

The 802.11b Wireless LAN Revolution Breaks Open Industrial Ethernet Barriers

Eric P. Marske
Industrial Automation Sales Manager
Electronic Systems Technology, Inc.
Kennewick, WA 99336

KEYWORDS

Wireless Networking, Wireless Ethernet, WLAN, Radio, Communication, IEEE 802.11b

ABSTRACT

As Ethernet based communication protocols open the future of industrial automation, true Ethernet speeds and security will be required for wireless solutions in industrial applications. This presentation will discuss the use IEEE 802.11b wireless Ethernet in industrial applications. This type of wireless Ethernet network can provide multiple configurations such as bridging remote Ethernet networks over distances of 5 miles, providing mobile Ethernet access from the office to the factory floor or a combination of the two networks all running at 11 Mbps data rate. The extra bandwidth provided by the 802.11b wireless network can be used for remote on-line programming, web-based management, data collection or any IP based communication.

INTRODUCTION

Any industrial control publication that you read today will contain a discussion of Ethernet being the protocol solution for the future of industrial automation. Support for using Ethernet on the factory floor continues to build, but many of the advantages gained from this protocol standard such as speed, security and open standards were lost when applying them to a wireless communication network. Today, wireless Ethernet systems based upon the IEEE 802.11 Wireless Local Area Network (WLAN) standard can be applied to solve these problems and add features such as network flexibility and mobility.

Ethernet in Industry

The first step in understanding the benefits and limitations of Ethernet applications in industry is defining the term "Ethernet". Ethernet is the worldwide networking standard that defines the two lowest levels of an International Standardization Organization (ISO) networking stack, the *Physical Layer* and

Data Link layer (Figure 1). The physical layer of the standard defines the cable types, connectors, and electrical characteristics. The data link layer defines the format for an Ethernet frame, the error checking method and the physical addressing method.

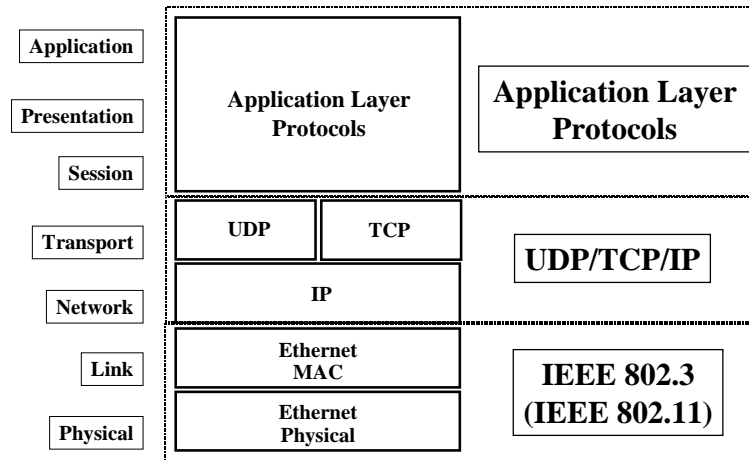


Figure 1: ISO Networking Model

The goal of an open Ethernet standard would be for a user to install a single interface that would work, regardless of their control vendor. The limitation to this is that Ethernet does not define higher levels of the networking model, the control system protocols called *Application Layer Protocols*, but only defines the *Physical Layer* and *Data Link Layer*. While the physical layer and data link layer are critical to the operation of a network, they are not enough to make a control system operational. TCP/IP is almost universally used on top of Ethernet to provide the network and transport layers in the open systems interconnect model to solve issues of routing and end-to-end data integrity. TCP/IP contains well-known Internet protocols such as File Transfer Protocol (FTP), Simple Mail Transport Protocol (SMTP) and Hypertext Transfer Protocol (HTTP). Different control vendors use one or more of these protocols, but these protocols by themselves can not provide all the functionality that the process control world needs. The *Application Layer Protocols* provide the definition for the tasks or command that can be executed over the network, but this is where the commonality between the differing control networks ends. Without a defined control networking standard, different vendors are providing application protocols bundled on top of TCP to complete their process tasks.

