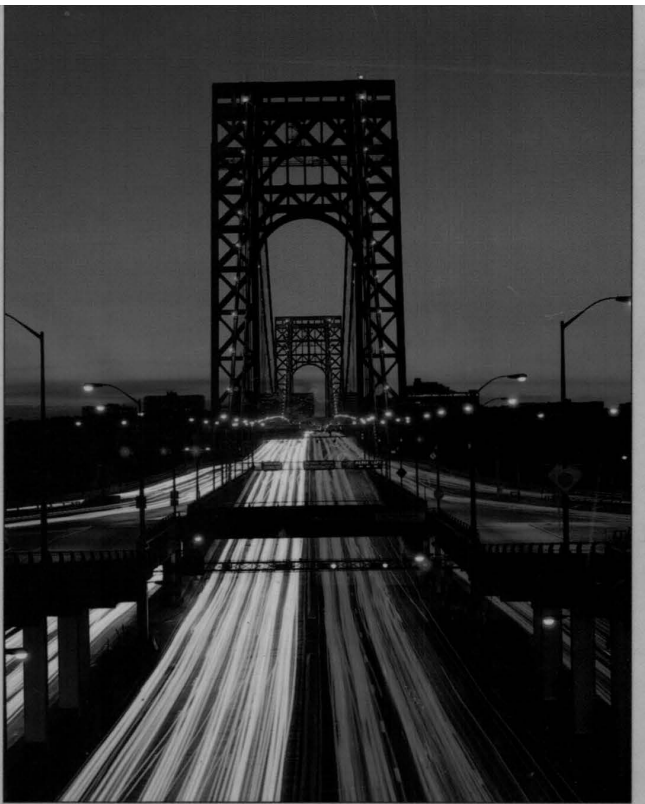
MTP
MACMILLAN TECHNICAL PUBLISHING U·S·A



MACMILLAN NETWORK ARCHITECTURE & DEVELOPMENT SERIES

WIRELESS LANs

Implementing Interoperable Networks

Jim Geier

Wireless LANs

Implementing Interoperable Networks

Jim Geier

MACMILLAN
TECHNICAL
PUBLISHING
U•S•A

Wireless LANs: Implementing Interoperable Networks

FIRST EDITION

International Standard Book Number: 1-57870-081-7

Library of Congress Catalog Card Number: 98-85498

2001 00 99 98 4 3 2 1

Interpretation of the printing code: The rightmost double-digit number is the year of the book's printing; the rightmost single-digit, the number of the book's printing. For example, the printing code 98-1 shows that the first printing of the book occurred in 1998.

Composed in Bergamo and MCPdigital by Macmillan Computer Publishing

Printed in the United States of America

Trademark Acknowledgments

Warning and Disclaimer

This book is designed to provide information about wireless LAN technology. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an as-is basis. The authors and Macmillan Technical Publishing shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

Feedback Information

At Macmillan Technical Publishing, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us at `networktech@mcp.com`. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher
Jim LeValley

Executive Editor
Linda Ratts Engelman

Managing Editor
Caroline Roop

Acquisitions Editor
Karen Wachs

Development Editor
Thomas Cirtin

Project Editor
Laura N. Williams

Copy Editor
Keith Cline

Indexer
Tim Wright

Proofreader
Julie Searls

Acquisitions Coordinator
Amy Lewis

Manufacturing Coordinator
Brook Farling

Book Designer
Gary Adair

Cover Designer
Sandra Schroeder

Production Team Supervisor
Tricia Flodder

Production
Eric S. Miller

About the Author

Jim Geier is an internationally known consultant, author, and speaker on wireless LAN technologies and implementation strategies. He is currently the director of Network and Software Systems at Monarch Marking Systems, an international leader in providing bar code system solutions. Jim's department develops wireless system tools and application software for companies and organizations worldwide.

Jim is the author of *Wireless Networking Handbook* (1996, New Riders Publishing) and *Network Reengineering* (1996, McGraw-Hill), as well as numerous articles in leading publications, including *Network Magazine* and *Byte*. Jim has instructed courses internationally on computer-related topics, including wireless networking, software development, and project management, for George Washington University and Technology Training Corporation. He speaks regularly at conferences and tradeshows held throughout the world.

Jim served as chairman of the Institute of Electrical and Electronic Engineers (IEEE) Computer Society, Dayton Section, and chairman of the IEEE International Conference on Wireless LAN Implementation. He was an active member of the IEEE 802.11 working group, responsible for developing international standards for wireless LANs.

Jim's past 20 years of experience include a variety of consulting and management positions. At Wright-Patterson Air Force Base in Ohio, Jim managed the design and operational support of numerous LANs and a wide area network that supports over 10,000 users. For the base, he evaluated the effectiveness of wireless network technologies for use in mobile and portable office environments. He led the development of a tool to aid engineers in the installation of wireless networks and evaluated commercial network technologies for use with U.S. government mobile sensor systems.

He was the principal investigator for a small business innovative research grant to develop an automated software tool that assists engineers in planning, upgrading, and maintaining information systems. He managed a test team responsible for testing computer networks throughout the world. He has developed corporate information system standards for companies migrating from mainframe to client/server systems.

Jim holds a B.S. degree from California State University, Sacramento, and an M.S. degree from Air Force Institute of Technology, both in electrical engineering with emphasis in computer networks. As part of his master's thesis, he developed and implemented an adaptive automatic routing algorithm for a worldwide packet radio network.

Jim's hobbies include sailing and amateur radio (KC8KQH). He resides with his wife and four sons in Yellow Springs, Ohio. You can reach him at `jimgeier@aol.com`.

Dedication

I dedicate this book to my wife, Debbie, for her loving support of my writing efforts.

Acknowledgments

When writing this book, I was fortunate to work with an excellent team at Macmillan Technical Publishing, whose contributions vastly improved the presentation of this book. In particular, Tom Cirtin, development editor, did an outstanding job guiding me through the revision of the text. Tom's ideas and his editing enhanced this book's readability and use as a tool for implementing wireless LANs.

I'd also like to give special thanks to Ed Lamprecht for performing the technical review of the book's manuscript. Ed's valuable suggestions greatly refined this book.

About the Technical Reviewers

These reviewers contributed their considerable practical expertise to the entire development process for *Wireless LANs*. As the book was being written, these folks reviewed all the material for technical content, organization, and flow. Their feedback was critical to ensuring that *Wireless LANs* fits our readers' need for the highest quality technical information.

D. Ed Lamprecht is a Senior Systems Engineer at Monarch Marking Systems with 15 years of programming experience in applications and operating systems. He received a bachelor's degree in 1983 from the University of Northern Iowa and started his career with NCR Corporation programming operating systems in assembly for retail computing systems. It was during this time that Ed also developed applications for other platforms, including UNIX and DOS.

In 1988, Ed joined Monarch Marking Systems, a company specializing in bar code printers and labels. Here he developed bar code applications for MS-DOS and Microsoft Windows 2.0 and later, including PC drivers and TSRs and connectivity software. Since 1996, Ed has been involved in data collection systems providing wireless network connectivity solutions of handheld printers and data collection terminals for retail, industrial, manufacturing, and health care markets.

At Monarch, Ed has developed client/server applications, visited customer sites for analysis and problem solving, and provided international training on products and wireless connectivity. Ed holds six patents in bar code software and handheld printer and data collectors.

Ed lives with his wife, Michelle, and his son, Colin, in Dayton, Ohio. When not tinkering with PCs and networks at home, he enjoys model railroading, railroad memorabilia collecting, golfing, traveling, and spending time with his son.

Peter Rysavy is a consultant specializing in wireless communication and other technologies related to personal and mobile communication. His firm, Rysavy Research, assists clients with market research, product and business development, and technology assessment. Peter is the chairman of the standards committee of the Portable Computing and Communications Association (PCCA), a standards group that produces wireless-data standards.

Since 1993, Peter has worked as a consultant with numerous clients on projects involving mobile and wireless communication. Clients include cellular carriers, communications software companies, network hardware companies, investment firms, automotive electronics companies, research organizations, and universities. He also teaches seminars and writes articles about wireless communication.

Peter graduated with an MSEE from Stanford University in 1979, where he was involved in several collaborations between academia and industry. Joining Fluke Corporation in 1979, he designed communications hardware and software for data-acquisition products. From 1981 to 1983, he designed ethernet networking hardware at Time Office Computers in Australia. He rejoined Fluke, and until 1988 managed the development of a family of communication-oriented touch terminals. From 1988 to 1993, Peter was VP of Engineering and Technology at Traveling Software (makers of LapLink). His last major project was LapLink Wireless. He also managed the development of LapLink and connectivity solutions for a broad variety of mobile platforms.

Contents at a Glance

Contents

Introduction

Wireless LAN technology is rapidly becoming a crucial component of computer networks, and its use is growing by leaps and bounds. Thanks to the finalization of the IEEE 802.11 wireless LAN standard, wireless technology has emerged from the world of proprietary implementations to become an open solution for providing mobility as well as essential network services where wireline installations proved impractical. Now companies and organizations are increasingly investing in wireless networks to take advantage of mobile, real-time access to information.

Most wireless LAN suppliers now have 802.11-compliant products, allowing companies to realize wireless network applications based on open systems. The move toward 802.11 standardization is lowering prices and enabling multiple-vendor wireless LANs to interoperate. This is making the implementation of wireless networks more feasible than before, creating vast business opportunities for system implementation companies and consultants.

Many end-user companies and system integrators, however, have little knowledge of, and experience in, developing and implementing wireless network systems. In many cases, there is also confusion over the capability and effectiveness of the 802.11 standard. The implementation of wireless networks is much different from traditional wired networks. In contrast to ethernet, a wireless LAN has a large number of setup parameters that affect the performance and interoperability of the network. An engineer designing the network and the person installing the network must understand these parameters and how they affect the network. To address wireless installation issues, this book is full of implementation notes, especially regarding 802.11-compliant solutions.

To optimize the operation of wireless systems, you need to be familiar with software options for interfacing wireless handheld appliances to application software and databases located on the network. Terminal emulation, direct database connectivity, and middleware are alternatives that provide connectivity depending on system requirements. This book describes each of these in detail, and explains how to choose one over the others.

Altogether, this book provides a practical overview of wireless network technologies, with emphasis on the IEEE 802.11 wireless LAN standard and implementation steps and recommendations.

Who Will Benefit from This Book?

This book is primarily intended for readers having knowledge of networking concepts and protocols. Readers should be familiar with basic communications protocol handshaking processes and ethernet network infrastructures, for example. Readers should also be conversant with basic computer terminology, such as *local area network*, *client/server*, and *application software*. Project managers can also benefit from the book by learning important project-planning steps for wireless network implementations.

This book is aimed at the following audience:

- Information system (IS) staff and system integrators involved with analyzing, designing, installing, and supporting wireless LANs
- Engineers developing wireless LAN products and solutions
- Managers planning and executing projects for developing wireless products or implementing wireless LAN systems

Key Features of This Book

This book contains the following features that make it a practical guide for developing and implementing wireless LANs:

- Roadmaps at the beginning of each chapter clearly summarize the topics addressed in the chapter.
- Various case studies throughout the book anchor the reader in real-life examples.
- Implementation notes provide practical instruction in the concepts described in this book.
- Diagrams throughout the book illustrate technical issues and procedures.
- Tables convey crucial technical information at a glance.

- The glossary defines terms related to wireless network systems. It is a handy reference to use when reading this book or working on a wireless network project.
- A list of all the case studies (on the inside of the cover of this book) provides a handy reference to the examples of real-world implementation.

The Organization of This Book

To expedite the learning process required in mastering wireless LAN technology, this book follows a three-part sequence of related topics—beginning with explanations of essential concepts and culminating in solid implementation procedures. The book's organization is described in detail in the following sections.

Part I: Wireless Networks—A First Look

The first part of this book addresses introductory material as a basis for understanding the remaining elements. This portion will help the reader understand the concepts, benefits, and issues dealing with radio network systems, clearing up confusion of competing wireless solutions.

If you are already familiar with wireless networks, you might want to skip Chapter 1, "Introduction to Wireless Networks," and Chapter 2, "Wireless Network Configurations." In any case, be sure to read Chapter 3, "Overview of the IEEE 802.11 Standard," if you need an introduction to the standard for wireless LANs.

Part II: Inside IEEE 802.11

Part II is more challenging and contains in-depth coverage of the medium access and physical layers of the IEEE 802.11 standard. Chapter 4, "Medium Access Control (MAC) Layer," describes MAC operations and frame structures, and Chapter 5, "Physical (PHY) Layer," explains PHY operations and frame structures and helps readers select the type of 802.11 physical layer that best fits their needs.

Engineers designing wireless LAN solutions will find this part useful for understanding design options and tuning of an 802.11 network. Engineers developing 802.11-compliant products will find the coverage of the 802.11 standard beneficial when specifying new 802.11-compliant products. IS operational support staff will also find this part most useful to understand frame formats when troubleshooting network behavior.

Part III: Deploying Wireless LANs

The final chapters contain all the steps necessary to deploy a wireless LAN. Chapter 6, "Wireless System Integration," explains the technologies and components needed in addition to what 802.11 covers, such as MobileIP and application connectivity software. Chapter 7, "Planning a Wireless LAN," and Chapter 8, "Implementing a

Wireless LAN," describe the steps you should follow when planning, analyzing, designing, and installing a wireless system. A single case study, threaded throughout Chapters 7 and 8, provides details of a real project that help you understand how to implement the ideas presented in the chapters' step-by-step procedures.

In addition, special implementation notes throughout the chapters of Part III enable readers to directly apply what they have read in earlier chapters to solving the needs for wireless networks within their companies or organizations. IS staff, system integrators, and project managers can strongly benefit by using this part of the book as a practical guide that is based on the experiences and lessons learned from many wireless network projects.

Appendices

The appendices provide supplementary information related to wireless networks. Appendix A, "Automatic Identification and Data Capture (AIDC)," gives the reader an understanding of implementing bar code systems—a primary application of wireless LANs.

Appendix B, "Products, Companies, and Organizations," principally identifies the wireless network product suppliers and system integration companies. This appendix is useful to people looking for products and services when implementing a wireless network. It is also a quick reference for the organizations mentioned in this book.

CHAPTER 3

Overview of the IEEE 802.11 Standard

- **The importance of standards**
  This chapter begins with an introduction to the types of LAN standards and the primary organization that makes the standards: the Institute for Electrical and Electronic Engineers (IEEE). You learn the important benefits of using the IEEE 802.11 wireless LAN standard.
- **IEEE 802 LAN standards family**
  It is important to know how the IEEE 802.11 standard fits into other LAN protocols to ensure proper interoperability. An overview of the 802 series of LAN standards describes the operation of the 802.2 Logical Link Control that directly interfaces with 802.11.
- **Introduction to the IEEE 802.11 standard**
  An explanation of the scope and goals of the 802.11 standard provides an understanding of the basic functionality of 802.11. Learn the peculiar wireless network issues that were addressed when developing the standard.
- **IEEE 802.11 topology**
  An overview of the physical structure of 802.11-compliant LANs provides an understanding of 802.11 topology. Understand how basic physical 802.11 elements, such as Basic Service Sets (single-cell wireless LANs) and access points, form integrated, multiple-cell wireless LANs that support a variety of mobility types.
- **IEEE 802.11 logical architecture**
  Coverage of the main elements of the 802.11 protocol stack provides an overview of how the 802.11 protocol works. Learn the main functionality of each of the following 802.11 protocol layers: MAC Layer and individual PHY (Physical) Layers (frequency hopping, direct sequence, and infrared).

- IEEE 802.11 services
  802.11-compliant LANs function based on a set of services that relate to stations and distribution systems. Discover how these services offer security equivalent to wired LANs.
- Implications of the IEEE 802.11 standard
  Although the long-awaited 802.11 standard offers several benefits over using proprietary-based wireless LANs, the 802.11 standard still has shortcomings that implementors should be aware of. Learn some of the 802.11 implications, such as relatively low data rates and lack of roaming.
- IEEE 802.11 standard compliance
  The compliance with 802.11 depends on those having the need for wireless networks. Become aware of how vendors are complying with 802.11, what end users need to do to be compliant, and how different regions of the world comply with 802.11 radio frequencies.
- IEEE 802.11 Working Group operations
  Involvement in IEEE 802.11 standards development is open to anyone with a desire to participate, but you need to understand the membership requirements and types of 802.11 members.
- Future of the IEEE 802.11 standard
  When making decisions about wireless LANs, be sure to include what the future holds for the 802.11 standard. Discover the projects IEEE 802.11 members are working on to increase the performance of 802.11-compliant wireless LANs.

The Importance of Standards

Vendors and some end users initially expected markets to dive headfirst into implementing wireless networks. Markets did not respond as predicted, and flat sales growth of wireless networking components prevailed through most of the 1990s. Relatively low data rates, high prices, and especially the lack of standards kept many end users from purchasing the wire-free forms of media.

For those having applications suitable for lower data rates and enough cost savings to warrant purchasing wireless connections, the only choice before 1998 was to install proprietary hardware to satisfy requirements. As a result, many organizations today have proprietary wireless networks for which you have to replace both hardware and software to be compliant with the IEEE 802.11 standard. The lack of standards has been a significant problem with wireless networking, but the first official version of the standard is now available. In response to lacking standards, the Institute for Electrical and Electronic Engineers (IEEE) developed the first internationally recognized wireless LAN standard: IEEE 802.11.

Types of Standards

There are two main types of standards: official and public. An *official standard* is published and known to the public, but it is controlled by an official standards organization, such as IEEE. Government or industry consortiums normally sponsor official standards groups. Official standards organizations generally ensure coordination at both the international and domestic level.

A *public standard* is similar to an official standard, except it is controlled by a private organization, such as the Wireless LAN Interoperability Forum. Public standards, often called *de facto standards*, are common practices that have not been produced or accepted by an official standards organization. These standards, such as TCP/IP, are the result of widespread proliferation. In some cases, public standards that proliferate, such as the original ethernet, eventually pass through standards organizations and become official standards.

