PUBLIC SAFETY
PSWN PROGRAM
WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Wireless Data Networking Standards Support Report: 802.11 Wireless Networking Standard

Final

October 2002

Table of Contents

1. INTRODUCTION

Wireless local area networks (WLAN) are becoming increasingly common in the private sector, and some public safety agencies are actively using or considering the use of this technology. WLANs provide wireless enabled devices with an always-on, wireless connection to each other, to local area networks (LAN), to wide area networks (WAN), and to the Internet. In addition, WLANs support connections to private intranets and virtual private networks (VPN).[1] A WLAN could facilitate the exchange of information between public safety personnel in and around facilities, between facilities, or potentially throughout a department's service area. The most recently approved standard, 802.11a, can potentially provide data transfer rates as fast as 54 megabits per second (Mbps).[2] As development of the technology progresses, data transfer rates may increase, products could become smaller, more powerful, and pervasive, and security features will likely be more robust. The benefits of WLANs may extend to improved employee timesaving and productivity efficiencies. However, as mobile data technology takes on a larger role in the day-to-day operations of public safety, those personnel charged with technology oversight are becoming increasingly burdened with keeping abreast of wireless technological advancements, implementation and support complexities, standards progression, and security requirements as they impact users.

Although several standards-setting bodies are guiding the standards development process in a variety of technical areas, the Institute of Electrical and Electronics Engineers (IEEE), a non-profit, technical professional association, is leading the development of wireless connectivity standards. Officially titled "IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Networks," this suite of standards, more commonly referred to as 802.11, defines Ethernet WLANs. Specifically, the 802.11 suite of standards defines the "over-the-air interface" between the user's device and the base station or access points (AP) for a WLAN. As the standards development process progresses, additional protocols are introduced or altered to define certain characteristics, such as the physical layer (i.e., equipment) and security. The complete suite of standards is detailed in Section 2 of this report.

1.1 Technology Overview

Prior to the development of the 802.11 standards, all radio frequency (RF) wireless communication was proprietary to specific vendor solutions. The IEEE designated a working group to develop a standard defining specifications for Ethernet WLANs to ensure interoperability among manufacturers' products.

Each of the 802.11 standards identifies technical requirements for wireless devices (e.g., notebook computers, personal digital assistants [PDA]) and APs in a WLAN infrastructure. In order to gain a general understanding 802.11 technology, it is important to understand the components required to form a basic WLAN. Figure 1 illustrates a typical WLAN.

1 A VPN is a private data network that uses the public telecommunication infrastructure, maintaining privacy using a tunneling protocol and security procedures.

[2] The peak data rate of 54 Mbps is based on the specifications of the IEEE standard for 802.11a.

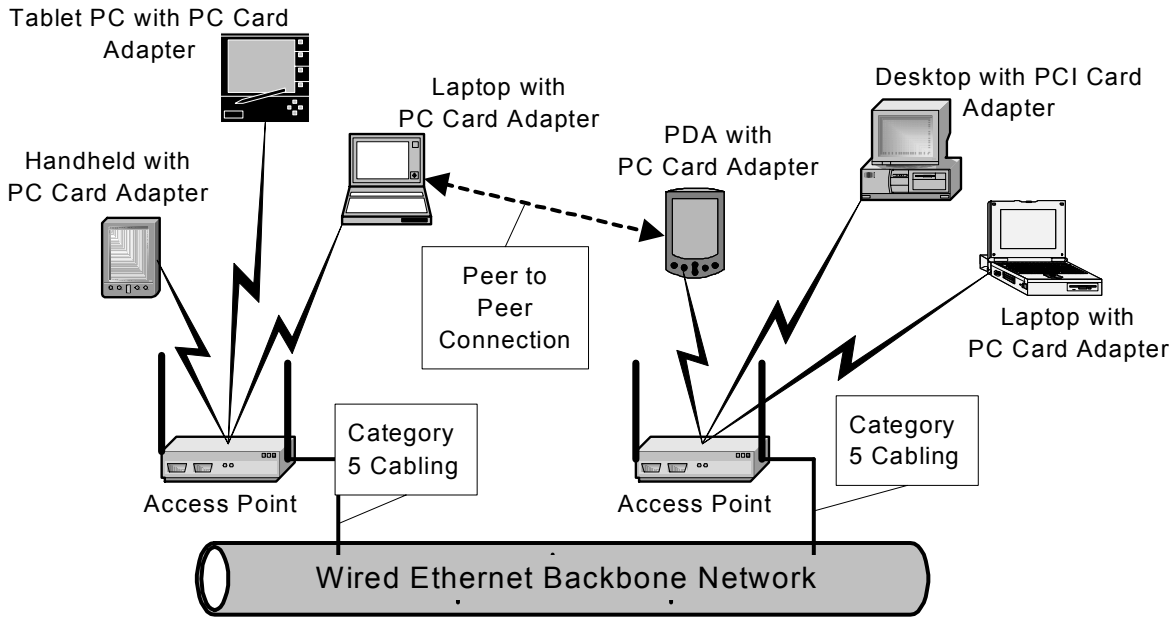

Figure 1
Typical WLAN

Typically, WLANs use the following equipment for wireless connectivity—

- **Compatible Devices—**802.11 compatible devices include desktop and laptop personal computers (PC), and handheld devices (e.g., PDA), scanners, digital cameras, or other wireless devices that incorporate WLAN components.

- **WLAN Client Adapter Card—**The WLAN client adapter is a peripheral component used in personal computer systems and other compatible devices to provide a connection to a WLAN. The WLAN client adapter may be designed as a credit card sized peripheral supporting the Personal Computer Memory Card International Association (PCMCIA) standard, also known as the CardBus or PC Card. PCMCIA cards can provide additional capabilities to the supporting device, including memory, modems for dialup connections, connection points for wired LANs, or connection points for WLANs. WLAN client adapters are also available in other forms supporting other PC connection standards such as personal computer interconnect (PCI) cards, universal serial bus (USB) connections, and Compact Flash cards. Regardless of the form, the WLAN client adapter incorporates the radio transmitter, receiver, amplifiers, and antennas. Figure 2 illustrates PCMCIA and PCI client adapters.

Source: Belkin Components

Figure 2
WLAN Client Adapters

- **Access Points—**The AP provides wireless connectivity to the wired network. Similar to a WLAN card, the AP incorporates the radio transmitter, receiver, amplifiers, and antennas. If an AP is to be installed outdoors, remote antennas, connected to the AP by cabling, can be used. Typically, in an outdoor installation, antennas are positioned on the sides of buildings and rooftops to maximize the AP's coverage area. Indoor installations generally use the APs attached antenna(s) with the AP typically mounted on walls or ceilings of rooms and in hallways. The only requirement when using an AP's integrated antenna is that the AP must be mounted so the antenna is oriented vertically.

Source: Belkin Components

Figure 3
WLAN AP

- **Category 5 Ethernet cabling—**In a WLAN, Category 5 (CAT 5) cabling is used to connect the individual APs to a hub, switch, or WLAN server of the wired network. CAT 5 is one of several standards developed by the American National Standards Institute/Electronic Industries Association that define the data rates that twisted pair

cabling systems can sustain. The specifications describe the cable material, types of connectors, junction blocks, and installation practices necessary to conform to the specification.

In addition to the equipment listed above, which is needed to operate a WLAN, the following equipment may be used in an enterprise network system—

- **Wireless Network Management Tools—**Several vendors have developed WLAN network management tools that provide centralized configuration management to effectively manage a large number of APs and wireless bridges. Network management tools can also be used to monitor and enhance vendor proprietary security capabilities by detecting misconfigurations on APs and other network elements. Network management tools provide the ability to perform proactive monitoring, troubleshooting, and notification of performance degradation, and to expand capabilities to improve capacity planning.