It is still in debate to what level Ethernet will be applied, but Ethernet does provide a proven common standard and is widely used in plant-floor applications today. Will Ethernet reach the device level? This question will only be answered in time and by customer demands placed on the control manufactures, but regardless of the outcome the need for wireless communication links will only increase.

Wireless in Industry

Wireless systems have always provided significant advantages over wired systems in certain applications. Good examples of cost-effective wireless solutions are in long distance communication networks such as water/wastewater systems, mobile equipment such as overhead cranes, and communications to inaccessible areas that are too difficult or too costly for cabled networks. As vendors

expand their communications requirements wireless communication becomes more cost effective. Quoting Martin Wojcik in the February 2001 edition of Control Solutions “One foot of wire can cost in total (i.e., initial cost plus installation cost plus maintenance cost) from \$40 in a typical plant to \$2000 or more in a nuclear facility.” As Ethernet communications proliferates throughout the factory floor, wireless communication can save both time and money. Wireless networks can be broken down into two major categories, licensed narrow-band radio and unlicensed spread-spectrum radio.

Narrow band licensed radios have been the workhorse for wireless industrial communication for over twenty years. As the name would imply, narrow-band radio technology uses a single frequency for wireless transmission on a very small channel bandwidth. Since Electronic Systems Technology, Inc. (EST) first combined a radio modem and radio transceiver into one unit in the patented ESTeem wireless modem in the early 1980’s, the evolution of narrow-band radio technology has allowed faster data rates on narrowing channel widths. In the U.S., the Federal Communications Commission (FCC) grants authority to operate radio transmitters and receivers either by licensed or unlicensed operation. The current channel widths allowed by the FCC are 12.5kHz with the latest technology providing data rates up to 19,200 bps. These data rates are more suitable for serial communication (RS-232C, RS-422 and RS-485) such as used in Supervisory Control and Data Acquisition (SCADA) networks between Human Machine Interface (HMI) computers, Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). The major advantages in narrow-band radio systems are better radio propagation in the lower frequencies of operation, higher output powers and exclusive use of frequencies due to licensing.

The term “spread spectrum” simply means that the energy radiated by the transmitter is spread out over a wider amount of the RF spectrum than would otherwise be used. By spreading out the energy, it is far less likely that two users sharing the same spectrum will interfere with the operation of each other. This is important considering spread spectrum radios use unlicensed bands. In 1985, the FCC made new rules under Part 15 authorizing unlicensed spread spectrum technology. Although spread spectrum techniques have been well known to the military since World War II, the commercial sector had not previously benefited from the technology. Spread spectrum radio communications systems can support much higher data capacities and with greater spectrum efficiency than the traditional forms of radio communications. Although limited to one watt of output power at very high carrier frequencies that greatly decreased the range when compared with a traditional narrow-band system, the unlicensed operation and vastly increased data rates (up to 11 Mbps) allowed this technology to make wireless Ethernet a reality.

Spread Spectrum

Spread Spectrum (SS) radio communication has two distinct methods; Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Both modulation methods can be applied to the three frequency bands allocated for unlicensed operation within the United States, 902-928 MHz, 2.400 - 2.483 GHz and 5.725 – 5.878 GHz collectively designated as Industrial, Science and Medicine (ISM). All spread spectrum radio equipment in the ISM band use these high frequency carriers and low output power, this then requires that all antennas have a Line-of-Site (LOS) for effective communication.

To better understand why Direct Sequence Spread Spectrum is more efficient for wireless Ethernet, let's take a quick look at both methods. Frequency Hopping Spread Spectrum is easiest to think of as a narrow-band radio with a frequency-agile design that permits fast movement or "hopping" to any channel within the total allocated spectrum. The carrier frequency hops from channel to channel in some pre-arranged sequence (Figure 2). The receiver is programmed to hop in sequence with the transmitter. If one channel is jammed, the data is simply retransmitted when the transmitter hops to a clear channel. The major drawback to this technique is a limited data rate. In the 2.4 GHz band, the FCC regulations require that the maximum occupied bandwidth for any single channel is 1 MHz. This effectively limits the data rate through this type of system to approximately 1 Mbps.

