresses are written using the letters of the alphabet.
4. There are three common classes of TCP/IP address.
5. In centralized routing, all decisions concerning the path the packet will take are made by a central device.
6. In multicast messaging, a message is addressed to a group of people in a distinct group or classification.
7. In broadcasting, a message is transmitted to an entire group that is bound by a physical restriction.
8. IP addresses are written in four distinct parts; each part is designated as either the network ID or the server ID.
9. There are five classes of TCP/IP addresses.
10. *De facto* standards are agreements that have no official or legal meaning.

Multiple Choice

1. The three common classes of TCP/IP addresses are:
    a. D, E, F
    b. A, B, C
    c. X, Y, Z
    d. All of the above
2. CICS does which of the following?
    a. Relieves the host computer operating system of the many tasks of telecommunications
    b. Turns personal computers on and off
    c. Stores customer information in a database
    d. All of the above

3. A version number is which of the following?
   a. The version of the operating software
   b. The version of the IP language
   c. A model number located on a PC
   d. All of the above
4. Source address is which of the following?
   a. Address of a certain software package
   b. Address that details where a person can be found
   c. IP address from which the message originated
   d. All of the above
5. Which is *not* a valid IP address?
   a. 210.9.4.3
   b. 250.1.2.3
   c. 9.3.256.4
   d. 3.4.5.6
6. LU stands for:
   a. Limited unified address
   b. Logical unit
   c. Less unit
   d. None of the above
7. Which of the following is the meaning of CICS?
   a. Center for Information and Communication Sciences
   b. Customer Integration Center for Service
   c. Customer Information Control System
   d. None of the above
8. Which program is IBM's effort to move the telecommunications access method from the mainframe computer and distribute it to the front-end processor?
   a. VTAM
   b. CICS
   c. NCP
   d. None of the above
9. Which are the common classes of TCP/IP addresses?
   a. A, D, F
   b. A, B, C
   c. C, D, E
   d. All of the above
10. Which of the following is accomplished by the path control mechanism?
    a. Prioritization of traffic
    b. Error detection and recovery
    c. Network monitoring and alerting
    d. All of the above

Short Essay Questions

1. What is the primary advantage of centralized routing, and why?
2. When is the SDLC framing session ended?
3. What layer of the OSI model do the languages of the network operate, and what do they do?
4. What is TCP/IP?
5. How are multicast messages transmitted?

Chapter 10

New and Emerging Technologies

In the previous two chapters, we looked at the fundamental parts of packet switching technology. These elements make up the basic building blocks for data communication. Using these basic elements, we can construct systems that can be extremely beneficial to human and business needs. This chapter looks at some of these systems, how they operate, and how they can be used for current and future business needs. In addition, this chapter focuses on some of these newer and upcoming technologies that allow telecommuting to happen effectively and efficiently. Discussed in this section are some of the characteristics of telecommuting, the concerns that it presents, and also the best situations for telecommuting.

The Business and Human Factors

Telecommuting (working at home or away from the office) has been around for a long time, but today telecommuting is gaining immense popularity for numerous reasons. Some of these reasons are:

- The sensitivity to environmental pollution that commuting is causing
- The frustration and cost of commuting to the workplace, as seen by employees
- The cost of maintaining office space for employees, as seen by employers
- The options and capabilities offered by the Internet and electronic communication technology

About two to three percent of the American workforce do some type of telecommuting. Half of these telecommuters have children under the age of

Exhibit 1 Common Job Titles and Employee Characteristics

Job Title	*Personal Characteristic*
Programmer	Independence
Accountant	Children at home
Engineers	Deep thought
Writers	Less sociable
Researchers	Self-starter

18. "Why telecommute?" you may ask. The answer lies in the benefits to both employers and employees. The benefits to employers are:

- *Compliance with the law:* Many states require urban corporations to limit the amount of commuting by employees.
- *Ability to attract and retain workers:* Workers do not want to commute, so the ability to telecommute is seen as an asset to a potential job offer.
- *Enhanced customer service:* Employees who telecommute tend to be happier and less distracted, thereby offering better service to the company and its customers.
- *Cut down on moves:* If the corporate office moves, the employee does not need to.
- *Reduced office space cost:* Office space in major cities can cost up to $30 per square foot. This cost must be recovered if offices are maintained.
- *Increased productivity:* Employees who telecommute tend to be more productive.

To an employee, the benefits of telecommuting include:

- *Flexibility in scheduling:* The ability to "take off" during the day to catch your child's soccer match is priceless.
- *Reduced expenses:* Reduced costs to maintain an automobile, to hire a babysitter, to purchase lunch and clothes are economic incentives.
- *Less stress:* The distractions in an office are intense. With the constantly ringing phone, the ad hoc meetings, the birthday parties, the background noise, and the crowds, it is a wonder any work gets accomplished.

To be successful with telecommuting takes a certain type of employee and job. Some of the more-common job titles and employee characteristics are shown in Exhibit 1.

If a company has job titles such as those listed and employees with the noted characteristics, telecommuting is a very viable option to explore. If properly applied, telecommuting is a win–win situation for those involved but it does require some changes. Management is one of the things that must

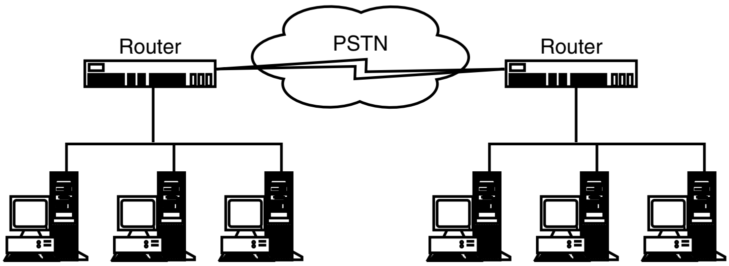


Exhibit 2 Local area networks connected to the wide area network.

change. The heavy-handed, in-your-face style of management will no longer work. A new breed of manager must be selected to deal with the telecommuting environment. Another aspect that needs adjustment is the creation of the virtual office. Not only must physical and ergonomic factors be considered but also the telecommuter must have full access to the company's technology in order to do the job properly. Following is a discussion of some of the prudent technical elements for the virtual office.

The Technical Factors

Following is a discussion of some of the present-day data-communication technology strategies used to enhance the workplace and home office environments.

Wide Area Networks

Up to this point, we have discussed networks within a close proximity (local area networks, LANs), which are crucial to networking. They form the access layer for users and their computers. Most of the communication that needs to occur tends to happen at this local level: employee to manager, employee to employee, etc. With the advent of the Internet and the plethora of databases, resources, facilities, and the globalization of companies, it has become common, if not imperative, to connect these LANs to each other and to the rest of the world. This is usually done by connecting to a wide area network (WAN) (Exhibit 2).

WANs differ from LANs in many respects.

- *Ownership:* LAN equipment (switches, computers, wires) are usually owned by the company. In a WAN, the equipment and actual service is leased from a provider. Providers include Regional Bell Operating Companies (RBOCs), long distance carriers, satellite companies, and cable TV firms. Usually RBOCs and long distance carriers are the predominant WAN providers as they have the infrastructure (wiring, etc.) in place around the world.

- *Reliability:* Due to the nature of WANs (size, capacity, and travel distance), they are far less reliable than LANs. Depending on the business need, this can cause a lot of hardship and often causes a company to install redundant or backup WAN lines to provide a measure of reliability.
- *Cost:* Rather than purchasing the equipment for a LAN at a one-time cost, a WAN is leased from a carrier. The service costs depend on travel distance, speed desired, protocol used, and contract length. Typically, line costs are billed monthly, e.g., a T-1 line from New York City to California can range from $300 to $1500 per month.
- *Protocols:* With LANs, the most common encapsulation methods are Ethernet (predominant) and Token Ring. WANs use a different set of protocols. An understanding of each is prudent, given the decisions that one has to make regarding WANs.
  - *ATM (asynchronous transfer mode [not Automatic Teller Machine]):* A strategy that came to fruition in the 1990s and was supposed to be the WAN and LAN panacea. ATM is widely used in WANs and is a packet switched, highly efficient method with an excellent quality of service (discussed later) and reliability.
  - *Frame relay:* A cost-effective packet switching technology that has risen to a very high rate of popularity.
  - *Point-to-point circuit:* With a point-to-point circuit, wires are allocated for use between two points (such as New York City and Indiana).
- *Speed:* LANs usually operate in the 10- or 100-Mbps (million bits per second) speed range; WANs operate at a much slower speed. A typical organization will have WAN speed of 1.5 Mbps (T-1 line) or a fraction thereof (768, 384, or 56 kbps). We experience this potential bottleneck with our dial-up connection to the World Wide Web (Web) (typical dial-up speed is 28.6 kbps). Of course, we can increase the speed of our connection in the WAN but at a much higher cost. WANs are considered Hardware-Defined Networks (HDNs) and they have dedicated hardware and physical media assigned to them. The next section looks at alternatives to HDN.

Virtual Private Networks

When we think of networks, we think of physical circuits that connect user devices together. In order to link an office in New York City to a manufacturing plant in Indiana, we connect or build a regional circuit that connects these two points together as an HDN.

To make the use of physical circuits more efficient and more cost-effective for the user, virtual private networks (VPNs) are created and constructed over the physical public-switch networks. VPNs are Software-Defined Networks (SDNs) that can leverage usage of the public network (Exhibit 3).

The software definition comes from commands given to the network that allocate bandwidth capacity to the user. Virtual refers to the nature of the network, meaning that when the user no longer needs the circuits (for example, the manufacturing plant in Indiana is closed for the day), its bandwidth can

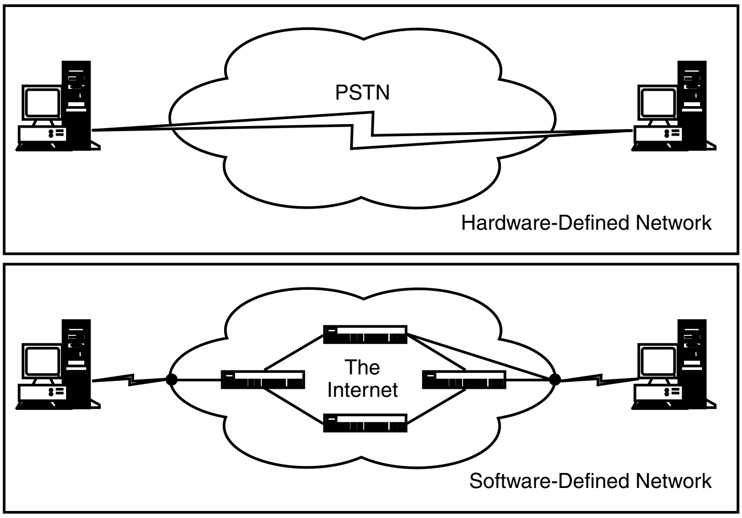


Exhibit 3 Hardware-Defined Network versus Software-Defined Network.

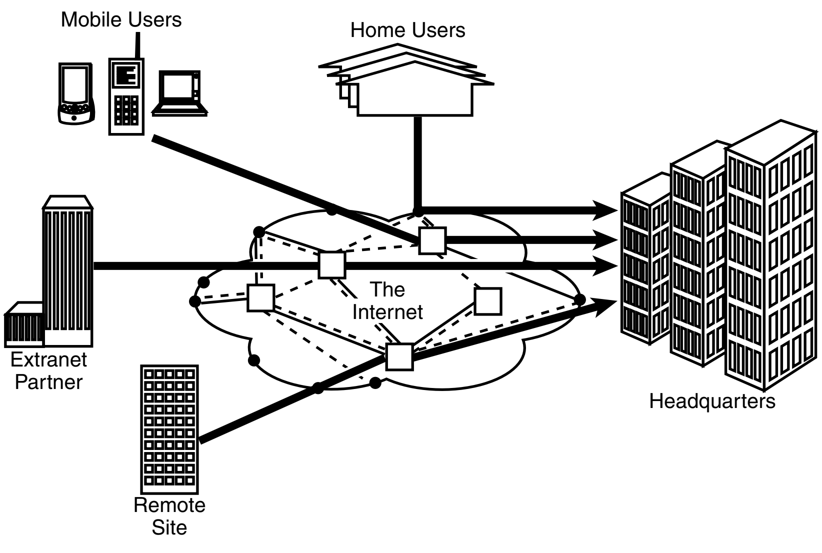


Exhibit 4 Virtual private network.

be quickly reallocated for other users. Private means that the bandwidth is for your use only, and during the transmission the packets get encrypted, implying that only the sender and receiver can read the information.

Why do this? HDNs give you the same capabilities as VPNs but at a higher cost and with lower flexibility (Exhibit 4). For the phone company to put up an HDN is laborious, slow to implement, and extremely costly. A VPN can be put up in a fraction of the time and is far less costly. Depending on whose data you choose to pay attention to, VPNs usually cost 30 to 50 percent less than an HDN and can be set up in much less time.

There are numerous providers of VPN services across the United States. All major carriers and many smaller firms implement VPNs. These services provide communication between most major U.S. cities and worldwide cities. Speeds allowable through a VPN run the gamut of business' needs, ranging from 56 kbps to T-3 circuits.

By making network reconfiguration easier (defined by software, customizable from a keyboard), the implementation costs are lower and the savings are passed on to the consumer.

Fast Ethernet, Giga Ethernet, and the Future of Speed

When Ethernet first appeared, it came with a speed of 10 Mbps, which was more than adequate. Using the networks for applications such as e-mail, file transfer, and remote log-on, the network was more than capable of effectively carrying these packets.

As networking became more popular and as more people were connected to the network, congestion began to grow. As you may recall, all computers (users) on a network segment share the same capacity. Typically, when a network starts hitting 50 percent of its capacity, collisions occur. These collisions start a downward trend in network efficiency, and when a network reaches 60 to 70 percent of its rated capacity, it becomes a traffic jam, totally ineffective.

The increased user population is coupled with a rise in network applications and a dramatic increase in network traffic. Starting in the early 1990s, people began using the Web to download information. This information, in text, audio, and even video form, required more packets to be transferred, resulting in more traffic on the network. As a result, networks started to become very ineffective. One of the solutions that was sought was to increase the packet transmission speed.

Ratified in 1996, the Institute of Electrical and Electronic Engineers standard for fast Ethernet came to the rescue. By increasing the speed tenfold, the performance of networks was enhanced. Fast Ethernet (also referred to as 100BaseT or 100BaseX) is an upgraded version of the traditional 802.3 Ethernet comprised of three data link protocols that provide 100 Mbps of throughput using standard Ethernet topology, standard Ethernet data link packets, and the standard CSMA/CD access protocol (discussed in previous chapters). The three common data link protocols differ only in the physical media used (allowing companies to use the capability they already have installed in their buildings). The three data link protocols are:

- *100BaseTX:* Uses Category 5 unshielded twisted pair cable. By far, 100BaseTX is the most common data link protocol, attesting to the installed base of Category 5 UTP in the world.
- *100BaseFX:* Uses multimedia fiber-optic cable.
- *100BaseT4:* Uses Category 3 cable (all four pairs of wires in this cable).

Network bandwidth, like closet space, is never enough and, by the late 1990s, Fast Ethernet began to reach its limits and the next generation or

Exhibit 5 Specifications for 10, 100, and 1000 Mbps Ethernet

Name	*Maximum Data Rate*	*Physical Media*	*Maximum Distance*
10BaseT	10 Mbps	UTP CAT 3 or CAT 5	100 meters
100BaseT	100 Mbps	UTP CAT 5, Fiber	1.2 miles
1000BaseT	1000 Mbps	UTP CAT 5, UTP CAT 5E, CAT 6, Fiber	1.2 miles
10 Gbps	10 Gbps	UTP CAT 5E, CAT 6, CAT 7, Fiber	1.2 miles

plateau was needed. Ratified in the late 1990s, Gigabit Ethernet began to appear in the marketplace. Used predominantly in backbone networks, Gigabit Ethernet (also referred to as 1000BaseTX) provided for 1000 Mbps of speed, a tenfold increase over Fast Ethernet (Exhibit 5).

At the time of this writing, the specifications for 10 Gigabit Ethernet are being sent through the ratification process. Clearly, the industry effort is on Ethernet, and not Token Ring or ATM, for LAN technologies. The effort is necessary to increase network speed to compensate for increasing numbers of users and traffic due to multimedia applications. Will there be a limit to how high the speed of Ethernet can go? Your guess is as good as mine.

VLANs

As discussed in previous chapters, a LAN is a series of cables, network interface cards (NICs), networking elements, and software that exists in a local area (usually under 2 kilometers). LANs provide connectivity between user devices, and between inside and outside resources. As one can imagine, much of this connectivity is at the physical level, i.e., the cabling, the NICs, and the networking equipment.

An interesting approach used with LANs is the application of VLANs (virtual LANs). Although the physical components are still necessary, the actual physical entry point of the VLAN does not dictate where on its network a user device is located; its location is dependent on software-defined elements.

Making an analogy to the public phone system, if you call your home phone, it will ring at your physical home location; but suppose you forward all incoming calls to your cell phone. When your home phone number is called, your cell phone rings, no matter where it is. Your physical entry point to the system is the same but the logical location (your cell phone) is dependent on the program your calls are forwarded to.

VLANs are very effective when physical placement of computers is different than logical placement. For example, suppose the third floor of a building is staffed with sales personnel who need to be on the same LAN segment as they communicate frequently with each other and share the same resources (printer, data files, etc.). A new salesperson is hired but there is no more room on the third floor. A cubicle is set up on the tenth floor for the new employee, or perhaps the employee is set up to work off-site. In either case,

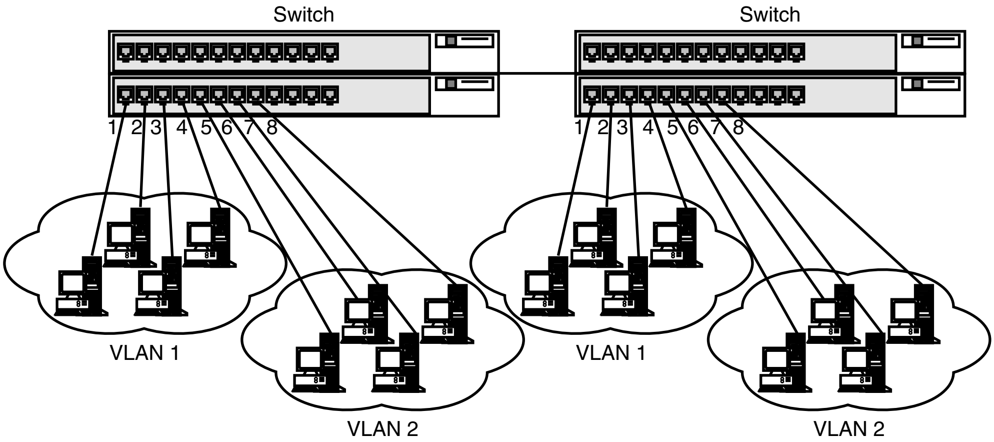


Exhibit 6 Port-based virtual local area network.

it needs to appear to the network that the employee is on the third floor (logically), although this is not the case physically.

VLANs come to the rescue. The heart of the VLAN is the network switch. You may recall that the switch is a piece of network equipment that acts on the media access control address of a network device. Smarter than a hub but less capable than a router, a switch is the key element in a VLAN. Think of VLANs as logical and not physical groupings of devices.

There are three major types of VLANs: (1) Layer 1 or port-based, (2) Layer 2 or MAC-based, and (3) Layer 3 or protocol-based.

Layer 1: Port-Based VLANs

A Layer 1 VLAN identifies the logical location of the end-user device, depending on which port of a switch the device is plugged into. The switch is "programmed" to determine which port belongs to a specific VLAN. In Exhibit 6, switch 1 has ports 1 to 4 in VLAN 1, and ports 5 to 8 in VLAN 2; switch 2 has the same configuration. All computers plugged into either switch on ports 1 to 4 are in VLAN 1 and ports 5 to 8 are in VLAN 2.

Port-based VLANs do not work in the tenth-floor and off-site scenarios described earlier; however, in the case where two separate departments, perhaps accounting and engineering, are on the same floor, this method works well.

Layer 2: MAC-Based VLANs

Our original problem of the new salesperson working off-site can be solved with MAC-based VLANs (Exhibit 7), where membership in a particular VLAN (logical group) is based on the MAC (Layer 2) address of the computer.

In this instance, the network administrator programs the switch to act as if a particular series of MAC addresses are part of the same logical grouping. Thus, no matter what switch a telecommuter is connected to, that person can

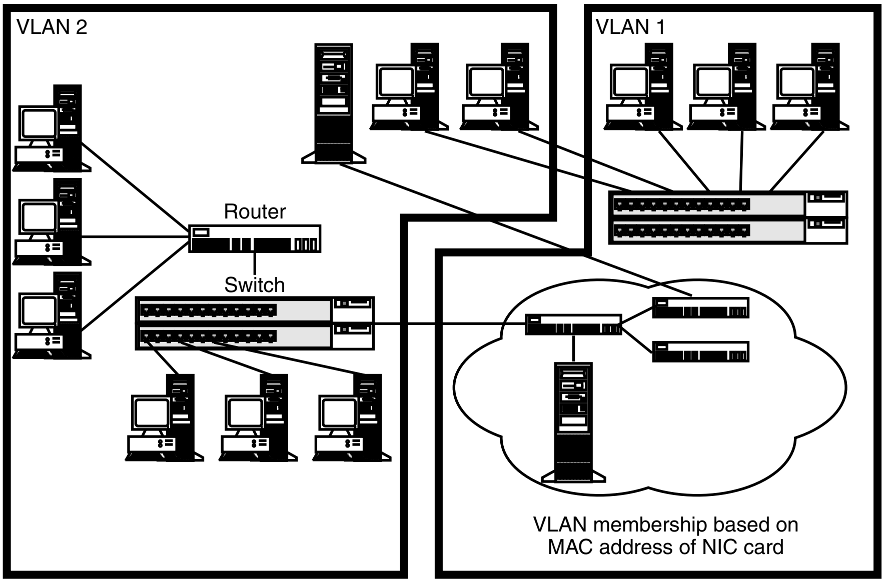


Exhibit 7 Media access control address-based virtual local area network.

be put into the same logical group (VLAN) as his peers, based on the MAC address (in the NIC) of his computer.

Layer 3: Protocol-Based VLANs

Another approach is to program the switch to put different computers in different VLANs based on the language (protocol) it speaks (Exhibit 8). For example, all machines speaking TCP/IP can be in VLAN 1, and all machines speaking IPX/SPX can be in VLAN 2. Assuming people in similar departments are using the same protocol to access their data, this approach works very well.

It makes all the sense in the world to put people of similar functions into similar departments; likewise, it makes sense to group them into similar network segments. With VLANs, any person can be put in any VLAN (logical group) based on the Layer 1, 2, or 3 information.

The only downside to VLANs is their administration. The switch must be programmed (at either Layer 1, 2, or 3) to put users in the appropriate VLAN. Personnel must do the programming and keep accurate records so that user devices are in the right logical groupings. Depending on the size and scope of the organization, this can be a laborious job, especially when originally being implemented.

Quality of Service (QoS)

QoS is the Holy Grail that data network personnel and users are seeking. Simply put, QoS is a technique used to assure that the applications running on the network get the adequate resources they need.

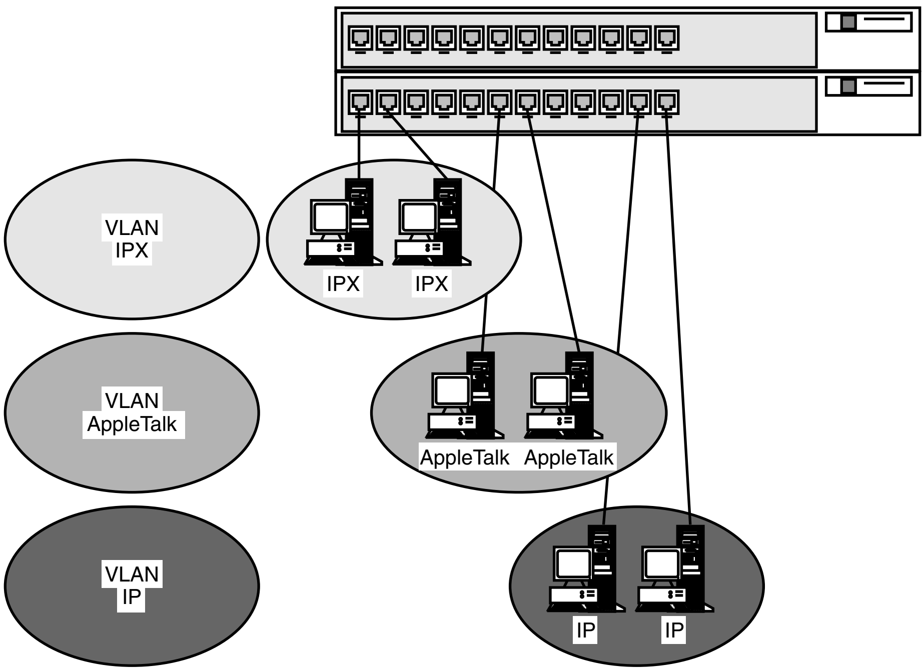


Exhibit 8 Protocol-based virtual local area network.