- **Power Supply—**A power supply is necessary to support the over-the-air interface for a group of APs. When the 802.11 wireless technology is used in an enterprise system, it is convenient to use a power supply to minimize the amount of cabling into the wired network. In this instance, only the power supply would be connected directly to the hub.

- **WLAN Bridge—**A bridge can potentially extend the range of a WLAN from a few hundred feet up to several miles. As the name implies, a bridge passes wireless packets over distances to be retransmitted. Bridges can be used singly or with multiple corresponding bridges. With the use of specialized antennas, the overall coverage area could be extended to 5 to 6 miles or more. Bridge connections are primarily used as alternatives to leased, wireline data circuits, thus eliminating monthly charges by the telephone carrier. The use of WLAN bridges is an attractive alternative because the data rates that can be achieved across a WLAN bridge are potentially greater than that of a leased line. For example, an 802.11b compliant AP can typically have a 3–5.5 Mbps data rate, whereas a leased T-1 class data circuit typically provides 1.54Mbps throughput. One disadvantage is that WLAN bridges require a line-of-sight path to operate; leased T-1 lines do not.

- **VPN Technology—**In a WLAN configuration, VPNs are used to provide additional security for information traveling across the WLAN network and into the enterprise network. This security measure is often used as an overlay in addition to the Wired Equivalent Privacy (WEP) already found in most 802.11 compliant equipment. A VPN is used to authenticate a user with a specific network. Once the VPN authenticates the user as a valid user, the VPN software encrypts data locally on the user device before sending it through the wireless network. At the receiving end, decryption is performed by the user device. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. A variety of companies have developed the Point-to-Point Tunneling Protocol, which

is a set of communication rules that allows users, primarily corporations, to extend their own networks through private "tunnels" over the public Internet or wireless infrastructures. VPN software is typically installed as part of an enhanced network security strategy.

1.2 Report Organization

In addition to this introduction, this report contains the following sections:

- **Section 2, 802.11 Established Standards**—details each of the four established standards included within the 802.11 suite and compares them to one another; also provides short descriptions of each of the additional standards being considered for inclusion in the suite.

- **Section 3, Equipment—**describes currently available 802.11 compliant equipment and discusses the interoperability of this equipment.

- **Section 4, Security**—discusses the security features and vulnerabilities of 802.11 compliant networks.

- **Section 5, Public Safety Considerations—**discusses the advantages and disadvantages of using 802.11 compliant networks and describes some current uses of 802.11 technologies in public safety projects.

- **Section 6, Future Impact—**summarizes the expected impact of 802.11 technologies.

2. 802.11 ESTABLISHED STANDARDS

The 802.11 suite has the four established standards with the 802.11 suite—802.11, 802.11a, 802.11b, and 802.11g—and the IEEE is continuing to work on new standards that will eliminate or mitigate the shortcomings of the existing standards. Additional standards are still under development that will extend the physical layer options, improve security, and add quality of service (QoS)[3] features. Among the IEEE 802.11 suite of standards used to define wireless Ethernet, similarities exist between the four established standards. Despite the apparent similarities evident among these four standards, each has unique characteristics, as described in the follow sections.

2.1 802.11

Introduced in July 1997, 802.11 was the first IEEE standard used for wireless data networking applications with maximum data transfer rates at 2 Mbps in the 2.4 gigahertz (GHz) radio band. Note that, as the distance between the user and the AP increases, data rates decrease. Within 802.11, two different modulation schemes are supported that can be used to transmit data signals.

One of the two modulation schemes used in 802.11 is frequency-hopping spread spectrum (FHSS). This transmission technique is used in WLAN transmissions where the data signal is modulated with a narrowband carrier signal that "hops" in a random sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces the chances of interference because another interfering signal will only affect the 802.11 signal if both are transmitting at the same frequency at the same time.

The other modulation scheme used in 802.11 is direct-sequence spread spectrum (DSSS), which is a transmission technique in which a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code, a redundant bit pattern for each bit that is transmitted, increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

Although the 802.11 standard supports both modulation schemes, the two types of spread spectrum technologies are not compatible. The number of channels used by 802.11 compliant products depends on the modulation scheme used. More specifically, FHSS-based products use 79 channels of the Unlicensed National Information Infrastructure (UNII) band, whereas DSSS-based products use either 3 non-overlapping channels or 6 overlapping channels of the Industrial, Scientific, and Medical (ISM) radio band. Some of the common characteristics specified by the 802.11 standard are listed in Table 1.

[3] QoS is a networking term that specifies a guaranteed throughput level.

Table 1
Characteristics Specified by the 802.11 Standard

Characteristic	802.11 Description
Application	Wireless data networking
Data Rate (Mbps)	1–2
Typical Operating Frequency Band	ISM band: 2.4 to 2.4835 GHz.
Reliability	FHSS or DSSS, CRC-16 in header
Coverage (m)	40 to 400
Mobility	Roaming between APs by mobile Internet Protocol (IP) devices
Security	128-bit WEP
Link Layer	Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) with request to send (RTS/clear to send (CTS)[4]

2.2 802.11a

802.11a, a physical layer standard for WLANs, was completed in September 1999. 802.11a specifies characteristics for high-speed broadband WLAN access. The standard can also be applied to wireless asynchronous transfer mode (ATM)[5] systems and is used in access hubs. It is offered in the 5 GHz radio (UNII) band, and operates on 8 channels; however, the available radio spectrum in some countries permits the use of 12 channels. The additional number of channels used in the higher spectrum yields less interference from neighboring APs. The Federal Communications Commission (FCC) has divided the total of 300 megahertz (MHz) frequencies used by 802.11a WLANs into 3 distinct 100 MHz domains, each with a different legal maximum power output. The "low" band operates in the 5.15–5.25 GHz range and has a maximum output power of 50 milliwatts (mW). The "middle" band is located in the 5.25–5.35 GHz range, with a maximum of 250 mW. The "high" band uses the 5.725–5.825 GHz range, with a maximum of 1 Watt. Because of the high power output, most devices transmitting in the high band are building-to-building bridge products. The low and medium bands are more suited to in-building wireless products.

Until recently, operating in the 5 GHz spectrum band was either limited or illegal in several European countries. Different regions of the world have allocated different amounts of spectrum, so geographic location determines how much of the 5 GHz band is available. In the

[4] CSMA/CA is a basic protocol used to avoid signal collision and canceling. It works by requesting authorization to transmit for a specific amount of time prior to sending information. The sending device broadcasts an RTS frame with information on the length of its signal. If the receiving device permits it at that moment, it broadcasts a CTS frame. Once the CTS is transmitted, the sending machine transmits its information. Any other sending devices in the area that "hear" the CTS realize another device will be transmitting and allow that signal to go out uncontested.

[5] ATM is a dedicated connection switching technology that organizes digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. Individually, a cell is processed asynchronously relative to other related cells and is queued before being multiplexed over the transmission path. ATM is designed to be implemented through by hardware instead of software and provides faster processing, and switch speeds. Speeds on ATM networks can reach 10 gigabits per second. ATM is a key component of broadband Integrated Services Digital Network and Synchronous Optical Network.

United States, the FCC has allocated all three bands for unlicensed transmissions. In Europe, only the low and middle bands are available for use. Although the 802.11a standard is not yet ratified in Europe, efforts are currently under way by the IEEE and the European Telecommunications Standards Institute (ETSI) to rectify this situation. In Japan, only the low band can be used.