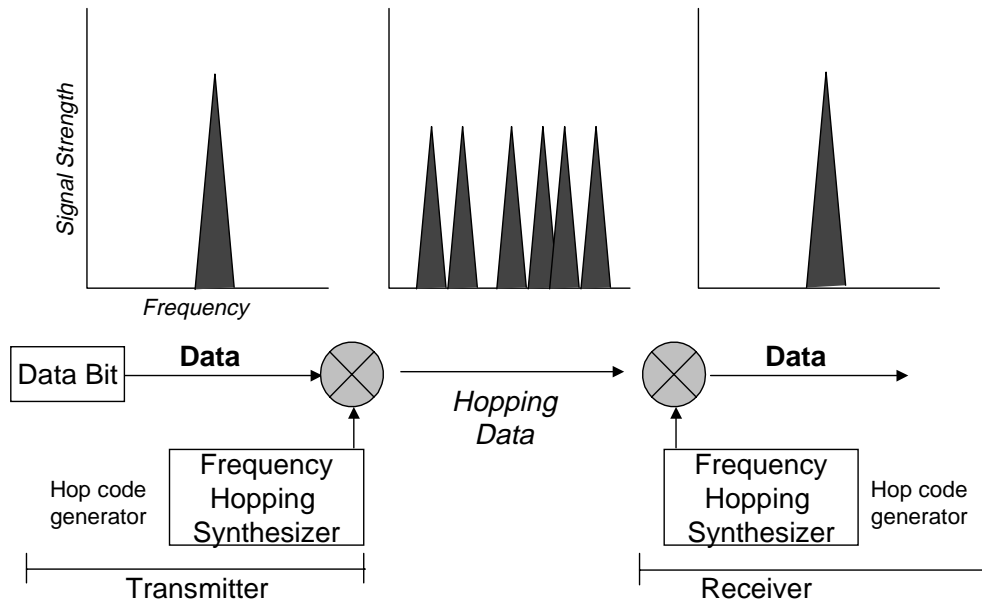


Figure 2: Frequency Hopping Spread Spectrum Diagram

By contrast, DSSS systems in the ISM band provide much higher data rates. The DSSS does not jump from frequency to frequency, but instead actually spreads the information across a much wider bandwidth. It sends pieces of each bit across the whole band and then adds them back up in the receiver. This is accomplished by modulating the original data with a high-speed, repeating digital bit stream known as a Pseudo Random Numerical (PRN) sequence via an XOR gate function. The result is a data stream at the same rate as the PRN. When the RF carrier is modulated by the higher speed digital stream, the result is a spreading of the RF energy (Figure 3) across the frequency band. In the receiver the same PRN code is used to "de-spread" the receiver data. If the transmitter and receiver in a DS system have the same PRN code, they can communicate with each other and the receiver is able to decode the original information out of the wide-band signal by a process of correlation. This process is called processing gain. In addition, any signal not matching the original PRN code is itself spread through the same process reducing the potential for interference. Direct Sequence can provide many users to be on the "same channel" at the same time and be distinguished from each other by a digital code.