Companies should strive to adopt standards and recommended products within their organizations for all aspects of information systems. What type of standards should you use? For most cases, focus on the use of an official standard if one is available and proliferating. This will help ensure widespread acceptance and longevity of your wireless network implementation. If no official standard is suitable, a public standard would be a good choice. In fact, public standards can often respond faster to changes in market needs because they usually have less organizational overhead for making changes. Be sure to avoid nonstandard or proprietary system components, unless there are no suitable standards available.

Case Study 3.1: 802.11 Versus Proprietary Standards

A large retail chain based in Sacramento, California, had requirements to implement a wireless network to provide mobility within their 10 warehouses located all over the United States. The application calls for clerks within the warehouse to utilize new handheld wireless data collectors that perform inventory-management functions.

The company, already having one vendor's data collection devices (we'll call these brand X), decides to use that vendor's brand Y proprietary wireless data collectors and their proprietary wireless network (the vendor doesn't offer an 802.11-compliant solution). This decision eliminates the need to work with additional vendors for the new handheld devices and the wireless network.

A year passes since the installation, and enhancement requirements begin to pour in for additional mobile appliances that are not available from the brand X

continues

continued

vendor. This forces the company to consider the purchase of new brand Z appliances from a different vendor. The problem, however, is that the brand Z appliances, which are 802.11-compliant, don't interoperate with the installed proprietary brand Y wireless network. Because of the cost associated with replacing their network with one that is 802.11 compliant (the brand Y wireless network has no upgrade path to 802.11), the company can't cost effectively implement the new enhancement.

The company could have eliminated the problem of not being able to implement the new enhancement if it would have implemented the initial system with 802.11-compliant network components, because most vendors offer products that are compatible with 802.11, but not all the proprietary networks. The result would have been the ability to consider multiple vendors for a wider selection of appliances.

Institute for Electrical and Electronic Engineers (IEEE)

The IEEE is a nonprofit professional organization founded by a handful of engineers in 1884 for the purpose of consolidating ideas dealing with electro-technology. In the last 100 plus years, IEEE has maintained a steady growth. Today, the IEEE, which is based in the United States, has over 320,000 members located in 150 countries. The IEEE consists of 35 individual societies, including the Communications Society, Computer Society, and Antennas and Propagation Society.

The IEEE plays a significant role in publishing technical works, sponsoring conferences and seminars, accreditation, and standards development. The IEEE has published nearly 700 active standards publications, half of which relate to power engineering and most others deal with computers. The IEEE standards development process consists of 30,000 volunteers (who are mostly IEEE members) and a Standards Board of 32 people. In terms of LANs, IEEE has produced some very popular and widely used standards. The majority of LANs in the world utilize network interface cards based on the IEEE 802.3 (ethernet) and IEEE 802.5 (token ring) standards, for example.

Before someone can develop an IEEE standard, he must submit a Project Authorization Request (PAR) to the IEEE Standards Board. If the board approves the PAR, IEEE establishes a standards working group to develop the standard. Members of the working groups serve voluntarily and without compensation, and they are not necessarily members of the institute. The working group begins by writing a draft standard, and then solicits the draft to a balloting group of selected IEEE members for review and approval. The ballot group consists of the standard's developers, potential users, and other people having general interest.

Before publication, the IEEE Standards Board performs a review of the Final Draft Standard, and then considers approval of the standard. The resulting standard represents a consensus of broad expertise from within IEEE and other related organizations. All IEEE standards are subjected to review at least once every five years for revision or reaffirmation.

Note

In May 1991, a group of people, led by Victor Hayes, submitted a Project Authorization Request (PAR) to IEEE to initiate the 802.11 Working Group. Victor became Chairman of the working group and led the standards effort to its completion in June 1997.

Benefits of the 802.11 Standard

The benefits of utilizing standards, such as those published by IEEE, are great. The following sections explain the benefits of complying with standards, especially IEEE 802.11.

Appliance Interoperability

Compliance with the IEEE 802.11 standard makes interoperability between multiple-vendor appliances and the chosen wireless network type possible. This means you can purchase an 802.11-compliant PalmPilot from Symbol and Pathfinder Ultra handheld scanner/printer from Monarch Marking Systems, and they will both interoperate within an equivalent 802.11 wireless network, assuming 802.11 configuration parameters are set equally in both devices. Standard compliance increases price competition and enables companies to develop wireless LAN components with lower research and development budgets. This enables a greater number of smaller companies to develop wireless components. As a result, the sales of wireless LAN components should boom over the next few years as the finalization of the IEEE 802.11 standard sinks in.

As shown in Figure 3.1, appliance interoperability avoids the dependence on a single vendor for appliances. Without a standard, for example, a company having a non-standard proprietary Symbol network would be dependent on purchasing only appliances that operate on a Symbol network. This would exclude appliances such as ones from Telxon that only operate on proprietary Aironet networks. With an 802.11-compliant wireless network, you can utilize any equivalent 802.11-compliant appliance. Because most vendors, including Symbol and Telxon, have migrated their products to 802.11, you have a much greater selection of appliances for 802.11 standard networks.

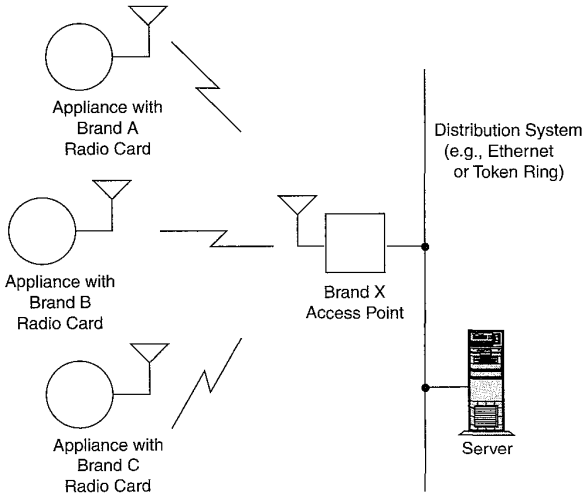


FIGURE 3.1 *Appliance interoperability ensures that multiple-vendor hardware works within equivalent wireless networks.*

Fast Product Development

The 802.11 standard is a well-tested blueprint that developers can use to implement wireless devices. The use of standards decreases the learning curve required to understand specific technologies because the standard-forming group has already invested the time to smooth out any wrinkles in the implementation of the applicable technology. This leads to the development of products in much less time.

Stable Future Migration

Compliance with standards helps protect investments and avoids legacy systems that must be completely replaced in the future as those proprietary products become obsolete. The evolution of wireless LANs should occur in a similar fashion as 802.3, ethernet. Initially, ethernet began as a 10 Mbps standard using coaxial cable media. The IEEE 802.3 Working Group enhanced the standard over the years by adding twisted-pair, optical-fiber cabling, and 100 and 1000 Mbps data rates.

Just as IEEE 802.3 did, the 802.11 Working Group recognizes the investments organizations make in network infrastructure and the importance in providing migration paths that maximize the installed base of hardware. As a result, 802.11 will certainly ensure stable migration from existing wireless LANs as higher performance wireless networking technologies become available.

Price Reductions

High costs have always plagued the wireless LAN industry; however, prices should drop significantly as more vendors and end users comply with 802.11. One of the reasons for lower prices is that vendors will no longer need to develop and support lower-quantity proprietary subcomponents, cutting design, manufacturing, and support costs. Ethernet went through a similar lowering of prices as more and more companies began complying with the 802.3 standard.

Avoiding Silos

Over the past couple of decades, MIS organizations have had a difficult time maintaining control of network implementations. The introduction of PCs, LANs, and visual-based development tools has made it much easier for non-MIS organizations, such as finance and manufacturing departments, to deploy their own applications. One part of the company, for example, may purchase a wireless network from one vendor, and then another part of the company may buy a different wireless network. As a result, *silos*—noninteroperable systems—appear within the company, making it very difficult for MIS personnel to plan and support compatible systems. Some people refer to these silos as *stovepipes*.

Acquisitions bring dissimilar systems together as well. One company having a proprietary system may purchase another having a different proprietary system, resulting in noninteroperability. Figure 3.2 illustrates the features of standards that minimize the occurrence of silos.

Case Study 3.2:

Problems with Mixed Standards

A company located in Barcelona, Spain specializes in the resale of women's clothes. This company, having a MIS group without much control over the implementation of distributed networks in major parts of the company, has projects underway to implement wireless networks for an inventory application and a price-marking application.

Non-MIS project managers located in different parts of the company lead these projects. They have little desire to coordinate their projects with MIS because of past difficulties. As a result, both project managers end up implementing noncompatible proprietary wireless networks to satisfy their networking requirements.

The project managers install both systems: one that covers the sales floorspace of their 300 stores (for price marking) and one that encompasses 10 warehouses (for doing inventory functions). Although the systems are noncompatible, all is fine for the users operating the autonomous systems.

The issues with this system architecture, however, are the difficulty in providing

continues

continued

operational support and inflexibility. The company must maintain purchasing and warranty contracts with two different wireless network vendors, service personnel need to acquire and maintain an understanding in the operation of two networks, and the company cannot share appliances and wireless network components between the warehouses and the stores.

As a result, the silos in this case make the networks more expensive to support and limit their flexibility in meeting future needs. The implementation of standard 802.11-compliant networks would have avoided these problems.

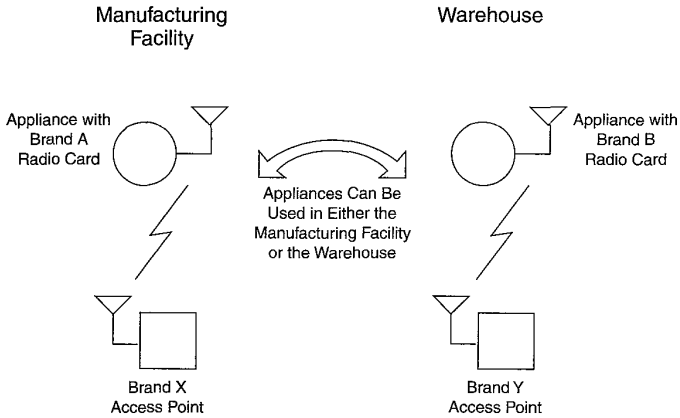


FIGURE 3.2 *Compliance with the IEEE 802.11 standard can minimize the implementation of silos.*

IEEE 802 LAN Standards Family

The IEEE 802 Local and Metropolitan Area Network Standards Committee is a major working group charted by IEEE to create, maintain, and encourage the use of IEEE and equivalent IEC/ISO standards. IEEE formed the committee in February 1980, and has met at least three times per year as a plenary body since then. IEEE 802 produces the series of standards known as IEEE 802.x, and the JTC 1 series of equivalent standards are known as ISO 8802-nnn.

IEEE 802 includes a family of standards, as depicted in Figure 3.3. The MAC and Physical Layers of the 802 standard were organized into a separate set of standards from the LLC because of the interdependence between medium access control, medium, and topology.

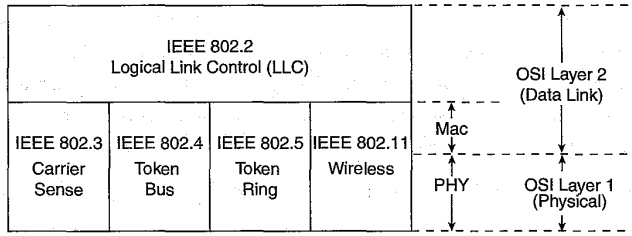


FIGURE 3.3 *The IEEE 802 family of standards falls within the scope of layers 1 and 2 of the OSI Reference Model. The LLC protocol specifies the mechanisms for addressing stations across the medium and for controlling the exchange of data between two stations; whereas, the MAC and PHY Layers provide medium access and transmission functions.*

The IEEE 802 family of standards includes the following:

- *IEEE 802.1: Glossary, Network Management, and Internetworking:* These documents, as well as IEEE 802 Overview and Architecture, form the scope of work for the 802 standards.
- *IEEE 802.2: Logical Link Control (LLC):* This standard defines Layer 2 synchronization and error control for all types of 802 LANs, including 802.11. Refer to the next section, "IEEE 802.2 LLC Overview," for more detail on the features and operation of the LLC.
- *IEEE 802.3: CSMA/CD Access Method and Physical Layer Specifications:* This defines the widely accepted 10, 100, and 1000 Mbps ethernet asynchronous protocol for use over twisted-pair wiring, coaxial cable, and optical fiber.
- *IEEE 802.4: Token-Passing Bus Access Method and Physical Layer Specifications:* This offers a token-passing protocol over a bus topology that can be embedded in other systems.
- *IEEE 802.5: Token-Passing Ring Access Method and Physical Layer Specifications:* This defines a 4 and 16 Mbps synchronous protocol that uses a token for access control over a ring topology.
- *IEEE 802.10: Security and Privacy Access Method and Physical Layer Specifications:* Provides security provisions for both wired and wireless LANs.
- *IEEE 802.11: Wireless Access Method and Physical Layer Specification:* Encompasses a variety of physical media, including frequency hopping spread spectrum, direct sequence spread spectrum, and infrared light for data rates up to 2 Mbps.

IEEE 802.2 LLC Overview

The LLC is the highest layer of the IEEE 802 Reference Model and provides similar functions of the traditional Data Link Control protocol: HDLC (High-Level Data

Link Control). The ANSI/IEEE Standard 802.2 specifies the LLC. The purpose of the LLC is to exchange data between end users across a LAN using a 802-based MAC controlled link. The LLC provides addressing and data link control, and it is independent of the topology, transmission medium, and medium access control technique chosen.

Higher layers, such as TCP/IP, pass user data down to the LLC expecting error-free transmission across the network. The LLC in turn appends a control header, creating an LLC protocol data unit (PDU). The LLC utilizes the control information in the operation of the LLC protocol (see Figure 3.4). Before transmission, the LLC PDU is handed down through the MAC service access point (SAP) to the MAC Layer, which appends control information at the beginning and end of the packet, forming a MAC frame. The control information in the frame is needed for the operation of the MAC protocol.

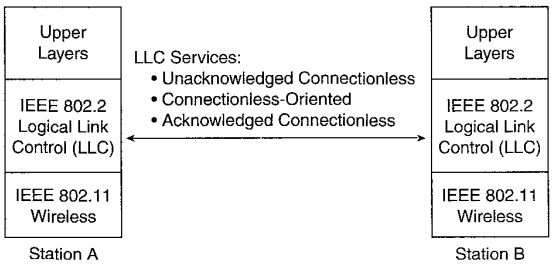


FIGURE 3.4 *The LLC provides end-to-end link control over an 802.11-based wireless LAN.*

IEEE 802.2 LLC Services

The LLC provides the following three services for a Network Layer protocol:

- Unacknowledged connectionless service
- Connection-oriented service
- Acknowledged connectionless service

These services apply to the communication between peer LLC Layers—that is, one located on the source station and one located on the destination station. Typically, vendors will provide these services as options that the customer can select when purchasing the equipment.

All three LLC protocols employ the same PDU format that consists of four fields (see Figure 3.5). The Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) fields each contains 7-bit addresses, which specify the destination and

source stations of the peer LLCs. One bit of the DSAP indicates whether the PDU is intended for an individual or group station(s). One bit of the SSAP indicates whether it is a command or response PDU. The format of the LLC Control field is identical to that of HDLC, using extended (7-bit) sequence numbers. The Data field contains the information from higher-layer protocols that the LLC is transporting to the destination.

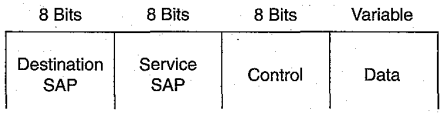


FIGURE 3.5 *The LLC PDU consists of data fields that provide the LLC functionality.*

The Control field has bits that indicate whether the frame is one of the following types:

- *Information:* Used to carry user data
- *Supervisory:* Used for flow control and error control
- *Unnumbered:* Various protocol control PDUs

Unacknowledged Connectionless Service

The *unacknowledged connectionless service* is a datagram-style service that does not involve any error-control or flow-control mechanisms. This service does not involve the establishment of a Data Link Layer connection (that is, a connection between peer LLCs). This service supports individual, multicast, and broadcast addressing. This service just sends and receives LLC PDUs, with no acknowledgment of delivery. Because the delivery of data is not guaranteed, a higher layer, such as TCP, must deal with reliability issues.

The unacknowledged connectionless service offers advantages in the following situations:

- If higher layers of the protocol stack provide the necessary reliability and flow-control mechanisms, it would be inefficient to duplicate them in the LLC. In this case, the unacknowledged connectionless service would be appropriate. TCP and the ISO transport protocol, for example, already provide the mechanisms necessary for reliable delivery.
- It is not always necessary to provide feedback pertaining to successful delivery of information. The overhead of connection establishment and maintenance can be inefficient—as an example, for applications involving the periodic sampling of data sources, such as monitoring sensors. The unacknowledged connectionless service would best satisfy these requirements.

Case Study 3.3: Using Unacknowledged Connectionless Service to Minimize Overhead

The executive office building of a high-rent advertising agency in Southern California has 20 sensors to monitor temperatures throughout its building as an input to the heating and air conditioning system. These sensors send short information packets every minute to an application on a centralized server that updates a temperature table in a database. The heating and air conditioning system uses this information to control the temperature in different parts of the building.

For this application, the server does not need to acknowledge the reception of every sensor transmission because the information updates are not critical. The system can maintain a comfortable temperature throughout the building even if the system misses temperature updates from time to time.

Additionally, it is not feasible to require the sensors to establish connections with the server to send the short information packets. As a result, designers of the system chose to use the LLC unacknowledged connectionless service to minimize overhead on the network, making the limited wireless network bandwidth available to other applications.

Connection-Oriented Service

The *connection-oriented service* establishes a logical connection that provides flow control and error control between two stations needing to exchange data. This service does involve the establishment of a connection between peer LLCs by performing connection establishment, data transfer, and connection termination functions. The service can only connect two stations; therefore, it does not support multicast or broadcast modes. The connection-oriented service offers advantages mainly if higher layers of the protocol stack do not provide the necessary reliability and flow-control mechanisms, which is generally the case with terminal controllers.