Several countries, including France and Ireland, allow the delivery and use of 802.11a compliant products, and other countries have placed their own regulations on using 802.11a products. For example, the Australian Communications Authority (ACA) has restricted the amount of power available to 802.11a compliant APs to a one-quarter of that for 802.11b APs, thus limiting the range of the APs. Additionally, the ACA has limited the outdoor use of 802.11a compliant products to only a portion of the 5 GHz spectrum. These developments may eventually lead to the acceptance of 802.11a compliant products in all of Europe and Asia.

802.11a compliant networks transfer data at rates of up to 54 Mbps in the available radio spectrum, which is up to five times faster than 802.11b compliant networks. More commonly, however, 802.11a compliant networks communications are at the 6 Mbps, 12 Mbps, or 24 Mbps data rates. Again, as the distance between the user and the AP increases, the data rate decreases. Home networking users may find the increased bandwidth of 802.11a compliant networks useful when using applications requiring large bandwidth, such as for streaming video, music, and large file transfers.

802.11a compliant networks use orthogonal frequency division multiplexing (OFDM) modulation to provide these data rates. OFDM is a type of digital modulation in which a signal is divided into separate channels at different frequencies. The 802.11a was the first in the suite of 802.11 standards originally proposed to the IEEE, but due to the complexity of the implementing OFDM, the 802.11b standard was approved first. Some of the common characteristics specified by the 802.11a standard are shown in Table 2.

Table 2
Characteristics Specified by the 802.11a Standard

Characteristic	802.11a Description
Application	Wireless Local Area Networking
Data Rate (Mbps)	6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Rates of 6, 12, and 24 Mbps are mandatory for all products.
Typical Operating Frequency Band	UNII band: 5.15-5.25 GHz, 5.25-5.35 GHz, and 5.725-5.825 GHz
Reliability	OFDM for modulating data before transmission. Forward error correction compensates for an errored packet without retransmission.
Coverage (m)	≤ 100
Mobility	Roaming between APs by mobile IP devices
Security	128-bit WEP, 64-bit WEP, 152-bit WEP
Link Layer	CSMA/CA with RTS/CTS

802.11a compliant networks are best suited for the following conditions—

- Higher performance requirements involving, but not limited to, the transmission of video, voice, and large data files

- Situations where significant RF interference is present within 2.4 GHz band (devices include 2.4 GHz cordless telephones, Bluetooth products, and microwave ovens)

- Use in a dense population of end users (e.g., computer laboratories, libraries, and airports).

Specific limitations associated with 802.11a compliant networks include path loss within the 5 GHz radio band and the shorter range (i.e., 50 meters compared with 802.11b networks' 100 meters). This short range requires the implementation of more APs to cover the same area as an 802.11b network. Additionally, 802.11a compliant products consume more power than those that comply with the other standards and do not interoperate with 802.11b products.

2.3 802.11b

802.11b, the second physical layer standard for WLANs, was completed in September 1999. Currently, a wide range of products is available to the public in North America, Europe, and Asia. Unlike users of 802.11a compliant products, who are encountering problems using the 5 GHz spectrum band in Europe, users of 802.11b compliant products have the support of global networking component manufacturers. The 802.11b standard specifies operation on three channels in the 2.4–2.4835 GHz spectrum and offers wireless throughput of up to 11 Mbps per channel. The maximum throughput is generally less than 11 Mbps due to the shared bandwidth split between users of a particular AP. As is common with WLANs, the data rates tend to decrease as the distance between the user device and the AP increases. Generally, 802.11b compliant products have a range of approximately 100 meters, but can realize a much greater range of coverage under optimal conditions where interference is limited.

The 802.11b compliant chipsets use the modulation scheme known as complementary code keying (CCK), a form of DSSS, to transmit data signals through the three available channels. This unlicensed portion of the radio band shares space with many low-power signals from home electronics, including microwave ovens, cordless telephones, Bluetooth-enabled devices, and garage-door openers. 802.11b compliant products have a range of up to 400 meters in ideal conditions and will be compatible with the products that meet the new 802.11g standard when it is finalized. Some of the key characteristics specified by the 802.11b standard are shown in Table 3.

Table 3
Characteristics Specified by the 802.11b Standard

Characteristics	802.11b Description
Application	Wireless data networking
Data Rate (Mbps)	1, 2, 5.5, 11
Typical Operating Frequency Band	ISM band: 2.4 to 2.4835 GHz
Reliability	DSSS and Alternative Regulatory Framework (ARF)
Coverage (m)	40 to 400
Mobility	Roaming between APs by mobile IP devices
Security	128 bit WEP
Link Layer	CSMA/CA with RTS/CTS

802.11b compliant networks are best suited for the following conditions—

- Significant range requirements
- Existing investment in 802.11b compliant devices
- Sparse end user population.

Speed and channel restriction are significant limitations of 802.11b compliant networks. Interference within one's own 802.11b network becomes more likely as the number of users and APs increase. Similarly, interference is more likely as 802.11b compliant networks are deployed near each other. In addition, because products that comply with this standard are restricted to three available channels, a limited amount of bandwidth is available. 802.11b products share the bandwidth with other low-power signals, and thus, problems may arise when the technology is used near some electronic devices such as microwave ovens, Bluetooth-enabled devices, and cordless telephones.

2.4 802.11g

IEEE formed Task Group G to develop a new standard, 802.11g, offering wireless communication over relatively short distances at up to 54 Mbps. This standard features increased data transmission rates while maintaining interoperability with 802.11b compliant products. The standard uses OFDM to achieve data rates from 22 Mbps to up to 54 Mbps (i.e., doubling the data rates of 802.11b compliant products); however, 802.11g compliant products will be backward compatible with 802.11b compliant products that use the modulation scheme CCK (i.e., a form of DSSS). The backward compatibility feature allows an 802.11b compliant client adapter card to interact directly with an 802.11g compliant AP. Communications between 802.11g and 802.11b compliant devices are limited to data rates up to 11 Mbps, depending on the range between the pieces of equipment.

802.11g compliant products also support packet binary convolution coding (PBCC) modulation, an option that provides faster data rates. This use of different modulation schemes makes it possible for 802.11g compliant products to be compatible with existing 802.11b compliant products. 802.11g compliant products use three channels in the 2.4 GHz spectrum. The common characteristics specified by the 802.11g standard are shown in Table 4.

Table 4
Characteristics Specified by the 802.11g Standard

Characteristics	802.11g Characteristics
Application	Broadband Wireless LAN Access
Data Rate (Mbps)	6, 9, 12, 18, 24, 36, 48, 54
Typical Operating Frequency Band (GHz)	ISM band: 2.4 to 2.4835 GHz
Reliability	OFDM with ARF and CRC-32
Coverage (m)	20 to 100
Mobility	Roaming between APs by mobile IP devices
Security	128 bit WEP
Link Layer	CSMA/CA with RTS/CTS

802.11g compliant networks are best suited for following conditions—

- Need for higher data rates and compatibility with other 802.11 technologies (using OFDM, CCK, and PBCC modulation schemes)
- Requirement for data transfer rates up to 54 Mbps
- Update of networks with existing investments in 802.11b products.

When comparing the 802.11g standard to the other standards within the suite, certain details are important. Since 802.11g compliant products operate in the 2.4 GHz range, there is less path loss than with 802.11a products, which operate in the 5 GHz range. As the frequency increases, the wavelength of the transmitted wave decreases, which in turn, causes more path loss. In other words, as the frequency increases, higher attenuation by walls, furniture, etc. may alter the transmitted wave. Due to the increased speed associated with 802.11g compliant products, it is possible to run applications that require high bandwidth such as multichannel DVD-quality video and CD-quality audio over the WLAN.