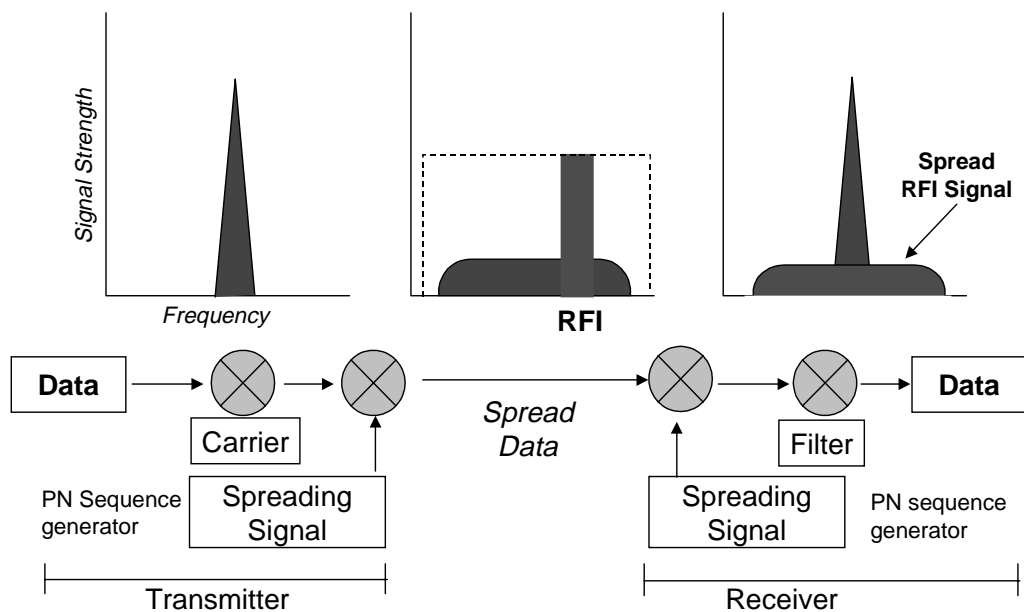


Figure 3: Direct Sequence Spread Spectrum Diagram

The most common problem when applying an unlicensed wireless system in an industrial environment is radio frequency interference (RFI) or better known as “radio noise”. Both FHSS and DSSS handle noise differently and can have certain advantages depending on the type of interference experienced. Broadband noise affects both the FHSS and DSSS similarly, but narrowband interference will have a more severe impact on a FHSS signal than a DSSS signal if it is on the same channel. Most RFI noise in industrial applications is narrow band in nature and not wideband (white noise). As long as the DSSS has a receive signal greater than the combined noise in the channel (signal-to-noise ratio), the DSSS system will completely reject the narrowband interference.

Wireless Ethernet

Wireless technology has now progressed to a point to where Ethernet speeds (10 Mbps or greater) are possible, but not all wireless Ethernet systems are the same. The first Ethernet radios systems on the market used proprietary communication schemes. These proprietary systems were essentially an Ethernet connection on a serial based spread spectrum radio. Although this allowed a standard Ethernet connection to be sent wireless, the throughput of the system was limited to about 115 K bps. In modern data intensive applications and networks this throughput would not be satisfactory. What was needed was a standard for wireless local area networks (WLAN) that could use the latest advancements in radio technology, and provide open protocol standard.

IEEE 802.11 – Wireless Local Area Networks (WLAN)

In 1997 IEEE adopted the first standard for wireless LAN networks, IEEE Std 802.11-1997. This standard was further updated in 1999 to include the IEEE 802.11b extension for DSSS in the 2.4 GHz band, delivering up to 11 Mbps data rates. The overall goal of the IEEE 802.11 standard is that the WLAN would look and feel like any other cabled LAN and replace the physical layer in the Ethernet network.

Of course, there were also a number of differences between wireless & wired LAN networks. The two most important differences were that the physical connection to a building network was replaced with a radio link and this led to the second major difference, mobility. These differences added significant advantages to a WLAN but also had some perceived drawbacks. The data on a network was no longer confined to a cable and there was concern that privacy could be compromised. In addition, the radio link exposed the WLAN to the changes in electromagnetic propagation that could drastically change the signal strength to a station or sever the link entirely. With the added complexity of a mobile computer in the network, these concerns had to be solved. The IEEE 802.11 standard was written to solve all these problems, but before we look at how each of the above concerns was addressed, we need to look at the three main network types to gain a point of reference to the possible network configurations.