Flow control is a protocol feature that ensures a transmitting station does not overwhelm a receiving station with data. With flow control, each station allocates a finite amount of memory and buffer resources to store sent and received PDUs.

Networks, especially wireless networks, suffer from induced noise in the links between network stations that can cause transmission errors. If the noise is high enough in amplitude, it causes errors in digital transmission in the form of altered bits. This will lead to inaccuracy of the transmitted data, and the receiving network device may misinterpret the meaning of the information.

The noise that causes most problems with networks is usually Gaussian and impulse noise. Theoretically, the amplitude of Gaussian noise is uniform across the frequency spectrum, and it normally triggers random single-bit independent errors.

Impulse noise, the most disastrous, is characterized by long quiet intervals of time followed by high-amplitude bursts. This noise results from lightning and switching transients. Impulse noise is responsible for most errors in digital communication systems and generally provokes errors to occur in bursts.

To guard against transmission errors, the connection-oriented and acknowledged-connectionless LLCs use error-control mechanisms that detect and correct errors that occur in the transmission of PDUs. The LLC ARQ mechanism recognizes the possibility of the following two types of errors:

- *Lost PDU:* A PDU fails to arrive at the other end or is damaged beyond recognition.
- *Damaged PDU:* A PDU has arrived, but some bits are altered.

When a frame arrives at a receiving station, the station checks whether there are any errors present by using a *Cyclic Redundancy Check* (CRC) error detection algorithm. In general, the receiving station will send back a positive or negative acknowledgment depending on the outcome of the error detection process. In case the acknowledgment is lost en route to the sending station, the sending station will retransmit the frame after a certain period of time. This process is often referred to as *Automatic Repeat-Request* (ARQ).

Overall, ARQ is best for the correction of burst errors because this type of impairment occurs in a small percentage of frames, thus not invoking many retransmissions. Because of the feedback inherent in ARQ protocols, the transmission links must accommodate half-duplex or full-duplex transmissions. If only simplex links are available due to feasibility, it is impossible to use the ARQ technique because the receiver would not be able to notify the transmitter of bad data frames.

Note

In cases for which single bit errors predominate or when only a simplex link is available, forward error correction (FEC) can provide error correction. FEC algorithms provide enough redundancy in data transmissions to enable the receiving station to correct errors without needing the sending station to retransmit the data.

FEC is effective for correcting single-bit errors, but it requires a great deal of overhead in the transmissions to protect against multiple errors, such as burst errors. The IEEE LLC, however, specifies only the use of ARQ-based protocols for controlling errors.

The following are two approaches for retransmitting unsatisfactory blocks of data using ARQ.

Continuous ARQ

With continuous ARQ, often called a *sliding window protocol*, the sending station transmits frames continuously until the receiving station detects an error. The

sending station is usually capable of transmitting a specific number of frames and maintains a table indicating which frames have been sent.

The system implementor can set the number of frames sent before stopping via configuration parameters of the network device. If a receiver detects a bad frame, it will send a negative acknowledgment back to the sending station requesting that the bad frame be sent over again. When the transmitting station gets the signal to retransmit the frame, several subsequent frames may have already been sent (due to propagation delays between the sender and receiver); therefore, the transmitter must "go back" and retransmit the erred data frame.

There are a couple ways the transmitting station can send frames again using continuous ARQ. One method is for the source to retrieve the erred frame from the transmit buffer and send the bad frame and all frames following it. This is called the *go-back-n technique*. A problem, however, is when *n* (the number of frames the transmitter sent after the erred frame plus one) becomes large, the method becomes inefficient. This is because the retransmission of just one frame means that a large number of possibly "good" frames will also be resent, thus decreasing throughput.

The go-back-n technique is useful in applications for which receiver buffer space is limited because all that is needed is a receiver window size of one (assuming frames are to be delivered in order). When the receive node rejects an erred frame (sends a negative acknowledgment), it does not need to buffer any subsequent frames for possible reordering while it is waiting for the retransmission because all subsequent frames will also be sent.

An alternative to the continuous go-back-n technique is a method that selectively retransmits only the erred frame, and then resumes normal transmission at the point just before getting the notification of a bad data frame. This approach is called *selective repeat*. It is obviously better than continuous go-back-n in terms of throughput because only the erred frame needs retransmission. With this technique, however, the receiver must be capable of storing a number of frames if they are to be processed in order. The receiver needs to buffer data that have been received after an erred frame was requested for retransmission because only the damaged frame will be sent again.

Stop-and-Wait ARQ

With stop-and-wait ARQ, the sending station transmits a frame and then stops and waits for some type of acknowledgment from the receiver on whether a particular frame was acceptable or not. If the receiving station sends a negative acknowledgment, the frame will be sent again. The transmitter will send the next frame only after it receives a positive acknowledgment from the receiver.

An advantage of stop-and-wait ARQ is that it does not require much buffer space at the sending or receiving station. The sending station needs to store only the current transmitted frame. However, stop-and-wait ARQ becomes inefficient as the propagation delay between source and destination becomes large. For example, data sent on satellite links normally experience a round-trip delay of several hundred milliseconds; therefore, long block lengths are necessary to maintain a reasonably effective data rate. The trouble is that with longer frames, the probability of an error occurring in a particular block is greater. Therefore, retransmission will occur often, and the resulting throughput will be lower.

Case Study 3.4: Using Automatic Repeat-Request (ARQ) to Reduce Errors

A mobile home manufacturer in Florida uses robots on the assembly line to perform welding. Designers of the robot control system had to decide whether to use ARQ or FEC for controlling transmission errors between the server and the robots. The company experiences a great deal of impulse noise from arc welders and other heavy machinery.

In the midst of this somewhat hostile environment, the robots require error-free information updates to ensure that they function correctly. Designers of the system quickly ruled out the use of FEC because of the likely presence of burst errors due to impulse noise. ARQ, with its capability to detect and correct frames having a lot of bit errors, was obviously the better choice.

Acknowledged Connectionless Service

As with the unacknowledged connectionless service, the *acknowledged connectionless service* does not involve the establishment of a logical connection with the distant station. But the receiving stations with the acknowledged version do confirm successful delivery of datagrams. Flow and error control is handled through use of the stop-and-wait ARQ method.

The acknowledged connectionless service is useful in several applications. The connection-oriented service must maintain a table for each active connection for tracking the status of the connection. If the application calls for guaranteed delivery, but there are a large number of destinations needing to receive the data, the connection-oriented service may be impractical because of the large number of tables required. Examples that fit this scenario include process control and automated factory environments that require a central site to communicate with a large number of processors and programmable controllers. In addition, the handling of important and time-critical alarm or emergency control signals in a factory would also fit this

case. In all these examples, the sending stations need an acknowledgment to ensure successful delivery of the data; however, the urgency of transmission cannot wait for a connection establishment.

Note

A company having a requirement to send information to multiple devices needing positive acknowledgment of the data transfer can make use of the acknowledged connectionless LLC service. A marina may find it beneficial to control the power to different parts of the boat dock via a wireless network, for example. Of course, the expense of a wireless network may not be justifiable for this application alone.

Other applications, such as supporting data transfers back and forth to the cash register at the gas pump and the use of data-collection equipment for inventorying rental equipment, can share the wireless network to make a more positive business case. For shutting off the power on the boat dock, the application would need to send a message to the multiple power controllers, and then expect an acknowledgment to ensure the controller receives the notification and that the power is shut off. For this case, the connectionless transfer, versus connection-oriented, makes most sense because it would not be feasible to make connections to the controllers to support such a short message.

LLC/MAC Layer Service Primitives

Layers within the 802 architecture communicate with each other via service primitives having the following forms:

- *Request:* A layer uses this type of primitive to request that another layer perform a specific service.
- *Confirm:* A layer uses this type of primitive to convey the results of a previous service request primitive.
- *Indication:* A layer uses this type of primitive to indicate to another layer that a significant event has occurred. This primitive could result from a service request or from some internally generated event.
- *Response:* A layer uses this type of primitive to complete a procedure initiated by an indication primitive.

These primitives are an abstract way of defining the protocol, and they *do not* imply a specific physical implementation method. Each layer within the 802 model uses specific primitives. The LLC communicates with its associated MAC Layer through the following specific set of service primitives:

- `MA-UNITDATA.request`: The LLC sends this primitive to the MAC Layer to request the transfer of a data frame from a local LLC entity to a specific peer LLC entity or group of peer entities on different stations. The data frame could be an information frame containing data from a higher layer or a control frame (for example, a supervisory or unnumbered frame) that the LLC generates internally to communicate with its peer LLC.
- `MA-UNITDATA.indication`: The MAC Layer sends this primitive to the LLC to transfer a data frame from the MAC Layer to the LLC. This occurs only if the

MAC has found that a frame it receives from the Physical Layer is valid, has no errors, and that the destination address indicates the correct MAC address of the station.

- *MA-UNITDATA-STATUS.indication:* The MAC Layer sends this primitive to the LLC Layer to provide status information about the service provided for a previous MA-UNITDATA.request primitive.

Note

The current ANSI/IEEE 802.2 standard (dated May 7, 1998) states that the 802.2 Working Group is developing a single-service specification of primitives that is common to all MAC Layers. IEEE will refer to this change in the 802.2 standard, not the individual MAC Layer standards (for example, 802.3, 802.5, 802.11).

Introduction to the IEEE 802.11 Standard

The initial 802.11 PAR states, "...the scope of the proposed [wireless LAN] standard is to develop a specification for wireless connectivity for fixed, portable, and moving stations within a local area." The PAR further says that the "purpose of the standard is to provide wireless connectivity to automatic machinery and equipment or stations that require rapid deployment, which may be portable, handheld, or which may be mounted on moving vehicles within a local area."

The resulting standard, which is officially called *IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications*, defines over-the-air protocols necessary to support networking in a local area. As with other IEEE 802–based standards (for example, 802.3 and 802.5), the primary service of the 802.11 standard is to deliver MSDUs (MAC Service Data Units) between peer LLCs. Typically, a radio card and access point provide functions of the 802.11 standard.

Note

To order a copy of the IEEE 802.11 standard, contact the IEEE 802 Document Order Service at 800-678-4333. You can also order the standard via IEEE's Web site at `www.ieee.org`.

The 802.11 standard provides MAC and PHY functionality for wireless connectivity of fixed, portable, and moving stations moving at pedestrian and vehicular speeds within a local area. Specific features of the 802.11 standard include the following:

- Support of asynchronous and time-bounded delivery service
- Continuity of service within extended areas via a distribution system, such as ethernet
- Accommodation of transmission rates of 1 and 2 Mbps
- Support of most market applications

- Multicast (including broadcast) services
- Network management services
- Registration and authentication services

Target environments for use of the standard include the following:

- Inside buildings, such as offices, banks, shops, malls, hospitals, manufacturing plants, and residences
- Outdoor areas, such as parking lots, campuses, building complexes, and outdoor plants

The 802.11 standard takes into account the following significant differences between wireless and wired LANs:

- *Power management:* Because most wireless LAN NICs are available in PCMCIA Type II format, obviously you can outfit portable and mobile handheld computing equipment with wireless LAN connectivity. The problem, however, is these devices must rely on batteries to power the electronics within them. The addition of a wireless LAN NIC to a portable computer can quickly drain batteries.

  The 802.11 Working Group struggled with finding solutions to conserve battery power; however, they found techniques enabling wireless NICs to switch to lower-power standby modes periodically when not transmitting, reducing the drain on the battery. The MAC Layer implements power-management functions by putting the radio to sleep (that is, lowering the power drain) when no transmission activity occurs for some specific or user-definable time period. The problem, however, is that a sleeping station can miss critical data transmissions. 802.11 solves this problem by incorporating buffers to queue messages. The standard calls for sleeping stations to awaken periodically and retrieve any applicable messages.

- *Bandwidth:* The ISM spread spectrum bands do not offer a great deal of bandwidth, keeping data rates lower than desired for some applications. The 802.11 Working Group, however, dealt with methods to compress data, making the best use of available bandwidth. Efforts are also underway to increase the data rate of 802.11 to accommodate the growing need for exchanging larger and larger files (see the section titled "Future of the IEEE 802.11 Standard" at the end of this chapter).

- *Security:* As mentioned in Chapter 1, "Introduction to Wireless Networks," in the "Network Security" section, wireless LANs transmit signals over much larger areas than that of wired media, such as twisted-pair, coaxial, and optical fiber cable. In terms of privacy, therefore, wireless LANs have a much larger area to protect. To employ security, the 802.11 Working Group coordinated their work with the IEEE 802.10 Standards Committee responsible for developing security mechanisms for all 802 series LANs.

- *Addressing:* The topology of a wireless network is dynamic; therefore, the destination address does not always correspond to the destination's location. This raises a problem when routing packets through the network to the intended destination. Therefore, you may need to utilize a TCP/IP-based protocol, such as MobileIP, to accommodate mobile stations. Chapter 6, "Wireless System Integration," provides details on the MobileIP protocol.

To ensure interoperability with existing standards, the 802.11 Working Group developed the standard to be compatible with other existing 802 standards, such as the following:

- *IEEE 802:* Functional Requirements
- *IEEE 802.2:* MAC Service Definition
- *IEEE 802.1-A:* Overview and Architecture
- *IEEE 802.1-B:* LAN/MAN Management
- *IEEE 802.1-D:* Transparent Bridges
- *IEEE 802.1-F:* Guidelines for the Development of Layer Management Standards
- *IEEE 802.10:* Secure Data Exchange

Note

At the time of this writing, key participants of the IEEE 802.11 standard effort included the following:

Victor Hayes, Chair
Stuart Kerry and Chris Zegelin, Vice Chairs
Bob O'Hara and Greg Ennis, Chief Technical Editors
George Fishel and Carolyn Heide, Secretaries
David Bagby, MAC Group Chair
Jan Boer, Direct Sequence Chair
Dean Kawaguchi, PHY Group and Frequency Hopping Chair
C. Thoman Baumgartner, Infrared Chair

HIPERLAN

High Performance Radio Local Area Network (HIPERLAN) is a European family of standards that specify high-speed digital wireless communication in the 5.15–5.3 GHz and the 17.1–17.3 GHz spectrum. These standards specify the Physical and Data Link Layers of network architecture, similar in scope to 802.11. However,

continues

continued

HIPERLAN operates using different protocols and is not compatible with other IEEE standards, such as IEEE 802.2 Logical Link Control.

Two stations in a HIPERLAN can exchange data directly, without any interaction from a wired network infrastructure. The simplest HIPERLAN consists of two stations. If two HIPERLAN stations are out of range with each other, a third station can relay the messages. HIPERLAN networks have the following specifications:

- Short range, approximately 150 feet (50 meters)
- Support of asynchronous and isochronous traffic
- Support of audio at 32 Kbps
- Support of video at 2 Mbps
- Support of data at 10 Mbps

HIPERLAN is unlikely to be a serious competitor to 802.11-based LANs, especially outside of Europe.

IEEE 802.11 Topology

The IEEE 802.11 topology consists of components, interacting to provide a wireless LAN that enables station mobility transparent to higher protocol layers, such as the LLC. A station is any device that contains functionality of the 802.11 protocol (that is, MAC Layer, PHY Layer, and interface to a wireless medium). The functions of the 802.11 standard reside physically in a radio NIC, the software interface that drives the NIC, and access point. The 802.11 standard supports the following two topologies:

- Independent Basic Service Set (IBSS) networks
- Extended Service Set (ESS) networks

These networks utilize a basic building block the 802.11 standard refers to as a BSS, providing a coverage area whereby stations of the BSS remain fully connected. A station is free to move within the BSS, but it can no longer communicate directly with other stations if it leaves the BSS.

Note

Harris Semiconductor was the first company to offer a complete radio chip set (called PRISM) for direct sequence spread spectrum that is fully compliant with IEEE 802.11. The PRISM chip set includes six integrated microcircuits that handle all signal processing requirements of 802.11.

Independent Basic Service Set (IBSS) Networks

An IBSS is a stand-alone BSS that has no backbone infrastructure and consists of at least two wireless stations (see Figure 3.6). This type of network is often referred to as an *ad hoc network* because it can be constructed quickly without much planning.

The ad hoc wireless network will satisfy most needs of users occupying a smaller area, such as a single room, a sales floor, or a hospital wing.

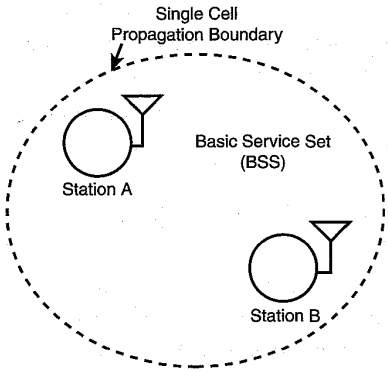


FIGURE 3.6 *An independent BSS (IBSS) is the most basic type of 802.11 wireless LAN.*

Extended Service Set (ESS) Networks

For requirements exceeding the range limitations of an independent BSS, 802.11 defines an Extended Service Set (ESS) LAN, as illustrated in Figure 3.7. This type of configuration satisfies the needs of large-coverage networks of arbitrary size and complexity.

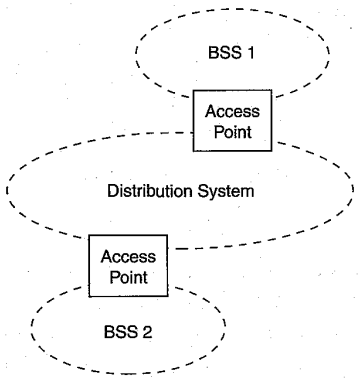


FIGURE 3.7 *An Extended Service Set (ESS) 802.11 wireless LAN consists of multiple cells interconnected by access points and a distribution system, such as ethernet.*

The 802.11 standard recognizes the following mobility types:

- *No-transition:* This type of mobility refers to stations that do not move and those that are moving within a local BSS.
- *BSS-transition:* This type of mobility refers to stations that move from one BSS in one ESS to another BSS within the same ESS.
- *ESS-transition:* This type of mobility refers to stations that move from a BSS in one ESS to a BSS in a different ESS.