On the other hand, use of 802.11g compliant products also has limitations. Because 802.11g products run on three non-overlapping channels—similar to 802.11b products—there might be difficulty in obtaining bandwidth on each of the individual channels, especially when covering a large area with a large number of users. A possible solution is lowering the power on individual APs, thus allowing placement of more APs closer together. Another limitation that 802.11g compliant products share with 802.11b products is the interference experienced by users due to other low-power signals in the 2.4 GHz range. The 802.11g standard is expected to be finalized in January 2003.

Table 5 provides a comparison of the primary 802.11 standards.

Table 5
Comparison of Characteristics Specified within the IEEE 802.11 Suite

Characteristics	802.11	802.11a	802.11b	802.11g
Application	Wireless data networking	Broadband LAN Access	Wireless data networking	Broadband LAN Access
Spectrum Band	ISM: 2.4 to 2.4835 GHz	UNII: 5.15-5.25 GHz, 5.25-5.35 GHz, and 5.725-5.825 GHz	ISM: 2.4 to 2.4835 GHz	ISM: 2.4 to 2.4835 GHz
Modulation Scheme	FHSS or DSSS	OFDM	DSSS	OFDM or DSSS
Number of Channels	79 channels with FHSS; 3 or 6 channels with DSSS	12	3	3
Optimum Data Rates (Mbps)	2	54	11	54
Range (meters)	100	50	100	100
Date established (Market Ready?)	July 1997	September 1999	September 1999	January 2002—draft specification; finalize in January 2003
Compatibility	802.11 only	802.11a	802.11g	802.11b
Operability	North America, Europe, Asia	North America, Europe, Asia	North America, Europe, Asia	North America, Europe, Asia

2.5 Pending Specifications Within the 802.11 Suite

As the standards process moves forward, changes are being made to the 802.11 suite of standards that have yet to be recognized as IEEE standards. In addition, IEEE working groups are reviewing additional specifications that have not been approved as standards. These additional specifications may become amendments to existing standards to correct or add features or functions. When considering 802.11 and its associated applications for WLANs, it is important to be aware of the following developing specifications—

- **802.11c**—This specification focused on bridge operations among WLANs; however, the effort resulted in the 802.1 standard.

- **802.11d**—This specification is intended to promote worldwide use of 802.11 WLANs. 802.11d will define requirements that will facilitate development of WLAN that permit APs and client adapters to communicate information on the 2.4 GHz radio channels in countries not currently using 802.11 technologies. More specifically, it will define requirements, such as channelization and hopping patterns, for these new markets. Because the 802.11 compliant products currently cannot be legally operated in some countries, the purpose of this specification effort is to add features and restrictions to allow WLANs to function within the rules of these countries. Most countries have now released the 2.4 GHz band after International Telecommunication Union recommendations and lobbying by equipment manufacturers. Spain remains the only country that has not accepted WLAN operations in the 2.4 GHz band.

- **802.11e**—This specification is intended to provide QoS standards for data, voice, and video applications for WLANs. The specification will be applied to update the physical layer standards 802.11a, b, and g. It will replace the Ethernet Media Access Control MAC[6] layer with a coordinated time division multiple access (TDMA)[7] scheme and may add extra error correction. The standard has not gained final approval due to disagreements regarding the number of classes of service to be included. IEEE estimates that final approval will be in January 2003.

- **802.11f**—This specification focuses on the Inter-Access Point Protocol, which ensures multivendor AP interoperability. Presently, users roaming between APs may experience a loss of some data packets, especially when moving between APs manufactured by different vendors. When finalized, 802.11f should set forth specifications so that users can maintain a connection while roaming between two switched segments (i.e., radio channels) or between APs that are attached to two different networks. It is anticipated that 802.11f will be finalized by March 2003.

- **802.11h**—This specification will specify Dynamic Channel Selection and Transmit Power Control mechanisms for 802.11a compliant equipment. In conjunction with 802.11e, it should provide compliance with European regulations for 5 GHz WLANs. Current European radio regulations for the 5 GHz band require all products to have transmission power control and dynamic frequency selection. The completion of this 802.11h will permit manufacturers to produce equipment that is compliant with radio standards of European countries.

- **802.11i**—This specification is intended to improve security capabilities of 802.11 compliant equipment and mitigate deficiencies of WEP, discussed in Section 4 of this report. Specifically, 802.11i focuses on several security enhancements, collectively known as Temporal Key Integrity Protocol (TKIP), to temporarily support WEP. The security enhancements include an authentication protocol, key-hashing function, combined with a real message integrity check (i.e., to avert forgery) and dynamic key management (i.e., rekeying). The new standard will specify the Advanced Encryption Standard (AES)[8]. The 802.11i working group is currently verifying TKIP's backward compatibility with WEP. The specification will be applied to the physical layer standards of 802.11a, b, and g. The standard is expected to be approved in September 2003.

---

[6] MAC layer is responsible for moving data packets across a shared channel, utilizing protocols that improve communications. Specifically, with 802.11, the MAC layer manages and maintains communications between 802.11 stations (radio network cards and access points), using an 802.11 Physical (PHY) Layer, such as 802.11a or 802.11b, to transmit and receive 802.11 frames.

[7] TDMA is a commonly used technology in digital cellular telephone communication that divides each cellular channel into three time slots to increase the amount of data that can be carried through the network.

[8] AESis a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S Government has adopted the algorithm as the new standard encryption technique, replacing the Data Encryption Standard (DES). AES works at multiple network layers simultaneously.

- **802.11j**—This is a relatively new standards project that will focus on the co-existence of 802.11a compliant WLANs and high-performance radio local area network (HiperLAN)[9] standard compliant wireless networks that exist in European countries.

Although these specifications have yet to become recognized IEEE standards, they provide a good estimate of the footprint for emerging WLAN connectivity, and despite the differences among the specifications for the 802.11 standard suite, future compliant equipment may be able to support the entire suite of standards.

[9] HiperLAN, a set of communication standards developed by ETSI, is used chiefly in European countries. HiperLAN is similar to the 802.11 WLAN standards used in the United States.

3. EQUIPMENT

Hundreds of different WLAN products are available that adhere to the 802.11 suite of standards. Of the four established standards in the 802.11 suite (i.e., 802.11, 802.11 a, 802.11b, and 802.11g), 802.11b compliant equipment are the most readily available and most popular WLAN products in use today. There are numerous WLAN equipment vendors. Many of these vendors manufacture 801.11b compliant equipment, and most have declared or initiated production of high-speed WLANs based on the 802.11a standard. The first 802.11a compliant products were shipped in early 2002 and more are expected to be available toward the end of the year. 802.11 compliant equipment is less readily available and usually does not fit user requirements for data throughput, so is not discussed in this section. As of the date of this report, 802.11g products were not available for wide-scale commercial consumption, and therefore, are not discussed in this section. This section describes only currently available 802.11 compliant user equipment and APs.

3.1 User Equipment

WLANs are inherently flexible, providing convenience and a reduced dependence on costly network cabling. In WLAN environments, users are equipped with a WLAN capable device—usually a PDA, or a PC with a PC card or USB interface. A PC card uses a 16-bit/32-bit interface and fits into a standard PCMCIA slot on laptops, notebooks, palmtops, tablets, and other portable computer systems or devices. PC cards are fast enough for 802.11a and 802.11b compliant networking and work in virtually all mobile devices that have PCMCIA slots. For some desktop applications, the WLAN user equipment can be connected to the PC via a USB interface.