Many things (such as e-mail, voice communication, etc.) can hog a network and therefore stop applications from working well. Among them are:

- The contention-based nature of Ethernet. Because all computers on a network segment are vying for the same resource, there is no guarantee that anyone will get through.
- Long messages often are broken up into different packets (by the TCP portion of TCP/IP). Because the message is now in different packets, the packets may not arrive in the same order they were sent.
- There are always bottlenecks in a network that slow down the delivery of packets. If you recall from a previous section, WANs have a very slow speed, compared with LANs and are therefore potential bottlenecks.

All of these factors inhibit packets from getting from source to destination in a timely manner and can inhibit quality of service.

For simplistic data communication needs, e-mail, file transfer, and web browsing, the quality needed is low, and most networks perform admirably. If your e-mail takes two seconds to go to the intended receiver, you will probably never notice the delay. If the packets arrive out of order, TCP reorganizes them in the right order. Even if you need to wait an extra second while Web browsing, you are satisfied.

Real demands on QoS come with applications that contain voice and video (sound and pictures). Not only are voice and video applications large in packet size (a single video picture requires a transfer of 150 Mb of information), they also must arrive in real- or synchronous time. Imagine having a phone call

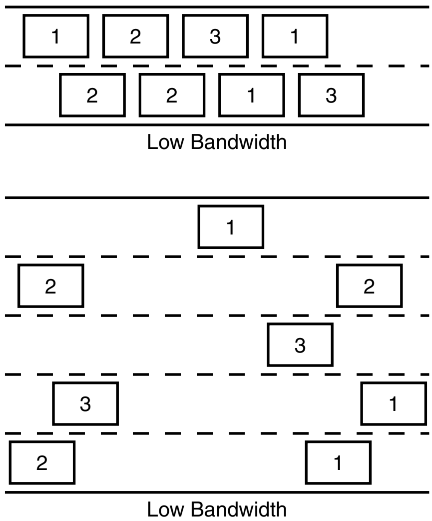


Exhibit 9 Quality of service bandwidth strategy.

with a person and the words come through jumbled, delayed by 10 seconds, out of order, or missing. The same with video pictures, each frame (60 times per second) must arrive quickly and in the right order so that the eye does not perceive a disruption in motion (video is discussed in Chapter 12). To ensure that these types of applications work effectively, there must be a QoS mechanism in place.

There are two general approaches to achieve QoS:

1. Increasing bandwidth
2. Prioritizing packets

Using the bandwidth strategy (Exhibit 9) requires building enough capacity into the network for all packets to get through without delays or errors. To create an analogy, this is like building an interstate highway system with 50 lanes. A move from the standard two lanes to fifty lanes almost guarantees that all traffic gets through quickly and efficiently, without delay. As you would expect, this strategy is expensive and resource-intensive but usually works. Utilizing high-speed strategies (Gigabit Ethernet or Fast Ethernet), this approach is a simple, expensive, but not-so-elegant method.

Using the prioritizing strategy (Exhibit 10) is a whole different approach that involves "tagging" each packet with a prioritization code and sending the prioritized packets through the network first. The prioritized packets are time- or message-sensitive. Referring back to the analogy about the interstate highway system, there is some traffic that should get priority: ambulances, fire trucks, or police cars are examples. Even when the road is crowded, sirens and lights clear a path and provide ease of transit.

Which packets get the priority? Typically, the packet that must arrive in real-time gets the priority 1 code. Voice and video packets must arrive quickly

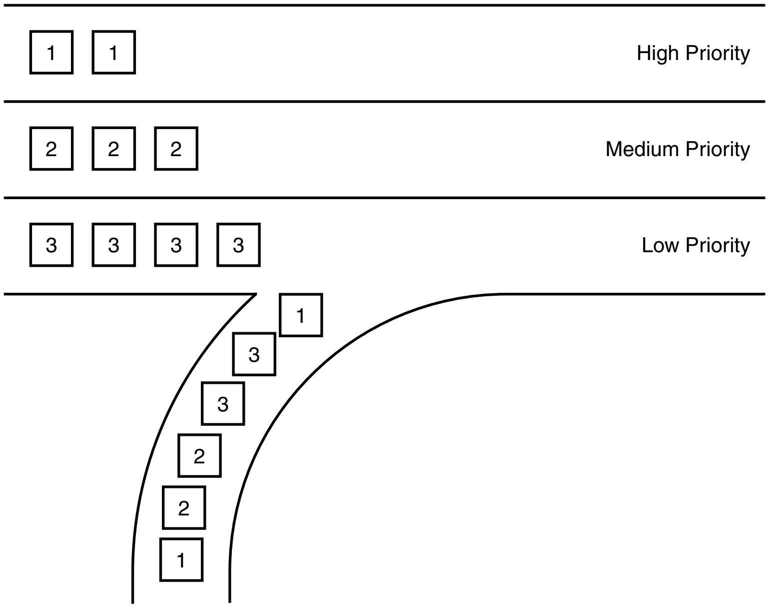


Exhibit 10 Quality of service prioritization strategy.

and in the proper order for us to comprehend the information clearly. The packets that get the least priority are e-mails, which can arrive in one second or ten and no one would notice; if e-mail packets arrive out of sequence, TCP reassembles them properly.

Although there are some standards for QoS, there are many more proprietary approaches that work with single-vendor products only. This continues to be an area that needs more work and standardization but is necessary for the data communications network to be viewed as *the* network-carrying all of our information on a single set of wires.

Network Security

An important element in everything we do is security. Whether locking a car door, or hiding a wallet, we all take some precautions for security against the predators in the world. If the data communications field and the Internet are to become places in which the public puts its confidence to send important financial information, these areas must be made secure.

To make a data network secure, three basic elements must be taken into account:

1. *Authentication:* Guarantees the person at the other end is who he or she claims to be.
2. *Encryption:* Ensures the safe transit of information through the network.
3. *Accounting:* Ensures all network elements are credible and that the network is not being compromised.

Exhibit 11 Secure ID card.

Authentication

Authentication is the process of ensuring the person with whom we are communicating is who he claims to be. In a phone conversation, we recognize a person's voice; in a face-to-face meeting, we recognize a person's facial features and mannerisms. In an e-mail or a paper file it is much harder to tell. There are three basic categories of authentication applied to data communication that provide a measure of authentication security.

1. *What you know.* A password is a good example. When you log on, you provide your account name and password, and the computer lets you use all its functions. When an e-mail comes from John, we assume he, and only he, knows his password.
2. *What you have.* More complex and secure systems demand that you know your password and have a device, typically a credit-card-looking device, that gives out random security numbers. When you enter this security number, the system recognizes it as valid (Exhibit 11).
3. *What you are.* The most secure system also requires physical evidence of your identity, typically garnered through a retinal scan, a voice recognition system, or a palm-print scan.

The security needs of your data communications network and the data you must protect dictate the approach to authentication you will use. Obviously, the most popular and least secure is the what-you-know password system. People typically choose their birthdate, the names of their children, or their own names as passwords and write them in their wallet or on the computer, practices that lead to potential security breaches.

Encryption

Although packets are in digital form as they traverse the network, it is easy to view them to see what information they contain. They can also be stolen

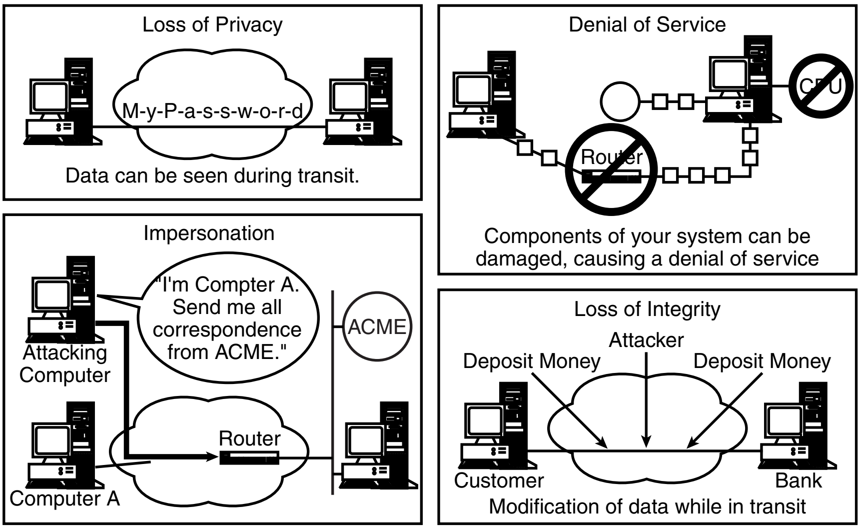


Exhibit 12 Security breaches.

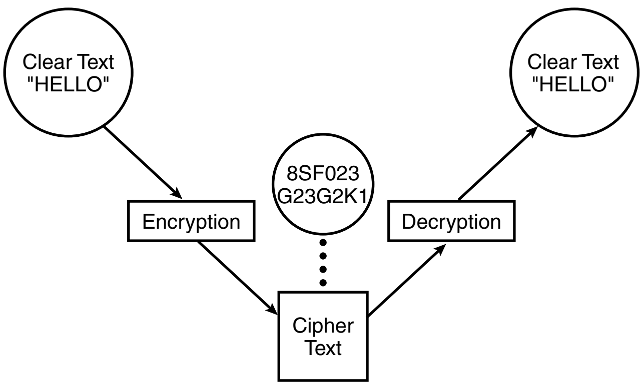


Exhibit 13 Encryption scheme. H = 8S, E = FO, L = 23G, O = 2.

or corrupted. When you send your password over a network, a criminal can view the password and use it later to log on as you. When you send your credit card number over a network to make a purchase, a criminal can steal the number and the transaction for later use (Exhibit 12). To prevent this from happening a technique called encryption is used.

Encryption works by substituting different symbols for the real ones using a predetermined code. For example, if A = 3, B = 4, and C = 5, then ABC = 345 (Exhibit 13). Because the language has certain pattern to it, encryption codes can be easy to break. As the encryption code gets larger, it is harder to break; theoretically, there are encryption codes with random keys that are impossible to break. A common encryption used today is Ipsec, which uses a 256-bit encryption key. Although not impossible to break, it takes a lot of resources, brain power, and time to do so. This is considered a good level of encryption and security.

Exhibit 14 Computer Emergency Response Team/Coordination Center Charter

Provide a reliable, trusted, 24-hour, single point of contact for emergencies.

Facilitate communication among experts working to solve security problems.

Serve as a central point for identifying and correcting vulnerabilities in computer systems.

Maintain close ties with research activities and conduct research to improve security of existing systems.

Initiate proactive measures to increase awareness and understanding of information security.

Accounting

The most mundane of the security triad, accounting is still an essential part of security. Accounting means active auditing of all network devices, logging of all activity on the network, and monitoring all events. If we suddenly saw ten more computers on the network than are authorized, we should start to wonder; if the log for the previous night shows someone repeatedly trying passwords to get into an account, we should step back and think. If the traffic flow changed from normal to extremely heavy without an obvious reason, we need to consider if criminals are breaking in. If a key engineer requests payroll data from the system, we should become suspicious.

Accounting is a laborious job that requires manpower and equipment to review logs, monitor the network, and watch for anything different; but without accounting, our system can be compromised and used against us.

The Regulatory and Legal Factors

Unfortunately, there are people in the world who try to break the security of our networks and computers. In fact, there are bands of people holding conferences, exchanging information, and doing whatever it takes to break down the world of data communication. IT professionals are trying to protect their businesses and data against these hackers. There is help for them.

In 1988, a worm was introduced into the old Internet (DARPA network) which brought 10 percent of the system to its knees. Seeing the growth of data communication and what can happen when hackers try hard, the federal government established the Computer Emergency Response Team/Coordination Center (CERT/CC). See Exhibit 14 for a list of CERT/CC's primary duties.

Funded by the federal government and located at the Software Engineering Institute at Carnegie Mellon University in Pennsylvania, CERT/CC has served its purpose well. It is a center where the "good guys" can go for solutions and to report problems. When a virus is introduced, it is usually the CERT team, working in conjunction with the antivirus vendors, that solves the problem and provides a fix. Additionally, CERT/CC publishes books, security alerts and notes, and provides training on security measures.

In the first three quarters of 2001, almost 35,000 problems were reported; remember, each of these problems can affect hundreds if not thousands of people. During this time period, CERT/CC also discovered almost 2000 vulnerabilities in software that it reported to the vendors for resolution. The majority of problems are reported to CERT/CC via e-mail (85,000 in 2001) but some are reported via hotline calls (more than 1000 in 2001). CERT/CC can be contacted at www.cert.org for more information or to seek resolution to a security issue.

Summary

In this chapter, we began to see how the basic building blocks of networks can be applied to human and business needs. Specifically, the idea of telecommuting was brought out with its unique characteristics and elements.

The technical factors of wide area networks with different protocols and unique attributes were discussed. We learned about virtual private networks which reduce costs and ensure privacy over the Internet through the use of encryption. The evolution of Ethernet through 10 Mbps to 1 Gbps with its impact on network use was discussed. Various forms of VLANs (port-based, MAC-based, protocol-based) and how they can help companies keep employees in logical groupings, regardless of physical location, was discussed next. QoS was discussed as it relates to ensuring that applications such as voice and video information work properly over the Internet. And finally, security was discussed in relation to its need for securing our data. The three elements of security, authentication, encryption, and accounting, were examined.

How can the technical elements work to help the problem of telecommuters located away from the corporate office and the information they need to do their jobs? Using a VPN as a cost-effective and secure method allows telecommuters secure access to corporate data. Providing a VLAN to the telecommuter puts him in the right logical location so that he can easily communicate with the network. Ensuring QoS for the telecommuter allows for voice traffic to the corporate office, reducing costs to the employer. And finally, guaranteed authentication aids employers and employee in assuring that data is not misused.

Exhibit 15 describes a case study that illustrates these lessons.

Data communication fits human and business needs. (This chapter showed how the basics of data networking can be used to aid the telecommuting business culture.)

Questions for Review

True/False

1. VPN stands for virtual personal network.
2. Software-Defined Networks are sometimes called virtual private networks.

Exhibit 15 Case Study: A Little Security[a]

Many organizations are deploying VPNs to secure remote access or to protect wireless networks, and handheld devices should not be excluded from these security measures. Certicom's movianVPN client allows Pocket PC and Palm users to connect their devices to VPN gateways using the IPsec VPN standard.

The easy-to-use movianVPN client works with eleven of the leading VPN gateways, including those from Check Point, Cisco, Nortel, and NetScreen. The client software is different for each gateway, supporting many of the gateways' features and functionalities, leading to higher interoperability levels. The client supports the most features with Cisco and Nortel VPN gateways. For example, movianVPN currently supports NAT Traversal with the Cisco VPN gateway.

Configuring the movianVPN client entails completing several steps. First, users define the vendor and IP address of the remote gateway. The information requested next depends on which gateway the user is using. In general, a user ID and password (preshared key) are entered, as well as the IP address or subnet on the remote network. Users also configure the IPsec options, such as encryption scheme, hash, and Diffie-Hellman Group (movianVPN supports elliptic curve cryptography, or Diffie-Hellman Group 7). Most of this information should either be configured by an administrator or be given to the user with specific instructions. The client includes several diagnostic and troubleshooting tools, such as a ping utility and IKE (Internet Key Exchange) log to troubleshoot IPsec VPN errors.

[a] Mandy Andress, *Infoworld,* January 18, 2002

3. Virtual private networks provide a high level of data security.
4. WANs cover a small, limited geographic area.
5. Authentication is the process of ensuring the person we are communicating with is who he claims to be.
6. There are generally three approaches to QoS.
7. MAC addresses are contained on the network interface card.
8. Two to three percent of the American population does some type of telecommuting.
9. Telecommuting reduces costs to employers.
10. A VPN costs up to 50 percent less than an HDN.

Multiple Choice

1. VLAN stands for:
   a. Virtual logical address nomenclature
   b. Virtual local area network
   c. Very large area network
   d. Various local area network
2. What does ATM stand for?
   a. Automatic teller machine
   b. Automatic transfer mode
   c. Asynchronous transfer mode
   d. Authentic telecommuter messaging

3. The technique of scrambling data to make it unreadable as it travels the Internet is called:
   a. Encryption
   b. Packet switching
   c. VPN
   d. VLAN
4. A wide area network is best described as:
   a. A network that covers a large geographic area
   b. A network that covers only a small area but connects several buildings within that area
   c. Another name for the Internet
   d. Two computers connected by a modem
5. The most popular type of LAN is:
   a. Token Ring
   b. Ethernet
   c. Fiber-optic
   d. Telephone system
6. A virtual private network is an example of:
   a. A Hardware-Defined Network
   b. A Software-Defined Network
   c. The Internet
   d. QoS
7. What is frame relay?
   a. A LAN protocol in which only the workstation that has a token has the right to send information
   b. A video technology that enables the frames of a video picture to move quickly enough to provide fluid motion
   c. A popular, cost-effective packet switch technology used in the WAN arena
   d. A wiring scheme in the local area network arena
8. A Layer 2 VLAN is also called a:
   a. VPN
   b. MAC-based VLAN
   c. Port-based VLAN
   d. Wide area network
9. Ethernet is available in which of the following speeds?
   a. 10 Mbps
   b. 100 Mbps
   c. 1000 Mbps
   d. All of the above

Short Essay Questions

1. Define QoS.
2. What is a Hardware-Defined Network?
3. What is a Software-Defined Network?

4. What three elements must be taken into account for a network to be secure?
5. Give three job classifications that can benefit from telecommuting.

This page intentionally left blank

Chapter 11

The Wonderful World of Wireless

In this chapter, we will explore the wonderful world of wireless communication. Wireless technology comes in many shapes and sizes that we see every day: simple devices such as the TV remote control and garage door openers, and more-complex devices such as cellular telephones, personal digital assistants, and satellite-based TV. Wireless is pervasive in our personal and professional lives. The scope of wireless is so wide that it would take a full book, if not a series of books, to explain the entire field.

In order to keep things simple and within the constraints of the purpose of this book, we will explore only one application of the world of wireless: wireless local area networks (WLANs). Although WLANs are only one small part of wireless, they have the same essential components and elements of all wireless systems, thus the basic principles can be brought forward. Additionally, WLANs build on the local area networks (LANs) that we have discussed in the previous chapters. WLANs are a tremendous growth area and promise to be an integral part of our everyday personal and professional lives.

The Business and Human Factors

Due to the fast and ever-changing needs of the customer, businesses also must change quickly. You want to return your rental car fast before you catch a plane. The doctor wants to see your x-rays from the previous year. You want to check the price on a piece of clothing you are buying. All are examples of how we need quick and readily available access to information. In order to do this, technology must be flexible, adaptable, and easily changed. WLANs fit this bill well.

The following are the major situations that WLANs fit into:

- *The need for remote access to data:* In the warehouse, retail, and medical fields, personnel are all over the workplace and need to quickly access and enter information for customers. Examples are a retail clerk wanting to check the price of an item or a UPS delivery person wanting to verify a package location. WLANs provide access from the employee's location to the data and allow for entry and modification of data. Prior to WLANs, personnel had to find a wired terminal to complete these tasks.
- *Reaction to fast-changing situations:* A meeting is called, the attendees gather in a room and they need access to the Internet as well as to data on each of their laptop computers. All of this can happen in minutes with WLANs. Additionally, people are making fast changes in location between buildings and within buildings. Stringing new cable can be the answer but the time frame for completion is too long. WLANs provide previously unheard-of mobility and flexibility.
- *Hazardous and rough situations:* Sometimes the location or conditions do not permit ease of wire installation. For example, if a building contains asbestos, digging into floors and walls becomes expensive and lengthy. In a historic building where modifications are not allowed, WLANs provide the solution. For a home situation where wiring is either unsightly or difficult to accomplish, a WLAN can be put into operation easily.

WLANs are not meant to replace wired LANs but, as a supplement to unique situations, WLANs make a perfect fit.

The Technical Factors

The Basics of Radio Frequency

Before we discuss the exploration of WLANs, a bit of knowledge about radio frequencies, specifically the electromagnetic spectrum, is necessary.

Almost all occurrences in life happen in waves, specifically sinusoidal waves. We speak in sinusoidal waves. When you throw a rock in the water, sinusoidal waves form (Exhibit 1). To measure these waves, we measure the time it takes for one wave to complete one cycle from start to finish. This measure of time is called cycles per second (or cps), or more commonly Hertz (1 Hz; named after the person who discovered this natural sinusoidal waveform motion.)

Sinusoidal waves behave consistently and have certain characteristics:

- The higher the frequency, the more waves tend to behave like light. They travel in a straight line and do not bend (although they do bounce). The higher the frequency, the more the waves travel in a line-of-sight characteristic; there must be a clear path between the sending antenna and the receiving antenna.

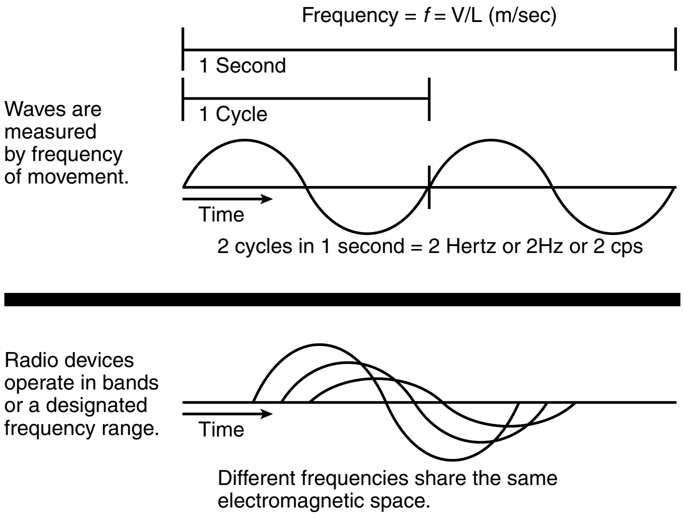


Exhibit 1 Sinusoidal wave form.

- Electromagnetic energy in the form of sinusoidal waves decreases in power exponentially as it travels further from the source. For example, 1 watt of power at 15 feet away from the antenna is only one quarter watt of power at 30 feet away. We also see this effect in light: as we move farther away from a light source, the light becomes dimmer. This is called attenuation.

We can hear sinusoidal waves in the air when there is a disturbance such as a noise or someone speaking. The lower frequency waves (around 20 cps or 20 Hz) sound to us like low rumbles — thunder is a good example of this. As the frequency increases up to 10,000 Hz (10 kHz), we can hear human speech. Most humans can hear from about 20 to 20,000 Hz (20 kHz). The lower frequencies sound like thunder and bass drums, the higher frequencies sound like whining or screeching. The waves that we can hear are at the low end of what is called the electromagnetic spectrum.

The electromagnetic spectrum (EMS) (Exhibit 2) does not stop where we stop hearing. It continues to increase and, therefore, many devices that operate at (can listen to) these different frequencies. As humans, we are sensitive to another portion of the EMS: light waves. Light and sound are parts of the same spectrum but we perceive them in different ways. Other devices (radios, TVs) listen and hear different parts of the EMS.

What Is a Wireless LAN?

WLANs are similar to wired LANs, the main difference being the physical media that connects the devices. Rather than using Category 5, coaxial, or fiber-optic wiring, the EMS is used. Because of this media change, WLAN

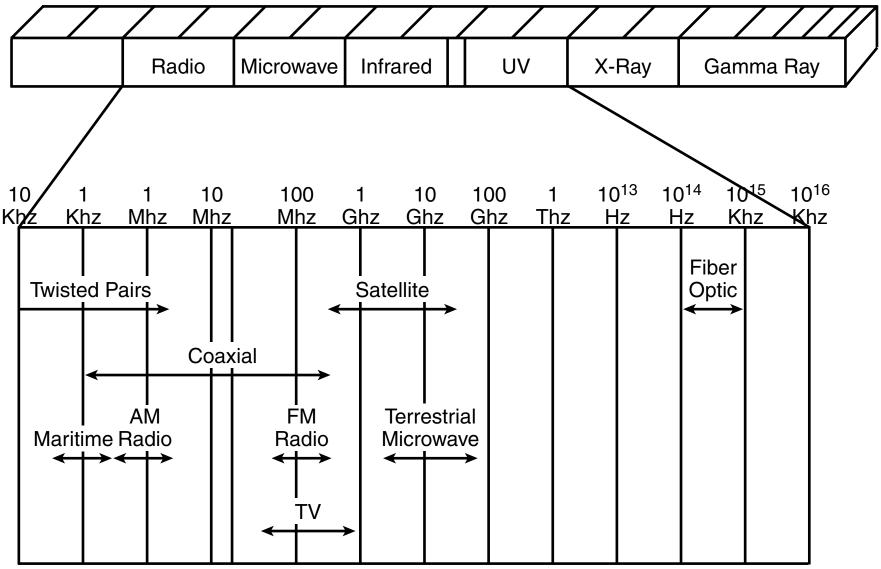


Exhibit 2 Electromagnetic spectrum.