The 802.11 standard clearly supports the no-transition and BSS-transition mobility types. The standard, however, does not guarantee that a connection will continue when making an ESS-transition.

The 802.11 standard defines the *distribution system* as an element that interconnects BSSs within the ESS via access points. The distribution system supports the 802.11 mobility types by providing logical services necessary to handle address-to-destination mapping and seamless integration of multiple BSSs. An *access point* is an addressable station, providing an interface to the distribution system for stations located within various BSSs. The independent BSS and ESS networks are transparent to the LLC Layer.

Within the ESS, the 802.11 standard accommodates the following physical configuration of BSSs:

- *BSSs that partially overlap:* This type of configuration provides contiguous coverage within a defined area, which is best if the application cannot tolerate a disruption of network service.
- *BSSs that are physically disjointed:* For this case, the configuration does not provide contiguous coverage. 802.11 does not specify a limit to the distance between BSSs.
- *BSSs that are physically collocated:* This may be necessary to provide a redundant or higher-performing network.

The 802.11 standard does not constrain the composition of the distribution system; therefore, it may be 802-compliant or some nonstandard network. If data frames need transmission to and from a non–IEEE 802.11 LAN, these frames, as defined by the 802.11 standard, enter and exit through a logical point called a *portal*. The portal provides logical integration between existing wired LANs and 802.11 LANs. When the distribution system is constructed with 802-type components, such as 802.3 (ethernet) or 802.5 (token ring), the portal and the access point become one and the same.

IEEE 802.11 Logical Architecture

A topology provides a means of explaining necessary physical components of a network, but the *logical architecture* defines the network's operation. As Figure 3.8 illustrates, the logical architecture of the 802.11 standard that applies to each station consists of a single MAC and one of multiple PHYs.

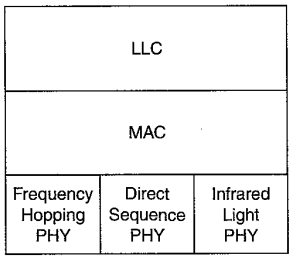


FIGURE 3.8 *A single 802.11 MAC Layer supports three separate PHYs: frequency hopping spread spectrum, direct sequence spread spectrum, and infrared light.*

IEEE 802.11 MAC Layer

The goal of the MAC Layer is to provide access control functions (such as addressing, access coordination, frame check sequence generation and checking, and LLC PDU delimiting) for shared-medium PHYs in support of the LLC Layer. The MAC Layer performs the addressing and recognition of frames in support of the LLC. The 802.11 standard uses CSMA/CA (carrier sense multiple access with collision avoidance); whereas, standard ethernet uses CSMA/CD (carrier sense multiple access with collision detection). It is not possible to both transmit and receive on the same channel using radio transceivers; therefore, an 802.11 wireless LAN takes measures only to avoid collisions, not to detect them.

IEEE 802.11 Physical Layers

The working group decided in July 1992 to concentrate its radio frequency studies and standardization efforts on the 2.4 GHz spread spectrum ISM bands for both the direct sequence and frequency hopping PHYs. The final standard specifies 2.4 GHz because this band is available license free in most parts of the world. The FCC Part 15 in the United States governs the radiated RF power in the ISM bands. Part 15 limits antenna gain to 6 dBi maximum and radiated power to one watt within the United States. European and Japanese regulatory groups limit radiated power to 10 milliwatts per 1 MHz. The actual frequencies authorized for use in the United States, Europe, and Japan differ slightly.

In March 1993, the 802.11 committee began receiving proposals for a direct sequence Physical Layer standard. After much discussion and debate, the committee agreed to include a chapter in the standard specifying the use of direct sequence. The direct sequence Physical Layer specifies two data rates:

- 2 Mbps using Differential Quaternary Phase Shift Keying (DQPSK) modulation
- 1 Mbps using Differential Binary Phase Shift Keying (DBPSK)

The standard defines seven direct sequence channels. One channel is exclusively available for Japan. Three channel pairs are defined for the United States and Europe. Channels in a pair can work without interference. In addition, the channels of all three pairs can be used simultaneously for redundancy or higher performance by developing a frequency plan that avoids signal conflicts.

In contrast to direct sequence, the 802.11-based frequency hopping PHY uses radios to send data signals by hopping from one frequency to another, transmitting a few bits on each frequency before shifting to a different one. Frequency hopping systems hop in a pattern that appears to be random, but really has a known sequence. A particular hop sequence is commonly referred to as a *frequency hopping channel*. Frequency hopping systems tend to be less costly to implement and do not consume as much power as their direct sequence counterpart, making them more suitable for portable applications. However, frequency hopping is much less tolerant of multiple-path and other interference sources. The system must retransmit data if it becomes corrupted on one of the hop sequence frequencies.

The 802.11 committee defined the frequency hopping Physical Layer to have a 1 Mbps data rate using 2-level Gaussian frequency shift keying (GFSK). This specification describes 79 channel center frequencies identified for the United States, from which there are three sets of 22 hopping sequences defined.

The infrared Physical Layer describes a modulation type that operates in the 850 to 950 nM band for small equipment and low-speed applications. The basic data rate of this infrared medium is 1 Mbps using 16-PPM (pulse position modulation) and an enhanced rate of 2 Mbps using 4-PPM. Peak power of infrared-based devices are limited to a peak power of 2 watts.

As with the IEEE 802.3 standard, the 802.11 Working Group is considering additional PHYs as applicable technologies become available.

For an inside look of each layer of the 802.11 standard, refer to Chapter 4, "Medium Access Control (MAC) Layer," and Chapter 5, "Physical (PHY) Layer."

IEEE 802.11 Services

The 802.11 standard defines *services* that provide the functions that the LLC Layer requires for sending MSDUs (MAC service data units) between two entities on the network. These services, which the MAC Layer implements, fall into two categories:

- Station services
  - Authentication
  - Deauthentication
  - Privacy
  - MSDU delivery
- Distribution system services
  - Association
  - Disassociation
  - Distribution
  - Integration
  - Reassociation

The following sections define the station and distribution system services.

Station Services

The 802.11 standard defines services for providing functions among stations. A station may be within any wireless element on the network, such as a handheld PC or handheld scanner. In addition, all access points implement station services. To provide necessary functionality, these stations need to send and receive MSDUs and implement adequate levels of security.

Authentication

Because wireless LANs have limited physical security to prevent unauthorized access, 802.11 defines authentication services to control LAN access to a level equal to a wired link. All 802.11 stations, whether they are part of an independent BSS or ESS network, must use the authentication service prior to establishing a connection (referred to as an association in 802.11 terms) with another station with which they will communicate. Stations performing authentication send a unicast management authentication frame to the corresponding station.

The IEEE 802.11 standard defines the following two authentication services:

- *Open system authentication:* This is the 802.11 default authentication method, which is a very simple, two-step process. First the station wanting to

authenticate with another station sends an authentication management frame containing the sending station's identity. The receiving station then sends back a frame alerting whether it recognizes the identity of the authenticating station.

- *Shared key authentication:* This type of authentication assumes that each station has received a secret shared key through a secure channel independent from the 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of shared key authentication requires implementation of the Wireless Equivalent Privacy algorithm.

Deauthentication

When a station wishes to *disassociate* with another station, it invokes the *deauthentication* service. Deauthentication is a notification, and cannot be refused. Stations perform deauthentication by sending an authentication management frame (or group of frames to multiple stations) to *advise* the termination of authentication.

Privacy

With a wireless network, all stations and other devices can "hear" data traffic taking place within range on the network, seriously impacting the security level of a wireless link. IEEE 802.11 counters this problem by offering a privacy service option that raises the security level of the 802.11 network to that of a wired network. The privacy service, applying to all data frames and some authentication management frames, is based on the 802.11 *Wired Equivalent Privacy* (*WEP*) algorithm that significantly reduces risks if someone eavesdrops on the network. This algorithm performs encryption of messages, as shown in Figure 3.9. With WEP, all stations initially start "in the clear"—that is, unencrypted. Refer to Chapter 4, in the section titled "Private Frame Transmissions," for a description of how WEP works.

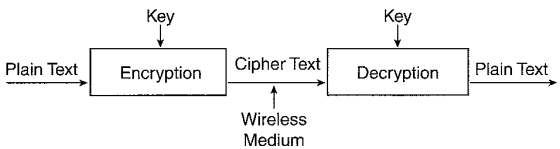


FIGURE 3.9 *The Wired Equivalent Privacy (WEP) algorithm produces ciphertext, keeping eavesdroppers from "listening in" on data transmissions.*

Note

The WEP protects RF data transmissions using a 64-bit seed key and the RC4 encryption algorithm. When enabled, WEC only protects the data packet information. Physical Layer headers are left unencrypted so that all stations can properly receive control information for managing the network.

Distribution System Services

Distribution system services, as defined by 802.11, provide functionality across a distribution system. Access points provide distribution system services. The following sections provide an overview of the services that distribution systems need to provide proper transfer of MSDUs.

Association

Each station must initially invoke the *association service* with an access point before it can send information through a distribution system. The association maps a station to the distribution system via an access point. Each station can associate with only a single access point, but each access point can associate with multiple stations. Association is also a first step to providing the capability for a station to be mobile between BSSs.

Disassociation

A station or access point may invoke the *disassociation service* to terminate an existing association. This service is a notification; therefore, neither party may refuse termination. Stations should disassociate when leaving the network. An access point, for example, may disassociate all its stations if being removed for maintenance.

Distribution

A station uses the *distribution service* every time it sends MAC frames across a distribution system. The 802.11 standard does not specify how the distribution system delivers the data. The distribution service provides the distribution system with only enough information to determine the proper destination BSS.

Integration

The *integration service* enables the delivery of MAC frames through a portal between a distribution system and a non-802.11 LAN. The integration function performs all required media or address space translations. The details of an integration function depends on the distribution system implementation and are beyond the scope of the 802.11 standard.

Reassociation

The *reassociation service* enables a station to change its current state of association. Reassociation provides additional functionality to support BSS-transition mobility for associated stations. The reassociation service enables a station to transition its association from one access point to another. This keeps the distribution system informed of the current mapping between access point and station as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the station remains associated with the same access point. The mobile station always initiates the reassociation service.

Note

IEEE 802.11 allows a client to roam among multiple access points that may be operating on the same or separate channels. To support the roaming function, each access point typically transmits a beacon signal every 100 milliseconds. Roaming stations use the beacon to gauge the strength of their existing access point connection. If the station senses a weak signal, the roaming station can implement the reassociation service to connect to an access point emitting a stronger signal.

Case Study 3.5:
Reassociation Provides Roaming

A grocery store in Gulfport, Mississippi, has a bar code–based shelf inventory system that helps the owners of the store keep track of what to stock, order, and so on. Several of the store clerks use handheld scanners during the store's closed hours to perform inventory functions. The store has a multiple cell 802.11-compliant wireless LAN (that is, ESS) consisting of access points A and B interconnected by an ethernet network. These two access points are sufficient to cover the store's entire floorspace and backroom.

At one end of the store in the frozen meat section, a clerk using a handheld device may associate with access point A. As the person walks with the device to the beer-and-wine section on the other end of the store, the mobile scanner (that is, the 802.11 station within the scanner) will begin sensing a signal from access point B. As the signal from B becomes stronger, the station will then *reassociate* with access point B, offering a much better signal for transmitting MSDUs.

Station States and Corresponding Frame Types

The state existing between a source and destination station (see Figure 3.10) governs which IEEE 802.11 frame types the two stations can exchange.

The following types of functions can occur within each class of frame:

- Class 1 Frames
  - Control Frames
    - Request to send (RTS)
    - Clear to send (CTS)
    - Acknowledgment (ACK)
    - Contention-free (CF)
  - Management Frames
    - Probe request/response
    - Beacon
    - Authentication

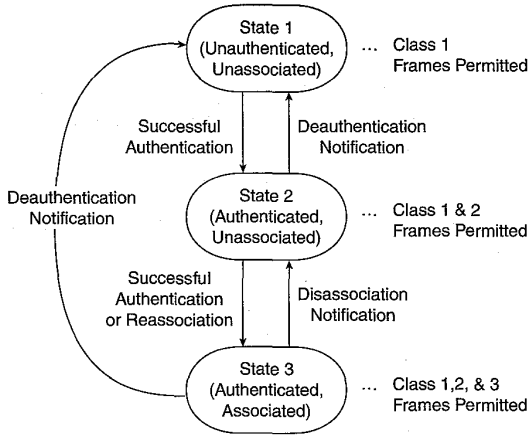


FIGURE 3.10 *The operation of a station depends on its particular state.*

Deauthentication

Announcement traffic indication message (ATIM)

- Data Frames

- Class 2 Frames
  - Management Frames

    Association request/response

    Reassociation request/response

    Disassociation

- Class 3 Frames
  - Data Frames
  - Management Frames

    Deauthentication
  - Control Frames

    Power Save Poll

To keep track of station state, each station maintains the following two state variables:

- *Authentication state:* Has values of either unauthenticated and authenticated
- *Association state:* Has values of either unassociated and associated

Implications of the IEEE 802.11 Standard

As with any technologies and standards, one must be aware of the implications surrounding the implementation of wireless networks based on the IEEE 802.11 standard. Chapter 1, in the section "Wireless Network Concerns," discusses the general issues of implementing wireless networks. In addition to these problems, the following are a couple of implications specifically related to the IEEE 802.11 standard:

- *Relatively low data rates:* As mentioned before, the 802.11 standard currently supports data rates up to 2 Mbps. Some end users and vendors claim this data rate is too low. In some cases, this is true; but in other cases, it is not true. Video transmissions, for example, may require higher data rates if applications need frame rates, pixel depth, and resolutions that require greater amounts of bandwidth. Large data block transmissions may also require higher data rates to keep transmission delays tolerable.

  On the other hand, bar code applications, such as receiving, inventory, and price marking, generally work well under the 2 Mbps limitation of the current 802.11 standard.

- *Lack of standard roaming across multiple-vendor access points:* The 802.11 standard does not define the protocols necessary to move 802.11 frames within the distribution system because it falls outside the scope of 802-type LANs. The Network and Transport Layers are left to address distribution system protocols. As a result, the 802.11 standard does not define communications *between* access points.

  Currently, it is up to the access point vendors to define the protocols necessary to support roaming from one access point to another. To be safe, you should consider purchasing access points from a single vendor, although you can mix-and-match radio cards in the appliances. Chapter 6, "Wireless System Integration," discusses industry standards, such as the Inter Access Point Protocol (IAPP) specification, that are beginning to define multiple-vendor roaming protocols.

IEEE 802.11 Standard Compliance

No standard is worthwhile unless vendors and end users comply with it. The following sections describe activities taking place to ensure compliance with 802.11.

Vendor Compliance

Most wireless LAN vendors (that is, manufacturers of the hardware) are releasing initial radio cards and access points throughout 1998 and 1999 that comply with the official 802.11 standard. Before deeming their devices as 802.11 compliant, they must follow the protocol implementation compliance procedures that the 802.11 standard specifies in its appendix. The procedures state that the vendor shall

complete a Protocol Implementation Conformance Statement (PICS) proforma. The structure of the PICS proforma mainly includes a list of fixed questions that the vendor responds to with yes or no answers, indicating adherence to the standard. The PICS can have the following uses:

- A checklist that helps the vendor reduce the risk of failure to conform to the standard
- For the vendor and system implementor to better understand what 802.11-compliancy means
- As a basis for designing an interface between the 802.11 device and another network or system
- As the basis for developing protocol conformance tests and simulations

To ensure proper compliance, vendors test their products at the InterOperability Laboratory located at the Leavitt Center on the campus of The University of New Hampshire. In March 1997, for example, Aironet Wireless Communications, Inc.; Breezecom Wireless Communications; Netwave Technologies, Inc.; Proxim Inc.; Raytheon Electronics; and Symbol Technologies performed joint interoperability testing to advance customer adoption of wireless technology. In some cases, users can upgrade their existing proprietary radio cards to be 802.11 compliant by just reinstalling NIC interface software on their appliances.

Note

Vendors are easing the transition to 802.11-compliant radio networks by offering relatively simple ways to upgrade existing radio LAN devices. Symbol, Inc., for example, offers a firmware upgrade to your existing Symbol 2.4 GHz (Spectrum 24) networks, avoiding the purchase of new network adapters.

The InterOperability Laboratory, founded in 1988, performs research and development work and is used by more than 100 vendors to verify the interoperability and conformance of their computer communications products. The University of New Hampshire encourages vendors to conduct interoperability testing by providing facilities for a multiple-vendor test environment. The goal of the laboratory is to provide complete testing for all networking products, including ethernet, ADSL, ATM, fast ethernet, FDDI, FDSE, Fibre Channel, gigabit ethernet, IP/Routing, Network Management, and Wireless.

Note

Be aware that in 1997 some vendors released "802.11-compliant" wireless LAN radio cards and access points that were not certified as compliant with the final 802.11 standard. These products may or may not operate within the final official standard.

WLI Forum

The Wireless LAN Interoperability Forum (WLI Forum), a not-for-profit corporation founded in March 1996, promotes the growth of the wireless LAN market by delivering interoperable products and services. The Forum consists primarily of appliance suppliers/vendors (such as Hewlett-Packard, Fujitsu, Monarch Marking Systems, and Handheld Products) having products that operate on the WLI Forum's OpenAir™ wireless network. The Forum provides certification via an independent third-party test lab to ensure proper compliance.

The OpenAir™ specification describes a MAC and radio frequency Physical Layer, similar in scope to the 802.11 specification. The OpenAir™ network is based on Proxim's RangeLAN2 protocol, employing frequency hopping spread spectrum technology in the unlicensed 2.4 GHz ISM band. The OpenAir™ operates at a data rate of 1.6 Mbps per channel, with 15 independent channels (hopping patterns) available. This architecture enables up to 15 wireless LANs to overlap independently in the same physical space, providing up to 24 Mbps of aggregate network bandwidth.