Network Types

The first network is the Point-to-Point or Ad Hock Network (Figure 4). This network allows two or more network devices (computers or PLCs) to transfer information directly between devices as long as they are within radio range. This type of network is most efficient with a minimum of networking overhead. Examples of this type of network would be the transfer of data files between two notebook computers not tied to a wired LAN and the direct linking of a computer to an Ethernet compatible PLC for programming or diagnostics. This is the simplest of network types that is usually short lived and created for a specific purpose.

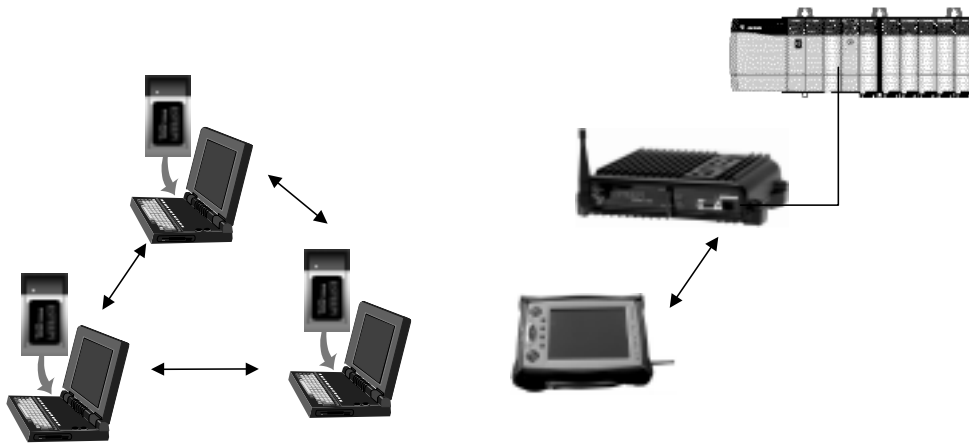


Figure 4: Point-to-Point Network Diagram

The second type of network is the most common WLAN application called the Access Point Network or Infrastructure Mode (Figure 5). In this network one of the Ethernet radio modems is configured as the “Access Point”. This Access Point is then used to bridge wireless network to the cabled LAN network. When configured in this type of network, all nodes (either wireless cards or other Ethernet radio modems configured as remotes) communicate only with the Access Point that serves the WLAN as a HUB. The

Access Point is responsible for maintaining a logical link between the clients, but the clients make the determination, based upon signal strength and data quality, as to what data rate they will use. We will further discuss this scaling of data rates when we look at mobile clients.

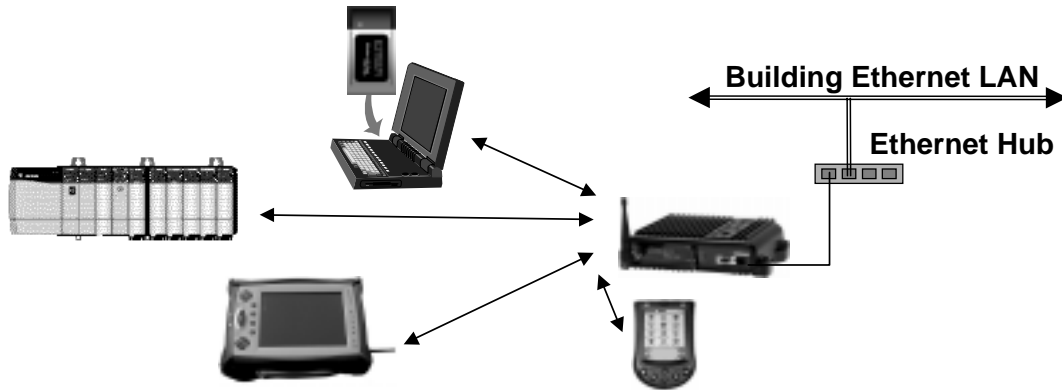


Figure 5: Access Point Network Diagram

The last type of network configuration is the Distribution Network. This is actually just an enhanced feature set of the Access Point Network that allows communication between multiple Access Points. Internal data management of this type of network is very complex and is not provided in all WLAN hardware but provides the user many solutions to difficult network configurations. Data frames must be forwarded to other stations in the network regardless of where they are located. The Access Points can communicate either through a hardwire or wireless connection. This wireless communication between Access Points can extend the range of the WLAN and have the Ethernet radio modem effectively serve as a repeater (Figure 6).