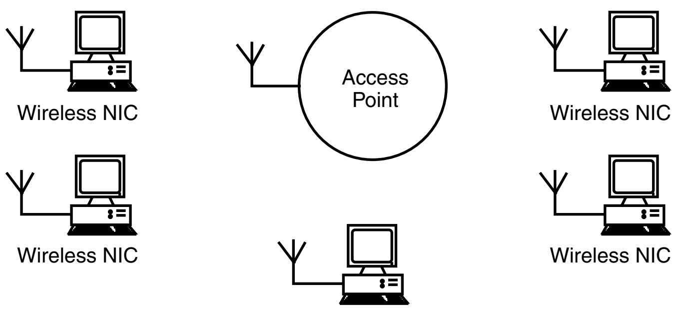


Exhibit 3 Elements of a wireless lan.

elements such as the network interface card (NIC) and the network equipment must be different. The major elements of a WLAN are (1) the access point and (2) the NIC (Exhibit 3).

The access point is where the wired LAN meets the WLAN. Connected to this access point is a wired connection (typically Category 5 UTP) that allows access to all the facilities and resources available on the wired LAN. The access point has an antenna that allows entrance to the radio frequency (RF) waves and to the WLAN. Think of an access point as a hub where each computer is connected to the network via radio waves.

The second major element of a WLAN is the NIC. Typically the NICs are used for WLANs in laptop computers. The NIC is generally of the PCMCIA format and has an antenna that allows connection to the access point. WLAN NICs are made for desktop computers also and come in varieties to match

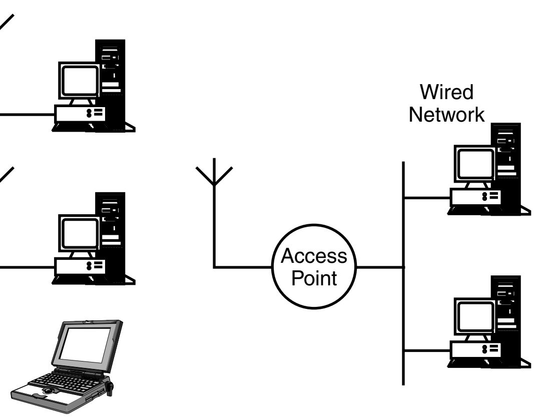


Exhibit 4 Wireless local area network with multiple devices.

the various bus structures of desktop PC architectures. The WLAN NIC also must be matched to the operating system. For example, most WLAN NICs support Windows 2000, 98, and 95, and many support Linux, UNIX, and OS-2. The support between the NIC and the operating system comes in the form of drivers that the NIC vendor supplies.

A single access point can handle many computers connected to it simultaneously. Think of an access point as a hub. Typically, an access point can handle 20 to 30 WLAN NICs and their different communication sessions. A separate NIC must be installed for each computer (whether portable or desktop) to be connected to a WLAN (Exhibit 4).

Many WLAN vendors allow ad hoc or peer-to-peer connections. Ad hoc connection has become a standard through IEEE Standard 802.11b. In this scenario, an access point is not necessary; the NICs communicate directly with each other. This is very useful for spontaneous meetings where the participants bring their laptops with them to exchange files. Of course, resources such as the Internet are not available in this situation (no connection to the wired LAN); however, for a very low cost and no prearrangement, communication can happen.

Things to Consider

There are five variables to consider when implementing a WLAN that affect its performance, its operating characteristics, and, of course, the cost:

1. Access technology
2. Frequency range
3. Antenna
4. Range and throughput
5. Interference

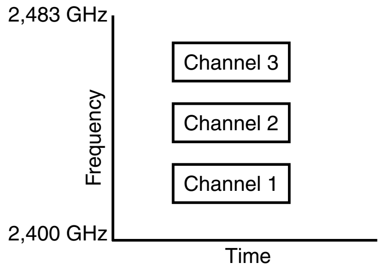


Exhibit 5 Direct sequence spread spectrum operation.

Access Technology

Access technology is the way that the WLAN puts information onto the radio frequency. It is a crucially important variable as it does affect WLAN performance and its operational characteristics. Although there are many access technologies used with wireless, two are predominant: (1) direct sequence spread spectrum (DSSS) and (2) frequent hopping spread spectrum (FHSS).

With DSSS, the packets are assigned to and sent over a specific channel (Exhibit 5). The channels, similar to TV channels, operate on a specific frequency; many channels can be on the same airways at any one point in time. These multiple channels allow different computers to operate at the same time without interfering with each other, similar to many people in a room all talking at once. Each person can speak with a different pitch (frequency or channel) without his voice mixing with that of another person.

The main advantage of DSSS is its ease of implementation and straightforward approach. Its main disadvantage is its susceptibility to interference. Because a particular channel is on a set frequency, interference on that frequency can cause the communication to be disrupted or lost. (Interference and WLAN standards are discussed later in this chapter.) The 802.11b standard selected DSSS as its preferred access technology.

With FHSS, a particular communication stream is broken down into sections and each section is put on a different channel or frequency (Exhibit 6). In addition, the frequency that these sections are placed on is constantly moving (hopping) around. The sections are then reassembled at the receiving end. This is similar to speaking each of your words at a different pitch (or frequency).

This may appear to be a complex way to do things but it gives FHSS its greatest advantage: resistance to interference. Because a particular communication stream is on different frequencies, it takes a large amount of interference to stop a full communication pattern. In this way, only small portions of the communication are lost and those small parts can be transmitted again without total loss of communication.

Frequency Range

The second variable to consider is the frequency range that the product operates within. The frequency range is important because it dictates the place

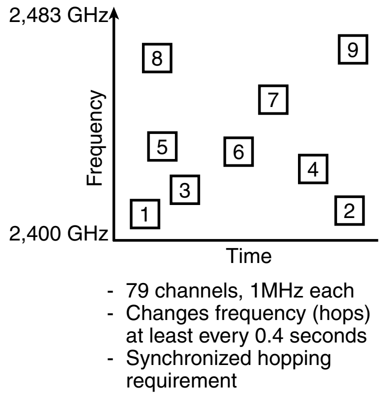


Exhibit 6 Frequency hopping spread spectrum operation.

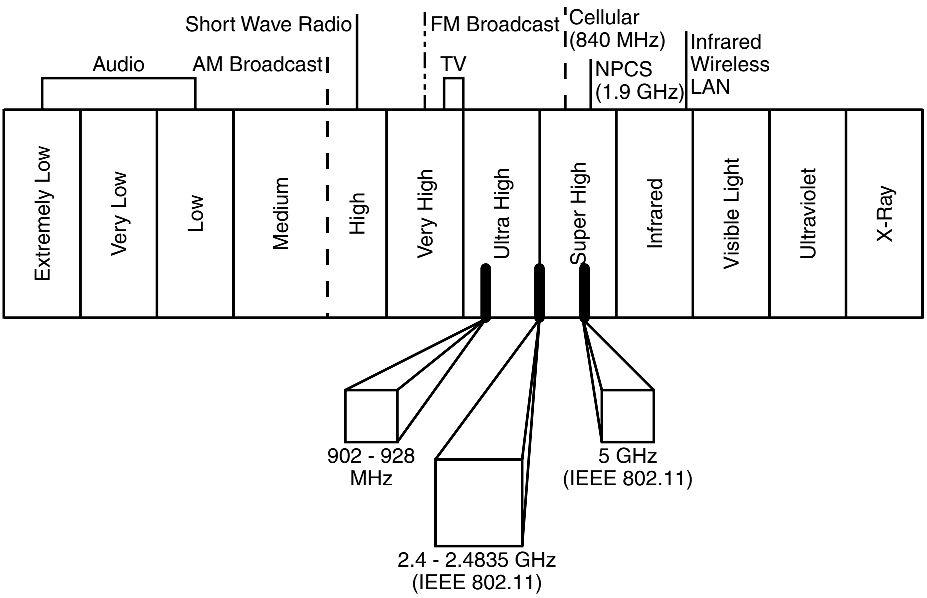


Exhibit 7 Wireless local area network frequency ranges.

on the EMS where the WLAN operates. There are three common frequency ranges or bands that WLANs operate within: (1) 900 MHz, (2) 2.4 GHz, and (3) 5.5 GHz (Exhibit 7).

The 900-MHz band was used first; however today's products do not typically use this frequency. This is the lowest frequency range for WLANs, so it has the greatest operational range. The 2.4-GHz frequency range is the most popular. It provides good operational range and many different channels where both access technologies can operate.

The 5.5-GHz band is used little today; however it will be used extensively in the future. This band provides a good degree of resistance to interference but suffers from range and line-of-sight issues.

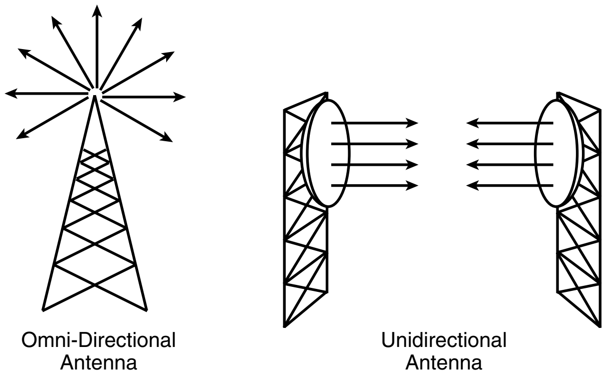


Exhibit 8 Omni- and unidirectional antennas.

Antennas

The third variable, the antenna, is the physical part of the WLAN where the electrical energy starts or ends its travels through the airwaves. Antennas are used both for transmitting (sending the electrical energy to the airwaves) and receiving (taking the electrical energy from the airwaves).

There are two basic types of antenna: omnidirectional and unidirectional (Exhibit 8). Similar to the difference between a standard light bulb and a floodlight, an omnidirectional antenna receives or transmits radio waves in all directions, a unidirectional antenna functions only in a specific direction (measured in degrees).

Omnidirectional antennas are most prevalent with WLANs as the two antennas (the access point and the NIC) are constantly changing their relationship to each other. Omnidirectional antennas seem very useful because they transmit in a 360-degree spherical arrangement. However, they lose focus, called gain, because the electromagnetic energy is transmitted in all directions, including straight up, straight down, and places where almost no one will receive it (see Exhibit 9). This is all wasted energy.

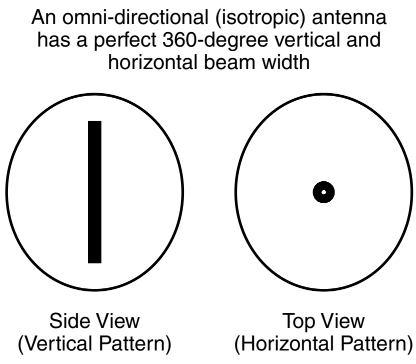


Exhibit 9 Omnidirectional gain.

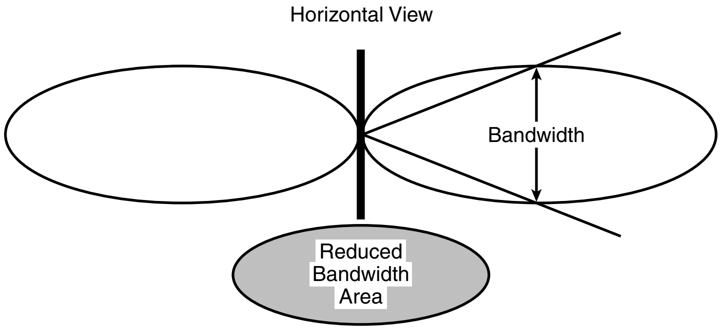


Exhibit 10 Dipole antenna design.

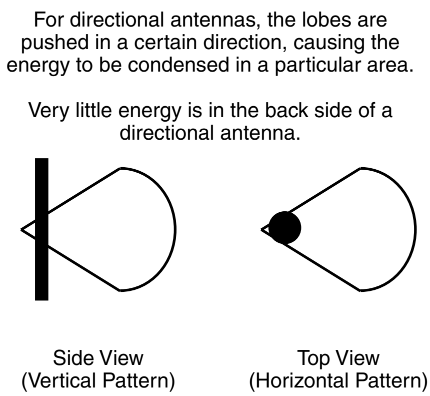


Exhibit 11 Unidirectional antenna.

A balloon is a good example of what an omnidirectional antenna does — putting out energy in all directions equally. Squeeze the top and bottom of the balloon. What happens? The sides expand and the balloon starts to look more like a doughnut as the air is pushed to the sides, making the sides bigger at the expense of the top and bottom. This same concept can be applied to an omnidirectional antenna, called a dipole antenna design

(Exhibit 10). A dipole has increased gain and range on the horizontal plane. Most WLANs access points use a dipole design.

A unidirectional antenna, like a floodlight, focuses the energy on the area where it is most needed, increasing its gain (Exhibit 11) and extending the range of the WLAN. Unidirectional antennas can be used effectively in a controlled environment. For example, students in a classroom sit in rows. If we make the assumption that they will have their computers at their seats, we can put a unidirectional antenna in the front of the room focused on the seats. This provides a higher gain, better communication, and more range.

Range and Bandwidth

The fourth variable in the use of WLANs is range and bandwidth (throughput), which are grouped together because they are related to each other as well as the other variables that we have discussed.

Range is the distance in feet or meters that the signal will travel. Similar to light, as range increases, power decreases. Throughput refers to the amount of information (packets) that can be put through (Exhibit 12). For comparison purposes, vendors list the maximum range of a product at the standard throughput. For example, 802.11b throughput is 11 Mbps. If a product range is given at 200 feet, you will get a full 11 Mbps throughput up to 200 feet; beyond 200 feet, the WLAN will continue to operate but you will get reduced bandwidth (reduced throughput). Be aware that these performance characteristics are seen in the most favorable conditions, e.g., in an open field where there are no obstacles to interfere with the transmission. In a typical office environment there are walls, windows, desks, concrete pillars, and other objects that interfere with and reduce the range of the WLAN.

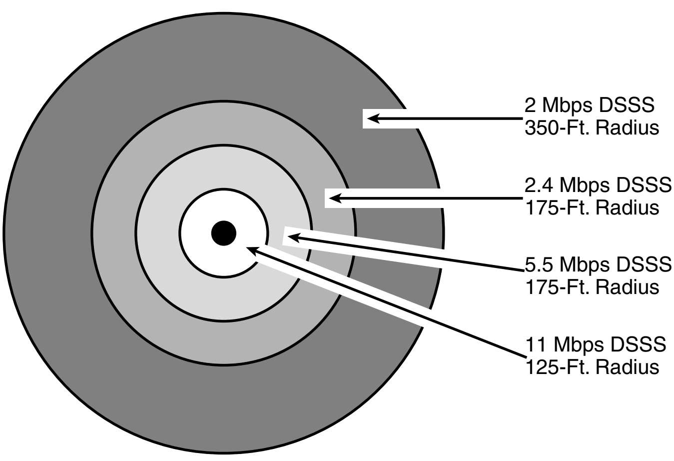


Exhibit 12 Range versus throughput.

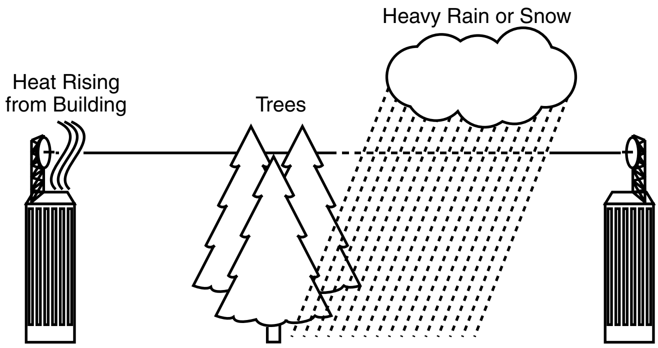


Exhibit 13 Possible causes of interference.

Interference

Interference refers to objects or conditions that reduce or stop the transmission of signals (Exhibit 13). The higher the radio frequency, the more the waves behave as light does. RF waves travel in straight lines and bounce off objects at right angles. The frequency range of WLANs is dictated and the two common frequencies (2.4 and 5.5 GHz) behave very much as light does. This means that all objects between the access point and the NIC cause some interference. Some objects (concrete walls, metal partitions) almost stop the transmission; other objects (wood walls, desks, or humans) just slow it down.

Interference is also caused by the operation of large motors and other power devices. Microwave ovens, heater fans, and electric motors create a band of interference that can travel quite far and interfere with WLAN transmission. Often it is necessary to move an access point away from these types of devices in order to assure proper operation.

Security

As we move from the wired LAN to the WLAN, network professionals have been forced to think more about network security to ensure that the data stays secure. They want to ensure that only authorized users are allowed on the network and that the data (now flowing around the airwaves) is not stolen or corrupted. The 802.11b standard defines a method providing access control and privacy on WLANs via wired equivalent privacy (WEP).

WEP uses a symmetric scheme where a key and algorithm are used to encrypt the data during transmission. The goal is to allow only authorized users on the WLAN and to ensure that the data cannot be stolen or corrupted as it travels the airwaves.

Although WEP sounds secure, most IT professionals warn that it should not be the only means of wireless security. WEP uses a 128-bit key for encryption and this has been shown to be vulnerable. The IEEE Task Group is currently working on providing more security to WEP for incorporation with future releases of the standard. The proposed new version will include different privacy algorithms and provisions for enhanced authentication.

The Regulatory and Legal Factors

Radio frequency is a scarce commodity. There are only a limited number of frequencies, so they must be controlled. Each country has its own government agency for controlling radio frequency; in the United States, it is the Federal Communications Commission (FCC). Because radio frequencies do not stop at an artificial national border, there must also be an international coordinating agency. The ITU (International Telecommunications Union) handles international disputes or issues concerning radio frequency.

In the United States, the FCC allocates licenses for frequencies to either the government (military, police) or to commercial firms (radio stations and mobile phone companies). The FCC assures that these transmissions do not interfere with each other. To operate at these controlled frequencies, the FCC grants a license to the operator.

The FCC has also allocated certain frequencies for industrial, scientific, and medical (ISM) use. Within these frequency bands, vendors can create devices that operate without licenses. Garage door openers and TV remote controls are examples of devices that are unlicensed because they are used within these ISM radio-frequency bands. WLAN operation falls within these ISM unlicensed frequencies. As previously mentioned, the 900-MHz, 2.4-GHz, and 5.5-GHz bands use unlicensed ISM frequency ranges.

Although unlicensed frequency bands have been allocated for WLANs, not all WLAN devices can operate together. In order for WLAN devices of different vendors to operate together seamlessly, there must be standards; the predominant standard for the WLAN is 802.11b. Modified from its parent 802.11 in early 2000, 802.11b provides rules for interoperability and sets the standard at 11-MHz bandwidth using DSSS. 802.11a was being released at the time this book was written, and it provides a 54-Mbps bandwidth for WLANs greater than 5.5-GHz.

However, even standards do not assure that devices will operate together because they can be interpreted differently by different people. An independent organization, WECA (Wireless Ethernet Compatibility Association) was created to test devices to assure their interoperability. When tested and passed, the WiFi logo appears on the product box, much as the Good Housekeeping seal of approval appears on consumer goods.

Summary

In this chapter, we explored some of the business needs for wireless devices, specifically wireless LANs. The ability to move data quickly and effectively, to adapt to the ever-changing environment of the business world, and to avoid hazardous spaces are all good reasons to implement wireless local area networks.

Exhibit 14 Case Study: Grand Ole Check-In[a]

Nashville's Opryland Hotel wants to keep its four million annual visitors zipping in and out. The world's largest hotel-convention center has installed an Internet reservation and wireless system to check guests in and out, process credit cards, print receipts, and program room keys at the curb or anywhere else in or near the hotel. The resort is using software from Inter-American Data and Lansa, smoothing guests' way from the get-go.

[a] Eileen Colkin, *InformationWeek,* 10/16/01

We explored the basic elements of wireless, sinusoidal waves, and characteristics of wave motion.

We looked into the basic elements of a WLAN and its operational characteristics. The NIC and the access port came out on the moving parts of a WLAN and we discussed five operational variables for WLANs: access technology, frequency range, antenna type, range and bandwidth, and interference.

We also looked at the agencies that control the electromagnetic spectrum in the United States, and the standards upon which current wireless LANs are based.

Exhibits 14 and 15 show two case studies that explore the lessons learned in this chapter.

Although WLANs are only a small part of the wireless world, they do characterize the fundamental elements of all wireless devices. You are encouraged to explore further the wonderful world of wireless, as it will certainly be a large part of the future.

Exhibit 15 Case Study: High-Speed WLANs to Debut[a]

At NetWorld+Interop in Atlanta, Intel plans to announce its Intel Pro/Wireless 5000 line of products that support the IEEE 802.11a specification, which pushes wireless connectivity as fast as 54 Mbps in the 5-GHz radio frequency band.

Intermec Technologies plans to introduce the MobileLAN 2106 Access Point that incorporates support for 802.11a.

WLAN systems currently in the market supporting the 802.11b standard are limited to 11 Mbps speeds in the 2.4-GHz band, which is also home to Bluetooth, HomeRF, and cordless phone links. The first generation of 54-Mbps WLAN products will likely be for specialized bandwidth-intensive applications such as engineering CAD designs or streaming video or audio but eventually 802.11a will see widespread adoption, according to Gemma Paulo, an analyst at Cahners In-Stat, in Scottsdale, Arizona. "Eventually 802.11a will take over 802.11b. It might take two or three years before this happens but eventually everyone will go with [802.11a systems]," Paulo said.

To help organizations phase in higher-speed systems, both Intel and Intermec are offering dual-mode capabilities for supporting both the current 802.11b standard and newer 802.11a. Intel will release a dual-mode expansion kit for enabling access points to service both networks, and Intermec plans to offer a line of dual-mode products.

Intel is targeting its first generation of 802.11a systems at the mid-size and small-enterprise segment, which officials at the Santa Clara, California-based company believe will drive wider market adoption. The Intel Pro/Wireless 5000 LAN Access Point will begin shipping in November, priced at $449. Also in November, Intel plans to ship a CardBus adapter priced at $179, and a PCI adapter priced at $229. Intermec's MobileLAN product line will be released in the fourth quarter, with pricing to be determined.

The race for dominance in the 802.11a space will heat up this year and early 2002, as vendors such as Cisco Systems, 3Com, and Enterasys Networks release products. Last month, Enterasys started shipping its dual-slot RoamAbout R2 WLAN access points, and expects to ship 802.11a PC cards by year's end.

[a] Cathleen Moore, *InfoWorld*, 9/10/01

Questions for Review

True/False

1. 802.3 is the current IEEE standard for 11 Mbps wireless connectivity.
2. In ad hoc mode, computers have no access to the Internet.
3. DSSS is more susceptible to interference than FHSS.
4. The access point is the physical part of any RF device where the electrical energy starts or ends its travels through the airwaves.
5. Omnidirectional antennas have increased gain and range on the horizontal plane.
6. Interference refers to objects or conditions that reduce or stop the transmission of signals.
7. WEP has to do with ways to avoid interference.

8. The 900-MHz, the 2.4-GHz, and the 5.5-GHz bands lie in unlicensed ISM frequency ranges.
9. The access point jack is where the wired LAN meets the WLAN.
10. Because people hardly ever move, companies do not make WLAN NICs for desktop computers.

Multiple Choice

1. Which of the following is a reason that a company might opt for a wireless (rather than a wired) local area network?
   a. Mobility
   b. Faster setup time
   c. Easier setup procedures
   d. Building restrictions
   e. All of the above
2. One cycle per second is commonly called one what?
   a. Megahertz
   b. Furlong
   c. Megabyte
   d. Hertz
   e. Byte
3. What does NIC stand for?
   a. Network and Internet carrier
   b. National Internet center
   c. Network interface card
   d. National integration carrier
   e. Network and Internet card
4. What is the name of the hardware device that allows the wired network to connect to the wireless network?
   a. Access point
   b. Antenna port
   c. External point
   d. Eternal port
   e. Serial port
5. What is another name for a peer-to-peer connection?
   a. Ad junk
   b. Ad lib
   c. Ad nauseum
   d. Ad hoc
   e. Ad dend
6. What does DSSS stand for?
   a. Different spectrum send simultaneously
   b. Direct sequence spread spectrum
   c. Different sequence spread simultaneously
   d. Direct spectrum send sequence
   e. Different sequence send simultaneously

7. What is the difference between DSSS and FHSS?
   a. In DSSS, the sending frequency stays the same; it changes in FHSS
   b. In DSSS, the sending amplitude stays the same; it changes in FHSS
   c. In DSSS, the sending carrier stays the same; it changes in FHSS
   d. In DSSS, the sending sequence stays the same; it changes in FHSS
   e. None of the above
8. Which of these frequency bands is not commonly used in WLANs?
   a. 900 MHz
   b. 2.4 Ghz
   c. 3.2 Ghz
   d. 5.5 Ghz
   e. All of the above
9. Which antenna type is not commonly used in WLANs?
   a. Undirectional
   b. Omnidirectional
   c. Dipole
   d. Omnipole
   e. All of the above
10. Which IEEE Standard applies to wireless LANs?
   a. 802.2
   b. 802.3
   c. 802.11
   d. 802.13
   e. 802.22

Short Essay Questions

1. Briefly explain a situation in which a company might choose a wireless rather than a wired LAN.
2. Explain the difference between computers in ad hoc mode and computers in infrastructure mode.
3. Describe a situation where it might be more advantageous to have an omnidirectional rather than a unidirectional antenna.
4. Give several examples of things in an office building that would cause interference.
5. Describe some of the security issues associated with wireless LANs.