The WLI Forum wrote the OpenAir™ specification to motivate third-party development of compatible products. At the time, with no official IEEE standard on wireless networking, the Forum decided to base its specification on Proxim's product. Soon after the release of the 802.11 specification in June 1997, the WLI Forum announced its support for the adoption of the IEEE 802.11 standard and urged the supplier community to move toward conformance. As a result, the WLI Forum is likely to establish conformity to the IEEE 802.11 standard as well.

The WLI Forum is a worldwide organization, and is completely self funded through membership dues and fees. Membership is open to all companies that develop, manufacture, or sell wireless LAN products or services. For more information on the WLI Forum, visit their Web site located at `http://www.wlif.com`.

End-User Compliance

Throughout 1999 and beyond, end users should begin widespread implementations of 802.11-compliant LANs. As an end user, do you need to purchase and use products that comply with the 802.11 standard? Of course the answer is no, but you should carefully consider the advantages and disadvantages of implementing 802.11-compliant networks. Most likely, complying with 802.11 will be favored over the use of proprietary networks unless extenuating circumstances prevail. If the decision is to go with 802.11, you will be starting with one of the following scenarios:

- No existing implementation of wireless LANs
- Existing implementation of proprietary wireless LANs

If you are an end user with no existing installation of wireless networking components, compliance with the 802.11 standard is easy. Right? Actually, it is not as sim-

ple as it seems. The 802.11 standard is not as Plug and Play as the 802.3 ethernet standard. With 802.11, you must first decide which version of 802.11 best satisfies your needs. You might consider the following questions:

- *What type of modulation do I need?* Do I have radio interference implications that lean toward using the infrared PHY? Does the application require wider area coverage that may depend on the longer range capability of one of the spread spectrum PHYs? If the choice is spread spectrum, should I use direct sequence or frequency hopping?
- *Will the application require roaming across BSS cells interconnected by access points of different vendors?* If yes, you will need to think about how to provide roaming between access points.
- *Does the network require the optional WEP security?* If the answer is yes, be sure to choose wireless devices having WEP available.
- *Do the appliances I need to comply with have the 802.11 options I have chosen?* If not, you need to choose options that comply with the appliance, or you must choose different appliances.

Answers to the preceding questions define the options you need to consider when planning to purchase radio cards and access points complying with 802.11.

If proprietary wireless LANs already exist, you will need to either upgrade or replace the existing network to make it compliant with 802.11. Many of the vendors offer free upgrades to make your existing wireless LANs (if they are of a recent enough version) compliant with 802.11. BreezeCOM, for example, guarantees software upgrades to the IEEE 802.11 standard for its BreezeNET PRO product line.

If it is not possible or feasible to upgrade your existing wireless LAN, then of course you must perform a complete replacement if benefits outweigh the expenses. The replacement of the network will be difficult to cost-justify; however, it may become necessary as proprietary wireless components become obsolete.

International Electromagnetic Compliance

The 802.11 standard specifies operation in the 2.4 GHz band; however, electromagnetic compatibility requirements vary from one country to another. Operating frequencies, power levels, and spurious levels differ throughout the world.

Regional and national regulatory administrations of each individual country demand certification of wireless equipment. The 802.11 standard, however, identifies the minimum technical requirements for interoperability and compliance based on established regulations for Europe, Japan, and the North America. Therefore, wireless LAN vendors must be aware of all current regulatory requirements prior to releasing a product for sale in a particular country. The following agencies and

documents specify the current regulatory requirements for various geographical areas:

Canada

- *Approval standards:* Industry Canada (IC)
- *Documents:* GL36
- *Approval authority:* Industry Canada

Europe

- *Approval standards:* European Telecommunications Standards Institute
- *Documents:* ETS 300-328, ETS 300-339
- *Approval authority:* National Type Approval Authorities

France

- *Approval standards:* La Reglementation en France por les Equipements fonctionnant dans la bande de frequences 2,4 GHz "RLAN-Radio Local Area Network"
- *Documents:* SP/DGPT/ATAS/23, ETS 300-328, ETS 300-339
- *Approval authority:* Direction Generale des Postes et Telecommunications

Japan

- *Approval standards:* Research and Development Center for Radio Communications (RCR)
- *Documents:* RCR STD-33A
- *Approval authority:* Ministry of Telecommunications (MKK)

Spain

- *Approval standards:* Supplemento del Numero 164 del Boletin Oficial del Estado (published 10 July 91; revised 25 June 93)
- *Documents:* ETS 300-328, ETS 300-339
- *Approval authority:* Cuadro Nacional De Atribucion De Frecuesias

The United States of America

- *Approval standards:* Federal Communications Commission (FCC)
- *Documents:* CFR47, Part 15, Sections 15.205, 15.209, 15.247
- *Approval authority:* FCC

Operation in countries within Europe and other areas outside Japan or North America may be subject to additional regulations.

IEEE 802.11 Working Group Operations

The 802.11 Working Group is a part of the IEEE LAN MAN Standards Committee (LMSC), which reports to the Standards Activity Board (SAB) of the IEEE Computer Society. IEEE 802.11 meetings are open to anyone. The only requirement to attend is to pay dues, which offset meeting expenses. Most of the active participants are representatives from companies developing wireless LAN components. The IEEE bylaws explain that to vote on standards activities, however, you must become a member by participating in at least two out of four consecutive plenary meetings. Then, you must continue to attend meetings to maintain voting status. The 802.11 Working Group meets three times a year during the plenary sessions of the IEEE 802 and three times a year between plenary sessions.

The IEEE 802.11 Working Group consists of about 200 members; membership falls into the following categories:

- *Voting members:* Those who have maintained voting status.
- *Nearly members:* Those who have participated in two sessions of meetings, one of which being a plenary session. Nearly members become voting members in the first session they attend following their qualification for nearly membership.
- *Aspirant members:* Those who have participated in one plenary or interim session meeting.
- *Sleeping voting members:* Those who were once voting members, but have chosen to discontinue.

Future of the IEEE 802.11 Standard

What is the future of IEEE 802.11? Will end users eventually fully comply with the standard? Will the 802.11 Working Group solve implications revolving around the standard? Only time will tell for certain. It is known today, however, that all major wireless LAN vendors are releasing 802.11-compliant wireless LANs throughout 1998, and these vendors are making it fairly easy for end users to upgrade their existing systems. This, combined with the advantages of standardization, should proliferate the use of 802.11-compliant networks.

To solve implications of the current release of the standard, the IEEE 802.11 Working Group is actively working on the following projects that will aid the widespread acceptance of the standard:

- *802.11rev: Revision of IEEE Standard 802.11-1997:* This project was charted to rectify a number of errors in the current standard and to accommodate input from the JTC1 review to result in a single JTC1/IEEE standard.

- *802.11a: Extension of the IEEE Standard 802.11-1997 with a higher data rate PHY in the 5 GHz band:* This project was initiated to develop a high speed (about 20 Mbps) wireless PHY suitable for data, voice, and image information services in fixed, moving, or portable wireless local area networks. The project concentrates on improving spectrum efficiency and will review the existing 802.11 MAC to ensure its capability to operate at the higher speeds.

  The IEEE 802.11 Working Group will actively correspond with regulatory bodies worldwide to encourage spectrum allocations that match these frequencies.

- *802.11b: Extension of the IEEE Standard 802.11-1997 with a higher data rate PHY in the 2.4 GHz band:* The purpose of this project is to extend the performance and the range of applications of the existing 802.11 standard. The header of the two existing radio-based PHYs can support data rates up to 4.5 Mbps for frequency hopping and up to 25.5 Mbps for direct sequence. This project will investigate ways to exploit these data rate capabilities and analyze the capability of the existing 802.11 MAC to support higher data rates.

  The actual data rates targeted by this project are at least 3 Mbps for the frequency hopping PHY and at least 8 Mbps for the direct sequence PHY. As with project 802.11a, IEEE 802.11 will correspond with regulatory bodies worldwide to ensure that the proposed extension will be applicable as widely as possible.

In addition to the preceding official projects, the 802.11 Working Group is actively studying the needs for standardization of wireless communications of wearable computing devices. The study is examining the requirements for Wireless Personal Area Networking (WPAN) of devices that are worn or carried by individuals. The objectives of the study group are as follows:

- Review WPAN requirements.
- Determine the need for a standard.
- If a standard is necessary, draft a PAR for submittal.
- Seek appropriate sponsorship within 802.

The study group is soliciting industry input on market requirements and technical solutions for a WPAN with 0-to-30–foot range, data rates of less than 1 Mbps, low power consumption, small size (less than 0.5 cubic inches), and low cost relative to target device.

As mentioned in this chapter, the 802.11 wireless LAN standard certainly has benefits that an organization should consider when selecting components that provide LAN mobility. IEEE 802 is a solid family of standards that will provide much greater multiple-level interoperability than proprietary systems.

Wireless LANs conforming to 802.11 provide interoperability between radio cards and access points. The 802.11 standard has the backing of IEEE, having an excellent track record of developing long-lasting standards, such as IEEE 802.3 (ethernet) and IEEE 802.5 (token ring). When designing a wireless LAN, definitely consider the use of 802.11-compliant products, but ensure that the data rates of 802.11 will support your application and that the chosen components support roaming between access points.

With 802.11, system implementors have several choices. You will need to choose the type of physical medium, for example: frequency hopping spread spectrum, direct sequence spread spectrum, or infrared light. This concept is similar to choosing between twisted-pair, optical-fiber, and coaxial cable in an ethernet LAN. You will also need to determine how to interface wireless devices with server operating systems and applications. In defining these elements, be sure the resulting network supports all requirements.

CHAPTER 4

Medium Access Control (MAC) Layer

- MAC Layer operations
  The 802.11 MAC Layer provides both contention and contention-free access to a shared wireless medium. An explanation of medium sensing and inter-frame timing shows how 802.11 networks provide multiple levels of priority to frame transmissions.
- MAC frame structure
  A description of MAC frame structure illustrates the makeup of a MAC frame, providing basic building blocks of different MAC frame types.
- MAC frame types
  The 802.11 MAC Layer uses various frame types to implement its functions. An overview of the various MAC management, control, and data frames gives a foundation for understanding MAC functionality.

MAC Layer Operations

Each station and access point on an 802.11 wireless LAN implements the MAC Layer service, which provides the capability for peer LLC entities to exchange MAC service data units (MSDUs) between MAC service access points (SAPs). The MSDUs carry LLC-based frames that facilitate functions of the Logical Link Control Layer (LLC). Overall, MAC services encompass the transmission of MSDUs by sharing a wireless radio wave or infrared light medium.

The MAC Layer provides these primary operations:

- Accessing the wireless medium
- Joining a network
- Providing authentication and privacy

The following sections describe these operations.

Accessing the Wireless Medium

Before transmitting a frame, the MAC coordination must first gain access to the network using one of the following modes:

- *Carrier-sense multiple access with collision avoidance (CSMA/CA):* A contention-based protocol similar to IEEE 802.3 ethernet. The 802.11 specification refers to this mode as the *distributed coordination function* (DCF).
- *Priority-based access:* A contention-free access protocol usable on infrastructure network configurations containing a controller called a point coordinator within the access points. The 802.11 specification refers to this mode as the *point coordination function* (PCF).

Both the distributed and the point coordination function can operate concurrently within the same BSS to provide alternating contention and contention-free periods. The following sections describe each of these MAC operational modes.

Distributed Coordination Function

The distributed coordination function is the primary access protocol for the automatic sharing of the wireless medium between stations and access points having compatible PHYs. Similar to the MAC coordination of the 802.3 ethernet wired line standard, 802.11 networks use a carrier-sense multiple access/collision avoidance (CSMA/CA) protocol for sharing the wireless medium.

Carrier Sense Mechanism

A combination of both physical and virtual carrier sense mechanisms enables the MAC coordination to determine whether the medium is busy or idle (see Figure 4.1). Each of the PHY layers provides a physical means of sensing the channel (as described in Chapter 5, "Physical (PHY) Layer"). The results of the physical channel assessment from the PHY coordination are sent to the MAC coordination as part of the information factored when deciding the status of the channel.

The MAC coordination carries out the virtual carrier sense protocol based on reservation information found in the Duration field of all frames. This information announces (to all other stations) a station's impending use of the medium. The

MAC coordination will monitor the Duration field in all MAC frames and place this information in the station's Network Allocation Vector (NAV) if the value is greater than the current NAV value. The NAV operates like a timer, starting with a value equal to the Duration field value of the last frame transmission sensed on the medium, and counting down to zero. After the NAV reaches zero, the station can transmit if the PHY coordination indicates a clear channel.

The physical channel assessment and NAV contents provide sufficient information for the MAC to decide the status of the channel. As an example, the PHY may determine that no transmissions are taking place on the medium, but the NAV may indicate that a previous frame transmission had a value in the applicable Duration field that disables transmissions for a specific time period. In this case, the MAC would hold off transmission of any frames until the Duration time period expires. If the channel is busy, the MAC protocol implements a backoff algorithm.

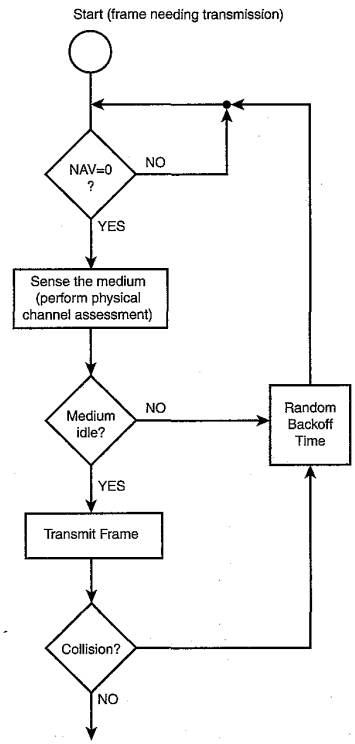


FIGURE 4.1 *This flowchart illustrates the operation of the CSMA/CA contention-based 802.11 distributed coordination function (DCF) medium access protocol.*

The CSMA/CA protocol avoids the probability of collisions among stations sharing the medium by utilizing a random backoff time if the station's physical or logical sensing mechanism indicates a busy medium. The period of time immediately following a busy medium is the highest probability of collisions occurring, especially under high utilization. The reason for this is many stations may be waiting for the medium to become idle and attempt to transmit at the same time. When the medium is idle, a random backoff time defers a station from transmitting a frame, minimizing the chance that stations collide.

The MAC coordination calculates the random backoff time using the following formula:

```
Backoff Time = Random() X aSlotTime
```

`Random()` is a pseudo-random integer drawn from a uniform distribution over the interval `[0,CW]`, in which `CW` (collision window) is an integer within the range of values of the Management Information Base (MIB) attributes `aCWmin` and `aCWmax`. The random number drawn from this interval should be statistically independent among stations. `aSlotTime` equals a constant value found in the station's MIB.

Note

The MAC Layer includes a management information base (MIB) *that stores parameters the MAC protocol needs to operate. Refer to the 802.11 standard for a complete description of these parameters. Most access points require you to supply an alphanumeric name if accessing configuration parameters via the network.*

The MAC Layer has access to the MIB via the following MAC sublayer management entity (MLME) primitives:

- `MLME-GET.request`: *Requests the value of a specific MIB attribute.*
- `MLME-GET.confirm`: *Returns the value of the applicable MIB attribute value that corresponds to an* `MLME-GET.request`.
- `MLME-SET.request`: *Requests the MIB set a specific MIB attribute to a particular value.*
- `MLME-SET.confirm`: *Returns the status of the* `MLME-SET.request`.

Figure 4.2 illustrates the value of `CW` as the station goes through successive retransmissions. The reason `CW` increases exponentially is to minimize collisions and maximize throughput for both low and high network utilizations.

Under low utilization, stations are not forced to wait very long before transmitting their frames. On the first or second attempt, a station will make a successful transmission within a short period of time. If the utilization of the network is high, the protocol holds stations back for longer periods of time to avoid the probability of multiple stations transmitting at the same time.

Under high utilization, the value of CW increases to relatively high values after successive retransmissions, providing substantial transmission spacing between stations needing to transmit. This mechanism does a good job of avoiding collisions; however, stations on networks with high utilization will experience substantial delays while waiting to transmit frames.

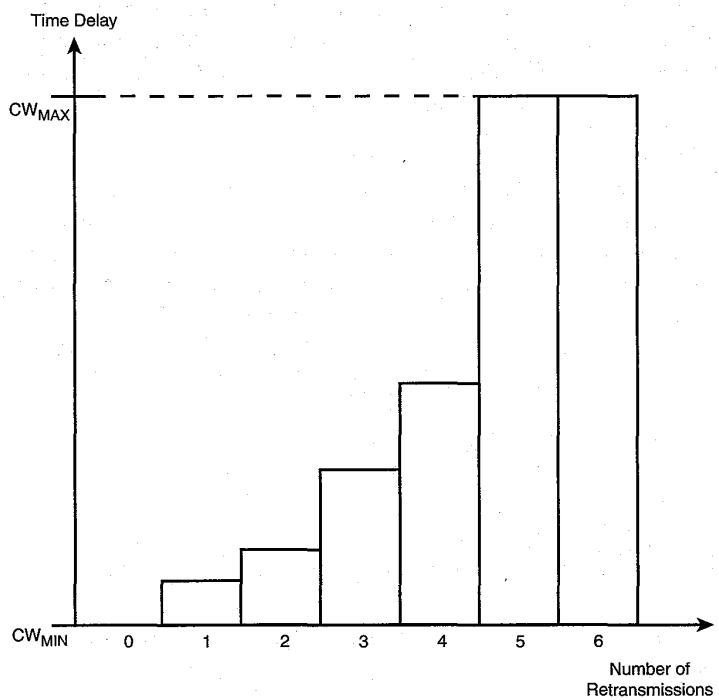


FIGURE 4.2 *The backoff time increases exponentially as between the minimum and maximum values of* CW.

Error Recovery Mechanisms

Because of transmission impairments, such as interference and collisions, bit errors can disrupt the sequencing of frames. Station A may send an RTS (Request to Send) frame and never receive the corresponding CTS (Clear to Send). Or, station A may send a data frame and never receive an acknowledgement. Because of these problems, the MAC coordination performs error recovery mechanisms.

