Wireless LANs: Implementing Interoperable Networks

- 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 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 nonstandard 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** Appliances 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 net-works 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 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 milli-seconds; 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
- 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

**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, 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:

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, WEP 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
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 simple 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
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.