Chapter 12

Video Basics Outline

We have discussed two forms of electronic communication: voice and data. There is a third type of communication that we will discuss in this chapter: video communication. Pictures, moving or still, are powerful forms of information and, as the saying goes, "a picture is worth a thousand words." Video can be powerful, but it is also very complex to create and to transmit. This chapter looks at the basics of video and how images are created and transmitted.

The Business and Human Factors

The ability to capture and transmit video images has led to the birth of multibillion dollar industries, such as television, that allows viewers to fantasize and "be there" without leaving the comfort of their own home.

A simpler, less-robust, and more down-to-earth flavor of video in the business world exists in the form of videoconferencing (VC) (Exhibit 1), which allows people to see and hear each other over great distances, reducing the amount of travel time and money spent. In a world of international companies and markets, videoconferencing is a blessing.

Like all communication systems, videoconferencing starts with basic elements: the sender, its transmission media, and the receiving station. Videoconferencing is full-duplex; the sender and receiver are constantly interchanging information, thus at any one point in time the person who is sending voice and video information to a far-off receiver is also receiving voice and video information. This provides the "next best thing to actually being there."

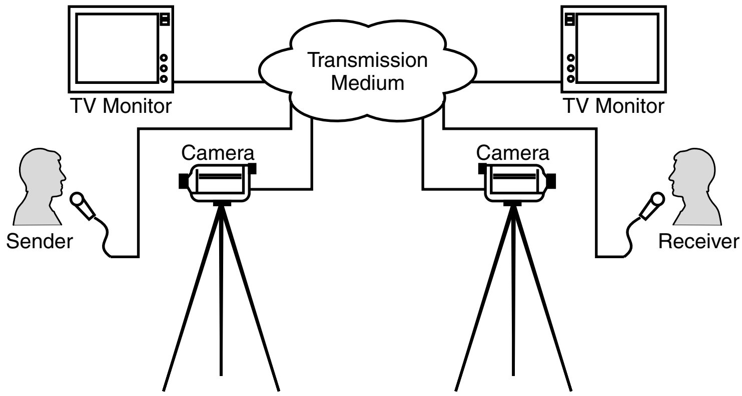


Exhibit 1 Basics of videoconferencing.

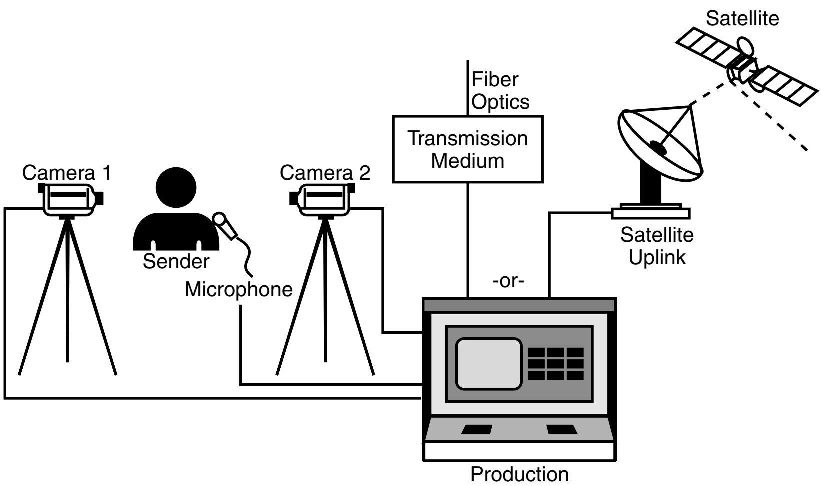


Exhibit 2 High-quality videoconferencing.

From the basic concepts of videoconferencing, there are three essential categories or qualities of VC systems: high-quality, medium-quality, and low-quality systems.

High-Quality

In high-quality VC systems (Exhibit 2), the transmission medium is called full frame, and the images seen are the same quality we see on our television sets. Video images are typically recorded in a professional studio with high-priced video cameras and microphones. From there, the video is sent via a high bandwidth transmission medium to the receiving site. The physical transmission medium is typically satellite or fiber-optics capable of carrying large amounts of data at very high speeds.

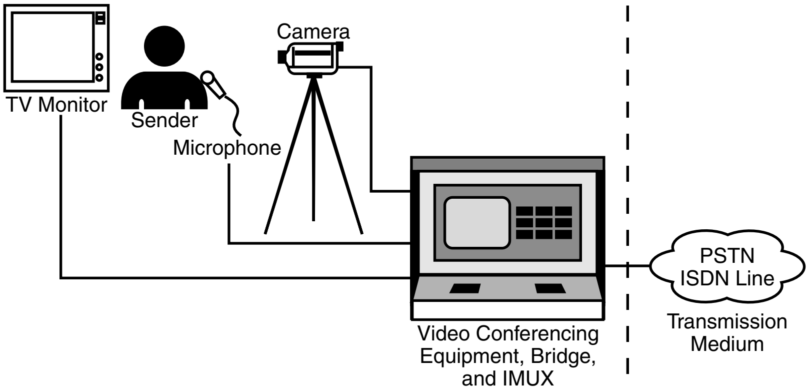


Exhibit 3 Medium-quality videoconferencing.

At the receiving end, the video information is transferred back into images and sound on high-resolution TV monitors and high-quality speaker systems. Because of the amount of data transferred and the speed necessary, high-quality VC is used very little and only by large firms with very deep pockets.

Videoconferencing can connect multiple sites, as well as one to one. For example, a central sending site can send its transmissions to all sales branches in the United States, and the central site will be able to see and hear all the remote sites. This is far more effective than a telephone call for getting large, dispersed groups together in a simple, affordable format.

Be aware that there are firms that specialize in videoconferencing, and one may rent facilities to do this, which means you can get the highest quality for a one-time videoconference at a reasonable cost.

Medium-Quality

A more-common type of videoconferencing is medium-quality VC (Exhibit 3). The compromise here is trading quality of sound and picture for cost. The video is of less quality than commercial-TV quality with sound that is a bit harsh but the cost is tremendously lower than with high-quality VC systems. In a medium-quality VC system, lower-priced cameras and microphones are used at the sender and receivers sites, and the video information is compressed and limited to reduce the amount of bandwidth needed to send over the transmission medium.

Typically, the transmission medium used is the Internet or a specialized phone line called ISDN (Integrated Services Digital Network). By using a more-commonly available transmission medium, the cost of VC is affordable by most companies and people.

Many companies, such as Picturetel, make equipment for medium-quality videoconferencing, which has become fairly common in the workplace. The equipment comes on a rolling cart with the cameras, monitors, and compression equipment, making it fairly easy to use.

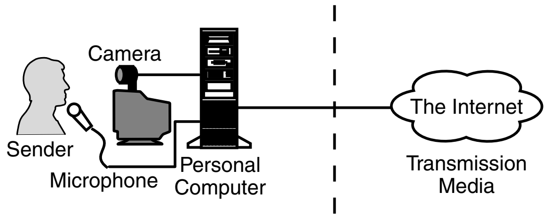


Exhibit 4 Low-quality videoconferencing.

Low-Quality

Low-quality VF systems (Exhibit 4) are becoming popular these days because they require minimal equipment at a minimal cost. Again the trade-off for low-cost VC is quality of video and sound. In a low-cost VC system, the images are erratic and delayed, with minimal color and sound quality. The essence of the message is there but when comparing the sound and video to television, the user is disappointed at the lack of quality.

The way low-cost VC systems function is by using commonly available equipment in a home or office. A low-cost camera and microphone (available for less than $200) are added to the personal computer and its Internet connection (LAN and WAN), providing a low-cost system. Computers with the Windows operating system are equipped with NetMeeting, a Microsoft package that helps in doing videoconferencing from the PC. Add a camera and a microphone, and you are ready to VC with friends and business associates.

Those of us who have traveled a full day to attend a one-hour meeting know that videoconferencing can save large amounts of time and money, two precious elements in our personal and business lives. Is VC the end-all solution? No but it is the "next best thing to being there" and offers tremendous advantages.

The selection of a VC system, whether high-, medium-, or low-quality, depends on the funds available and the quality needed. We would all like the highest quality but oftentimes we do not need it nor can we afford it.

The Technical Factors

We must first start off with a human principle: persistence of vision. Persistence of vision is when video information frames presented in rapid succession give the illusion to the TV viewer of smooth motion. Each of us has seen this in our childhood in the form of cartoons — still pictures photographed in rapid succession where the inanimate characters come alive. Maybe we have actually produced this effect drawing stick figures on a pad and flipping through the pages. We even see this effect with light bulbs: light bulbs go on and off 60 times per second but our eyes and brains see only a continuous light form with no flicker.

Images appear free of flicker and smooth when the presentation rates are above 40 times per second. Motion pictures use a shutter rate of 45 images

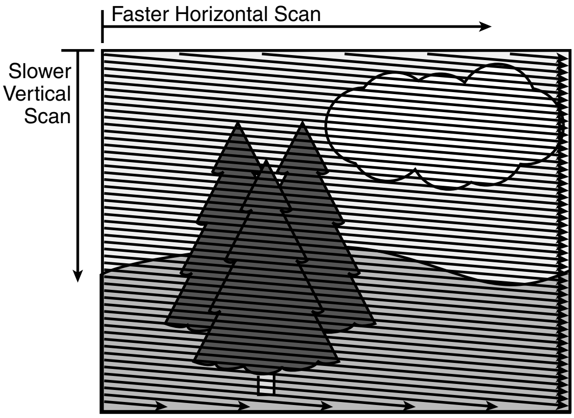


Exhibit 5 Electronic image scanning.

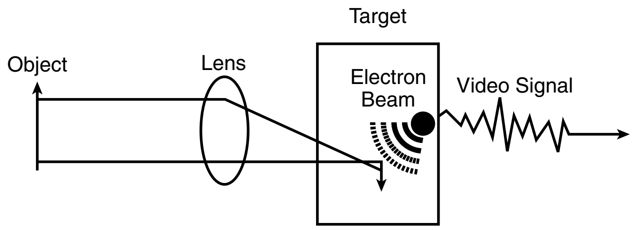


Exhibit 6 Scanning a focused image.

per second and television images use a rate of 60 images per second to give continuity to the action. The result is that the human eye and the brain see images that are seamless.

At this point, we must also differentiate film pictures from video pictures. With film pictures, as seen at the movie theater, the complete picture is projected in front of us at a moving rate of 45 images per second. On the other hand, video pictures (in the form of TV images) are scanned, line-by-line, at a high rate of speed (6 million bits per second) to produce a visual image rate at 60 images per second.

Image Scanning

Scanning starts by taking light, bouncing if off a subject, and focusing it on a target (Exhibit 5). Image scanning (Exhibit 6) consists of "looking" in horizontal passes across the target image and measuring the instantaneous amplitude that represents the reflected light energy. Each pass across the image by the scanning element is called a scan line. The video camera contains an image tube or target that automatically scans the scene and generates a corresponding electric output, which replicates the image that the camera sees

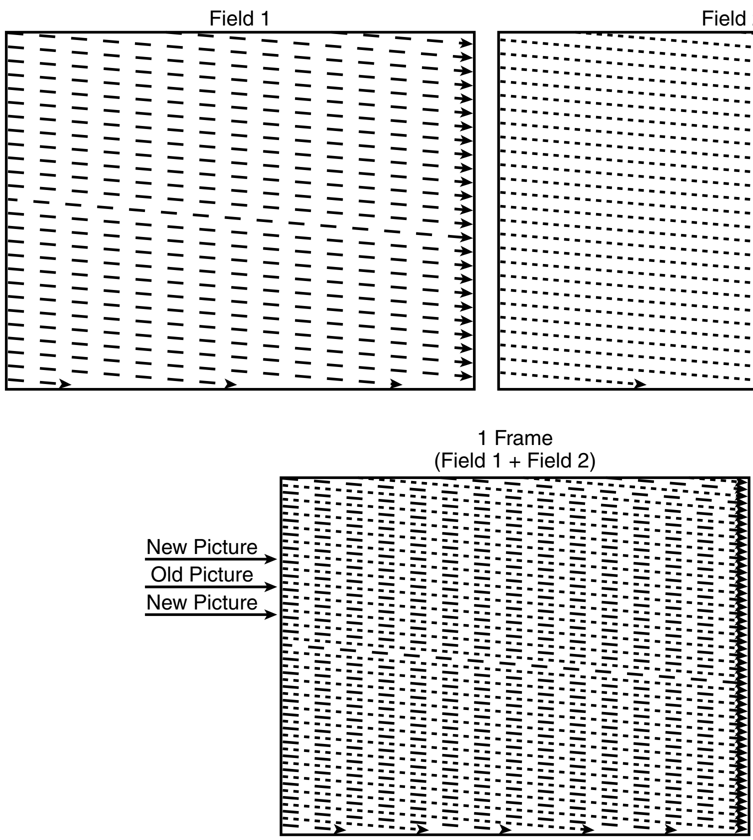


Exhibit 7 Interlace scanning.

in electronic form. Similarly, the video receiver reproduces the scanned image on the viewing screen. The process of reproduction is done by a spot that scans across the viewing screen and varies its intensity in accordance with the signal of the video camera.

The scan line is horizontal; the scanning begins at the top left of the image, then moves to the top right. The scan line then moves vertically a short distance so that the next horizontal scan can be performed. The image or target is scanned faster in the horizontal plane and slower in the vertical plane; for video, a complete image or target is scanned every one thirtieth of a second.

During a scan, the information about the light intensity of the image produces luminance (brightness) information, which is then transmitted to the receiver where it is displayed on the receiving screen. To appear smoother in form, an interlace scanning (Exhibit 7) method is used. Here an image is scanned one time in field 1, and a second time in field 2. This gives the appearance of an image scanned one sixtieth of a scan. This transfers with no visual jitter or error and provides for 525 frames, 30 frames per second, or 60 fields per second. For the vertical resolution, the image scan is capturing 367,000 dots or 525 frames (vertical) to give a clear and jitter-free image. Exhibit 8 shows the luminance signal of a video image.

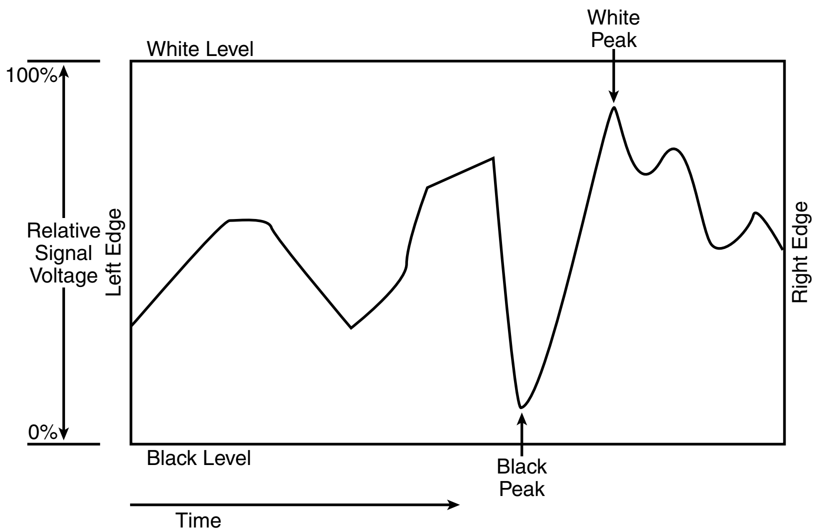


Exhibit 8 Luminance signal of a video image.

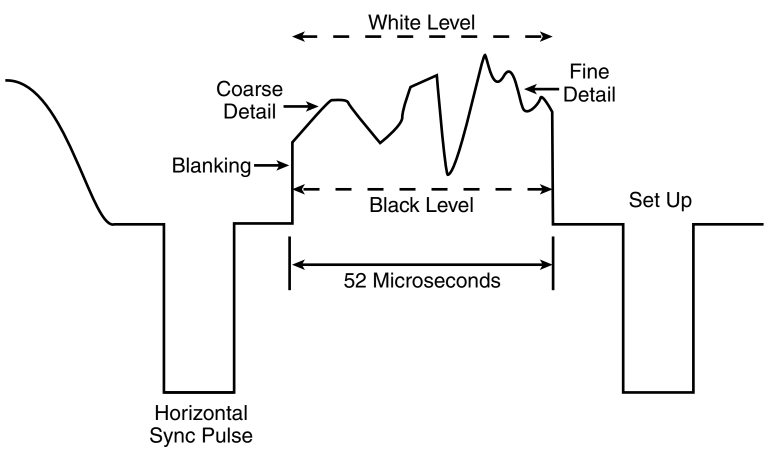


Exhibit 9 Luminance signal with sync pulses.

Obviously, the image created at the camera must be synchronized perfectly with the pace of the receiver (TV monitor) in order for the signal to appear correctly; this is achieved by horizontal and vertical synchronization pulses (Exhibit 9) within the video camera or transmitter and is linked with the luminance signal.

Additionally, audio (sound) information is put on the signal, along with a blanking pulse which tells the electronic beam when to turn off as it is traversing the image but not collecting or putting information on the signal. For example, in the horizontal scan it starts at the left and gets to the right of the image, then it must traverse back to the left-hand side to continue another horizontal sweep (at a lower vertical level).

For a television signal to be complete, it carries:

- Luminance information (picture brightness)
- Synchronization pulses (synchronizes images at receiver and transmitter)
- Blanking pulses (tells the image when to turn on and off)
- Audio and sound information

Color

So far, we have captured the luminance or brightness information of the image but what about the color? If we just capture and display the luminance information, we have what is commonly called a black-and-white image (ranging from white to black with shades of gray in between). For most of us, the world exists in color, brightness, and hue. In order to capture these aspects of color, we must first find the primary colors, the elements that make up all color. The three primary additive colors are:

- R = Red
- B = Blue
- G = Green

Mixing the primary additive colors together produces the three primary subtractive colors:

- B + G = Cyan
- G + R = Yellow
- B + R = Magenta

Using the additive or subtractive primary colors, all the colors (technically called hues) can be captured and reproduced. To capture these hues, a color video camera must be a bit different: it must separate the color into its primary elements (Exhibit 10).

As can be seen from Exhibit 10, the image is broken up into its primary additive colors by dichroic mirrors. Each of these separate colors (R, G, B) go to a separate target camera that records the level of the specific color. As these images leave the camera, they are amplified and added together into a Y signal (composite signal), which is then transmitted and decoded at the receiving end for a color picture.

Transmission of Video

A black-and-white image is fairly complex (luminance, blanking pulse, synchronization pulses, audio information); however, with color it gets even more complex (having the R, G, B information included in the signal) (Exhibit 11). The color images require large amounts of bandwidth to be transmitted, and

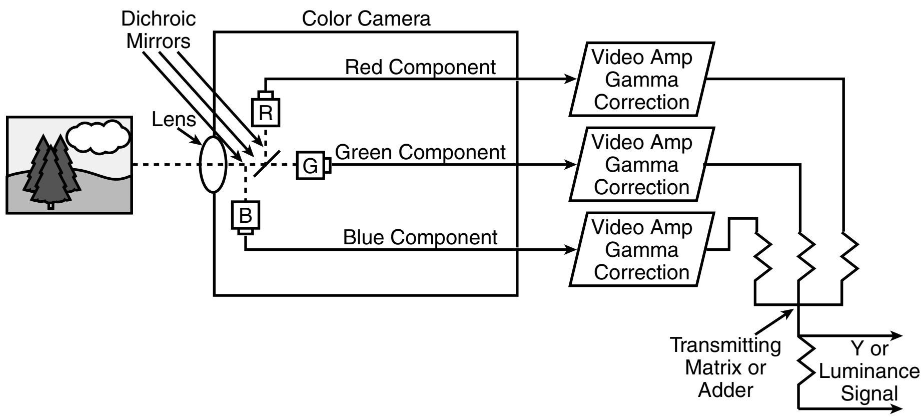


Exhibit 10 Block diagram of color camera.

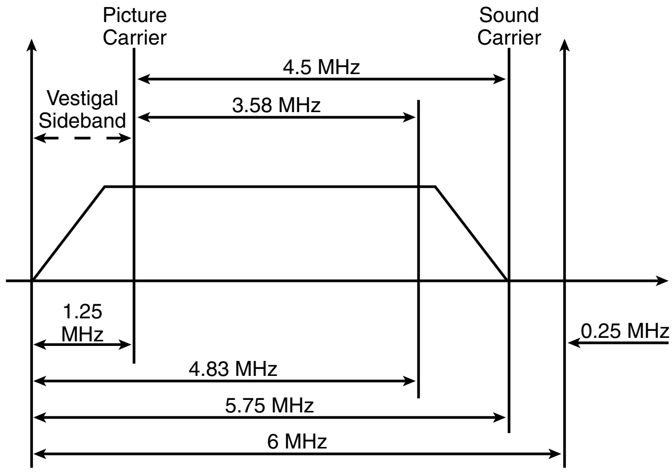


Exhibit 11 Color TV signal.

each color signal requires a full 6 MHz to be transmitted properly. To make matters more confusing, TV signals are transmitted differently in various parts of the world. There are essentially three worldwide standards:

1. NTSC: National Television System Commission (1953)
2. PAL: Phase Alternative Line (1967)
3. SECAM: Seque Coulear Aver Memoire (1967)

These three basic standards are again modified slightly in their base form for many countries. Exhibit 12 shows the variations and differences of these primary standards.

Exhibit 12 Worldwide TV Standards

Country	*Standards*
Australia	PAL-B
Austria	PAL-B
Belgium	PAL-B
Brazil	PAL-B, H
Canada	PAL-M
Chile	NTSC-M
China	NTSC-M
Colombia	PAL-D
Egypt	NTSC-M
France	SECAM-B
Germany (East)	SECAM-L
Germany (West)	PAL-B, G
Hong Kong	PAL-B, I
Japan	NTSC-M
Korea (South)	NTSC-M
Mexico	NTSC-M
New Zealand	PAL-B
Peru	NTSC-M
Saudi Arabia	SECAM-B, G
Singapore	PAL-B
South Africa	PAL-I
Switzerland	PAL-B, G
Taiwan	NTSC-M
United Kingdom	PAL-I
United States	NTSC-M
Russia	SECAM-D, K
Venezuela	NTSC-M

High-Definition Television

High-definition television (HDTV) is gathering much media attention these days. Walk into any electronics store and you will see a good selection of the sets available. As we see, they are much sharper and larger (with proportions more like a movie screen than a TV screen) than the old analog TV sets.

As we discussed, analog TV has 525 scan lines for the image and each image is refreshed every thirtieth of a second in an interlaced pattern. Horizontal resolution is about 500 dots for a color set. If we compare this with computer resolution it is much lower. Computer resolution is usually 800 by 600 or 1024 by 768 pixels. We have grown to prefer the computer resolution and wonder why TV cannot do the same. HDTV basically turns your TV into a computer monitor that accepts pure digital signals and provides a high-resolution picture that is very stable and crisp. In these cases, the original analog signal must be digitized and transmitted in digital form.

The HDTV format uses a high-resolution digital television (DTV) format combined with Dolby Digital Surround Sound (AC-3). This combination creates very sharp images with theatre-quality sound. The HDTV format uses a progressive scanning system. Rather than the interlaced method that shows every odd line at one scan of the screen and then follows with the even lines in another scan, progressive scanning shows the entire picture in one field every sixtieth of a second. This is a much smoother image but it does use a bit more bandwidth.

In order to squeeze this additional information into a typical TV broadcast bandwidth (6 MHz), broadcasters use MPEG-2 as a compression technique. This compression software records the important parts of the image; subsequent frames record only the changes to the image and leave the rest of the image as-is from the previous frame. MPEG-2 reduces the amount of data by approximately 50 percent. Although some detail is lost in the compression, the resulting picture is perceived by the human eye and brain as exceptional and tremendously better than traditional analog TV.

The Regulatory and Legal Factors

> The transition to digital television will bring tremendous benefits to the public, both in enclosed broadcast series and in the return of valuable spectrum for public use. Our actions today go a long way toward moving that transition forward.
>
> **—William E. Kennard**
> *Chairman, Federal Communications Commission*
> *January 18, 2001*
> *Biannual Review of the Commission's Rules and Policies affecting the conversion to digital television*

In the mid-1990s, the Federal Communications Commission (FCC) started an initiative to move the United States from the current analog television transmission media to a digital television media. This is a major change that affects not only every television broadcasting station in the United States but also every television owner.