Stations initiating the exchange of frames have the responsibility of error recovery. This generally involves the retransmission of frames after a period of time if no

response is heard from the destination station. This process, commonly referred to as automatic repeat-request (ARQ), takes into account that bits errors could have made the ACK frame unrecognizable.

To regulate the number of retransmissions, the MAC coordination differentiates between short and long frames. For short frames (frames with length less than the MIB attribute `aRTSThreshold`), retransmissions continue until the number of attempts reaches the MIB value `aShortRetryLimit`. The MAC coordination retransmits long frames similarly based on the MIB value `aLongRetrylimit`. After exceeding the retry limit, the station discards the frame.

Access Spacing

The 802.11 specification defines several standard spacing intervals (defined in the MIB) that defer a station's access to the medium and provides various levels of priority. Figure 4.3 illustrates these intervals. Each interval defines the time from the end of the last symbol of the previous frame to the beginning of the first symbol of the next frame.

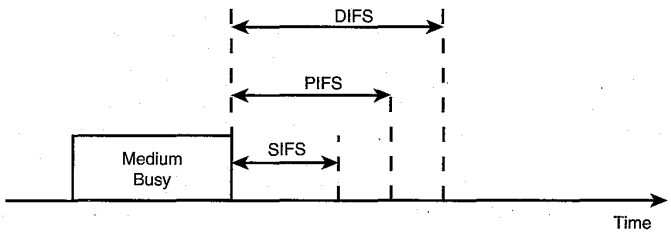


FIGURE 4.3 *The interframe space (IFS) illustrates the spacing between different aspects of the MAC access protocol.*

The following describes each of the interframe space (IFS) intervals:

- *Short IFS (SIFS):* The SIFS is the shortest of the interframe spaces, providing the highest priority level by allowing some frames to access the medium before others. The following frames use the SIFS interval:
  - ACK (Acknowledgement) frame
  - CTS (Clear to Send) frame
  - The second or subsequent MSDU of a fragment burst

  These frames require expedient access to the network to minimize frame retransmissions.

- *PCF IFS (PIFS):* The PIFS is the interval that stations operating under the point coordination function use to gain access to the medium. This provides priority over frames sent by the distributed coordination function. These stations can transmit contention-free traffic if they sense the medium is idle. This interval gives point coordination function-based stations a higher priority of access than DCF-based (CSMA) stations for transmitting frames.
- *DCF IFS (DIFS):* All stations operating according to the distributed coordination function use the DIFS interval for transmitting data frames and management frames. This spacing makes the transmission of these frames lower priority than PCF-based transmissions.
- *Extended IFS (EIFS):* All DCF-based stations use the EIFS interval—which goes beyond the time of a DIFS interval—as a waiting period when a frame transmission results in a bad reception of the frame due to an incorrect FCS value. This interval provides enough time for the receiving station to send an ACK frame.

Point Coordination Function (PCF)

The optional priority-based point coordination function provides contention-free frame transfer. With this operating mode, a point coordinator resides in the access point to control the transmission of frames from stations. All stations obey the point coordinator by setting their NAV value at the beginning of each contention-free period. Stations can optionally respond to a contention-free poll (CF-Poll frame), however.

At the beginning of the contention-free period, the point coordinator has an opportunity to gain control of the medium. The point coordinator follows the PIFS interval as a basis for accessing the medium; therefore, it may be able to maintain control during the contention-free period by waiting a shorter time between transmissions than stations operating under the distributed coordination function.

The point coordinator senses the medium at the beginning of each contention-free period. If the medium is idle after the PIFS interval, the point coordinator sends a Beacon frame that includes the CF Parameter Set element. When stations receive the beacon, they update their NAV with the `CFPMaxDuration` value found in the CF Parameter Set. This value communicates the length of the contention-free period to all stations and prevents stations from taking control of the medium until the end of the contention-free period.

After sending the Beacon frame, the point coordinator then transmits one of the following frames after waiting at least one SIFS interval:

- *Data frame:* This frame is directed from the access point's point coordinator to a particular station. If the point coordinator does not receive an ACK frame from the recipient, the point coordinator can retransmit the unacknowledged frame during the contention-free period after the PIFS interval. A point coordinator can send individual, broadcast, and multicast frames to all stations, including stations in power save mode that are pollable.
- *CF Poll frame:* The point coordinator sends this frame to a particular station, granting the station permission to transmit a single frame to any destination. If the polled station has no frame to send, it must send a Null data frame. If the sending station does not receive any frame acknowledgement, it cannot retransmit the frame unless the point coordinator polls it again. If the receiving station of the contention-free transmission is not CF pollable, it acknowledges the reception of the frame using distributed coordination function rules.
- *Data+CF Poll frame:* In this case, the point coordinator sends a data frame to a station and polls that same station for sending a contention-free frame. This is a form of piggybacking that reduces overhead on the network.
- *CF End frame:* This frame is sent to identify the end of the contention period, which occurs when one of the following happens:
  - The `CFPDurRemaining` time expires.
  - The point coordinator has no further frames to transmit and no stations to poll.

Stations have an option of being *pollable*. A station can indicate its desire for polling using the CF-Pollable subfield within the Capability Information field of an Association Request frame. A station can change its *pollability* by issuing a Reassociation Request frame. The point coordinator maintains a polling list of eligible stations that may receive a poll during the contention-free period. The point coordinator will send at least one CF-Poll if entries exist in the polling list in order by ascending AID value. When associating with an access point, a station may request to be on the polling list via the Capability Information field.

The point coordination function does not routinely operate using the backoff time of the distributed coordination function; therefore, a risk of collisions exists when overlapping point coordinators are present on the same PHY channel. This may be the case when multiple access points form an infrastructure network. To minimize these collisions, the point coordinator utilizes a random backoff time if the point coordinator experiences a busy medium when attempting to transmit the initial beacon.

Implementing the Wireless Access Method

By default, all 802.11-compliant stations operate using the *distributed coordination function (DCF)*, which is a carrier sense access mechanism. As an option, you can initialize the stations to also implement the priority-based *point coordination function (PCF)*.

In most cases, the DCF will suffice; however, consider activation of the PCF if needing to support the transmission of time-bounded information, such as audio and video. The PCF, however, will impose greater overhead on the network because of the transmission of polling frames.

Joining a Network

After a station is turned on, it needs to first determine whether another station or access point is present to join before authenticating and associating with an applicable station or access point. The station accomplishes this discovery phase by operating in a passive or active scanning mode. After joining with a BSS or ESS, the station accepts the Service Set Identifier (SSID), Timing Synchronization Function (TSF), timer value, and PHY setup parameters from the access point.

With passive scanning, a station listens to each channel for a specific period of time, as defined by the `ChannelTime` parameter. The station just waits for the transmission of Beacon frames having the SSID that the station wishes to join with. After the station detects the beacon, the station can negotiate a connection by proceeding with authentication and association processes, respectively.

Note

You can configure a station to passively scan for other stations for a particular amount of time before enabling the station to form its own network. The typical default time for this setting is 10 seconds.

Active scanning involves the transmission of a Probe frame indicating the SSID of the network that the station wishes to join. The station that sent the probe will wait for a Probe Response frame that identifies the presence of the desired network.

Some vendors enable you to set up each radio card so that it associates with a preferred access point even if the signal from that particular access point is lower than the signals from other access points. This may be useful if there is a need to regulate the flow of traffic through particular access points. In most cases, however the station will reassociate with another access point, if it doesn't receive beacons from the preferred access point.

A station can also send Probe frames using a broadcast SSID that causes all networks within reach to respond. An access point will reply to all probe requests in the case of infrastructure-based networks. With independent BSS networks (that is, one access point), the station that generated the last Beacon frame will respond to probe

requests. The Probe Response frame indicates the presence of the desired networks, and the station can complete its connection by proceeding with the authentication and association processes.

Station Synchronization

Stations within the BSS must remain in synchronization with the access point to ensure all stations are operating with the same parameters (such as using the correct hopping pattern) and enabling power saving functions to work correctly. To accomplish this, the access point periodically transmits Beacon frames.

A Beacon frame contains information about the particular Physical Layer being used. The Beacon identifies the frequency hopping sequence and dwell time, for example, so the station can implement the applicable demodulation. The Beacon frame also contains the access point's clock value. Each station receiving the Beacon frame will use this information to update its clock accordingly, so the station knows when to wake up (if in sleep mode) to receive beacons.

Providing Authentication and Privacy

Because of the open broadcast nature of wireless LANs, designers need to implement appropriate levels of security. The 802.11 standard describes two following types of authentication services that increase the security of 802.11 networks:

- *Open system authentication:* The default authentication service that just announces the desire to associate with another station or access point
- *Shared key authentication:* Involves a more rigorous exchange of frames, ensuring the requesting station is authentic

The following sections describe the operation of each of these authentication types, as well as the *Wired Equivalent Privacy (WEP)* function.

Choosing Authentication Type

When setting up your wireless LAN, base your consideration of the type of authentication to use on security requirements. Vendors enable you to easily configure a station or access point to operate using either open encryption or shared key, or no security. The default operation is generally open encryption. If you implement the shared key mode, you will need to configure all stations with the same key.

Open System Authentication

An organization may wish to utilize open system authentication if it is not necessary to positively validate the identity of a sending station. A station can authenticate with any other station or access point using open system authentication if the

receiving station designates open system authentication via the MIB parameter `aAuthenticationType`.

Figure 4.4 illustrates the operation of open system authentication. The Status Code located in the body of the second authentication frame identifies success or failure of the authentication.

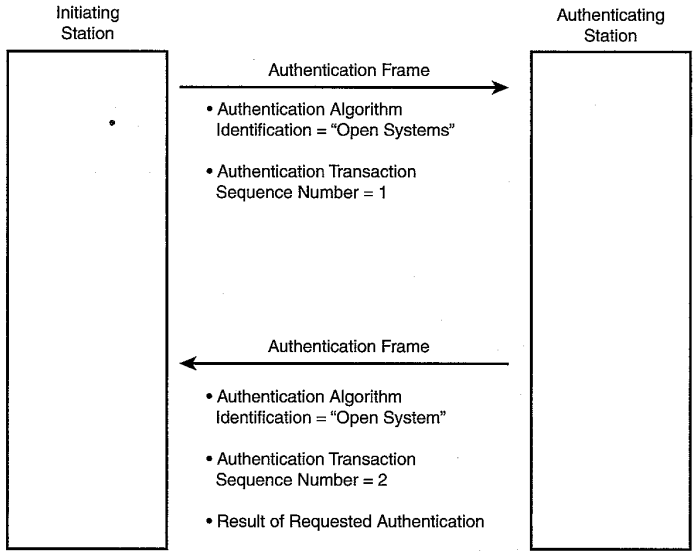


FIGURE 4.4 *The first frame of the open system authentication service requests authentication, and the second frame transmission indicates acceptance or rejection.*

Shared Key Authentication

The shared key authentication approach provides a much higher degree of security than the open system approach. For a station to utilize shared key authentication, it must implement WEP. Figure 4.5 illustrates the operation of shared key authentication. The secret shared key resides in each station's MIB in a write-only form to make it available to only the MAC coordination. The 802.11 standard, however, does not specify the process of installing the key in stations.

The process is as follows:

1. A requesting station sends an Authentication frame to another station.
2. When a station receives an initial Authentication frame, the station will reply with an Authentication frame containing 128 octets of challenge text that the WEP services generate.

3. The requesting station will then copy the challenge text into an Authentication frame, encrypt it with a shared key, and then send the frame to the responding station.
4. The receiving station will decrypt the value of the challenge text using the same shared key and compare it to the challenge text sent earlier. If a match occurs, the responding station will reply with an authentication indicating a successful authentication. If not, the responding station will send a negative authentication.

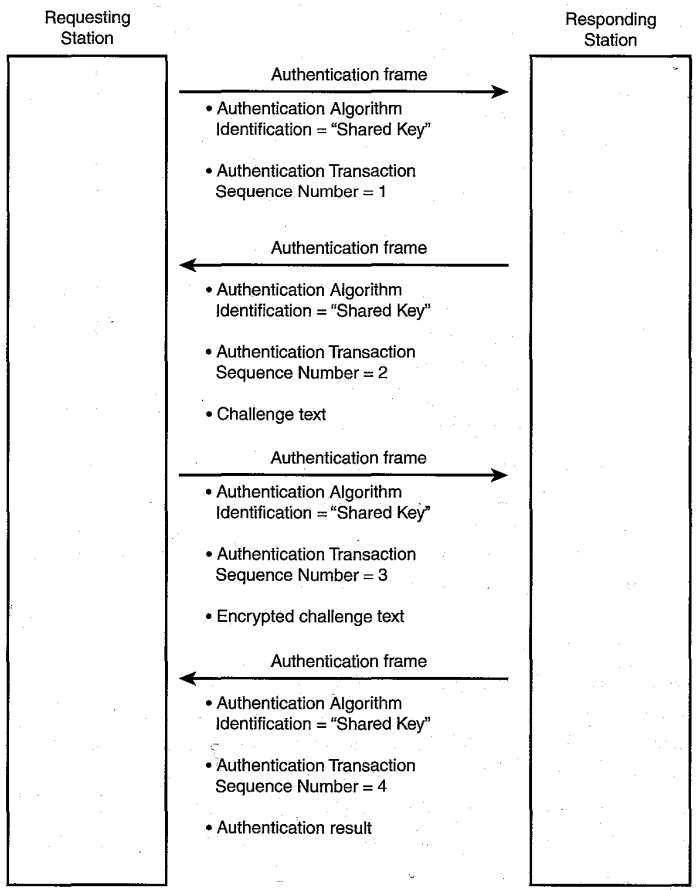


FIGURE 4.5 *The shared key authentication service uses the transmission of frames that (1) request authentication, (2) deliver challenge text, (3) deliver an encrypted frame, including the challenge text, and (4) accept or reject the authentication.*

Private Frame Transmissions

To offer frame transmission privacy similar to a wired network, the 802.11 specification defines optional WEP. The WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers. This process is also known as *symmetric encryption*. Stations can utilize WEP alone without authentication services, but they should implement both WEP and authentication together to avoid making the LAN vulnerable to security threats.

Figure 4.6 shows the processing that occurs with the WEP algorithm:

1. At the sending station, the WEP encipherment first runs the unencrypted data located in the Frame Body field of a MAC frame through an integrity algorithm that generates a four-octet integrity check value that is sent with the data and checked at the receiving station to guard against unauthorized data modification.
2. The WEP process inputs the secret shared encryption key into a pseudo-random number generator to create a key sequence with length equal to the `plaintext` and integrity check value.
3. WEP encrypts the data by using `bitwise XOR` on the `plaintext` and integrity check value with the key sequence to create `ciphertext`. The pseudo-random number generator makes key distribution much easier because only the shared key must be made available to each station, not the variable length key sequence.
4. At the receiving station, the WEP process deciphers the `ciphertext` using the shared key that generates the same key sequence used initially to encrypt the frame.
5. The station calculates an integrity check value and ensures it matches the one sent with the frame. If the integrity check fails, the station will not hand the MSDU off to the LLC, and a failure indication is sent to MAC management.

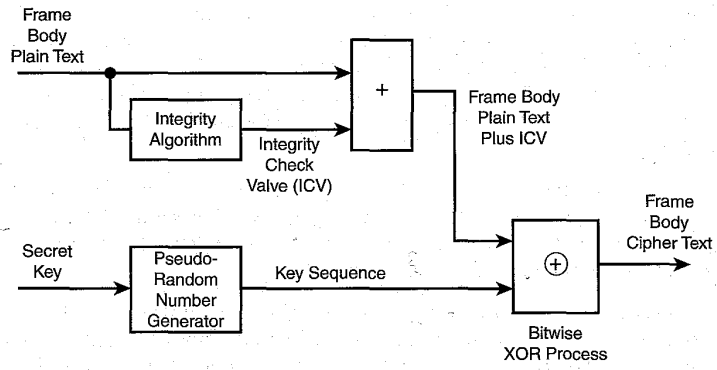


FIGURE 4.6 *The Wired Equivalent Privacy (WEP) safeguards data transmissions by performing a series of operations using a secret shared key.*

MAC Frame Structure

The following sections define each field and subfield of the MAC frame. For a formal description (using the ITU Specification and Description Language) of the MAC Layer operation, refer to Appendix C of the 802.11 standard.

Overall MAC Frame Format

The IEEE 802.11 standard specifies an overall MAC frame format, as shown in Figure 4.7. This frame structure is found in all frames that stations transmit, regardless of frame type. After forming the applicable frame, the MAC coordination passes the frame's bits to the physical layer convergence procedure sublayer (PLCP), starting with the first bit of the Frame Control field and ending with the last bit of the frame check sequence (FCS).

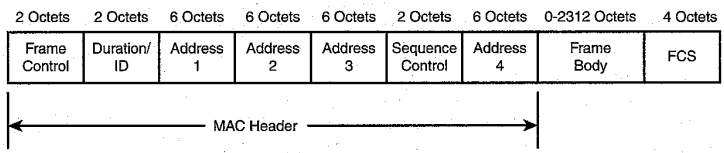


FIGURE 4.7 *The MAC frame consists of a header, variable length frame body, and a 32-bit frame check sequence (FCS), all of which support MAC Layer functionality.*

The following list defines each of the main MAC frame fields:

- *Frame Control:* This field carries control information being sent from station to station. Figure 4.8 illustrates specific subfields within the Frame Control field.
- *Duration/ID:* In most frames, this field contains a duration value, depending on the type of frame sent. (See the section "MAC Frame Types" later in this chapter for possible values.) In general, each frame contains information that identifies the duration of the next frame transmission. As an example, the Duration/ID field in data and acknowledegment (ACK) frames specifies the total duration of the next fragment and acknowledgement. Stations on the network monitor this field and hold off transmissions based on the duration information.