Installation is as simple as inserting the PC card into devices with compatible PC card slots or plugging in the USB cable, and installing the driver software. Once the wireless network is established, the WLAN device interfaces with the AP, allowing wireless communication.

Additionally, manufacturers have begun to integrate 802.11 compliant components within notebook computers, PDAs, and other devices to support WLAN connections. These integrated components would eliminate the need to use a WLAN PC card, thus freeing up a PC card slot for use by another PC card component.

Because USB WLAN devices are targeted more for desktop PC applications, and this report is more specifically focused on mobile applications, only 802.11 compliant devices for mobile computing (e.g., laptops PCs and PDAs) were investigated for inclusion in Table 6. Table 6 provides a list of 802.11a and 802.11b compliant PC cards along with their cost.

Table 6

Manufacturers of WLAN PC Cards

Manufacturer	PC Card	Price Range ($)
3Com	11 Mbps WLAN PC Card	82.00–149.00
Agere Systems	Orinoco Gold or Silver 11mb Wireless PC card	59.99–69.99
Cisco	**Cisco Aironet PCM352	115.00
Compaq	Compaq WL110-Wireless PC card	99.00
Enterasys	High-Rate PC Card	75.00–149.00
Intel	*Intel Pro/Wireless 5000 LAN CardBus	179.00
Nokia	Nokia C111 Wireless LAN Card	99.00–199.00
Proxim	*Proxim CardBus Card	150.00–200.00

*Manufacturer has both 802.11b and 802.11a compliant equipment available.
**Manufacturer has ruggedized WLAN equipment.

3.2 Access Points

The AP is the primary wireless network infrastructure device. An AP contains the radio receiver and transmitter that link the WLAN to the wired Ethernet network. The APs and wireless client adapters must incorporate equipment that is compliant with the same wireless standard in order to operate. For example, 802.11a compliant APs communicate only with 802.11a clients, and 802.11b compliant APs or gateways communicate only with 802.11b clients.

Installation of the AP in a basic network is very simple. For example, one can easily plug the device into the network and configure it with the accompanying installation disk. In a typical commercial WLAN configuration, the AP connects to a fixed wired network through a network hub or switch using CAT 5 cabling and acts as a conduit for transmitting data between the WLAN and the wired network.

Because the WLAN is connected to a fixed network, purchasing additional servers is not usually required. However, some implementations, in more complex networks, may actually incorporate a WLAN server solely dedicated to supporting WLAN APs and wireless users. Many APs allow for the retrieval of an IP address from an existing Dynamic Host Configuration Protocol (DHCP)[10] server; therefore, no special implementation is required to communicate with the traditional wire-based LAN. In addition, APs may also provide transparent bridging and seamless roaming capabilities from one AP's coverage area to another, thereby providing full user mobility.

Several equipment manufacturers are contemplating production of APs that will support both 802.11b and 802.11a standards to improve interoperability between existing and newly deployed products. The chipset manufacturers that produce the actual radios that are used in the APs and client adapter cards are also indicating support for dual mode (i.e., 802.11a *and* b) components, as well as new products that will support the 802.11g standard. Equipment

[10] DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also will support a mix of static and dynamic IP addresses.

characteristics for the products of several of the major manufacturers' WLAN APs are shown in Table 7.

Table 7
Manufacturers of WLAN APs

Manufacturer	Access Point	Price ($)
3Com	3Com 11Mbps WLAN Access Point 6000	599.00
Agere Systems	Orinoco AP-500 Access Point	349.99
Cisco	**Cisco Aironet 340 and 350	515.00–909.00
Compaq	Compaq WL510 Wireless Enterprise Access Point	749.00
Enterasys	RoamAbout Access Point	300.00–600.00
Intel	*Intel Pro/Wireless 5000 LAN Dual Access Point (802.11b and 802.11a capable)	649.00
Nokia	Nokia A032 WLAN Access Point	500.00–1000.00
Linksys	*WAP11 (802.11b) WAP54A (802.11a) Wireless Access Points	225.00–500.00
Proxim	*Harmony and Skyline Access Points	600.00–1000.00

*Manufacturer has both 802.11b and 802.11a equipment available.
**Manufacturer has ruggedized WLAN equipment.

3.3 Interoperability of 802.11 Compliant Equipment

Although 802.11a compliant equipment is becoming more readily available, 802.11b, often referred to as "Wi-Fi," is the more widely recognized physical layer standard. The term Wi-Fi originated with Wireless Ethernet Compatibility Alliance (WECA), an organization influencing the development and application of 802.11 compliant products. The WECA mission is to "certify interoperability of Wi-Fi (IEEE 802.11b) products and to promote Wi-Fi as the global WLAN standard across all market segments." This organization grants interoperability certification to products based on conformance and testing. As a result, products bearing the Wi-Fi symbol should be interoperable.

4. SECURITY

For any network, whether it is wireline or wireless, security of the network components and the data traversing the network are key considerations. Often, especially in the corporate environment, users transmit private or sensitive materials over company data networks. In a wired network, physical security can be controlled, preventing unauthorized users from physically connecting to the wires of the network and thus preventing data from being viewed by unintended users.

As technology advances and wired networks expand, more and more networks use wireless APs and mobile terminals (MT) to give users mobility and flexibility. For the purposes of this section, MTs are considered to be any WLAN compliant user devices including, but not limited to, laptop PCs with PC cards and PDAs.

Recently, WLAN security limitations have received attention in technology publications and many other mainstream media outlets. Currently in development, 802.11i, a new specification within the 802.11 suite, will specify a set of security features that will overcome many of the security limitations of currently available WLAN equipment. This section will discuss the most prevalent security limitations of current WLAN equipment and discuss strategies that may help mitigate these security limitations.

The wireless medium, by its very nature, cannot be readily or easily contained or secured. Physical security is not as simple as preventing unauthorized users from attaching to a physical wire of the network. In the wireless environment, any user within an AP's coverage area can "see" the network. This fact makes security critical, especially in instances where private or sensitive information is being transferred.

The 802.11a and 802.11b standards specify Wired Equivalent Privacy (WEP), also known as Shared Key Authentication, as a security measure. WEP was developed to protect the wireless network from casual browsing by unauthorized users. It simulates physical security by denying access to the wireless network if the client is not authenticated as an authorized user. WEP is an option in 802.11 standards that provides confidentiality and integrity for wireless traffic. It uses the RC4[11] algorithm based on a 40-bit "pre-shared" secret key and a 24-bit Initialization Vector (IV). An Integrity Check Value (ICV) is included in every packet to ensure data integrity. When WEP is used, the IV is sent between the AP and MT unencrypted, and the data and ICV are sent encrypted. Figure 4 illustrates the general encapsulation and encryption of the data using WEP.

[11] RC4 is a standard encryption algorithm from RSA Security Inc., and is used in a number of applications, but most specifically in the WEP encryption scheme used with 802.11 compliant WLAN systems.