Under the guidance of broadcasters and equipment manufacturers, the FCC adopted the Advanced Television System Committee (ATSC) and Digital Television (DTV) Standard, and set the goal of 2004 for all stations to be transmitting in the new format.

We have discussed analog television, the kind we all know and love and have in our living rooms. The signals for these televisions arrive in our homes via cable, satellite, or a rooftop television antenna, and the commonality of the signal is that it is analog in nature. With the rest of the electronic communication industry fiercely intertwined with digital transmission (voice and data fields) and the push for network convergence (voice, data, and video networks) to combine into one "supernetwork," the idea arose to move from

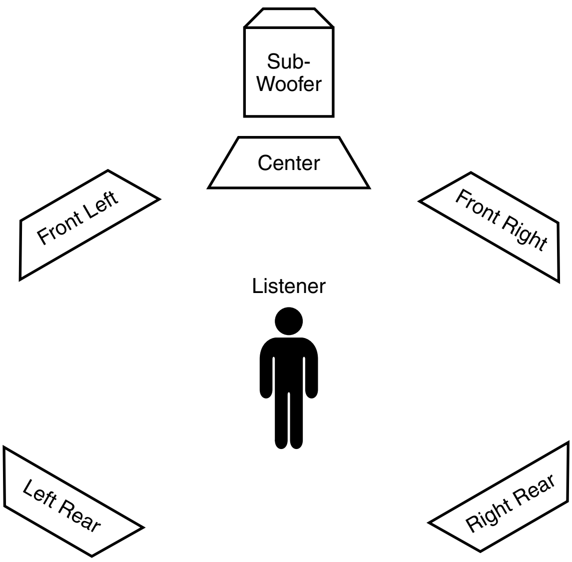


Exhibit 13 Digital "surround sound" 5.1 audio.

our present analog TV system to newer digital technologies. Because the change involved too many parties and was fraught with economic and political pitfalls, the FCC, in charge of the radio and television frequencies in the United States, accepted the challenge to move this initiative ahead.

One may fairly ask, why move to digital? What does it do for the consumer? The producer? A few misconceptions need to be cleared up; digital audio or video does *not* use less bandwidth and is *not* easier to do. Then why the shift from analog. There are two distinct advantages to a digital format:

- It is easier to stop or inhibit noise (interference) in the system, allowing for a cleaner signal that is free of jitter and other elements we are used to seeing in normal analog TV.
- Enhanced image. Using a digital format, one can manipulate the images easily, allowing for new capabilities, e.g., picture in picture and carrying 5.1 audio.

These two features will allow the industry to change and better enrich our lives. For example, the audio portion of the television signal will now carry 5.1 audio (Exhibit 13), which has five different sound sources, including a subwoofer. No longer will there be a single audio speaker on a TV, the sound will be theater-quality.

One of the technologies used to transmit digital television is a concept called compression (Exhibit 14). Compression is used to squeeze a large amount of information into a small space by using mathematical algorithms to reduce the bandwidth required. Even though digital transmission is less efficient (uses more bandwidth) than analog, and carries more information (5.1 audio versus stereo), DTV with compression will take up less of our national bandwidth, freeing up more of a finite commodity for our use.

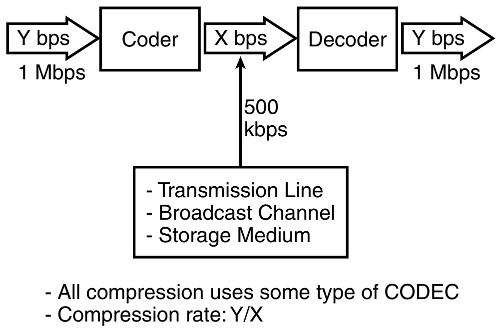


Exhibit 14 Compression block diagram.

Progress toward DTV is advancing, and the FCC conducts a review every two years to "ensure that the introduction of digital television and the return of spectrum at the end of the transition fully serves the public interest." In a report released in January 2001, the Commission found:

- As of November 15, 2000, 98 percent of TV licensees and permittees in all markets had filed DTV construction permit applications.
- 37 of 40 DTV stations in the top ten markets were on the air.
- 79 percent of the broadcasters stated that they had no difficulty in obtaining financing for the DTV transition.
- Phillips Electronics North American corporate reported DTV sales in 2000 quadrupled those of 1999.
- Thompson Consumer Electronics noted that the consumer chose from more than 150 DTV products at steadily increasing performance levels and steadily decreasing prices.

The change is on and will be big. For a while, we will still be able to watch our analog TV sets with their limited features but their days are numbered.

Summary

In this chapter, we explored the world of video. As we all know, pictures and especially moving pictures are an excellent way of expressing ideas and thoughts.

We looked at a common method of video communication: videoconferencing, which is very prevalent in today's business environment. Three types of videoconferencing were discussed: high-, medium-, and low-quality.

We then explored the technical elements of video communication beginning with the psychological principle of persistence of vision. We next explored how a video image is captured, created, and synchronized. We looked at the difference between black-and-white and color images and what it takes to produce color video images. We ended this section looking at how the images are broadcast in different countries.

Exhibit 15 Case Study: Networks Fill Travel Shoes[a]

Enterprise IT managers are contemplating the future of their communications networks following the recent terrorist attacks. At the same time, vendors such as Avaya continue to roll out new offerings that capitalize on user interest in IT alternatives to travel.

"After September 11, we're going to be more cautious about when to travel and when to get people on airplanes," said Chris Lauwers, CTO of Avistar Systems, a networking firm headquartered in Redwood Shores, California. "We'll just decide to travel less. And that will probably be a permanent [change]."

Hence, companies such as Avistar, which links eighty employees in six cities across the United States, are continuing to look to videoconferencing to connect their workers. In addition to concerns about airline safety, many companies are considering the technology as a way to circumvent the time constraints now imposed by greater airport security.

"For short hops, it used to be that we'd just pop down from Seattle to San Francisco for a day," said Bill Hankes, a spokesman for Seattle-based service provider Internap. "I don't know that we're doing to that anymore, because now you spend two hours on each side sitting in the airport," he said.

Indeed, stories such as Robert Mason's are now far from uncommon. Mason, vice president of business development at V-SPAN, a networking company, recently held a videoconference with business partners in Austin, Texas, from V-SPAN's office in King of Prussia, Pennsylvania.

"Austin's not a convenient place to get to from Philadelphia," Mason said, "and I knew that my 6 AM flight would now be complemented by another two hours of security at each end, which would mean that it would take me twenty-four hours to do a three-hour meeting. So I did the meeting on video, and I felt pretty good when I hung up about not having to take that flight back from Austin."

[a] Stephen Lee, *InfoWorld,* 10/22/01

Exhibit 15 shows a case study in which the lessons of this chapter are put to use.

In the regulatory section, we looked at the movement in the United States toward digital television and all the elements that need to be changed in order for this to take effect.

Questions for Review

True/False

1. Videoconferencing is simply allowing people to hear and see each other at a distance.
2. Because videoconferencing is half-duplex, the sender and receiver are constantly interchanged, so at any one point in time the person who is sending is also receiving.

3. High-quality videoconferencing systems are becoming very prevalent and require minimal equipment at a minimal cost.
4. Motion pictures use a shutter rate of 45 images per second and television images produce 60 images per second.
5. Electronic scanning consists of looking in vertical passes across the target image and measuring the instantaneous amplitude.
6. For video, a complete image or target is scanned every one thirtieth of a second.
7. Chrominance means brightness; this information is transmitted to the receiver where it is displayed on the receiving screen.
8. A complete television signal carries luminance information, synchronization pulses, blanking pulses, and audio information.
9. The three primary additive colors are red, yellow, and green.
10. Each color signal requires a full 6 MHz to be transmitted properly.

Multiple Choice

1. The standard currently used in the United States to transmit video signals is:
   a. PAL
   b. SECAM
   c. NTSC
   d. None of the above
2. The technology used to squeeze a lot of information into a small space by using mathematical algorithms to reduce bandwidth is:
   a. Transmission
   b. Compression
   c. Progression
   d. Synchronization
3. What tells the electronic beam when to turn off as it is traversing the image but not collecting or putting information on?
   a. Blanking pulses
   b. Y signal
   c. Synchronization pulses
   d. Luminance signal
4. The correct interlace scanning method provides for:
   a. 400 frames, 30 frames per second, or 60 fields per second
   b. 525 frames, 30 frames per second, or 30 fields per second
   c. 400 frames, 60 frames per second, or 60 fields per second
   d. 525 frames, 30 frames per second, or 60 fields per second
5. For video, a complete image or target is scanned:
   a. Every one thirtieth of a second
   b. Every one sixtieth of a second
   c. Every one hundredth of a second
   d. Every one fiftieth of a second

6. The rapid presentation of frames of video information to give the illusion of smooth motion is:
   a. Continuity of action
   b. Interlace scanning
   c. Persistence of vision
   d. Electronic scanning
7. The videoconferencing systems that are becoming very prevalent and require minimal equipment at a minimal cost are:
   a. Low-quality
   b. Medium-quality
   c. High-quality
   d. None of the above
8. The transmission media typically used in medium-quality videoconferencing is:
   a. Internet
   b. ISDN
   c. Fiber-optics
   d. Satellite
9. The image of a video signal is broken up into its primary additive colors by:
   a. Reflective mirrors
   b. Image mirrors
   c. Scanned mirrors
   d. Dichroic mirrors
10. The FCC adopted the ATSC and DTV standard to move the United States from its current analog television transmission media to a digital television media by the year:
    a. 2002
    b. 2010
    c. 2006
    d. 2004

Short Essay Questions

1. What are two distinct advantages of the digital video format?
2. Explain the concept of compression used in digital television.
3. What are the three basic elements of videoconferencing?
4. What is the main difference between film pictures and video pictures?
5. What are the four parts that make up a complete television signal?
6. What are the three primary additive colors? Primary subtractive colors?
7. Compare the three essential qualities of videoconferencing systems.
8. Explain the principle of persistence of vision.
9. Describe the process of electronic image scanning.
10. What are some of the facts reported on digital television in 2001?

Chapter 13

Network Convergence Objectives

The name of the network game these days is convergence, bringing varied and disparate networks into one converged network. Different networks cause inefficiencies and are very expensive to build and maintain (Exhibit 1). We see the problem caused by disparate networks in our personal lives. The telephone company conscientiously installs our voice communication network to allow us to talk on the phone. The cable TV company installs our video connection to allow us to view the plethora of TV channels out there. The electric company installs wires to provide power to all these devices. And finally, the satellite TV company installs a dish that allows access to the Internet and more TV channels. Somewhere along the line, one of the cables will be cut by one of the installers. Too many wires, too many connections, too much inefficiency.

All these companies are under the umbrella of electronic communication systems but they each work in different ways, with different standards, equipment, pricing schemes, and attributes.

The same confusion happens in the workplace but with even more complexity. Different support personnel train us to use the phone, the computer, and other devices in the office. Trained and expensive personnel must support each of these systems. Each system requires a different set of wires. There has to be a better way.

Can we converge or combine these networks and end-user devices into one? Will this save money and cause less frustration? The preliminary answer to this question is a resounding yes, and this is the focus of this chapter: the attempt to converge the various networks in today's environment.

One of the more popular forms of convergence is voice over IP, or VoIP, a strategy that is attempting to combine voice and data networks into one. It

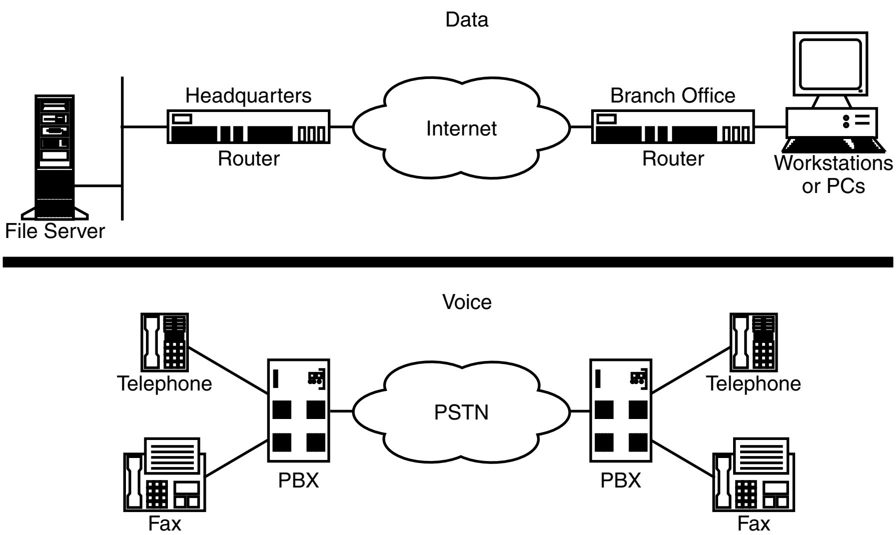


Exhibit 1 Separate voice and data networks.

is a technique that has taken hold and promises to be a success for our personal and professional lives.

The Business and Human Factors

Businesses and individuals endeavor to lower expenses in order to have more money for profit or pleasure. We also seek ways to accomplish our tasks more efficiently and effectively. This is human nature — or at least a part of life in the United States. These are the same reasons network convergence is being pursued. More specifically, VoIP is being sought to:

- Reduce telephone costs
- Enhance telephone services
- Increase network efficiency

Reduce Telephone Costs

With today's multinational companies and ongoing mergers and acquisitions, businesses spend large sums of money on telephone service. These costs are from (1) the use of national and international telephone circuits, and (2) the cost of telephone equipment (PBX) and lines within the site. Many of the costs are high because of the proprietary nature of the voice world and the limited number of competitors in this field. VoIP, the new paradigm costing about 30 percent less than traditional phone calls (according to many providers), seems like an appropriate place to look for cost savings.

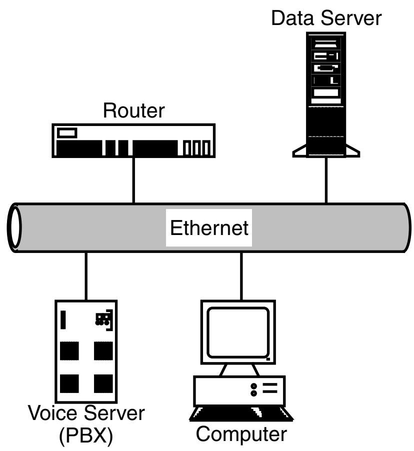


Exhibit 2 PBX as a local area network server.

Enhance Telephone Services

The digital world and the digitization of the phone system will provide many features for us. By pressing the * key and entering a code, we can use features such as call return, call forward, and three-way calling. These enhancements are beyond the basic voice service but have become key to our personal and business lives. If we combine the voice and data communication systems into one, we can extrapolate many more services to be offered (Exhibit 2).

When the voice is digitized and stored on a computer, voice recognition can be used as an authentication device. E-mails, phone messages, and faxes can all show up on a computer screen — a unified messaging center. The list continues with time- and cost-saving services that can be gained from the combined networks.

Increase Network Efficiency

In today's public switched telephone network (PSTN), a voice call takes about 64 kbps of bandwidth to transfer. Typically, this is done using a form of voice digitization called PCM (pulse code modulation). During the 1960s when this was first introduced within the parlance of the PSTN, it was the state-of-the-art approach to telephone calls.

Today's use of compression and better voice digitization circuits can carry a voice call at well below 64 kbps (8 kbps is the norm). This is a great savings in bandwidth. Additionally, if we send the data in packet switched form rather than circuit switched, we can fill in the on-hold and silence moments with other voice data. The bottom line, using TCP/IP and modern digitization methods (in the form of VoIP), along with the old PSTN phone wires, we can put much more information on the network, making it more effective.

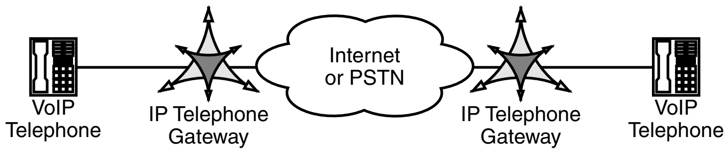


Exhibit 3 Basic parts of VoIP.

The Technical Factors

Before getting into a description of the working parts of VoIP, some discussion on "why" might help you.

Why should we digitize voice? We speak in analog waveforms, we hear analog waveforms, VoIP begins and ends with analog waves, so why should we digitize the voice in between? The reasons are mostly technical and relate little to the actual user.

- *Signal combination:* Combining digitized signals (technically called multiplexing) is easier with digitized waveforms than analog waves. When signals are combined over a line, their efficiency is increased and cost is reduced.
- *Generic equipment:* When all the voice is in digitized 1s and 0s, PC platforms can be used to help the signals along, replacing, at least partially, multimillion dollar specialized equipment.
- *Security:* It is easier, cheaper, and more secure to communicate over a digitized line than an analog line, making eavesdropping far more difficult.
- *Clarity:* Analog signals and lines are more susceptible to noise than digitized signals. With analog lines and signals, the noise (hisses, pops, clicks, and distortions) is cumulatively amplified along with the voice signal. With digital lines, it is easier to sort and filter out the noise.

The Basic Parts of VoIP

Similar to a regular analog telephone call, it starts with a handset, where our voice is transformed into an analog waveform. From here things change (Exhibit 3). The analog voice signals go through an IP telephone gateway, which performs three essential tasks, discussed in detail later in the chapter:

1. Sampling
2. Digitizing
3. Coding

The call travels over the Internet cloud through routers and switches, based on the IP address of the callee. At this point, the IP packets look just like any other data packets, except their content (payload) is actually digitized voice.

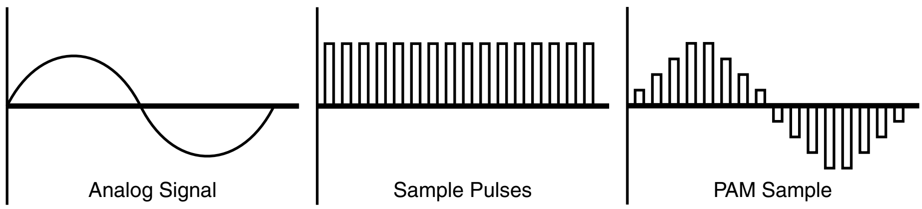


Exhibit 4 Sampling.

At the other end of the Internet cloud, the digitized data is transformed back to an analog signal through a second IP telephone gateway and sent to your handset where the receiver changes the analog signal into sound waves for you to hear. From a human perspective, a VoIP call is the same as a circuit switched telephone call; from a transmission perspective, the call is totally different.

Sampling

The first step in digitizing voice is sampling. Sampling means measuring the analog waveform at an instant in time in order to gain a discrete number. As shown in Exhibit 4, a single sinusoidal wave form is measured at regularly spaced intervals called samples. These samples, called pulse amplitude modulation (PAM), can be discretely measured and used later in the process to recreate the analog waveform for our ears.

The question you may be asking is: How often do I sample the waveform in order to accurately recreate the wave at the end? In 1933, Harry Nyquist developed the minimum sampling rate for analog waveform, called the Nyquist sampling rate. He noted that samples should be taken at two times the highest frequency component of the analog input waveform. For example, if the analog waveform we want to sample ranges from 500 to 1000 Hz, the sample should be taken at 2000 times per second (1000 Hz [the highest frequency] × 2 = 2000 samples per second). If we sample below the Nyquist sampling rate, the analog waveform at the end will sound distorted and lack clarity; if we sample above the Nyquist sampling rate, we are oversampling.

Why oversample? When we oversample we have too much information; if information gets lost along the way, this “extra” information proves valuable. Additionally, the Nyquist rate is the *minimum* and in instances where high quality is desired, such as audio CDs of a symphony orchestra, oversampling is required to catch the nuances and subtleties of the music.

Returning to our VoIP goal, if we wish to sample a telephone call, what frequencies of sampling should be used? It has been determined that the “intelligence” of a voice call happens in the 1000- to 4000-Hz range. Although we speak and hear at frequencies above and below this (typically 100 to 15,000 Hz), the meat of our call (intelligence) occurs between 1 and 4 kHz. Following Nyquist’s guidelines, we would use an 8000-Hz sampling rate (4000 Hz, the highest frequency, multiplied by 2 equals 8000 samples per second).

It should be noted that these PAM samples are not yet digitized. Each measurement is a number (such as +12.926, or –10.248). Another step, called

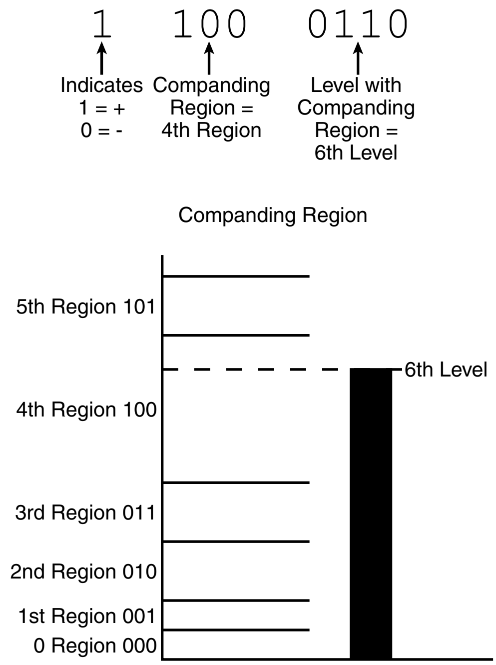


Exhibit 5 8-bit PCM word.

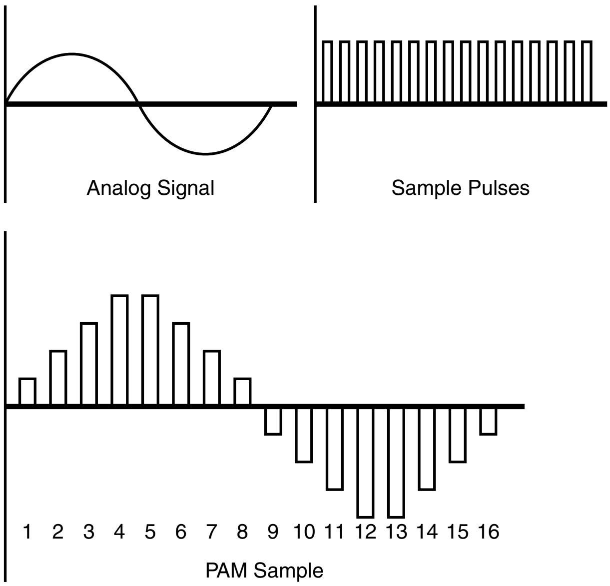
quantitizing, must take place to convert the number to the 1s and 0s of the binary world.

Quantitizing

In the quantitizing step, we take the measurements procured in the sampling step and convert them into 1s and 0s. This is true digitization. A question arises now: how accurate should we be? A PAM sample of +12.36781 may be represented by a base 10: 12, 12.4, 12.37, or 12.36781. Each of these base-10 numbers must then be converted into binary 1s and 0s.

It has been agreed that the quantitizing "word" size would be 8-bits long, meaning eight 0s or 1s to represent every PAM sample. This allows sampling at 8 kbps to be sent over a 64-kbps speed, a base of the current telecommunications system (8,000 samples × 8 bits per word = 64,000 bps).

Another issue needs to be brought up before we continue. In analyzing the patterns of human speech, which is the heart of VoIP, it was discovered that human voice is made up largely of two parts: (1) high-volume voice sounds that are made when we speak, and (2) low-volume voices and noises in the background. If we quantitize the PAM samples equally throughout the amplitude range, much of the voice intelligence is lost. To compensate for this characteristic, a process called companding is used. Companding is a technique that allows for more detail at the low-volume levels (when they are needed) and less at the high-volume levels (when they are not needed).



	Base 10	Base 2 with Companding
PAM Sample 1	+1.05	1 000 0001
PAM Sample 2	+1.12	1 001 0011
PAM Sample 3	+2.13	1 010 0100
PAM Sample 4	+2.50	1 110 1100
PAM Sample 5	+2.13	1 010 0110
PAM Sample 6	+1.12	1 001 0011
PAM Sample 9	-1.05	0 000 0001
PAM Sample 10	-1.12	0 001 0011
PAM Sample 11	-2.13	0 010 1100
PAM Sample 12	-2.50	0 011 1100
PAM Sample 13	-2.13	0 010 0110

Exhibit 6 Analog to sampled to quantitized signal.

Looking back at our original voice signal (represented by a sample analog waveform, Exhibit 4) takes us through the sampling and quantitizing step in order to get digital information from an analog waveform.

The 8 bits allotted to us are further broken down into three parts (Exhibit 5). Part 1 is used to show the polarity of the signal (+ or –), part 2 is used to show the companded region, and part 3 is used to show the level within that region (Exhibit 6).