  In Power Save (PS)-Poll control frames only, the Duration/ID field carries the 14 least significant bits of the association identity of the sending station. The two remaining bits for this field are set to 1. Possible values for this identification are currently in the decimal range 1–2007.
- *Address 1, 2, 3, and 4:* The address fields contain different types of addresses, depending on the type of frame being sent. These address types may include the Basic Service Set Identification (BSSID), source address, destination address, transmitting station address, and receiving station address. IEEE standard 802-1990 defines the structure of the addresses, which are all 48 bits in length.

The addresses can be either individual or group addresses. There are two types of group addresses: *multicast*, which associate with a group of logically related stations; and *broadcast* addresses, which refer to all stations on a given LAN. A broadcast address consists of all 1s.

- *Sequence Control:* The leftmost 4 bits of this field consist of a Fragment Number subfield, indicating the fragment number of a particular MSDU. This number starts with 0 for the first fragment, and then increments by one for each successive transmission. The next 12 bits of this frame are the Sequence Number subfield starting at 0 and incrementing by 1 for each subsequent MSDU transmission. Each fragment of a specific MSDU will have the same sequence number.

  Only one MSDU can be outstanding at a time. On reception of a frame, a station can filter duplicate frames by monitoring the sequence and fragment numbers. The station knows the frame is a duplicate if the sequence number and fragment number are equal to the frame immediately preceding, or if the Retry bit is set to 1.

  Duplicate frames can occur when a station receives a frame without errors, sends an ACK frame back to the sending station, and transmission errors destroy the ACK frame en route. After not receiving the ACK over a specific time period, the sending station retransmits a duplicate frame. The destination station performs an acknowledgement of the retransmitted frame even if the frame is discarded due to duplicate filtering.

- *Frame Body:* This field has a variable length payload and carries information that pertains to the specific frame being sent. In the case of a data frame, this field may contain an LLC data unit (also called an MSDU). MAC management and control frames may include specific parameters in the Frame Body that pertain to the particular service the frame is implementing. If the frame has no need to carry information, this field has a length of zero. The receiving station will determine the frame length from a field within the applicable Physical Layer headers. (See Chapter 5, "Physical (PHY) Layer," for more information.)

- *Frame Check Sequence (FCS):* The MAC Layer at the sending station calculates a 32-bit *frame check sequence* (*FCS*) using a *Cyclic Redundancy Check* (*CRC*) and places the result in this field. The MAC Layer uses the following generator polynomial over all fields of the MAC header and Frame Body to calculate the FCS:

  $$G(x)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1.$$

  The result's highest-order coefficient is placed in the field, from the leftmost bit. The receiver implements a CRC to check for transmission errors in the frame.

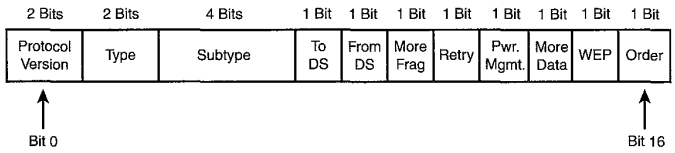


FIGURE 4.8 *The Frame Control field defines the frame as a management, control, or data frame.*

Setting Up a Network ID

The *Basic Service Set Identification (BSSID)*, also known as a network ID, is a 6-byte address that distinguishes a particular access point from others. Most access points will ship with a default BSSID, and you can change the ID through configuration parameters if you are installing a network with multiple access points.

Be sure to avoid conflicts by assigning a different BSSID for each access point. Typically, you can set up the access point via its management utility to automatically choose a BSSID that doesn't conflict with other BSSs operating in the same area.

Frame Control Field

The following defines each of the subfields within the Frame Control field:

- *Protocol Version field:* For the current standard, the protocol version is zero; therefore, the Protocol Version field always contains a `0`. IEEE will add additional version numbers in the future if a newer version of the standard is fundamentally incompatible with an earlier version.
- *Type field:* This field defines whether the frame is a management, control, or data frame as indicated by the bits in the following table:

Bit 3, Bit 2	Frame Type
0,0	Management frame
0,1	Control frame
1,0	Data frame
1,1	Reserved

Note

All reserved bits are transmitted as value `0` and are ignored by the receiving station.

- *Subtype field:* This field defines the function of the frame, as shown in the following table:

Frame Type	Subfield (Bits 7, 6, 5, 4)	Frame Function
Management Type	0000	Association Request
(bit 3, bit 2)=00	0001	Association Response
	0010	Reassociation Request
	0011	Reassociation Response
	0100	Probe Request
	0101	Probe Response
	0110–0111	Reserved
	1000	Beacon
	1001	Announcement Traffic Indication Map (ATIM)
	1010	Disassociation
	1011	Authentication
	1100	Deauthentication
	1101–1111	Reserved
Control Type	0000–1001	Reserved
(bit 3, bit 2)=01	1010	Power-Save (PS) Poll
	1011	Request to Send (RTS)
	1100	Clear to Send (CTS)
	1101	Acknowledgement (ACK)
	1110	Contention Free (CF) End
	1111	CF End + CF ACK
Data Type	0000	Data
(bit 3, bit 2)=10	0001	Data + CF ACK
	0010	Data + CF Poll
	0011	Data + CF ACK + CF Poll
	0100	Null (no data)
	0101	CF ACK
	0110	CF Poll
	0111	CF ACK + CF Poll
	1000–1111	Reserved
Reserved Type (bit 3, bit 2)=11	0000–111	

Limiting Multicast Traffic

A *delivery traffic indication message* (*DTIM*) determines how often the MAC Layer forwards multicast traffic. This parameter is necessary to accommodate stations using power save mode. You can set the DTIM value via the access point. If you set the value to 2, the access point will save all multicast frames for the BSS and forward them after every second beacon.

Smaller DTIM intervals deliver multicast frames in a more timely manner, causing stations in power save mode to wake up more often and drain power faster. Higher DTIM values, however, delay the transmission of multicast frames.

- *To DS field:* The MAC coordination sets this single-bit field to `1` in any frame destined to the distribution system. It is `0` for all other transmissions. An example of this bit being set would be the case when a frame's destination is in a radio cell (also called BSS) of a different access point.
- *From DS field:* The MAC coordination sets this single-bit field to `1` in any frame leaving the distribution system. It is `0` for all other transmissions. Both the To DS and From DS fields are set to `1` if the frame is being sent from one access point through the distribution system to another access point.
- *More Frag field:* This single-bit field is set to `1` if another fragment of the same MSDU follows in a subsequent frame.

Implementing Fragmentation

The MAC services provide fragmentation and defragmentation services to support the division of MSDUs into smaller elements for transmission. Fragmentation can increase reliability of transmission because it increases the probability of a successful transmission due to smaller frame size. Each station can support the concurrent reception and defragmentation of fragments for up to three MSDUs. The MAC Layer fragments frames having a unicast receiver address only. It never fragments broadcast and multicast frames because of significant resulting overhead on the network.

If the length of the MSDU needing transmission exceeds the `aFragmentationThreshold` parameter located in the MAC's management information base (MIB), the MAC protocol will fragment the MSDU. Each fragmented frame consists of a MAC header, FCS, and a fragment number indicating its ordered position in the MSDU. Each of the fragments is sent independently and requires separate ACKs from the receiving station. The More Fragment field in the Frame Control field indicates whether a frame is the last of a series of fragments.

After decryption takes place (if the station is implementing WEP), the destination station will combine all fragments of the same sequence number in the correct order to reconstruct the corresponding MSDU. Based on the fragment numbers, the destination station will discard any duplicate fragments.

If there is significant interference present or if there are collisions resulting from high network utilization, try setting the fragment size to send smaller fragments. This will enable the retransmission of smaller frames much faster. It is more efficient, however, to

set the fragment size larger if very little or no interference is present (because it requires overhead to send multiple frames). The fragment size value can typically be set between 256 and 2048 bytes.

- *Retry field:* If the frame is a retransmission of an earlier frame, this single-bit field is set to 1. It is 0 for all other transmissions. The reason for retransmission could be because the errors in the transmission of the first frame resulted in an unsuccessful FCS.

Setting the Transmission Retry Time

You can set the retry time on stations to govern the amount of time a station will wait before attempting to retransmit a frame if no acknowledgement appears from the receiving station. This time value is normally set between 1 and 30 seconds. You can also set the number of retries that will occur before the station gives up. This value can normally be set between 0 and 64.

- *Power Management field:* The bit in this field indicates the power management mode that the sending station will be in after the current frame exchange sequence. The MAC Layer places 1 in this field if the station will be in a sleep mode (802.11 defines this as power-save mode). A 0 indicates the station will be in full active mode. A receiving station can utilize this information to adjust transmissions to avoid waking up sleeping stations. In most cases, battery-operated devices should be kept in power-save mode to conserve battery power.
- *More Data field:* If a station has additional MSDUs to send to a station that is in power-save mode, then the sending station will place 1 in this field. The More Data field is 0 for all other transmissions. The more data feature alerts the receiving station to be ready for additional frames. An example of using this feature is when a station is sending a group of fragments belonging to a single MSDU.
- *WEP field:* A 1 in this field tells the receiving station that the WEP algorithm has processed the Frame Body; that is, the data bits have been encrypted using a secret key. The WEP field bit is 0 for all other types of transmissions. Refer to the section "Private Frame Transmissions" earlier in this chapter to learn how the WEP algorithm works.
- *Order field:* This field is set to 1 in any data frame being sent using the StrictlyOrdered service class, which tells the receiving station that frames must be processed in order.

Note

The IEEE 802.11 standard makes use of the same 48-bit MAC address that is compatible with the entire 802 LAN family. The 802.11 architecture can handle multiple logical media and address spaces, which makes 802.11 independent of the distribution system implementation.

continues

The vendor you purchase the radio card and access points from usually guarantees that the MAC address loaded in the radio is unique from all other radios, even ones from other vendors. You normally have the ability to change the MAC address of the card; however, you should use the factory-set address to avoid the potential of address conflicts.

IEEE 802.11 defines the following address types:

- Destination address (DA): *The final destination of the MSDU located that is in the Frame Body of the MAC frame*
- Source address (SA): *The address of the MAC entity that initiated the MSDU transmission*
- Receiver address (RA): *The address of the access point that is to receive the frame next*
- Transmitter address (TA): *The address of the immediate preceding access point sending the frame*

MAC Frame Types

To carry out the delivery of MSDUs between peer LLCs, the MAC Layer uses a variety of frame types, each having a particular purpose. The IEEE 802.11 specification divides MAC frames into three broad categories that provide management, control, and data exchange functions between stations and access points. The following sections describe the structure of each major frame type.

Management Frames

The purpose of Management frames is to establish initial communications between stations and access points. Thus, Management frames provide such services as association and authentication. Figure 4.9 depicts the common format of all Management frames.

2 Octets	2 Octets	6 Octets	6 Octets	6 Octets	2 Octets	0-2312 Octets	4 Octets
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS

FIGURE 4.9 *The Management frame format includes destination address, source address, and BSSID in Address fields 1, 2, and 3, consecutively.*

The Duration field within all Management frames during the contention-free period (as defined by the point coordination function) is set to decimal 32,768 (hexadecimal value of 8000), giving Management frames plenty of time to establish communications before other stations have the capability to access the medium.

During the contention period (as defined by the CSMA-based distributed coordination function), all Management frames have the Duration field set as follows:

- If the destination address is a group address, the Duration field is set to 0.
- If the More Fragments bit is set to 0 and the destination address is an individual address, the Duration field contains the number of microseconds required

to transmit one ACK frame and one short *interframe space*. (The section "Access Spacing" earlier in this chapter defines the interframe space.)

- If the More Fragments bit is set to 1 and the destination address is an individual address, the Duration field contains the number of microseconds required to transmit the next fragment, two ACK frames, and three short interframe spaces.

A station receiving a Management frame performs address matching for receive decisions based on the contents of the Address 1 field of the MAC frame, which is the destination address (DA). If the address matches the station, that station completes the reception of the frame and hands it off to the LLC Layer. If a match does not occur, the station ignores the rest of the frame.

The following defines each of the management frame subtypes:

- *Association Request frame:* A station will send this frame to an access point if it wants to associate with that access point. A station becomes associated with an access point after the access point grants permission.
- *Association Response frame:* After an access point receives an Association Request frame, the access point will send an association response frame to indicate whether it is accepting the association with the sending station.
- *Reassociation Request frame:* A station will send this frame to an access point if it wants to reassociate with that access point. A reassociation may occur if a station moves out of range from one access point and within range of another access point. The station will need to reassociate with the new access point (instead of merely *associate*) so that the new access point knows that it will need to negotiate the forwarding of data frames from the old access point.
- *Reassociation Response frame:* After an access point receives a Reassociation Request frame, the access point will send a Reassociation Response frame to indicate whether it is accepting the reassociation with the sending station.
- *Probe Request frame:* A station sends a Probe Request frame to obtain information from another station or access point. For example, a station may send a Probe Request frame to determine whether a certain access point is available.
- *Probe Response frame:* If a station or access point receives a Probe Request frame, the station will respond to the sending station with a Probe Response frame containing specific parameters about itself (for example, parameter sets for the frequency hopping and direct sequence PHYs).
- *Beacon frame:* In an infrastructure network, an access point periodically sends a Beacon frame (according to the `aBeaconPeriod` parameter in the MIB) that provides synchronization among stations utilizing the same PHY. The Beacon frame includes a timestamp that all stations use to update what 802.11 defines as a timing synchronization function (TSF) timer.

If the access point supports the point coordination function, it uses a Beacon frame to announce the beginning of a contention-free period. If the network is an independent BSS (that is, having no access point), all stations periodically send Beacon frames for synchronization purposes.

- *ATIM frame:* A station with frames buffered for other stations sends an ATIM (announcement traffic indication message) frame to each of these stations during the ATIM window, which immediately follows a Beacon frame transmission. The station then transmits these frames to the applicable recipients. The transmission of the ATIM frame alerts stations in sleep state to stay awake long enough to receive their respective frames.
- *Disassociation frame:* If a station or access point wants to terminate an association, it will send a Disassociation frame to the opposite station. A single Disassociation frame can terminate associations with more than one station through the broadcast address of all 1s.
- *Authentication frame:* A station sends an Authentication frame to a station or access point that it wishes to authenticate with. The authentication sequence consists of the transmission of one or more Authentication frames, depending on the type of authentication being implemented (that is, open system or shared key). Refer to the section "Providing Authentication and Privacy" earlier in this chapter.
- *Deauthentication frame:* A station sends a Deauthentication frame to a station or access point with which it wants to terminate secure communications.

The content of the Frame Body field of management frames depends on the type of management frame being sent. Figure 4.10 identifies the Frame Body contents of each management frame subtype.

Implementing Power Management

The power-management function of an IEEE 802.11 network enables stations to go into sleep mode to conserve power for long periods of time without losing information. The 802.11 power management is supported with the use of access points; therefore, it is not available when implementing ad hoc networks. You should definitely consider implementing this feature if the conservation of batteries powering the radio card and appliance is a concern.

You implement power management on IEEE 802.11 LANs by first setting the access points and radio cards to power save mode via the vendor's parameter initialization routines. The access points and radio cards will then carry out the power-management functions automatically. As part of the power-management routine, the access points will maintain a record of the stations currently working in power save mode by monitoring the single-bit power-management field in the Frame Control field of the MAC header for frames sent on the network. The access points will buffer packets addressed to the stations in power save mode.

The access points will forward the buffered packets to the applicable stations when they return to active state (awake state) or when the stations request them. The access point knows when a station awakens because the station will indicate its active state by toggling the power-management bit in the Frame Control field of the MAC frames.

A station can learn that it has frames buffered at the access point by listening to the beacons sent periodically by the access point. The beacons will have a list (called a *traffic indication map*) of stations having buffered frames at the access point. A station uses a Power-Save Poll frame to notify the access point to send the buffered packets.

Frame Body Contents	Association Request	Association Response	Reassociation Request	Reassociation Response	Probe Response	Probe Request	Beacon	Disassociation	Authentication	Deauthentication
Authentication Algorithm Number									X	
Authentication Transaction Sequence Number									X	
Beacon Interval					X		X			
Current AP Address			X							
Listen Interval	X		X							
Reason Code								X		X
Association ID(AID)		X		X						
Status Code		X		X					X	
Timestamp					X		X			
Service Set Identity (SSID)	X		X		X	X	X			
Supported Rates	X	X	X	X	X	X	X			
FH Parameter Set					X		X			
DS Parameter Set					X		X			
CF Parameter Set					X		X			
Capability Information	X	X	X	X	X		X			
Traffic Indication Map (TIM)							X			
IBSS Parameter Set					X		X			
Challenge Text									X	

FIGURE 4.10 *The Frame Body contents of a management frame depend on the frame subtype.*

The 802.11 standard describes the Frame Body elements of the management frame subtypes. Refer to the standard if you need detailed information, such as field formats. The following, however, summarizes each of the elements:

- *Authentication Algorithm Number:* This field specifies the authentication algorithm that the authenticated stations and access points are to use. The value is either `0` for open system authentication or `1` for shared key authentication.

- *Authentication Transaction Sequence Number:* This field indicates the state of progress of the authentication process.
- *Beacon Interval:* This value is the number of time units between beacon transmission times.
- *Capability Information:* This field announces capability information about a particular station. For example, a station can identify its desire to be polled in this element.
- *Current AP Address:* This field indicates the address of the *access point* that the station is currently associated with.
- *Listen Interval:* This value identifies, in units of Beacon Interval, how often a station will wake to listen to Beacon management frames.
- *Reason Code:* This field indicates the reason (via a numbered code) a station is generating an unsolicited disassociation or deauthentication. Examples of the reasons are as follows:
    - Previous authentication no longer valid
    - Disassociated due to inactivity
    - Station requesting association is not authenticated with responding station
- *Association ID (AID):* This ID, which is assigned by an access point during association, is the 16-bit identification of a station corresponding to a particular association.
- *Status Code:* This code indicates the status of a particular operation. Examples of status are as follows:
    - Successful
    - Unspecified failure
    - Association denied because the access point is unable to handle additional associated stations
    - Authentication rejected due to timeout waiting for next frame in sequence
- *Timestamp:* This field contains the timer value at the sending station when it transmits the frame.
- *Service Set Identify (SSID):* This field contains the identity of the Extended Service Set (ESS).
- *Supported Rates:* This field identifies all data rates a particular station can accept. This value represents the data rate in 500 Kbps increments. The MAC coordination has the capability to change data rates to optimize performance of frame transmissions.
- *FH Parameter Set:* This field indicates the dwell time and hopping pattern needed to synchronize two stations using the *frequency hopping* PHY.