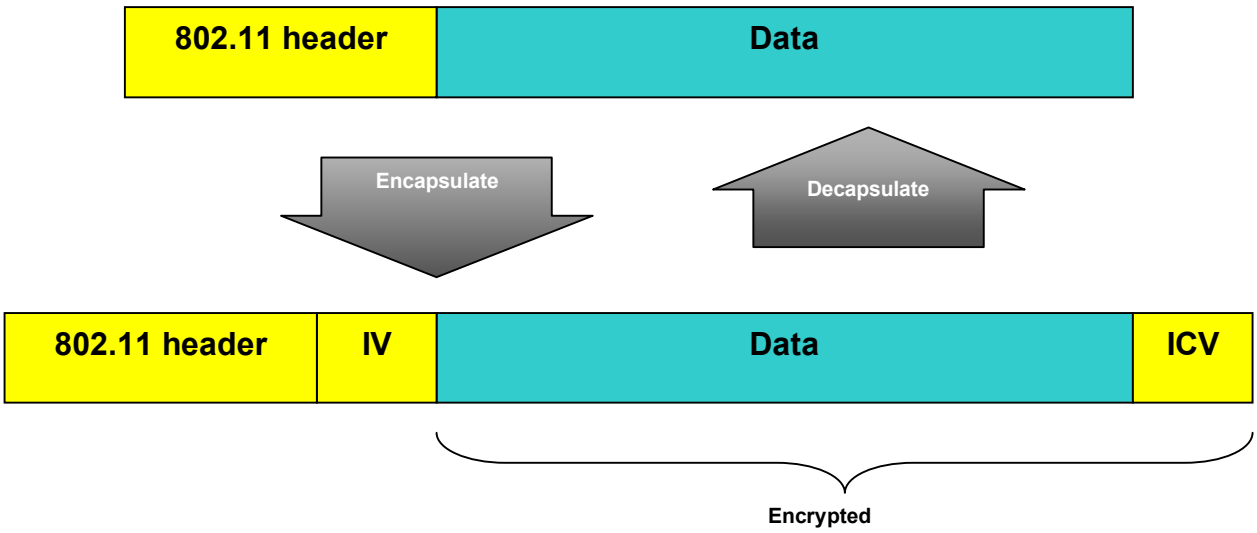

Figure 4
Data Encapsulation Using WEP

If WEP is not employed, the only other security measure available to 802.11 compliant networks is Open Systems Authentication (OSA). OSA is essentially no authentication (i.e., no security). In this mode, the AP grants access to any MT requesting access to the network without performing any authentication procedures to verify the identity of the MT.

4.1 How WEP Authentication Works

With WEP, the AP uses a "pre-shared" key-based challenge-response system to authenticate the MT. Figure 5 illustrates the process. In WEP, the AP sends a random number to the MT when it receives an access request from the MT (Step 1 in Figure 5). At this point, the AP is "challenging" the MT. Upon receiving this random number, the MT signs this random number using the secret key (known by both AP and MT) and responds to the challenge sent by the AP (Step 2 in Figure 5). The AP then verifies that the random number has been signed by the correct key. After the AP verifies that the response was signed with the correct shared key, it authenticates the MT (Step 3 in Figure 5). After the AP grants access to the MT, data packets exchanged between the AP and the MT are encrypted and signed using WEP.

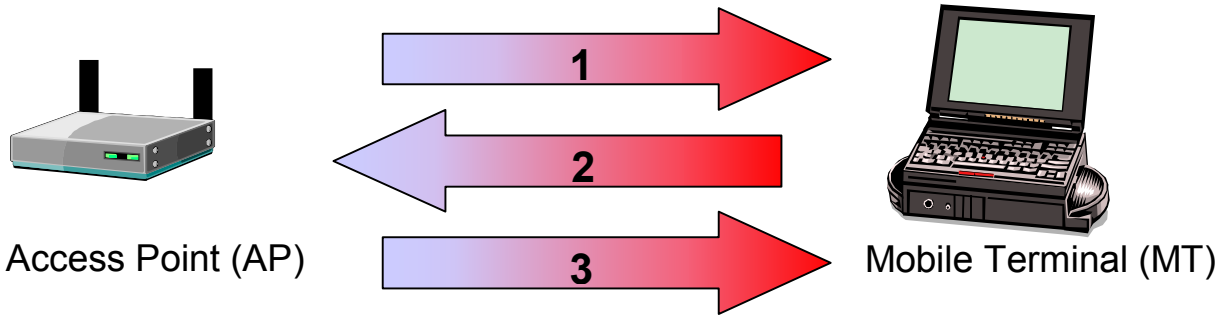

Figure 5
WEP Authentication

4.2 Known Security Vulnerabilities Affecting 802.11 Compliant Networks

As previously stated, WEP is intended to provide access control only. With the proper tools and time, WEP can be broken, and all privacy of the network can be lost. Although a host of other techniques can be used to physically compromise the integrity of a wireless network (e.g., signal jamming), this section focuses on some of the known non-physical security vulnerabilities in 802.11 compliant networks. With each of these known vulnerabilities, different security protocols are introduced that may be used to mitigate the particular vulnerability. The 802.11 task groups are currently developing additional security measures to address these known vulnerabilities. This section of the report is intended to familiarize the reader with the known vulnerabilities of 802.11 compliant networks; it is not intended to be a full primer on security protocols. Therefore, the security protocols mentioned as possible mitigation techniques against each vulnerability are not explained in detail.

- **Use of 802.11 Compliant Networks Without WEP—**Unencrypted 802.11 compliant sessions (i.e., those using OSA), are subject to snooping and hijacking. To avoid unwanted snooping and hijacking of data, users should operate 802.11 compliant networks with WEP enabled. Again, WEP only provides a low level of security—given the motive, enough time, and the right tools, WEP can be broken.

- **Weaknesses in WEP—**Weaknesses of WEP are well documented. These weaknesses are easily accessible to anyone via the public Internet and cannot be effectively addressed by the application of new and enhanced authentication techniques or new key management schemes. For example, WEP does not support per-packet integrity protection and does not offer extremely robust encryption—allowing for a wide variety of attacks, including insertion of packets into the data stream. As a result, organizations using 802.11 compliant networks with WEP as their primary security method should consider transitioning to alternative security measures under development by IEEE 802.11 Task Group I, such as TKIP and Wireless Ready Appliance Protocol.

- **Denial of Service Attacks—**802.11 compliant networks are susceptible to a host of different denial of service attacks. In this type of attack, the AP does not allow service to any MTs, even MTs that can be authenticated. The IEEE 802.11 Task Group I is in the process of specifying new measures to eliminate many of the denial of service vulnerabilities inherent in the current versions of the 802.11 standard.

- **Lack of Authentication for 802.11 Compliant Network Management Messages—**802.11 compliant networks use management messages such as beacon, probe request/response, association request/response, reassociation request/response, disassociation, and deauthentication. If these management messages are sent without authentication, denial of service attacks are possible. The attached can be accomplished using an unauthorized MT to insert false management messages that can essentially prevent the use of the AP by any other MT. Some advanced 802.11 security protocols in development address these vulnerabilities by specifying that all

authentication processes take place prior to the exchange of any management messages. If available, these enhancements to 802.11 security standards should always be used.

- **Dictionary Attacks—**Because the wireless medium is inherently susceptible to eavesdropping by unauthorized MTs, data packets sent on an 802.11 compliant network are easily sniffed. To mitigate eavesdropping and packet sniffing, the IEEE 802.11 Task Group I recommends use of methods that are resistant to dictionary attacks. Dictionary attacks enable an attacker to steal the user password. Because many users do not have unique passwords for each program, it is possible that if a user password is stolen, more than just the 802.11 compliant network is compromised—all connected networks may be compromised. For this reason, dictionary attacks are more serious than the other WEP attacks described above. Protocols exist that have dictionary attack-resistant authentication methods, including Transport Layer Security, Secure Remote Password, Tunneled Transport Layer Security, and Protected Extensible Authentication Protocol.