Coding

Now that the analog waveform is in the form of 1s and 0s (arranged in 8-bit PCM words, one representation for each PAM sample), one would think that it can be sent over the telecommunications system. These digital 1s and 0s travel well around a single computer, and even a local area network, but when traveling over long distances using a WAN, the digital PCM words must be coded into a package that will travel well (Exhibit 7).

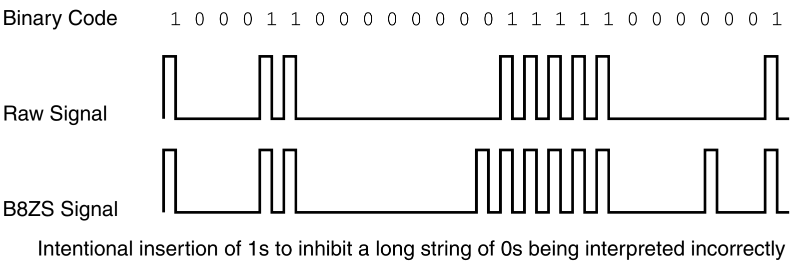


Exhibit 7 Signal coding.

A typical package used in the United States is called binary 8 zero substitution, or B8ZS for short. Another common package, in fact 8BZS's parent, is alternate mark inversion, or AMI.

Putting It Back Together

When the digital 1s and 0s are received, they are:

- Decoded back into their original PCM 8-bit words
- Dequantitized for the original PAM sample.
- Run through a low-pass filter to get an analog waveform
- Sent to a speaker so we can hear it

Sounds like a complex process — and it is — but in practice, small microcircuitry handles each element reliably and accurately so the concept actually does work well.

Packet Transmission

After it is sampled, quantitized, and coded, sending the packets over the Internet (packet network) seems easy but it is not. As a packet switched network, the Internet was designed for bursty, variable bit-rate data applications that do not occur in real-time. File transfers, web browsing, and e-mail are what the packet switched network was designed for and does well. None of these applications needs to occur in synchronous or real-time. An e-mail can get to you in three seconds or three minutes after it is sent and you will not care and probably not notice. Even when waiting for a file transfer from a web page, the synchronous nature is not important; waiting two seconds may be noticeable and annoying, but it still works well.

A voice conversation must happen in real-time. Experiencing a delay of two seconds is intolerable and even misleading as far as the conversation goes. The question arises: Can we adapt the packet switching network so that real-time conversations can take place? The issues with sending VoIP over the packet switched network are discussed next.

Delays in Packetizing

The time needed to sample, quantitize, and code the packets is minimal but we need to factor in loading the IP packets. We would not expect an 18-wheel truck to travel cross-country with one box on board, nor do we do this with IP packets. You may recall that the payload section of an IP packet is variable with a maximum of 1500 bytes payload, which translates to at least 60 different voice PAM samples that are put into an IP packet before it is sent. This delay of loading up the IP packet, added to the slight digitization delay, can add enough delay to make VoIP most ineffective.

Jitter

The easiest way to handle jitter is with quality of service (QoS), as we have previously discussed. Flagging these packets as priority and sending them to the head of the line can solve most problems, but not all problems. QoS proposals have been brought forward and many have been tried but there is still no one solid winner that the IT world is rallying around.

Even with QoS, jitter may occur. The router may move you to the front of the line but as it sends you out on the next highway, you may encounter a total traffic jam, which will delay the packets getting to their destination. Jitter buffers, helpers at the receiving site, can be used to assemble the voice stream to make it appear that these packets are arriving consistently. Depending on the scheme used, jitter buffers can be extremely reliable.

As the IP packets traverse the network, they come to routers which, operating on a first-come, first-served basis, route each IP packet to its final destination. The router may handle a large file transfer before handling a smaller voice packet, which again delays the travel time for the packets (like coming to a toll booth on a highway), causing VoIP to be ineffective.

Traffic Capacity

Although voice packets are small, there are 69,000 of them per second. This large amount of traffic may overload a typical data pipe, causing traffic congestion, jams, or total outages. Compression technologies, as previously discussed, can be applied here to cut the required network capacity. Another technique to cut traffic is silence suppression. It has been noted that 50 to 60 percent of voice calls are silence (people listening, thinking). If we send only the voice packets and ignore the silence, this could save a lot of traffic capacity. The question raised is what is silence and what is voice? Special voice-activation detector circuitry has been developed to tell when the voice has risen above background noise and it selects and sends this information.

Interestingly, not sending silence over a line causes human difficulties: if we detect no voice or noise at all, we wonder if the line has failed. To compensate, a technology known as comfort noise generation (CNG) has been created to add comfort noise at the receiving end so that silence packets do not get over the network.

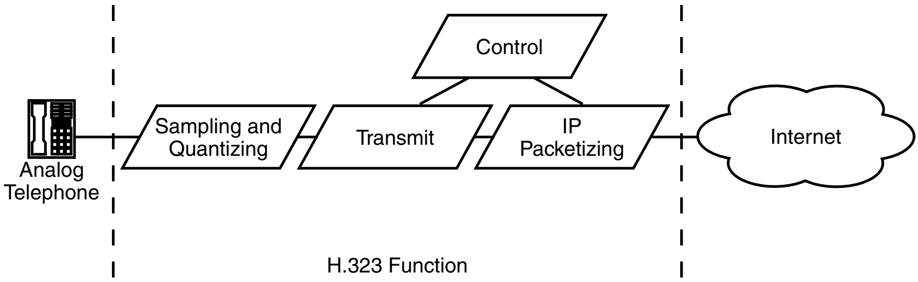


Exhibit 8 H.323 protocol functions.

Transmitter

Each of these sounds like a showstopper but, again, the technology engineers have determined methods to alleviate or at least attenuate these major issues.

Packet Size

The only way to deal with the delay of loading up an IP packet is to avoid the issue and send out a very lightly loaded one. Although this is not the most effective use of IP packets, it is the best approach to the delay in packetizing.

The Regulatory and Legal Factors

As with the other technologies discussed in this book, there are standards that VoIP uses in order to fulfill the call request. The standard most often used is H.323 (Exhibit 8). First released in 1996 by the ITU-T, it forms the foundation for VoIP products and is one of the umbrella standards for the VoIP field.

H.323 is a full-bodied architecture whose tenets encompass videoconferencing, file transfer, and of course, VoIP. The specific parts of the H.323 protocol used for VoIP are the audio portion, or more specifically the G.xxx series. For example, G.711 specifies audio sent at a speed of 69 kbps whereas G.723 specifies audio at 8.4 kbps. Because of the Internet delays caused with TCP (as discussed previously), the "G" series of audio specifies UDP at the transport layer and a protocol called RTP (real-time transport protocol) is added to the header to provide quality of voice.

Besides the audio portion of the VoIP call, there must be some signaling and control between the end devices (Exhibit 9). Signaling means telling the phone at the receiving end to ring and sending back a busy signal to the caller if the phone is busy. This is done with another aspect of the H.323 protocol, called H.225 or H.245; which of these is used is dictated by whether UDP or TCP is the underlying protocol.

Not only has ITU-T developed a protocol for VoIP, but so has another body, the Internet Engineering Task Force (IETF). In the world of the Internet, the IETF is a fast-moving and robust body that claims that H.323 has too many

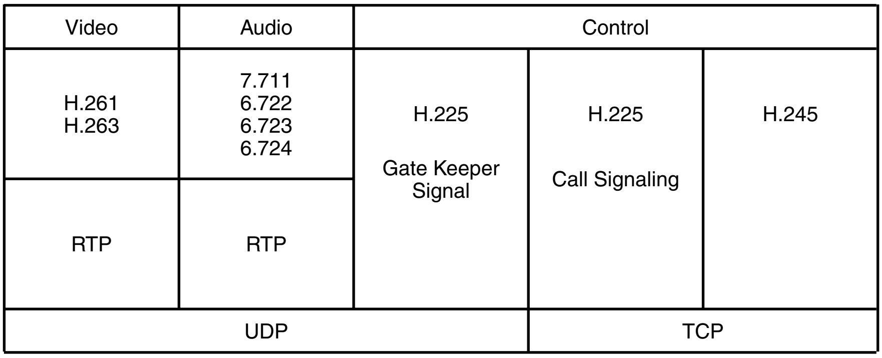


Exhibit 9 Protocol functions of VoIP system.

moving parts and that its roots are those of the public switched telephone network and not the Internet (where VoIP should reside). Therefore, IETF has released the Session Initialization Protocol (SIP), which it claims is designed with the Internet in mind and avoids the complexity of H.323. SIPs philosophy and design architecture come from the Hypertext Transfer Protocol (HTTP), the transfer protocol of the World Wide Web. It is a client–server protocol and has built-in reliability rather than using the underlying TCP protocol. Additionally, SIP relies on another IETF standard, the Session Description Protocol (SDP), to negotiate for a call and to carry information to negotiate multiport conference parameters.

The debate about which standard to use to build products is intense, and because of the maturity or lack of maturity of the field, the debate continues. Surely this has to reach a final decision.

LAN Telephony

In an office environment, there is a data network with all its component pieces and a voice network with its assorted pieces. What would happen if they were combined? Savings, or so it is thought. Maintaining the separate pieces is difficult and expensive, so why not combine them into one?

An office environment typically has a PBX (private branch exchange) system, which is essentially a small-circuit switched telephone company connected to your LEC via one or more T-1 or ISDN lines. Calls are placed by lifting the handset, detecting a dial tone (generated by the PBX), dialing "9" (to get an outside line) and dialing the desired number. The PBX also handles interoffice communication (Exhibits 10 and 11).

Benefits of LAN Telephony

It sounds complicated, and it is; nevertheless, the lure of lower costs and other benefits is driving the trend. What are the other benefits?

Exhibit 10 Case Study: Modest Victories for VoIP[a]

Large enterprises are investigating voice over IP but are treading cautiously in deployment.

Large-scale conversions of networks, transitions from entrenched traditional phone systems, and redesigns of business processes require extensive planning. However, smaller businesses with less complex environments and, in some cases, faster decision-making processes are more often jumping into VoIP — and some are reaping early returns on their investment.

Archer Engineers, with nine offices in Kansas, Missouri, and Kentucky, is going full-speed ahead with a VoIP rollout. It's seeing cost savings, easier management, and improved productivity.

Archer's initial savings came quickly after migrating its Lee's Summit, Missouri headquarters and three other offices in the Kansas City, Missouri area to VoIP last year. With a 3Com NBX 100 IP PBX at its headquarters handling calls between the four locations over frame relay connections, Archer was able to cut the number of phone lines it leased to 18 from 40, according to Michael Medsker, vice president of Archer's integrated solutions group.

Archer's level of phone service ebbs and flows. The company periodically experiences floods of traffic when an engineering bid is out and a high number of calls come in from clients, contractors, and other parties. Previously, that meant that the company had to maintain many phone lines that often sat idle.

Now the IP PBX centrally manages calls for the branch offices, load balancing those calls which come in through the headquarters among the branches. Previously, lines at some branches were overloaded during peak times. The IP system has remained comfortably below full capacity, according to Medsker.

The company has saved on capital expenditures on an ongoing basis. Archer's phone calls had been managed by a key system, and the company was ready for an upgrade. The IP PBX cost about one quarter of what a traditional PBX deployment would have cost. Archer's ongoing savings is about $1800 per month, approximately 75 percent of the total telephone bill, according to Medsker.

Buying IP phones themselves are often cited as a serious cost barrier to VoIP deployments, but Medsker estimated that the 3Com handsets cost only about $20 to $30 more than traditional business phones.

Upgrade Costs

Another major issue in enterprise VoIP plans is the cost of upgrading data networks to ensure voice quality and reliability. Archer, however, has gotten by without significant networking additions, besides equipment it had to buy for a new branch office. "By experimenting, we found we could do it with the routers and hubs we had," Medsker said. "We've been lucky so far, and we're getting the quality we want. I'm sure down the road we'll find things we have to change."

Easier management of the voice system has been an important benefit. Engineers often must move from office to office. The use of IP which recognizes users, not ports, allows phones to be moved without IT intervention. IP phones can be simply plugged into LAN ports and up and running with full functionality. "Allowing that level of mobility would be a major undertaking for IT staff otherwise," Medsker said.

Exhibit 10 Case Study: Modest Victories for VoIP[a] (Continued)

Archer is also getting more productivity from features such as direct dialing among branches and unified messaging built into the IP PBX. Reporting functions have shown Archer when employees were taking excessively long calls, helping the company explain to employees the need to shorten personal calls.

Archer's next step is installing a second, smaller IP PBX in its Springfield, Missouri office. This will enable that office's voice system to run off the headquarters' system.

Telecom costs at that office are expected to be halved, as Archer will be able to run a dedicated frame relay connection between headquarters and Springfield to handle the branch's phone calls and Internet service. This will enable the company to eliminate Springfield's phone lines and ISP connections, according to Medsker.

Archer has experimented with telephony over the Internet, instead of the WAN in some of its smaller branches. Employees in those branches can call other Archer locations by dialing an ISP, with their phones connected to small office routers.

Archer hopes to leverage such Internet telephony methods as it plans to do business with Australian partners through its start-up subsidiary, Universal Asset Management, which handles extended warranties. "Not using voice over IP to handle all those overseas calls would make doing business with Australia cost-prohibitive," Medsker said.

[a] David Drucker

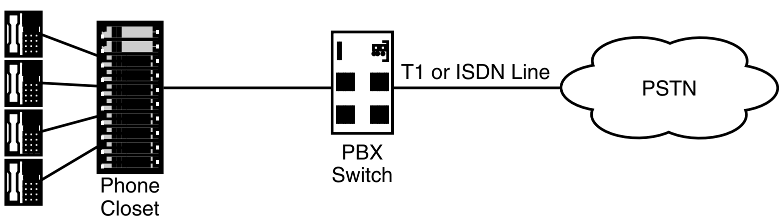


Exhibit 11 Office PBX network.

- *Simplified management:* People move around all the time in an office, and each move causes much work with the PBX system. An IP phone can be literally walked around the office and plugged into any IP Ethernet port and your extension will follow you. The PBX usually needs a bit of programming to make the move.
- *Computer-telephony integration:* By providing a common IP-based format, unified messaging can be achieved. Imagine going to your computer screen and seeing e-mails, voice mails (which will be read to you) and faxes all in one place. Imagine responding to an e-mail with a voice mail to an IP telephone! The world will be a better place when we do not have to check our e-mail, voice mail, fax mail, and snail mail to see if an important message has arrived.

In order to put the PBX and its many features (conference calling, call forwarding, music on hold) within the data communication network, its

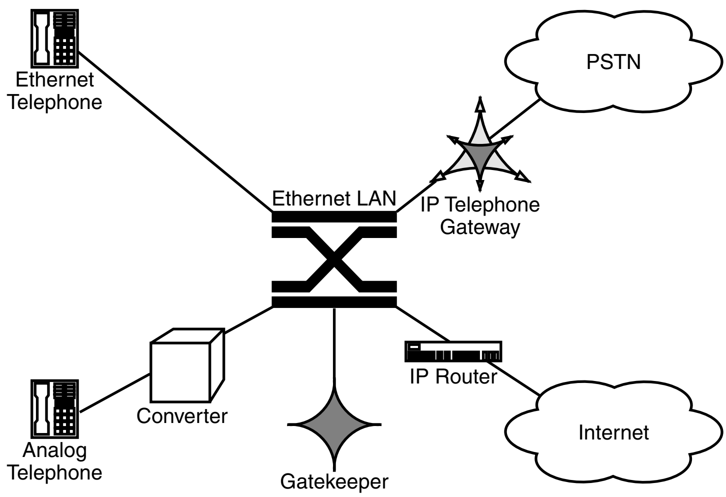


Exhibit 12 Office local area network telephone system.

function must be placed in the LAN-based components (Exhibit 12), which are discussed next.

Ethernet Phone

Ethernet phones look and feel like regular handsets but they are considerably different. For one thing, the electricity to power the phone must come from a LAN component or a separate power cord. An interesting approach that is being used is to send the required voltage over an unused pair of wires in the Category 5 E cable. Next, the phone must plug into the Ethernet network and have a MAC and an IP address. The MAC addresses come from the manufacturer's card and using DHCP (dynamic host configuration protocol), the device is given an IP address. After it is configured with an IP address, an Ethernet phone is a fully functioning part of the LAN that can send voice packets through; of course, the phone must also sample and quantitize the signal.

Analog Phone/Converter Gateway

Because there are so many analog phones already in place, why not use them for the office LAN system? The problem is that the output of these phones must first be sampled and quantitized in order to digitize the voice. The converter gateway does just this: it samples and quantitizes the voice signal and supplies power to the analog phone.

Gatekeeper

The gatekeeper is the call manager for the VoIP call. The gatekeeper has the telephone number to the IP address translator (so you can dial just the extension four-digit number rather than the full IP address). The gatekeeper also indicates the call by ringing the called phone or returning a busy signal if the line is in use. Other brain functions such as call hold, call forward, and call waiting also happen because of this gatekeeper function.

Ethernet LAN

The heart of VoIP is the Ethernet LAN (discussed in Chapters 7 and 8), and the building blocks of internetworking devices (hubs, routers, and switches), and physical media.

PSTN Access Gateway

You will also want to send and receive calls through your office LAN to talk with businesses in other cities and states but, not everybody has IP telephones. The PSTN access gateway allows the VoIP call to be connected back to a state the PSTN Access Gateway can route to all telephones in the world. The PSTN gateway also allows you to receive calls from callers not using VoIP.

IP Router

If you are calling another branch of your company or a person with an IP telephone in another city, the IP router's job is to get your packets (using the Internet) to their final destination.

Summary

In this chapter, we explored the hows and whys of network convergence and took an in-depth look at VoIP. The reasons for convergence go beyond cost savings and include added features and ease of management.

We explored how analog voice can be digitized and the basic components of digitization: sampling, quantitizing, and coding. VoIP does not come without its issues to be addressed (packet size, prioritization, jitter, compression, and silence) but the engineers have solved most of the problems.

VoIP, like other technical systems, relies on standards to work. H.323 is the standard involved with VoIP; SIP is a competing standard.

We also discussed how VoIP can be used within an office LAN environment and what benefits it can bring.

Yes, there are challenges with VoIP but the goals seem worth the risk.

Questions for Review

True/False

1. SIP was developed by the IEEE.
2. Comfort noise generation is put into a voice stream to decrease noise in the line.

3. Quality of service is a method of packetizing information.
4. Compression provides a signal that takes up less bandwidth.
5. The main reason for seeking VoIP is to enhance services.

Multiple Choice

1. PAM signals are a result of:
   a. Sampling
   b. Quantitizing
   c. Coding
   d. None of the above
2. What is the proper order for digitization of an analog signal?
   a. Sampling, coding, quantitizing
   b. Sampling, quantitizing, coding
   c. Quantitizing, sampling, coding
   d. Coding, sampling, quantitizing
3. Due to the standards imposed by the PSTN, the typical PCM word bandwidth is:
   a. 56 kbps
   b. 64 kbps
   c. 128 kbps
   d. 35 Mbps
4. In an 8-bit PCM word, the second field deals with:
   a. Sample polarity
   b. Companding region
   c. Range within companding region
   d. None of the above
5. The H.323 protocol is made up of all of the following except:
   a. The G series
   b. The H.225 signaling protocol
   c. The UDP transport layer
   d. The H.245 signaling protocol

Short Essay Questions

1. Explain why VoIP is being sought as a method of network convergence.
2. Explain the benefits of LAN telephony.
3. Explain the difficulties or issues involved in sending VoIP packets over the Internet.
4. Describe the digitization of an analog voice signal.
5. Explain what jitter is and how it affects VoIP packets.

Appendix A

Answer Key

Chapter 1

Multiple Choice

1. b
2. d
3. d
4. d
5. d
6. d
7. b
8. c
9. c
10. b

Matching Questions

1. g
2. a
3. d
4. i
5. c
6. h
7. e
8. b
9. j
10. f

Short Essay Questions

1. According to the Shannon-Weaver model of communication, a source sends an encoded message to a receiver that decodes the message, which passes through a channel that is susceptible to noise. In terms of human communication, a person may speak English to another person who understands English but the speaker's words may be muffled by the wind.
2. Using a standard model in which to discuss networks or computers allows for many different vendors to create products that are compatible. If no standards existed, it would be extremely difficult to create networks or computing devices that are compatible because each vendor has its own way of doing things, and that way may not be compatible with another vendor's method.
3. The components of the von Neumann stored-program concept are:
   - *Main memory:* The working area of the computer; it stores data and instructions.
   - *Arithmetic and Logic Unit:* Performs computational functions on binary data.
   - *Control unit:* Interprets the instructions in the memory and executes.
   - *Input/output equipment:* Devices operated by the control unit, such as a printer.
   - *Bus structure:* The interconnection medium that allows all communications to occur within a computer.
4. The layers of the OSI model are:
   - *Layer 7 (application):* Provides a final integrity check for the data (user interface, FTP, HTTP).
   - *Layer 6 (presentation):* The data translator and interpreter (form, syntax, encryption, and compression).
   - *Layer 5 (session):* Establishes, manages, and terminates connections between devices (resource control).
   - *Layer 4 (transport):* Responsible for end-to-end integrity of communications (TCP).
   - *Layer 3 (network):* Logical addressing (IP) also formats data from higher layers into packets that are passed to the data link layer.
   - *Layer 2 (data link):* Concerned with physical addressing (MAC).
   - *Layer 1 (physical):* Describes how data are sent through a network (mechanical, electrical, bits).
5. The von Neumann model is the foundation of all digital devices. Originally presented in 1946, it can be used to explain how digital devices work. If every device had a different method of storing, collecting, modifying, or transmitting information; designing networks; and computing devices would be extremely difficult. The von Neumann model allows every computing device to be analyzed in terms of the components explained in the model.

6. The steps of the communication process are:
   - *A source:* A man speaking over the radio.
   - *Transmits a message:* His words.
   - *That is encoded:* The language he is speaking.
   - *Through a channel:* The medium he uses (i.e., telephone, air, or radiowaves).
   - *That is susceptible to noise:* Anything that changes or alters the original message; in the case of radio atmospheric conditions can weaken a signal.
   - *The message is decoded:* By the receiver; a person listening to the radio understands the language of the source.
   - *By the receiver:* A person listening to the radio.
7. The fifth component of the stored-program concept is the bus structure. It is not often included in many diagrams explaining the concept but it is important. The bus structure is critical for any computing device because it connects everything. It is the physical path upon which signals are carried.
8. The theory of Claude Shannon explained the relationship between the signal and noise in a given transmission based on the bandwidth or frequency at which the signal is being transmitted. The capacity of information being transmitted is determined by all of these factors. The formula demonstrates that as the noise in a transmission increases, the capacity to send information decreases, and as the frequency (or bandwidth) in which we transmit increases, we have a greater capacity for information transfer.
9. Answers will vary.
10. As a professional in the IT field, one must be able to speak the language. Even if you are not designing or developing new technologies, you are managing people who do. To effectively lead requires more than management experience, one must also have an understanding of the basic concepts that comprise the IT world.

Chapter 2

Multiple Choice

1. d
2. e
3. a
4. c
5. d
6. d
7. b
8. a
9. e
10. d

Matching Questions

1. 1b 2d 3c 4a
2. 1c 2a 3b 4d
3. 1d 2b 3a 4c
4. 1c 2a 3d 4b
5. 1b 2d 3a 4c
6. 1a 2c 3d 4b
7. 1a 2d 3b 4c
8. 1d 2b 3a 4c
9. 1d 2c 3b 4a
10. 1b 2a 3d 4c

Short Essay Questions

1. A waveform is a picture produced by a specific piece of measuring equipment (e.g., an oscilloscope) that shows the highs and lows of the voltage or current associated with the signal. The waveforms vary in intensity, shape, duration, and complexity.
2. The frequency (unit: Hertz, Hz) of a signal is defined as the number of cycles divided by the time in which they occur. The period (unit: second, s) is the time it takes a waveform to complete one complete cycle.
3. Bandwidth is a range of frequencies a communication channel is defined within for specific signaling functions. As an example, telephone company circuits operate over a range of frequencies from 300 to 3400 Hz.
4. Current flow (unit: ampere, A) is the movement in the same direction in a conductor of the free electrons. Alternating current (AC) is the type of electrical power we have at our wall outlets. The other type of current flow is direct current (DC). AC can be thought of as changing direction as it goes from its positive position to its negative one; DC can be considered a continuous flow of current as opposed to the periodic condition of AC.
5. Resistance (unit: ohm, Ω) is the force that opposes the flow of electrons in a material.
6. The ability to do work or the energy potential of the electrical charges is called voltage (unit: volt, V).
7. The ability of an electrical conductor to hold a charge is considered its capacitance.
8. Inductance is the resistance of a conductor to allow current to change direction.
9. When electrons are forced to move between points of potential difference (e.g., positive and negative terminals on a battery), work is being accomplished. The measure of the rate at which work can be accomplished is called power (unit: watt, W).