- *DS Parameter Set:* This field identifies the channel number that stations are using with the *direct sequence* PHY.
- *CF Parameter Set:* This field consists of a series of parameters that support the *point coordination function* (*PCF*).
- *TIM:* The *traffic indication map* (*TIM*) element specifies the stations having MSDUs buffered at the access point.
- *IBSS Parameter Set:* This field contains parameters that support the Independent Basic Service Set (IBSS) networks.
- *Challenge Text:* This field contains the challenge text of a shared key authentication sequence.

Note

Some vendors add optional extensions to 802.11 management frames that provide functionality beyond the standard. As an example, additional information of an Association Request frame could set priorities for which access point a station associates with.

If you're using access points from multiple vendors, you should disable the transmission of the extensions.

Control Frames

After establishing association and authentication between stations and access points, control frames provide functionality to assist in the delivery of data frames. Figure 4.11 shows a common flow of control frames.

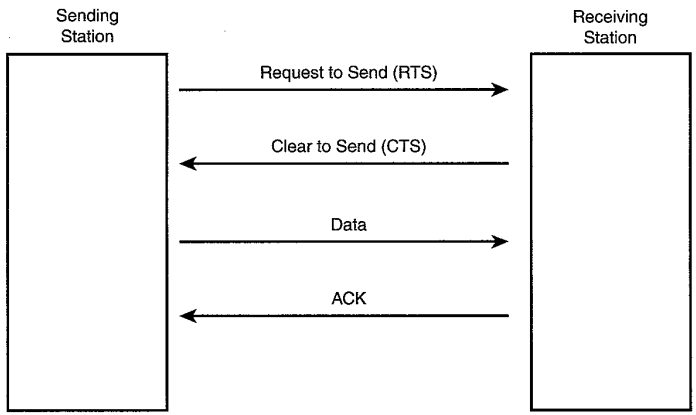


FIGURE 4.11 *Control frames provide synchronization between sending and receiving stations.*

The following defines the structure of each control frame subtype:

- *Request to Send (RTS):* A station sends an RTS frame to a particular receiving station to negotiate the sending of a data frame. Through the `aRTSThreshold` attribute stored in the MIB, you can configure a station to either always, never, or only on frames longer than a specified length, initiate an RTS frame sequence.

  Figure 4.12 illustrates the format of an RTS frame. The value of the Duration field, in microseconds, is the amount of time the sending station needs to transmit the frame, one CTS frame, one ACK frame, and three *short interframe space* (*SIFS*) intervals.

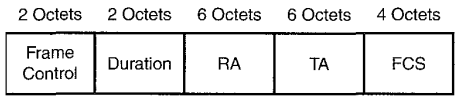


FIGURE 4.12 *The Request to Send frame format includes the receiver address (RA) and transmitter address (TA).*

- *Clear to Send (CTS):* After receiving an RTS, the station sends a CTS frame to acknowledge the right for the sending station to send data frames. Stations will always pay attention to the duration information and respond to an RTS frame, even if the station was not set up to initiate RTS frame sequences.

  Figure 4.13 illustrates the format of a CTS frame. The value of the Duration field, in microseconds, is the amount of time from the Duration field of the previous RTS frame minus the time required to transmit the CTS frame and its SIFS interval.

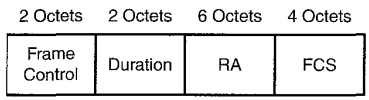


FIGURE 4.13 *The Clear to Send and Acknowledgement frame formats include the receiver address (RA).*

- *Acknowledgement (ACK):* A station receiving an error-free frame can send an ACK frame to the sending station to acknowledge the successful reception of the frame. Figure 4.13 illustrates the format of an ACK frame.

  The value of the Duration field, in microseconds, is equal to zero if the More Fragment bit in the Frame Control field of the preceding data or management frame is set to `0`. If the More Fragment bit of the previous data or management frame is set to `1`, the Duration field is the amount of time from the

Duration field of the preceding data or management frame minus the time required to transmit the ACK frame and its SIFS interval.

- *Power-Save Poll (PS Poll):* If a station receives a PS Poll frame, the station updates its *network allocation vector (NAV)*, which is an indication of time periods that a station will not initiate a transmission. The NAV contains a prediction of future traffic on the medium. Figure 4.14 illustrates the format of a PS Poll frame.

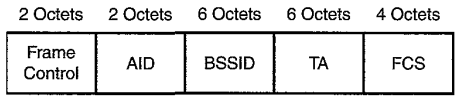


FIGURE 4.14 *The Power-Save Poll frame format includes the association identifier (AID), Basic Service Set Identification (BSSID), and the transmitter address (TA).*

- *Contention-Free End (CF End):* The CF End designates the end of a contention period that is part of the point coordination function. Figure 4.15 illustrates the format of a CF End frame. In these frames, the Duration field is always set to 0, and the receiver address (RA) contains the broadcast group address.

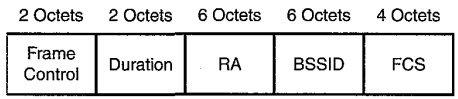


FIGURE 4.15 *The CF End and CF End + CF ACK frame formats include the receiver address (RA) and Basic Service Set Identification (BSSID).*

- *CF End + CF-ACK:* This frame acknowledges the Contention-Free End announcement of a CF End frame. Figure 4.15 illustrates the format of a CF End + CF ACK frame. In these frames, the Duration field is always set to 0, and the receiver address (RA) contains the broadcast group address.

Using RTS/CTS

Because of the possibility of partial network connectivity, wireless LAN protocols must account for potential hidden stations. You can activate the RTS/CTS mode via the setup utility for the access point.

The RTS/CTS operation provides much better performance over basic access when there is a high probability of hidden stations. In addition, the performance of RTS/CTS degrades more slowly than basic access when network utilization increases. The use of RTS/CTS, however, will result in relatively low throughput in a situation where there is very little probability of hidden stations.

The Handover Protocol performs the following procedure:

1. It informs an access point that one of its stations has reassociated with a different access point.
2. The old access point forwards buffered frames for the station to the new access point.
3. The new access point updates filter tables to ensure MAC-level filtering (that is, *bridging*), and forwards frames appropriately.

Implementing Roaming

Normally, you won't have the luxury to choose a type of roaming protocol for the wireless system you are implementing. Vendors generally implement a proprietary roaming protocol that works only with their products. When making a selection of which access points to use, be sure to include the presence of multiple-vendor roaming protocols (for example, IAPP) as a factor when comparing access points.

As with other product procurements, however, it is most effective to plan on purchasing components, such as access points and radio cards, from a common vendor. Similar to implementing an ethernet network with common hubs and switches, this will make the resulting wireless system easier to manage.

Communications Protocols

The wireless and wired networking technologies provide lower-level connections among the network interface cards located in end-user appliances, access points, servers, and printers. A communications protocol operates at a higher level (typically Transport and Network Layers) and establishes end-to-end connections between the application software within devices on the network. This is necessary to provide a common path for entities to communicate.

The most common protocol for providing communications among network devices and applications are the Transmission Control Protocol (TCP) and Internet Protocol (IP). These protocols are the basis of standards for connecting to the Internet and providing open systems connectivity in other systems. The IETF has many RFCs (Request for Comments) that explain the operation of TCP/IP protocols. You can purchase TCP/IP software from a variety of vendors for different platforms. In fact, UNIX includes TCP/IP as part of the operating system.

Transmission Control Protocol (TCP)

Transmission Control Protocol (TCP) operates at the OSI Transport Layer and is commonly used for establishing and maintaining communications between applications on different computers. TCP provides highly reliable, full-duplex, connection-oriented, acknowledged, and flow-control services to upper-layer protocols and

applications. A mainframe computer, for example, employing TCP software enables a user, having TCP software as well, to log on to the mainframe and run the application using Telnet. Connection-oriented services, such as Telnet, FTP, rlogin, X Windows, and SMTP, require a high degree of reliability and therefore use TCP. Figure 6.13 illustrates the header of the TCP protocol.

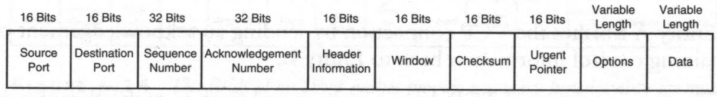


FIGURE 6.13 *The fields of a TCP datagram provide necessary functionality for reliable communications between a source and destination network device.*

The following list describes the fields of TCP datagram:

- *Source Port and Destination Port:* Identifies the service access points at which upper-layer source and destination processes and applications receive TCP services. Most server processes associate with a fixed port number (for example, 23 for Telnet and 161 SNMP) to provide application developers a standard port to point to when communicating with a server.

  Most client processes, however, request a port number from the server's operating system at the beginning of execution. This enables the server processes to differentiate which client process it is communicating with.

- *Sequence Number:* Specifies the sequence number of the datagram being sent.
- *Acknowledgement Number:* Contains the sequence number of the next datagram the sender of the immediate packet expects to receive.
- *Header Information:* Carries information about the TCP header, such as the length and control flags.
- *Window:* Specifies the size of the sender's receive window (that is, buffer space available for incoming data).
- *Checksum:* Used to determine whether the header contains errors.
- *Urgent Pointer:* Points to the first data in the packet byte that the sender wanted to mark as urgent.
- *Options:* Specifies various TCP options.
- *Data:* Contains upper-layer information and control data.

Tip

Firewalls can filter incoming datagrams based on the port addresses found in the TCP header. This enables system designers to restrict access to specific applications on a network residing behind the firewall. Be sure to incorporate a firewall with appropriate TCP filters to block access to specific applications.

The operation of the TCP protocol is fairly straightforward:

1. Entity A, wishing to establish a connection with Entity B, initiates a three-way handshake protocol starting with a connection request datagram sent to Entity B.
2. Entity B responds to Entity A with an acknowledgement containing control information (for example, window size).
3. Entity A finishes the TCP connection by sending an acknowledgement containing control information back to Entity B.
4. The two entities send TCP datagrams back and forth to each other associated to a particular port address.

Internet Protocol (IP)

The Internet Protocol (IP) operates at the OSI Network Layer. Routers commonly use IP to route TCP datagrams from source to destination. Figure 6.14 illustrates the fields of an IP packet. The following list describes these fields:

- *Version:* The version number of the IP protocol. For example, a value of 4 represents IPv4, and a value of 6 represents IPv6.
- *Internet Header Length:* The length of the IP header in 32-bit words.
- *Type of Service:* The level of service (for example, precedence, delay, throughput, and reliability) the IP datagram should be given as it traverses the network.
- *Total Length:* The length of the datagram in bytes.
- *Identification:* The identification number of the datagram for purposes of combining datagram fragments.
- *Flags:* Data bits for controlling whether fragmentation should take place.
- *Fragment Offset:* The location of a datagram (if it is a fragment) within the complete datagram. The receiving entity uses this to combine fragments.
- *Time-to-Live:* The maximum amount of time the datagram can exist as the datagram traverses the network.
- *Protocol:* The protocol that associates with the data in the Data field of the datagram. A value of 6 indicates that the Data field contains a TCP datagram, for example, and a value of 17 indicates that the Data field contains a UDP datagram.
- *Header Checksum:* 16-bit checksum of the datagram header (up to and including the Protocol field).
- *Source IP Address:* The IP address of the sender of the datagram.
- *Destination IP Address:* The IP address of the destination of the datagram.

- *Options:* A set of fields that describe specific processing that must take place on the packet. Options are generally used for debugging and testing.
- *Padding:* Additional data bits to ensure the packet is a complete set of 32-bit words.

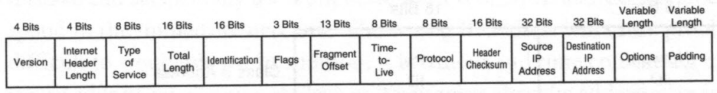


FIGURE 6.14 *The fields of an IPv4 packet provide necessary functionality for routing across dissimilar networks.*

If you plan to use applications requiring TCP/IP interfaces or if users will need access to the Internet, you will have to assign a unique IP address to each device connected to the network (handheld appliance, access point, workstation, printer, server, and so on). Actually, the IP address corresponds to a network connection; therefore, a server having two network interface cards requires two IP addresses, one for each card.

The IP packet header contains the source and destination IP address that routers will use, along with a routing table, to determine where to send the packet next. The IP address is 32 bits long; therefore, there are 4,294,967,296 unique IP addresses.

IP Address Classes

The developers of the Internet decided to base IP addressing on the hierarchical format shown in Figure 6.15, distinguishing the address into three classes: Class A, Class B, and Class C. If your organization never plans to interface with the Internet, then you are free to use the IP address space in any way. Otherwise, you must obtain official IP addresses (ones that are unique from others assigned) to operate over the Internet.

You can obtain an official IP address through an Internet service provider (ISP) in your nearest metropolitan area. For an official IP address, you will be given a unique network number, and you are free to assign addresses within the domain. If you are assigned a Class C address, for example, you are free to assign up to 255 addresses.

Troubleshooting Tip

Because of the vast number of organizations deploying Web servers and gaining access to the Internet, IP addresses are quickly running out. In fact, it is impossible to obtain a Class A address and very difficult if not impossible to obtain a Class B address. Therefore, you will probably be issued multiple Class C addresses.

The problem, however, is that it is difficult to manage multiple Class C addresses if they are not contiguous. Therefore, you must predict the number of addresses you will need for the long term to maintain a contiguous series of addresses.

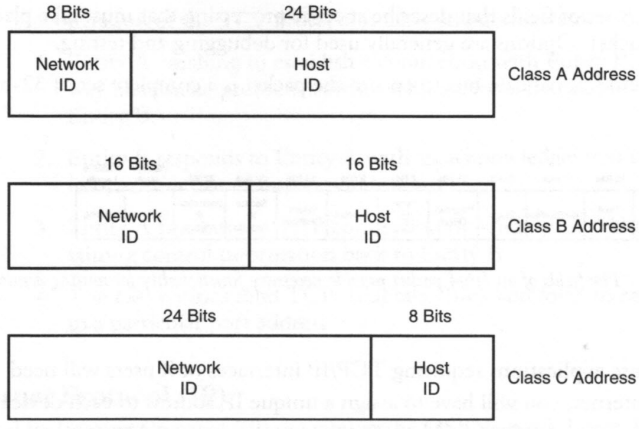


FIGURE 6.15 *A router forwards packets on to a particular network segment based on the network ID portion of the IP address. When the packet arrives at the correct network, the network will deliver the packet to the final destination based on the host ID.*

When planning the allocation of address, ensure that you obtain enough official unique IP addresses for each network connection. An organization having 350 users, 10 access points, and 4 servers, for example, would require at least 364 addresses. You could satisfy this requirement by obtaining one Class B address or two Class C addresses.

Note

Most systems currently use IPv4, having been in use since the early 1980s. Some companies, however, are beginning to migrate their systems to a newer version, IPv6. The main differences are that IPv6 offers much larger IP addresses—128 bits each—providing a solution to the small number of IPv4 IP addresses, and IPv6 includes extensions to support authentication, data integrity, and data confidentiality.

Implementing IP Address Assignment with a Limited Number of Official IP Addresses

If your network implementation requires a large number of IP addresses, or if it is difficult to predict the number of addresses needed in the future, consider private addressing techniques. The Network Information Center has set aside a single Class A address (10.X.X.X) that you can use within your network, giving you a large number of addresses to assign to network devices. You have to agree, however, to not use these addresses on the Internet.

If you need Internet access, you can deploy a proxy server that translates your private addresses into legal Internet addresses. This means that you need to obtain at least one Class C address to support the connections to the Internet. As a result, the outside world sees only a few IP addresses, not the many used within the company.

Static Versus Dynamic IP Addresses

For smaller wireless LANs (fewer than 50 users), it may be feasible to install static IP addresses within the configuration files for each appliance. The problem with installing static IP addresses in larger LANs is that you will more than likely make a mistake and accidentally use a duplicate address or an IP address that doesn't correspond to the immediate network. The wrong IP address will cause problems that are difficult to troubleshoot. In addition, it is tedious and time consuming to change the IP address on all network devices if you must alter the address plan in the future.

For larger LANs, consider the use of a dynamic address assignment protocol, such as Dynamic Host Configuration Protocol (DHCP). DHCP issues IP addresses automatically within a specified range to devices, such as PCs when they are first powered on. The device retains the use of the IP address for a specific license period that the system administrator can define. DHCP is available as part of the Microsoft Windows NT Server NOS and UNIX operating systems, and offers the following advantages over manual installation:

- *Efficient implementation of address assignments:* With DHCP, there is no need to manually install or change IP addresses at every client workstation during initial installation or when a workstation is moved from one location to another. This saves time during installation and avoids mistakes in allocating addresses (such as duplicate addresses or addresses having the wrong subnet number). It is very difficult to track down address-related problems that may occur when using permanently assigned addresses.
- *Central point of address management:* With DHCP, there is no need to update the IP address at each client workstation if making a change to the network's configuration or address plan. With DHCP, you can make these changes from a single point in the network. If you move the Domain Name Service software to a different platform (for example, from a Sun to an NT platform), for example, you would need to incorporate that change for each client workstation if using permanently assigned addresses. With DHCP, you just update the configuration screen from a single point at the Windows NT Server or remote location. Again, this advantage is strongest for larger networks.

TCP/IP: Wireless LAN Issues

TCP/IP provide an excellent platform for high-speed wired LANs with constant connections; however, the use of TCP/IP over wireless LANs offers significant problems. The following explains issues that may affect the performance of the wireless LAN when using standard TCP/IP:

- *High overhead:* Because TCP is connection oriented, it often sends packets that only perform negotiations or acknowledgements and do not contain real data.