- **Attacks on the Default Key—**Some 802.11 implementations encrypt data using the multicast/broadcast keys (i.e., default keys). If only default keys are used, these networks are vulnerable to many of the WEP attacks described above. This is especially true if the default keys are not changed in a frequent and unpredictable way. Because APs typically do not randomly change default keys securely and automatically, administrators of 802.11 compliant networks may wish to automate the process. Default key changes can be automated using scripts or other methods such as Simple Network Management Protocol version 3 (SNMPv3). For this automated procedure to be accomplished in a secure manner, the AP must support secure management mechanisms such as SNMPv3 or Secure Shell.

5. PUBLIC SAFETY CONSIDERATIONS

Since the mid-1970s, the public safety community has been at the forefront in the use of wireless data capabilities. As technology continues to evolve, so have the capabilities and the alternatives for wireless data transmissions. As "early adopters" of wireless data technologies, public safety agencies have benefited from the progress and development of many new and innovative concepts that have facilitated extensions of existing critical information services and resources.

The proliferation of 802.11 technologies in the commercial enterprise environment has promoted the use of these new alternatives in public safety agencies. Public safety agencies continue to look for cost-effective, robust, secure solutions that will provide higher data transmission rates that can handle larger user data loads over wider coverage areas. Although they are functional, present private RF and commercial solutions provide a maximum theoretical throughput of 32 kilobits per second and do not provide the bandwidth necessary for many of the emerging graphical, photographic, and biometric applications that public safety agencies desire to deploy. These applications normally require and will result in the need to transfer large amounts of data over a wireless network. Shown in Figure 6 is a common public safety WLAN application, followed narrative describing the data transfer process.

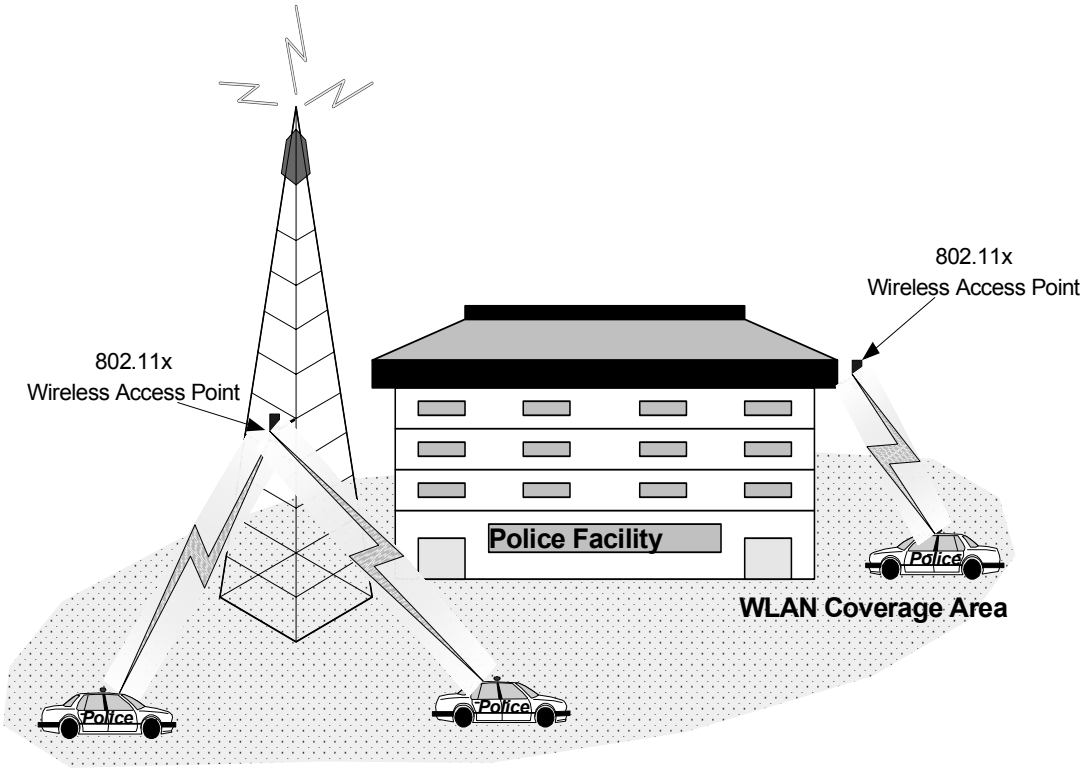

Figure 6
Public Safety Scenario

1. In the police car, a notebook computer is equipped with WLAN equipment. Whenever an officer brings the vehicle near the WLAN AP at the police station, the notebook computer can be connected to the WLAN and data is sent to the department's wired network through the AP. In some system deployments, the user must initiate the connection to the WLAN resources. In other deployments, the network components automatically sense the presence of the vehicular WLAN device and make the appropriate connections without user intervention.

2. The APs, which are typically mounted outside the police facility, receive a signal from the vehicle's notebook computer. The AP is connected to the police department's fixed wired network via a network hub or switch. As a result, the police vehicle near the AP can access the resources of the department's network consistent with the network's access and security provisions. The WLAN provides an extension of the network and its resources to the coverage area. This allows the police officer to upload and download necessary information to and from available applications and systems in much the same manner as working at a fixed workstation.

3. APs may also be deployed within the facility to extend the LAN and provide mobility and flexibility to personnel using other types of WLAN enabled devices.

In response to an emerging need, many of the technology vendors who supply information and wireless systems and services to the public safety market have added 802.11 compliant WLAN capabilities to support their suite of products. The following public safety technology providers have indicated that they are currently providing or supporting 802.11 compliant WLAN technologies to supplement their public safety information systems or wireless data systems—

- Aether Systems, Inc.
- Dataradio, Inc.
- Intergraph Public Safety
- Motorola—Printrak Division
- Northrop-Grumman (formerly PRC, Inc.)
- PADCOM, Inc.
- Voyager Systems, Inc. (formerly Tritech Secure Data Systems, Inc.).

The deployment of WLANs to support mission-critical public safety applications requires prudent consideration of various factors that could impact the suitability and usability of the connected resources. The following sections list some of the advantages and disadvantages agencies should consider.

5.1 Advantages

Agencies contemplating the use of WLANs to augment existing mobile data systems or to expand existing wired networks should consider the following advantages:

- The FCC recently allocated licensed channels in the 4.9 GHz spectrum that may be useable for public safety services, including WLANs and personal area networks, thus limiting or eliminating co-user/co-equipment interference.

- Costs for additional network cabling in facilities can be avoided or minimized.

- Costs for common-carrier data communications circuits to extend network communications into adjacent buildings or facilities can be avoided or minimized.

- Personnel can make appropriate connections to available resources when and where they need to, thus increasing productivity.

- Software updates for mobile clients can be expedited through wireless connections either eliminating or minimizing the downtime usually associated with manual installations.

- Field reporting opportunities expand by allowing personnel to remain in the field and upload reports when near APs.

- Information resources that have been commonly "station based" are extended to the field resources without the need of an intermediary.

- More expedient and timely data exchanges can occur between host and client systems for large bandwidth applications such as geographic information systems (GIS), mapping applications, photo arrays and mug shots, biometric sampling, and advanced database queries.

- Existing public safety and governmental offices and facilities can be leveraged for locating additional APs that will potentially increase efficiency though more available access.

- More information is available and should allow more effective problem solving in real time.

5.2 Disadvantages

Agencies contemplating the use of WLANs to augment existing mobile data systems or to expand existing wired networks should consider the following disadvantages:

- Commercial vendors operating as wireless Internet service providers (WISP) can deploy multiple APs within an area, creating substantial interference or rendering existing unlicensed 802.11b compliant networks unstable or unusable.