10. DC is derived from AC by a device known as a rectifier, a device that uses special components to control the flow of AC current and bring the negative or alternating side of the signal together with the positive side of the signal. Devices called diodes allow current to flow through them in one direction only. The diode acts like a switch to current. Coupled with a capacitor, diodes can create a constant current flow for components within electronic equipment.

Chapter 3

Multiple Choice

1. a
2. c
3. c
4. c
5. a
6. c
7. a
8. a
9. a
10. c

Matching Questions

1. g
2. j
3. b
4. e
5. f
6. i
7. a
8. c
9. h
10. d

Short Essay Questions

1. The International Telecommunications Union.
2. The Federal Communications Commission.
3. Government (navigation, military, aviation, secure communications, and public safety), licensed (cellular, wireless local loop, satellites, radio and television stations), and unlicensed (ISM, cordless phones, wireless Internet, and microwave ovens).

4. Frequencies above 6 GHz are dependent on line-of-sight.
5. Line-of-sight, distance, and curvature of the earth.
6. It can multiplexed, or modulated.
7. AM radio signals use a longer wavelength and a lower frequency; this, combined with the ionosphere acting as a reflectant, allows the signal to travel much further than FM.
8. Because power or amplitude is modulated if the signal encounters a power spike, that spike is added to the signal in the form of static and interference.
9. The higher the frequency the shorter the wavelength, the lower the frequency the longer the wavelength.
10. Amplitude modulation uses the waveform to modulate the amplitude or power. Frequency modulation uses amplitude as the carrier for the frequency.

Chapter 4

Multiple Choice

1. b
2. a
3. b
4. b
5. a
6. d
7. c
8. c
9. a
10. c

Matching Questions

1. d
2. j
3. h
4. c
5. i
6. e
7. g
8. a
9. b
10. f

Short Essay Questions

1. Half-duplex allows for transmission in one direction at a time, where as full duplex sends information in both directions at the same time. If in a cost-prohibitive situation, half-duplex might be more economical. Full-duplex would be a more logical choice for high transmission. An example of full-duplex is a phone conversation or a videoconference.
2. An advantage is the consistency by which the circuit checks for errors; a disadvantage is the ease with which an error can occur. In AMI, you have an effective technique to detect errors. The prior four binary formats will detect an error only if there is a consecutive string of 0s.
3. Bipolar RZ (AMI) is the most reliable signaling format. This process is used because of the power requirements necessary for transmission and the ability to detect errors in the signal stream more effectively. When a bipolar violation occurs, the circuit is immediately made aware without the use of any more energy.
4. ZCS and B8ZS are keep-alive signals. In ZCS, the signal is kept alive by inserting a mark in a string of eight consecutive 0s, which causes a bipolar violation that keeps the signal alive. In B8ZS, the signal is kept alive by inserting a code into the string of 0s. This is done by placing a mark at the fourth, fifth, seventh, and eighth intervals.
5. The difference between the three formats is that AMI is used for error detection, while ZCS and B8ZS are used as keep-alive signals.
6. The CSU/DSU must be programmed to the particular signaling format that you are looking to use. If a digital circuit is ordered with ZCS keep-alive signaling while the carrier provides B8ZS, alarms, faulty operation, and flaky problems start appearing in relation to the circuit. If your system is looking for ZCS and a packet of 1s and 0s comes down the line as B8ZS, the system tries to analyze the data bits as information.
7. If a digital circuit is ordered with ZCS keep-alive signaling while the carrier provides B8ZS, alarms, faulty operation, and flaky problems start happening in relation to the circuit. If the system is looking for ZCS and a packet of 1s and 0s comes down the line as B8ZS, the system tries to analyze the data bits as information.
8. Both FDM and TDM are techniques used to send information in a serial transmission. The way in which they multiplex is different: FDM separates the information by frequency, while TDM assigns time slots to the various signals. TDM is a more widely used method because the synchronization of the TDM signal is critical in the delivery of information. Each time slot requires special framing and coordination bits that tell the receiving end where each information slot stops and starts. TDM is based on digital signaling from end-to-end.

9. A major disadvantage of TDM is the waste of available "time slots." When a particular channel has no information to send, that time slot will contain nothing more than a zero. This wasted space makes this transmission method inefficient in some respects.
10. 24 DS-0s × 64,000 kbps (the throughput of 1 DS-0) = 1.536 Mbps. You then add back the 8000 bits used for sampling for a total of 1.544 Mbps.

Chapter 5

Multiple Choice

1. c
2. b
3. c
4. c
5. c
6. b
7. a
8. b
9. c
10. a

Matching Questions

1. f
2. h
3. e
4. i
5. j
6. c
7. g
8. a
9. d
10. b

Short Essay Questions

1. A digital key system is a highly reliable component used to connect eight PSTN trunks to twenty-four subsets. They are sealed components that are difficult to repair when they do break, which often results in the entire component needing to be replaced.
2. Least cost routing (LCR) and automatic route selection (ARC) refers to the system that automatically selects the most economical route that a call is to take. This is often based on the carrier, the time of day, and the call destination.

3. Automatic call distribution (ACD) is an economically advantageous system of routing incoming calls to a group so that each member of that group receives an equal amount of incoming calls. This technology also enables the queueing of incoming calls in the case of high-volume traffic.
4. A PABX is a specialized stand-alone unit capable of connecting outbound and inbound traffic to an available trunk, station-to-station communication, and offers feature-rich options of call processing. An organization chooses a PABX for many reasons, but the primary motive is economic. The PABX allows multiple internal users to connect to a limited number of outside trunks.
5. A Centrex essentially has the same feature-rich services as a PABX; however, the equipment is housed and maintained by the LEC at the CO. This structure originally benefited organizations with a dispersed geographic presence.
6. Loop start lines are found at nearly all residential connections. Loop start lines are characterized by the immediate dial tone the end user hears when taking the handset "off-hook," closing the circuit ground which allows the dial tone to be carried to the circuit. Ground start lines are almost always used in a PABX environment. When the end user takes the handset "off-hook," a message is sent to the CO. After this message has been received, the CO sends dial tone to the PABX. The primary reason this type of line is used is to prevent glare, which is caused when an incoming call collides with an outgoing call.
7. An interexchange carrier (IXC) is also known as a long-distance service provider. Until 1984, this market was dominated by AT&T. After the 1984 divestiture of AT&T, the market became wide open, and costs to consumers have dropped drastically.
8. Signaling System 7 (SS7) is an out-of-band method of call transmission setup and teardown. This out-of-band signal is sent over a different network than the one used for voice traffic to secure a connection, and was primarily instituted as a method to combat fraud employed by sending frequencies over the voice network that instructed the phone company's equipment not to charge a toll for that call.
9. Dual tone multifrequency (DTMF) is a method of transferring call setup information using a Touch-Tone™ phone. Essentially, each number pressed on the keypad sends a set of two numbers (as frequencies) to the CO to define the intended call party.
10. The terms tip and ring relate to the times when telephone operators transferred and connected calls by inserting a plug. The plug had both a tip (the ground) and a ring (the portion of the plug carrying the current). Today, it means nearly the same thing, except that this manually inserted, physical plug no longer exists. In today's environment, the tip side is still the ground and registers zero voltage when read with a voltmeter. The ring side measures –48 V DC.

Chapter 6

Multiple Choice

1. b
2. b
3. a
4. d
5. c
6. d
7. d
8. d
9. c
10. a

Matching Questions

1. g
2. j
3. a
4. f
5. i
6. c
7. h
8. d
9. e
10. b

Short Essay Questions

1. PVC is a connection that is permanently up or always connected. As networks grow, this becomes impossible to maintain. In this environment, a switch is introduced, which now makes it an SVC. The SVC sets up and tears down the connection every time a connection is needed. Once the call or data transmission is complete, the virtual circuit is terminated.
2. The process of setting up the communication link between the endpoints requires the establishment of connection prior to information being transferred. You must first request the connection, after which you receive a confirmation. Upon receipt of the confirmation, the transfer of information occurs. After you complete the transmission, the connection is terminated.
3. Out-of-band signaling is a signal in which there is no transfer information. The band contains nothing more than the actual data being transferred. This data, by itself, has no idea where it needs to go. An example of this is in an ISDN circuit, either BRI or PRI.

4. The points that a call may hit are the service switching points (SSP), service transfer points (STP), and the service control points (SCP). SSPs are the locations closest to the user. These are points in which the initial information about a call is collected and passed along the network. The STPs can be considered the points on the SS7 network that transfer link information to the next switch to help establish the circuit. SCPs can be visualized as databases containing all the addressing information about a particular area of the country.
5. The two most common forms of ISDN are BRI and PRI circuits. A BRI is used where data transmission needs high reliability but the amount of data that needs to be pushed or pulled is not much. A PRI is equivalent to a T-1 in throughput. It is reliable also with the capability to push more information.
6. BRI: 2 B channels (64 kbps), 1 D channel (16 kbps), total throughput = 144 kbps, actual throughput = 128 kbps. PRI: 23 B channels (64 kbps), 1 D channel (64 kbps), total throughput = T-1, actual throughput = T-1 (64 kbps).
7. NT is responsible for physical layer and electronic connectivity between the user and the CO. TE either can be directly compatible (TE-1) with an ISDN circuit or requires conversion from its current configuration to make it compatible with the ISDN circuit. TA is responsible for this conversion.
8. The main reason that ATM is implemented in any environment is its high QoS, which is of utmost importance in many data networks.
9. The ATM conversion can take place in a few different locations. It can be converted to a cell format at the workstation or computer. The network interface card (NIC) can be installed as an ATM NIC, giving the network a LAN ATM environment. An internal network switch can also convert packet data into the ATM cell-based protocol. An edge router connecting the internal network to the wide area network can also be the site of conversion to ATM cells.
10. GFC allows for the handshake to occur to guarantee the connection. The CLP tells the importance of that particular cell. On a congested network, the lower priority cells can be discarded to make way for those of higher importance. The VPI/VCI are logical connections between endpoints. The PT tells what type of information is contained within that cell.

Chapter 7

Multiple Choice

1. d
2. c
3. c
4. b

5. c
6. a
7. d
8. ac
9. ad
10. b

Matching Questions

1. 1b 2d 3c 4a
2. 1c 2d 3a 4b
3. 1c 2a 3d 4b
4. 1a 2c 3d 4b
5. 1d 2c 3b 4a
6. 1c 2a 3d 4b
7. 1b 2c 3d 4a
8. 1d 2b 3a 4c
9. 1a 2c 3d 4b
10. 1b 2c 3a

Short Essay Questions

1. From its inception, AMPS has been referred to as cellular service because of the configuration of the antenna propagation field. Though theoretically shaped like honeycomb cells on the engineering layout, the cell sites provide a way to reduce power, increase access, and reuse frequencies in the limited bandwidth allotments for cellular services. The *reuse of seven* rule, which states that no adjacent cell can use a frequency from an cell, forced diversity in frequency placement in the network.
2. Frequency division multiple access (FDMA) is a multiple access technique in which users are allocated specific frequency bands. The user has singular right of using the frequency band for the entire call period.
3. Time division multiple access (TDMA) is an assigned frequency band shared between a few users. However, each user is allowed to transmit in predetermined time slots.
4. Code division multiple access (CDMA) is a technique in which users engage the same time and frequency segment and are channelized by unique assigned codes.
5. The mobile switching center (MSC), which is known by a number of different names including mobile telephone switching office (MTSO), provides the system control for the mobile base stations (MBS) and connections back to PSTN. The MSC is in constant communication with the MBS to coordinate handoffs (or switching) between cell sites, connections to the landlines, and to provide database information about home and visiting users on the network.

6. An antenna is a circuit element that provides a changeover from a signal on a transmission line to a radio wave and for the gathering of electromagnetic energy (i.e., incoming signals). An antenna is a passive device in the network because it is a receiver and transmitter of electromagnetic energy but is not responsible for amplifying the signal. An antenna is defined by four characteristics: reciprocity, polarization, radiation field, and gain.
7. Smart antennas are base station antennas with a pattern that is not fixed but adapts to the current radio conditions. Smart antennas include switched lobe (also called switched beam), dynamically phased array, and adaptive array.
8. Smart antennas add a new way of separating users, namely by space, through space division multiple access (SDMA). This can be visualized as the antenna directing a beam toward the communication link only. SDMA implies that more than one user can be allocated to the same physical communications channel simultaneously in the same cell, only separated by angle.
9. Microwave signals are radio frequency (RF) signals that range from 1 to 40 GHz. As we move up the spectrum, the radio waves become susceptible to conditions that affect the transmission of light. Frequencies below 6 GHz in frequency are not greatly affected by line-of-sight issues or obstructions blocking signals. Beyond 6 GHz, we are constrained by issues of distance forced on us by the curvature of the earth, atmospheric conditions such as fog and rain, and buildings and other structures that could impede the signal's transmission path.
10. The bit error rate (BER) is a performance measure of microwave signaling throughput. It represents the number of pieces of information corrupted or lost during transmission. There are four primary diversity issues that need to be considered with microwave placement: space diversity, frequency diversity, hot standby, and the use of a PRI connection for a failover. The mean time between failure (MTBF) of the equipment being used is an estimated time frame in hours for the durability of the equipment, provided by the manufacturer.

Chapter 8

True/False

1. F
2. T
3. F
4. F
5. T
6. F
7. T
8. T
9. F
10. F

Multiple Choice

1. c
2. b
3. d
4. b
5. a
6. b
7. b
8. a
9. a
10. d

Short Essay Questions

1. CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection. It is used with Ethernet networks and works as a contention-based protocol. The computers on the network listen until they hear nothing (meaning the bus is clear) and then they put their packets on the bus (the CSMA part). If the bus is busy with another computer's data, the computer waits until the bus is clear before it transmits. A collision occurs when two computers put their packets on the bus at the same time. When a collision occurs, all computers stop all transmissions, then wait for a random time period before starting transmission again.
2. The four components of a LAN are (1) the end-user devices, (2) the physical media, (3) the networking equipment, and (4) the network operating system. The end-user devices are network-connected devices that the users see and interface with. They are the transmit-and-receive ends of the human side of the network. Examples of shared end-user devices are printers, fax machines, and scanners. The physical media is the wiring between the end-user devices that allows the communication to occur. The type of media used depends on what is currently existent in the building or the characteristics of the organization. The networking equipment is what allows the network to send information to the correct destination. It is basically the core of the network. Hubs, switches, routers, and NICs are the most common types of network equipment. The network operating system (NOS) controls the order of communication between end-user devices (both personal and shared). Unlike a PC operating system that controls an individual piece of equipment, the NOS controls communication between the devices.
3. Packet switching is an efficient use of resources where the path (or circuit) is shared by many users at once. Information is sent in packets, and each packet carries information that is destined for different locations. In circuit switched networks, a dedicated path is carved out of a larger network to form a communication path. This path or circuit is

set up by signaling created at the time you want to communicate, and terminated at the time the communication is ended. The entire circuit is reserved during the length of the call.

4. Two broad categories of network costs are initial and ongoing costs. Initial costs are incurred during setup and installation, including costs for wiring, equipment, network devices, and software. Ongoing costs are those incurred during the life of the network, including maintenance, personnel, MACs, and licensing.
5. There are two possible problems that can exist with the Token Ring access method: lost token and captured token. A lost token occurs when a token is corrupted or lost in the ring and no computer gets the token, therefore no computer is able to transmit. A captured token occurs when a computer has so much data to transmit, it hogs the network and never gives up the free token, or the computer crashes while holding the token. In either of these cases, the network cannot transmit data and is therefore disabled.

Chapter 9

True/False

1. T
2. F
3. F
4. F
5. F
6. T
7. T
8. F
9. T
10. T

Multiple Choice

1. b
2. a
3. b
4. c
5. c
6. b
7. c
8. c
9. b
10. d

Short Essay Questions

1. The primary advantage of centralized routing is network efficiency. Centralized routing uses one routing table that keeps track of the whole network. As such, computer resources and network capacity are used by one managing device only.
2. The session is ended when one of the logical unit (end-user device) sends a deactivate request.
3. The languages of the network, routed protocols, operate at the network layer of the OSI model. They form the information that is communicated between computers.
4. TCP/IP is the most common routed protocol. It is made up of two separate parts: TCP and IP. The primary function of the IP part is to address and route the packets. The other part, TCP, has the function of packing and unpacking the data (reassembling the data packets) and ensuring reliability.
5. Multicast messages are transmitted by sending a message to people in a distinct group or classification. Only those to whom the message is addressed can hear the broadcast message.

Chapter 10

True/False

1. F
2. T
3. T
4. F
5. T
6. F
7. T
8. F
9. T
10. T

Multiple Choice

1. b
2. c
3. a
4. a
5. b
6. b
7. c
8. a
9. b
10. d

Short Essay Questions

1. QoS is an acronym for quality of service. In the telephone industry, the QoS is known as *five nines or 99.999 percent uptime. This is directly reflected in network reliability* .
2. WANs are considered Hardware-Defined Networks that have dedicated hardware and physical media assigned to them. In order to go from an office in New York City to a manufacturing plant in Indiana, a regional circuit must be built that connects these two points together. This is a Hardware-Defined Network.
3. Software-Defined Networks (SDNs), or virtual private networks (VPNs), are created and constructed over the physical public switch networks. VPNs are SDNs that can leverage usage of the public network.
4. The three elements of network security are:
   - *Authentication:* Guarantees the person at the end is who he claims to be.
   - *Encryption:* Ensures the safe transit of information through the network.
   - *Accounting:* Ensures all the network elements are credible and the network is not being compromised.
5. Three job classifications that can benefit from telecommuting are:
   - *Salesperson:* Has the ability to maintain accounts on the road without having to work out of an actual office.
   - *Consultant:* Has the ability to request and receive information from a home office in order to close a deal with a customer.
   - *Construction project manager:* Can order and purchase supplies needed on the job through the home office.

Chapter 11

True/False

1. F
2. T
3. T
4. F
5. F
6. T
7. F
8. T
9. F
10. F

Multiple Choice

1. e
2. d
3. c
4. a
5. d
6. b
7. a
8. c
9. d
10. c

Short Essay Questions

1. Wireless LANs provide physical flexibility and mobility. If a company needs to physically move people and computers, wireless LANs provide instant mobility. If a company is housed in a building with a structure that is difficult or dangerous to change, or if the building is protected by historical preservation laws, a wireless LAN can take the place of drilling through walls.
2. Ad hoc connected computers talk only to each other, whereas computers that are functioning in infrastructure mode connect to a central access point in a logical star topology. In infrastructure mode, computers can have access to the local LAN and possibly to the outside Internet; in ad hoc mode, this is not possible.
3. Omnidirectional antennas are advantageous when connectivity must come from all directions. If the connecting computers are on all sides of the access point, an omnidirectional antenna can connect with everyone. If the access point is in a corner, a unidirectional antenna can focus the connections toward the connecting computers.
4. Interference can be caused by walls, buildings, people, objects, or anything that the radio signal must travel through or around. In multistoried buildings, interference can be caused by ceilings and floors. Radio interference can be caused by anything that transmits electromagnetic waves, including electric devices (motors), area radio towers, and even mobile phones.
5. Wireless LANs are easy to break into if no security precautions are set up. Anyone with a wireless card can hop onto a wireless network unless protections such as WEP are in place. These security issues include access to sensitive material, as well as use of purchased uplinks.

Chapter 12

True/False

1. T
2. F
3. F
4. T
5. F
6. T
7. T
8. T
9. F
10. T

Multiple Choice

1. c
2. b
3. a
4. d
5. a
6. c
7. a
8. b
9. d
10. d

Short Essay Questions

1. It is easier to stop or inhibit noise (interference) in the system, allowing a cleaner signal that is free of jitter and other elements we are accustomed to seeing in normal analog TV. Enhanced image: In a digital format, one can manipulate the images easily, allowing new capabilities, e.g., picture in picture, carrying 5.1 audio.
2. Compression is a process by which a mathematical computation is placed on a video and audio file. This process decreases the bandwidth necessary to carry the digital television transmission and enables the information to be carried in the original 6 MHz bandwidth. The digital broadcasting utilizes the MPEG-2 compression format in its transmission.
3. The three basic elements of videoconferencing are the sender, its transmission media, and the receiving station.

4. With film pictures (as seen at the movie theater), the complete picture is projected in front of us at a moving rate of 45 images per second; video pictures (in the form of TV images) are scanned, line-by-line, at a high rate of speed (6 million bits per second) to give a visual image rate at 60 images per second.
5. In order for the carrier to contain the complete television signal, it must carry:
   - *Luminance information:* Picture brightness
   - *Synchronization pulses:* Synchronize the transmitter and receiver
   - *Blanking pulses:* Tell the image when to turn on and off
   - *Audio:* Sound information
6. The three primary additive colors are red, blue, and green. The three subtractive colors are:
   - *Cyan:* A combination of blue and green
   - *Yellow:* A combination of red and green
   - *Magenta:* A combination of blue and red
7. The three essential qualities of videoconferencing systems are:
   - *High-Quality:* The transmission system is called *full–frame,* and achieves the quality expected from professional studios. Transmissions are sent over high bandwidth media and are typically fiber-optics or satellite. Utilizes high resolution TV and high-quality speakers on the receiving end. High cost.
   - *Medium-Quality:* Compromises the video and sound quality in order to carry the image over limited bandwidth. Video quality is less than commercial TV quality. Medium-priced VC systems, with lower-priced camera and microphones. Video and audio are compressed to enable travel over the bandwidth.
   - *Low-Quality:* Images are jerky and audio is harsh. Equipment is low cost and available for use in homes and home offices. Typically used over a broadband connection such as cable modem and DSL. Low cost and low quality.
8. Persistence of vision is the rapid presentation of frames of video information that give the illusion of smooth motion.
9. Image scanning consists of “looking” in horizontal passes across the target image and measuring the instantaneous amplitude that represents the reflected light energy. Each pass across the image by the scanning element is called a scan line. The video camera contains an image tube, or target, that automatically scans the scene and generates a corresponding electric output which replicates, in electronic form, the image that the camera sees.
10. Some of the facts reported on digital television in 2001 are:
   - As of November 15, 2000, 98 percent of TV licensees and permittees in all markets had filed DTV construction permit applications.
   - 37 of 40 DTV stations in the top ten markets were on the air.
   - 79 percent of the broadcasters stated that they had no difficulty in obtaining financing for the DTV transition.

- Phillips Electronics North American corporate reported DTV sales in 2000 quadrupled those in 1999.
- Thompson Consumer Electronics noted that the consumer chose from more than 150 DTV products at steadily increasing performance levels and steadily decreasing prices.

Chapter 13

True/False

1. F
2. F
3. F
4. T
5. F

Multiple Choice

1. a
2. b
3. a
4. b
5. c

Short Essay Questions

1. VoIP is being sought as a means of network convergence to reduce telephone costs and to allow for enhanced telephone services. VoIP also promises to enhance network productivity and efficiency. Enhanced productivity and efficiency are achieved through modern compression schemes that better utilize bandwidth. Using VoIP allows a user to use the old PSTN to put a lot more information on the network.
2. There are several benefits of LAN telephony, the most obvious is cost savings. There are several other benefits that may not be so obvious, such as simplified management and computer and telephone integration.
3. There are several difficulties involved with VoIP. There can be delays in packetizing, which causes VoIP to be ineffective. Jitter is also a problem, as well as traffic capacity. Both of these factors can cause problems such as network overload and congestion.
4. There are several steps to digitization of an analog voice signal. The analog signal is sampled, according to the Nyquist sampling rate. After a signal is sampled, it is quantitized. This step involves assigning a binary 1 or 0 to the sample. Encoding is the last step. Encoding is

simply packaging the quantitized signal (the 1s and 0s) so they can be sent over the network. There are several coding packages available, the most common in the United States are B8ZS and AMI.

5. Jitter is caused when IP packets travel through routers, which operate on a first-come, first-served basis. Routers may handle large file transfers prior to handling a small voice packet. The delay causes network congestion, making VoIP ineffective. This delay is similar to stopping at a toll both on a highway: traffic must slow down or stop to pass through the gate, causing traffic congestion.

Appendix B

Glossary

Adaptive array (AA): Continually monitors received signal for interference. The antenna automatically adjusts its directional characteristics to reduce the interference. Also called adaptive antenna array.

Adjacent channel interference: Interference of a signal caused by signal transmissions of another frequency too close in proximity.

Alternate mark inversion (AMI): The line coding format in T-1 transmission systems whereby successive 1s (marks) are alternately inverted (sent with polarity opposite that of the preceding mark).

Alternating current (AC): Typically, the 120-V electricity delivered by the local power utility to the three-pin power outlet in the wall. The polarity of the current alternates between plus and minus, 60 times per second.

Ampere (amp): A unit of measurement for electric current. One volt of potential across a 1-ohm impedance causes a current flow of 1 ampere.

Amplitude modulation (AM): Carrier signal added to by an information signal to create a joint effort to deliver the original signal as far and efficiently as possible.

Analog: A way of sending signals in which the transmitted signal is analogous to the original signal. Also, telephone switching that is not digital.

Antenna gain: The measure in decibels of how much more power an antenna will radiate in a certain direction with respect to that which would be radiated by a reference antenna.