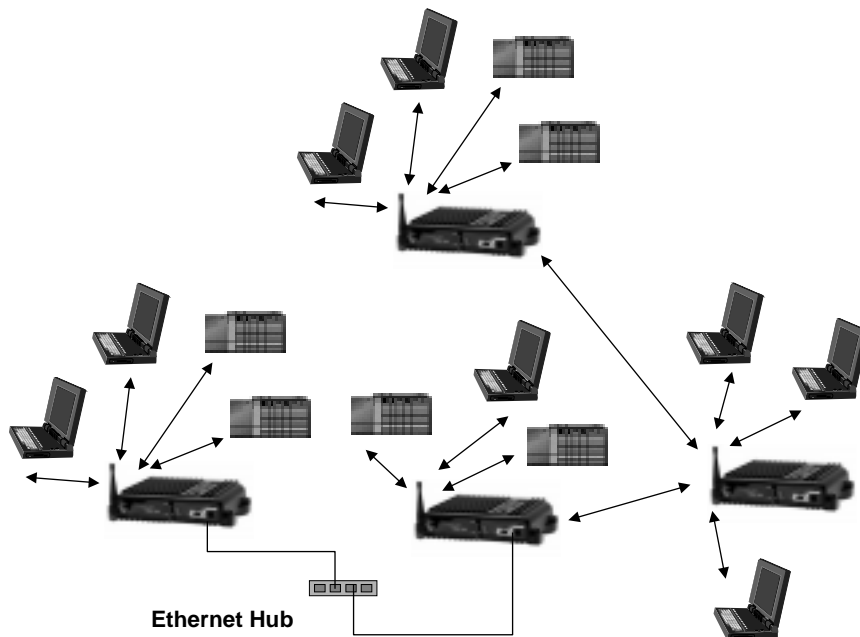


Figure 6: Distribution Network Diagram

Security of Data

The security of the network data IEEE 802.11 WLAN is a concern because it is transferred through the airwaves and being further complicated by being an open standard. A wired LAN network must be physically compromised to gather the data, but a WLAN could be compromised by anyone with a compatible radio system. The IEEE 802.11 Wired Equivalent Privacy (WEP) mechanism provides protection at a level that is felt to be equivalent to that of a wired LAN. WEP is an encryption mechanism that takes the contents of the data frame and passes it through an encryption algorithm of up to 128 bits in length. This result then replaces the frame body of the data frame and is transmitted over the wireless network. Only those stations with a matching WEP code will be able to receive the Ethernet data.

Potential Radio Problems

Any radio system is susceptible to interruption or interference that can cause a problem in reception. We have seen how the direct sequence spread spectrum deals with radio noise in an industrial environment but there is another radio phenomenon that must be addressed when looking at applying wireless systems. Multipathing occurs when waves emitted by the transmitter travel along a different path and interfere destructively with waves traveling on a direct line-of-site path. The phenomenon occurs because waves traveling along different paths may be completely out of phase when they reach the antenna, thereby canceling each other out (Figure 7). Overall spread spectrum systems are fairly robust in the presence of multipath. Since the cancellation is almost never complete, methods for overcoming this problem are higher output power and maintaining a line of site between the antennas. DSSS will reject reflected signals that are significantly delayed relative to the direct path or strongest signal. Line of site indoors or on a plant floor is difficult to maintain so the more sophisticated radio equipment employ an additional component called adaptive channel equalizer that also helps reduce the effects of multipathing. In the adaptive equalizer the signal is received and digitized, it is then fed through a series of adaptive delay stages which are summed together via feedback loops. The net effect of this process is the removal of signals that were delayed or out of sequence in the receiver.