Application programs: Computer software designed for a specific job, such as word processing, accounting, spreadsheet, etc.

Application layer: The seventh and highest layer of the open source interconnect data communications model of the International Standards Organization. It supplies functions to applications or nodes, allowing them to communicate with other applications or nodes.

Arithmetic and Logic Unit (ALU): The part of the CPU that performs the arithmetic and logical operations.

Asynchronous transfer mode (ATM): Very high-speed transmission technology that uses high bandwidth, low delay, and connection-oriented packet-like switching and multiplexing technique. Usable capacity is segmented into 53 byte fixed-size cells consisting of header and information fields.

Atoms: The smallest particle of an element that can exist alone or in combination.

Attenuation: The decrease in power of a signal, light beam, or light wave, either absolutely or as a fraction of a reference value. The decrease usually occurs as a result of absorption, reflection, diffusion, scattering, deflection, or dispersion from an original level and usually not as a result of geometric spreading.

Automatic call distribution (ACD): A specialized phone system originally designed simply to route incoming calls to all available personnel so that calls are evenly distributed. An ACD recognizes and answers an incoming call, looks in its database for instructions on what to do with that call, sends the call to a recording or voice response unit or to an available operator.

Availability formula: This formula is used to calculate how reliable the equipment that is being installed will be for a particular application.

Bandwidth: The width of a communications channel. In analog communications, bandwidth is typically measured in Hertz (cycles per second). In digital communications, bandwidth is typically measured in bits per second (bps).

Basic rate interface (BRI): Supports a total signaling rate of 144 kbps, which is divided into two B or bearer channels running at 64 kbps, and a D or data channel runing at 16 kbps. The bearer channels carry the actual voice, video, or data information and the D channel is used for signaling.

Beamwidth: The width of the main lobe of an antenna pattern, usually defined as 3 db down from the peak of the lobe.

Binary: Where only two values or states are possible for a particular condition, such as "on" or "off" or "1" or "0." Binary is the way digital computers function because it represents data as on or off.

BIOS: Basic Input/Output System of desktop computers. The BIOS contains the buffers for sending information from a program to an actual hardware device.

Bipolar 8 zero substitution (B8ZS): A technique used to accommodate the density requirement for digital T-carrier facilities in the public network, while allowing 64 kbps clear data per channel. Rather than inserting a 1 for every seven consecutive 0s, B8ZS inserts two violations of bipolar line encoding technique for digital transmission links.

Bit error rate (BER): The percentage of received bits in error compared to the total number of bits received.

Bus: An electrical connection that allows two or more wires or lines to be connected together. Typically, all circuit cards receive the same information that is put on the bus, but only the card the information is "addressed" to will use that data.

Bus structure: A network topology in which nodes are connected to a single cable with terminators at each end.

Caller identification (CLID): One of several custom local area signaling services (CLASS) provided by the local exchange carrier. The service that allows you to see the name and number of the person who is calling you.

Capacitor: Capacitors provide a means of storing electric charge so that it can be released at a specific time or rate. A capacitor acts as a battery but does not use a chemical reaction.

Carrier Sense Multiple Access/Collision Detection (CSMA/CD): Also known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

Cell sites: A transmitter-receiver location, operated by the wireless service provider, through which radio links are established between the wireless system and the wireless unit.

Cellular service: Also known as cellular mobile telephone system. A wireless telephone system using multiple transceiver sites linked to a central computer for coordination.

Central processing unit (CPU): The part of a computer that performs the logic, computation, and decision-making functions. It interprets and executes instructions as it receives them. PCs have one CPU, typically a single chip.

Channel: Typically what you rent from the telephone company, voice-grade transmission facility with defined frequency response, gain, and bandwidth. A path of communication, either electrical or electromagnetic, between two or more points. Also a circuit, facility, line, or path.

Channel service unit (CSU) or digital service unit (DSU): Devices used to interface between transmitting equipment and the external circuit in the wide area network that will carry the information.

Circuit switching: A dedicated connection or circuit between two parties. The circuit is maintained as long as the connection remains open. When one party hangs up or disconnects, the dedicated circuit is broken and the call ends.

Code division multiple access (CDMA): Spread-spectrum cellular phone service that assigns a code to all speech bits, sends a scrambled transmission of the encoded speech over the air and reassembles the speech to its original format.

Companding: The process where there is a greater number of samples provided at lower power conditions of the signal waveform rather than at the higher power portions of the same waveform.

Competitive local exchange carriers (CLECs): A competitive access provider that also provides switched local services, such as local dial tone and Centrex. CLECs are authorized by state commissions to resell existing incumbent LEC services at wholesale rates and lease component facilities for use with their own facilities.

Compression: Reducing the representation of information, but not the information itself. Reducing the bandwidth or number of bits needed to encode information or encode a signal, typically by eliminating long strings of identical bits or bits that do not change in successive sampling intervals. Compression saves transmission time or capacity. It also saves space on storage devices such as hard disks, tape drives, and floppy disks.

Conductor: A material that allows the easy transfer of electrons from one atom to another.

Current: A measure of how much electricity passes a point on a wire in a given time frame. Current is measured in amperes or amps.

Cycle: One complete sequence of an event or activity. Often refers to electrical phenomena. One electrical cycle is a complete sine wave.

Cyclical redundancy check (CRC): A process used to check the integrity of a block of data. It provides an integrity check of the data before it is sent out into the wide area network. Its value depends on the hexadecimal value of the number of 1s in the data block. The transmitting device calculates the value and appends it to the data block; the receiving end makes a similar calculation and compares its results to the added character. If there is a difference, the recipient requests retransmission.

Data link layer: The second layer of the Open Systems Interconnection data communications model of the International Standards Organization. It puts messages together and coordinates their flow. Also used to refer to a connection between two computers over a phone line.

Data networking switches: Equipment that performs the functions of establishing and releasing connections on a data network.

Decoding: Changing a digital signal into analog form or another type of digital signal. The opposite of encoding.

Dielectric: A nonconducting or insulating substance that resists passage of electric current, allowing electrostatic induction to act across it, as in the insulating medium between the plates of a condenser.

Diffraction: Signal loss as a result of variations in the terrain the signal crosses.

Digital modem: A piece of equipment that joins a digital phone line to a piece of communication equipment, which may be a phone or a PC. Such equipment allows testing, condition, timing, interfacing, etc. But it does not do what a modem does: namely convert digital signals from machines into analog signals which can be carried on analog phone lines. The term digital modem, thus, is somewhat of a misnomer.

Digital PABX: An automatic switching system. No operator is needed to complete the call. In the original PBX system operators were sometimes needed to complete the calls. Also called Private Automatic Branch Exchange.

Digital subscriber line: A generic name for a family of digital lines being provided by CLECs and local telephone companies to their local subscribers.

Digitize: Converting an analog or continuous signal into a series of 1s and 0s, i.e., into a digital format.

Diode: Devices that conduct electricity in one direction only. They are sometimes referred to as PN (positive-negative) devices because they are made of a single semiconductive crystal with a positive terminal and a negative terminal.

Direct current: A flow of electricity always in the same direction.

Direction of arrival (DoA): The electromagnetic waves arrive at the directional antenna and are received more readily from one direction than from another. The antenna needs to be aligned with the direction of arrival.

Downlink frequencies: Frequencies used in the transmission link reaching from a satellite to the ground.

DS-0: Digital Signal, level 0. A DS-0 is a voice-grade channel of 64 kbps.

Dual tone multifrequency (DTMF): A term describing push button or touch-tone dialing. When you push a button, it makes a tone that is actually a combination of two tones, one high frequency and one low frequency.

Dynamically phased array (PA): Type of radio antenna used in certain satellite and wireless communications. This small flat antenna mounts on the side of a building or on a rooftop. It has an array of chip-based radio receivers, which lock in on the target transmission frequency on a dynamic basis. Also called a "pizza box antenna."

Electron: A light, subatomic particle that carries a negative charge.

Encapsulation: An electronic messaging term. The technique used by layered protocols in which a layer adds header information to the protocol data unit from the layer above.

Encoding: The process of converting data into code or analog voice into a digital signal.

Ethernet: A local area network standard officially known as IEEE 802.3. A physical and data link protocol that uses CSMA/CD.

Expand: To increase in extent, number, volume, or scope.

Extended SuperFrame: A new version of the SuperFrame that allows for more frames to be grouped together. In a T1 circuit, each of the 24 DS0 channels are sampled every 125 microseconds and 8 bits are taken from each. If you multiply the 8 bits by the 24 channels, you get 192-bits in a chain, and then add one bit for timing, you get 193 total bits in one frame. Twelve frames comprise the SuperFrame. For the Extended SuperFrame, we double the number of frames, making the total 24.

Fading: Signal disruption caused by multipath signals and heavy rains.

Fiber-optic: A strand of very pure, very clear glass that can carry more information longer distances.

Fixed wireless access (FWA): Replaces the last mile from the central office to the customer. This process usually consists of a pair of digital radio transmitters placed on rooftops, one at the central office and one at the users' site. These systems usually operate at the 38 Ghz portion of the spectrum. Also known as wireless fiber (because of the high speeds of throughput) and as fixed wireless local loop.

Frame relay: An access standard defined by the ITU-T. Frame relay employs a form of packet switching analogous to a streamlined version of X.25 networks. The packets are in the form of frames, which are variable in length, with the payload anywhere between 0 and 4096 octets.

Free electrons: Electrons that are not attached to an atom or molecule. Also known as static electricity.

Free space and atmospheric attenuation*:* Defined by the loss the signal undergoes traveling through the atmosphere. Changes in air density and absorption by atmospheric particles are principle reasons for affecting the microwave signal in a free air space.

Frequency: The rate at which an electromagnetic waveform alternates, usually measured in Hertz.

Frequency diversity: A form of backup used to protect a radio signal. A second signal continually operates on a separate frequency and assumes the load when the regular channel fails.

Frequency division multiplexing (FDM): An older technique in which the available transmission bandwidth of a circuit is divided by frequency into narrow bands, each used for a separate voice or data transmission channel, which many conversations can be carried on one circuit

Frequency division multiple access (FDMA): FDMA is the allocation of specific channels within a defined radio frequency bandwidth to carry a specific user's information. FDMA is a mature, reliable method of RF communication, but requires more spectrum than competing technologies to deliver its payload.

Frequency modulation (FM): A modulation technique in which the carrier frequency is shifted by an amount proportional to the value of the modulating signal. The amplitude of the carrier signal remains constant. The information signal causes the carrier signal to increase or decrease its frequency based on the waveform of the information signal.

Full wave rectifier: Diodes designed to be placed in an alternating current circuit and to convert alternating current into direct current.

Full-duplex: A transmission mode that supports transmissions in two directions simultaneously or, more technically, bidirectional simultaneous two-way communications.

GSM: Originally stood for Groupe Speciale Moble, but is now known as Global System for Mobile Communications. It is the standard for cellular phone service in Europe, Japan, and Australia, and will soon be the standard for 30 to 50 percent of the cellular networks in the Untied States.

Half-duplex: A circuit designed for data transmission in both directions but not at the same time.

Handoffs (or switching): A cellular call is switched from one cell tower to another as the user moves from one area to the next. The switch is usually unnoticed by the user.

Hard handoff: Sometimes a cell phone user being switched from one site to the next will need to be disconnected and reconnected to make the switch possible. Also called a "break and make" handoff, it is usually unnoticed by the user.

Hertz: The basic measurement of bandwidth frequency in cycles per second. 1 Hertz equals 1 cycle per second.

Hot standby: Secondary equipment in place as a back up in case of primary equipment failure.

In band: Made up of tones that pass within the voice frequency band and are carried along the same circuit as the talk path established by the signals. Also known as in-band signaling.

Inductor: Inductance allows a circuit to store up electrical energy in electromagnetic form. An inductor is formed by winding a conductor into a coil. This helps overcome resistance.

Insulator: A material that does not conduct electricity but is suitable for surrounding conductors to prevent the loss of current.

Interference: Electromagnetic energy that is picked up with the signal you are receiving. This extra energy distorts the signal and interferes with its transmission.

International Standards Organization: A voluntary, nontreaty organization based in Geneva chartered by the UN. Its role is to define international standards covering all fields other than electrical and electronic engineering, which fall under the International Electrotechnical Commission.

Internet service provider (ISP): A vendor who provides access for customers to the Internet and the World Wide Web.

Intracell handovers: A cellular call is passed from one frequency to the next or carrier to the next within a single cell site.

ISDN (Integrated Services Digital Network): There are two forms of ISDN: PRI and BRI. BRI interface supports a total signaling rate of 144 kbps, which is divided up into two B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps. The bearer channels carry the actual voice, video, or data information, and the D channel is used for signaling. PRI or primary rate interface provides the same throughput as a T-1 1.544 Mbps, has 23 B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps.

ISM (industrial, scientific, and manufacturing) frequencies: A term describing several frequencies in the radio spectrum set aside for specific purposes.

Least cost routing (LCR): The automatic selection of the most economically available route for each outgoing trunk call. Also known as automatic route selection.

Line-of-sight (LOS): Defined by the Fresnel Zone. Fresnel zone clearance is the minimum clearance over obstacles that the signal needs to be sent over. Reflection or path bending occurs if the clearance is not sufficient.

Local loop: The physical connection from the subscriber's premises to the carrier's point of presence (POP). The local loop can be provided over any suitable transmission medium.

Local multipoint distribution services (LMDS): A method of distributing TV signals to households in a local community. LMDS uses broadcast microwave signals to contact local dishes. The received signal is then distributed through the central CATV system.

Mobile base stations (MBS): Component of cellular network that provides data link relay functions for a set of radio channels serving a cell.

Mobile switching center (MSC): The location of the digital access and cross-connect system (DACS) in a cellular telephone network.

Mobile telephone switching office (MTSO): Controls the entire operation of a cellular system. It is a sophisticated computer that monitors all cellular calls, arranges handoffs and manages billing information.

Molecules: The smallest particle of a substance that retains all the properties of the substance and is composed of one or more atoms.

Multichannel multipoint distribution services (MMDS): An FCC name for a service where multiple video channels are broadcast within a limited geographic area. Often called wireless cable.

Multiplexing: To transmit two or more signals over a single channel.

Network layer: The third layer of the OSI model of data communications. It involves routing data messages through the network on alternate routes. Also called the packet layer.

Neutron: A subatomic particle with no charge. Along with protons, neutrons make up the nucleus.

Node: A point of connection into a network. In multipoint networks, is a unit that is polled. In LANs, it is a device on the ring. In packet switched networks, it is one of the many packet switches that form the network's backbone.

Nucleus: The core of the atom that is made up of neutrons and protons.

Nyquist theorem: Theorem that dictates that sampling should occur at a rate that is twice the highest frequency being sampled.

Ohm's law: This law applies to any resistive circuit with one of the values unknown and will allow the discovery of the unknown value.

Operating system: A software program that manages the basic operations of a computer system. It calculates how the computer main memory will be apportioned, how and in what order it will handle tasks assigned to it, how it will manage the flow of information into and out of the main processor, how it will get material to the printer for printing and to the screen for viewing, how it will receive information from the keyboard, etc.

Optical modulation: The process of varying some characteristics of light pulses over a fiber-optic cable in order to pass information from one point to another.

Out of band: A LAN term which refers to the capacity to deliver information via modem or other asynchronous connection. Out-of-band signaling refers to signaling that is separated from the channel carrying the information. Signal and control information does not interfere with the data transmission.

Overreach interference: Caused by a signal feeding past a repeater (or receive antenna) to the receiving antenna at the next station in the route.

Period: The time it takes a waveform to complete one complete cycle.

Physical layer: Layer 1 of the OSI data communications model. This layer includes all electrical and mechanical aspects relating to the connection of a device to a transmission medium, such as the connection of a workstation to a LAN.

Polarization: The direction of the electric field, the same as the physical attitude of the antenna (e.g., a vertical antenna transmits a vertically polarized wave). They receive and transmit antennas need to possess the same polarization.

Power (P): The measure of the rate at which work can be accomplished.

Presentation layer: The sixth layer of the Open Systems Interconnect model controls the formats of files, screens, and graphics for display or printing. Its main function is to code and decode data transmitted within the OSI communication protocol as well as data encryption. Examples of presentation layer protocols include HTTP, Telnet, and AppleTalk Filing protocol (AFP).

Primary rate interface (PRI): Provides the same throughput as a T-1, 1.544 Mbps, has 23 B or bearer channels, which run at 64 kbps, and a D or data channel, which runs at 16 kbps.

Private branch exchange (PBX): A small version of the phone company's central switching office. Also known as a private automatic branch exchange.

Protons: A heavy subatomic particle that carries a positive charge.

Public switched telephone network (PSTN): Refers to the local, long distance, and international phone system which we use every day. In some countries, it is a single phone company. In countries with competition, PSTN refers to the entire interconnected collections of local, long distance, and international phone companies, of which there could be thousands.

Pulse amplitude modulation (PAM): The first step in converting analog waveforms into digital signals for transmission.

Pulse code modulation (PCM): The most common and most important method that a telephone system in North America can use to sample a voice signal and convert that sample into an equivalent digital code. PCM is a digital modulation method that encodes a pulse amplitude modulated signal into a PCM signal.

Quality of service (QoS): A measure of the telephone service quality provided to a subscriber.

Quantitizing: The systematic method of providing standard binary numbering to PAM samples for PCM conversion.

Radiation field: The radio frequency field that is created around the antenna and has specific properties that affect the signal transmission

Rain attenuation or raindrop absorption: The scattering of the microwave signal, which can cause signal loss in transmissions.

Range: The distance a signal travels before it degrades and needs to be repeated.

Reciprocity: An antenna characteristic that essentially states that the antenna is the same regardless of whether it is sending or receiving electromagnetic energy.

Rectifier: A diode designed to be placed in an alternating current circuit, used for converting AC to DC.

Reflections: When the microwave signal traverses a body of water or fog bank and causes multipath conditions.

Resistance (Ω): The opposition to the flow of electric charge and is generally the function of the number of free electrons available to conduct the electric current.

Resistor: A component made of a material that has a specified resistance or opposition to the flow of electrical current. A resistor is designed to oppose but not completely obstruct the passage of electrical current.

Resonant frequency: The frequency where inductive reactance equals capacitive reactance. Helps to define the maximum current or maximum voltage in a circuit.

Ring side: The side of the cable pair that when measured will read –48 V DC.

Rotary (or pulse) dialing: The circular telephone dial. As it returns to its normal position, it opens and closes the electrical loop sent by the central office. Rotary dial telephones momentarily break the DC circuit to represent the digits dialed.

Router: In software, a router is a system-level function that directs a call to an application. In hardware, routers are the central switching offices of the Internet and corporate intranets and WANs. Routers operate at Layers 3 and 4 of the OSI data communications model.

Server: A shared computer on the local area network that can be as simple as a regular PC set aside to handle print requests to a single printer it may be used as a repository and distributor of data.

Service control points (SCP): The local versions of the national 800 number database. They contain the intelligence to screen the full ten digits of an 800 number and route calls to the appropriate long distance carrier.

Service switching points (SSP): A switching system, including its remotes, that identifies calls associated with intelligent network services and initiates dialog with the SCP.

Service transfer points (STP): A signaling point with the function of transferring messages from one signaling link to another and considered exclusively from the viewpoint of the transferor.

Session layer: The fifth layer of the OSI data communications model. Also known as the network-processing layer. It sets up the conditions whereby individual nodes on the network can communicate or send data to each other.

The session layer is responsible for binding and unbinding logical links between users. It manages, maintains, and controls the dialog between the users of the service.

Signal-to-interference ratio (SIR): The ratio of the usable signal being transmitted to the noise or undesired signal.

Signaling System 7 (SS7): SS7 employs a dedicated 64-kb data circuit to carry packetized machine language messages about each call connected between and among machines of a network to achieve connection control.

Single sideband carrier: An amplitude modulation technique for encoding analog or digital data using either analog or digital transmission. Single sideband suppresses one sideband of the carrier frequency at the source. As such, less power is used, and less bandwidth is required.

Skin affect: The concept that high-frequency energy travels only on the outside skin of a conductor and does not penetrate into it any great distance.

Space diversity: Protection of a radio signal by providing a separate antenna located a few feet below the regular antenna on the same tower to assume the load when the regular transmission path on the tower fades.

Space division multiple access (SDMA): Intelligent antenna systems use this access method to increase the capacity of cellular radio networks by separating frequencies within a cell site and allowing the same frequencies to be reused.

Spectrum: The radio frequency that is available for personal, commercial, and military use.

Statistical time division multiplexing (STDM): This form of multiplexing uses all available time slots to send significant information and handles inbound data on a first-come, first-served basis.

Stored-program concept: The location of the instructions placed in the memory of a common controlled switching unit and to which it refers while processing a call.

Subscriber loop: The circuit that connects the telephone company's central office to the demarcation point on the customer's premises. The circuit is most likely a pair of wires.

SuperFrame: A synchronization-framing format for a T1. In a T1 circuit, each of the 24 DS0 channels are sampled every 125 microseconds and 8 bits are taken from each. If you multiply the 8 bits by the 24 channels, you get 192-bits in a chain, and then add one bit for timing, you get 193 total bits in one frame. Twelve frames comprise the SuperFrame. A newer version of this T1 formatting is called Extended Super Frame (ESF).

Switch: A mechanical, electrical, or electronic device that opens or closes circuits, completes or breaks an electrical path, or selects paths or circuits. A switch looks at incoming data to determine the destination address. Based on that address, a transmission path is set up through the switching matrix between the incoming and outgoing physical communications ports and links.

Switch Control Point (SCP) also known as Service Control Point (SCP): Provides computer services, such as database information, that defines the possible services and their logic.

Switched beam: Also called switch lobe. Smart antennas use power patterns that are more concentrated and directed than the regular antenna. The far end device receives a much more powerful signal from the antenna.

Switched lobe (SL): Also called switch beam. Smart antennas use power patterns that are more concentrated and directed than the regular antenna. The far end device receives a much more powerful signal from the antenna.

Switched virtual circuit (SVC): A virtual circuit connection established across a network on an as-needed basis and lasting only for the duration of the transfer.

System: An organized assembly of equipment, personnel, procedures, and other facilities designed to perform a specific function or set of functions.

T-1: Trunk Level 1. A digital transmission link with a total signaling speed of 1.544 Mbps.

Tandem switch: A tandem switch connects one trunk to another. An intermediate switch or connection between an originating telephone call location and the final destination of the call. The tandem point passes the call along.

Throughput: The actual amount of useful and nonredundant information that is transmitted or processed. Throughput is the end result of a data call.

Time division multiple access (TDMA): One of several technologies used to separate multiple conversation transmissions over a finite frequency allocation of through-the-air bandwidth. TDMA is used to allocate a discrete amount of frequency bandwidth to each user in order to permit many simultaneous conversations. However, each caller is assigned a specific time slot for transmission.

Time division multiplexing (TDM): A technique for transmitting a number of separate data, voice, and video signals simultaneously over one communications medium by interleaving a piece of each signal one after another.

Tip side: Side of the line when measured with a voltmeter to an earth ground that should read zero voltage.

Transport layer: The fourth layer in the OSI data communications model. It is partly responsible for the end-to-end control of transmitted information and the use of network resources. Layer 4 defines the protocols governing message structure and portions of the network's error-checking capabilities.

Transport layer protocol: A protocol that provides end-to-end data integrity and service quality on a network.

Uplink frequencies: In satellites, the frequency used from the earth station up to the satellite. In data, the frequency used to send data from a station to a head end or mainframe.

Voice mail (VM): An application that allows you to receive, edit, and forward messages to one or more mailboxes.

Voice processing: A system that recognizes spoken words as well as touch tones from telephones. Basically, a "voice" computer in that it (theoretically) can do anything a computer can do, and can recognize voice commands.

Volt: The unit of measurement of electromotive force. It is expressed as the potential difference in available energy between two points. One volt is the force required to produce a current of one ampere through a resistance or impedance of 1 ohm.

Voltage: The pressure under which a flow of electrons moves through a device.

WAN (Wide Area Network): A computer and voice network that encompasses a large area (larger than a metropolitan area network).

Watt: The unit of electricity consumption and representing the product of amperage and voltage.

Waveforms: The characteristic shape of a signal usually shown as a plot of amplitude over a period of time.

Waveguide: A conducting or dielectric structure able to support and propagate one or more modes. More specifically, a hollow, finely engineered metallic tube used to transmit microwave radio signals from the microwave antenna to the radio and vice versa.

Wavelength: The length of a wave measured from any point on one wave to the corresponding point on the next wave.

Wireless local loop (WLL): A means of provisioning a local loop facility without wires. Employing low power, omnidirectional radio systems, they allow carriers to provision loops up to T-1 capacity to each subscriber.

Zero code suppression (ZCS): The insertion of a “1” bit to prevent the transmission of eight or more consecutive “0” bits.

Index

A

B

C

D

E

F

G

H

I

J

L

M

P

T

U

V

W

X

Z