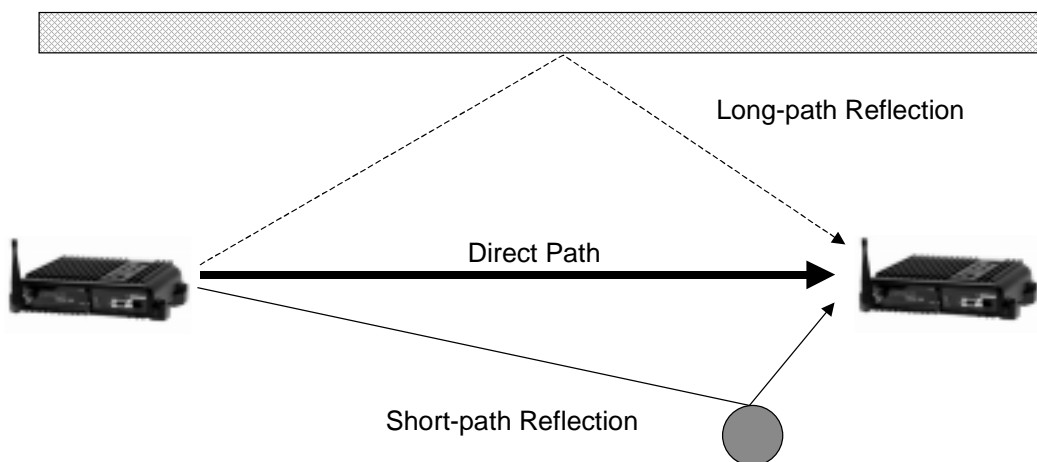


Figure 7: Radio Multi-Path Diagram

Mobility – Network Roaming

The last concern for the WLAN is the mobility of the client. Maintaining a reliable Ethernet link as a computer moves throughout WLAN is a very complex process. The IEEE 802.11 standard compensates for this by a process of association and disassociation from the mobile client as it moves throughout the network. Most of the decision making in the WLAN is distributed to the mobile stations. As the data throughput for the radio begins to scale down due to a loss in signal strength or quality, the mobile device will begin to search for a new Access Point with which to communicate. If a new Access Point is located and has a greater signal strength and data quality, the client will begin the process of disassociating itself from the first Access Point and associating itself with the new Access Point. This process is necessary to effectively locate the client in the network for routing of Ethernet packets.

IEEE 802.11 Uses in Industry

The use of wireless Ethernet equipment in industrial applications is in its infancy. As hardware vendors provide more equipment with an Ethernet interface, the number of solutions will be endless. The following are a few applications where industrial wireless Ethernet equipment can be put to use today:

- **Backbone For Current And Future Ethernet Networks** – Consider not only the needs of your networking requirement for today, but also consider what may be needed in the future. Although your data collection network may not need the 11 Mbps of bandwidth today, the future of data collection, HMI requests and web-based management will only increase in the future.
- **Added Bandwidth For Remote Programming, Web Monitoring Etc.** – Use the additional bandwidth and speed provided with an IEEE 802.11 based network to simplify control system tasks such as on-line programming or web based system monitoring.
- **Implement New Ethernet Projects without Cabling** – The cost and difficulty of running Ethernet cable throughout the factory floor can be replaced by high-speed wireless Ethernet.
- **Replacement Of High-Speed Data Lines** – Data lines to remote locations or facilities can be replaced with Ethernet speed communications with no residual costs.
- **Provide Mobile Access to Maintenance Personnel** – Maintenance or system operators can now move throughout the plant floor and still have access to an Ethernet connection. This will allow maintenance personnel to monitor or program a PLC without removing it from operation or disconnecting from the Ethernet network.

Whether Ethernet is the future for industrial application communication remains to be seen. Providing this type of proven interface is the first step in developing truly open protocol architectures. As Ethernet becomes more popular in control systems, the need for true Ethernet speeds and security will be required in wireless networks. By using wireless Ethernet equipment designed for industry and based on the IEEE 802.11 standard, will again provide the convenience and cost savings that industrial control systems have been gathering out of wireless networks for years.