- Adequate and appropriate security features are not presently found in the wireless network equipment thus requiring use of additional third-party products at additional costs.

- Depending on the manner of the wireless deployment, the usability and functionality may not be seamless for the user community, which could create some resistance to its use and requirements for additional training.

- Appropriate management tools for the wireless APs are limited and immature and may require increased manual efforts for troubleshooting.

- Interference from other WLANs, cordless telephones, microwave ovens, Bluetooth enabled devices, or other wireless devices or sources can disrupt or obliterate connections.

- Coverage can be impacted by the composition of structures or materials around APs, as well as the existence of other WLANs in the area.

- The 5 GHz spectrum used for 802.11a compliant network equipment is more susceptible than the 2.4 GHz spectrum to fading and decreases in coverage due to signal absorption during rain events or in areas where water is present.

- 802.11b compliant equipment operates in the very crowded 2.4 GHz unlicensed spectrum, which can contribute to vast opportunities for interference with other equipment using the same area of spectrum.

- 802.11b compliant equipment, operating in the 2.4 GHz range, incorporates only three available channels, making it less desirable to install multiple APs near each other because of potential overloading of the limited bandwidth.

- Existing 802.11 standards are currently under revision and are poised to change rapidly, which could make existing products obsolete in the near term.

- Presently, some manufacturers' devices do not interoperate well with those of other manufacturers, possible making those devices prone to losing data packets as users move between dissimilar APs or multiple WLANs.

5.3 Current Uses of 802.11 Technologies

Notwithstanding the challenges in deploying 802.11 compliant WLAN technologies for public safety applications, several governmental entities have been successful in recent wireless projects. The following sections provide an overview of their efforts.

5.3.1 U.S. Army

After significant study of the technology, the Army has added 801.11b compliant networks to portable field network systems that are to be deployed worldwide. The Army is meeting the security challenges by implementing add-on security technology that will meet the National Institute of Science and Technology FIPS 140-1 cryptography certification requirements. Additionally, the Army only intends to permit Sensitive But Unclassified information on these wireless networks. The security technology is provided by Fortress Technologies of Oldsmar, Florida. The Fortress technology incorporates 128-bit AES technology end to end, with compression that is purported to actually increase the wireless networks throughput.

The Army intends to use these new wireless links in its Combat Service Support Automated Information System Interface Project (CAISI), which will link small stand-alone wired LANs in the field in an 802.11b compliant "last-mile" network and connect them into the military's wide area mobile radio network.

The CAISI networks are primarily used to track information related to vehicle and weapons maintenance in the field as well as supply systems.

5.3.2 Lower Valley Wireless Public Safety Network

The Lower Valley Wireless Public Safety Network (LVWPSN), located in and around Yakima, Washington, has deployed an 802.11b compliant wireless network infrastructure to support area law enforcement agencies. Yakima County is the second largest land area county and supports the seventh largest population, 222,581[12] in Washington State. The county also has been designated as a high-impact drug trafficking area.

The LVWPSN consists of a series of antenna sites at the network's nodes connected through Cisco Systems Aironet 340 series wireless bridges arranged in a line-of-sight pattern. The five backbone sites reach police agencies in the communities of Wapato, Toppenish, Zillah, Grandview, Sunnyside, and Granger. The network also supports connections to the County Courthouse in the City of Yakima and the U.S. Immigration and Naturalization Service and the Drug Enforcement Administration. The design is purported to ensure high-speed, long-range point-to-point and point-to-multipoint wireless connections between Ethernet networks. DSSS technology can deliver a data rate of up to 11 Mbps. The point-to-point connections span 80 miles through the valley and deliver network services to fixed facilities at each of the participating police agencies. Wireless connectivity is accomplished through the placement of omnidirectional antennas at these fixed backbone sites. Public safety vehicles accomplish connectivity through the placement of a wireless bridge in the vehicle connected to a notebook computer. PDAs are also supported in this wireless network environment using the Cisco Aironet 340 PC card.

The wireless network has also been used to facilitate video surveillance, hold network meetings, and manipulate Web cameras to observe police officers during traffic and subject stops, as well as the normal mix of data applications and queries to state and national criminal justice networks.

The network and its components support enhanced security capabilities that provide end-to-end 128-bit encryption to maintain confidentiality of law enforcement information as it travels the network. The Cisco Aironet components also provide remote management capabilities to assist in network monitoring and troubleshooting.

5.3.3 Glendale, California

The City of Glendale, California, is the third largest of 88 cities within Los Angeles County, spanning 30 square miles. The city has a reported population of approximately 200,000.

[12] Source: 2000 U.S. Census.

The city is currently replacing an existing cellular digital packet data (CDPD) mobile data system with a WLAN based on 802.11 technologies. The new system will serve the police, fire, and public works departments. The reasons for replacement of the system are twofold—a desire to reduce costs associated with commercial CDPD services and the need for increased throughput to support high-bandwidth applications such as GIS, mobile office functionality, and in-field reporting.

The city is building a new WLAN with components from Alvarion, Ltd., of Tel Aviv, Israel. These components are based on the original 802.11 standards that will provide 1 Mbps throughput throughout 85 percent of the city's 30 square mile land area. The other 15 percent of the land area is composed of uninhabited areas. 802.11 compliant equipment provides for lower throughput than 802.11b equipment, but offers better coverage. The city expects to deploy 20 to 30 wireless APs to achieve the high-speed access and coverage desired. Initially, 200 mobile units will populate the system. The police department intends to install notebook computers that will permit field-deployed officers to file various reports, access local, state, and national criminal information databases, and communicate with other fixed and mobile units.

The city has taken additional steps to ensure that the wireless law enforcement data communications and networks are protected from unauthorized access and eavesdropping. The city is using the Viatores software package from Ecutel Inc., of Alexandria, Virginia, to enhance the extremely vulnerable built-in WEP security protocol. Viatores incorporates two recognized industry standards, Mobile IP[13] and IP Security (IPSec),[14] to increase security and protection of sensitive data traffic. This client-server software provides opportunities for authentication, key exchange, VPN tunneling, and the triple data encryption standard (Triple DES), while maintaining uninterrupted sessions when roaming between APs.

5.3.4 Baltimore, Maryland, Police Department

The City of Baltimore has embarked on an innovative wireless data communications system project. The city's police department, like other major metropolitan agencies, was experiencing significant delays in processing incoming calls for services and information requests from field resources. The police department supports 9 district stations and an average of 160 deployed police vehicles to provide services to 650,000 residents in the 87 square miles area.

The Baltimore solution incorporates two distinctly different wireless communications systems to provide ubiquitous coverage throughout the service area. To achieve the desired coverage, the system incorporates both a commercial CDPD service as the WAN component and multiple site 802.11b compliant WLAN connections at each of the nine district stations. This solution incorporates a switching mechanism that provides intelligent mobile routing that allows

[13] Mobile IP is standard that allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address.

[14] IPSec is a set of protocols developed by the Internet Engineering Task Force to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement VPNs. IPSec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion of each packet, but leaves the header untouched. The more secure tunnel mode encrypts both the header and the payload.

the transmission of data across several dissimilar networks. The intelligent routing mechanism creates a single virtual WLAN that allows field-deployed officers to connect automatically and seamlessly to a variety of network resources.

The system is composed of network management equipment from Padcom of Bethlehem, Pennsylvania, wireless CDPD modems from Sierra Wireless, 802.11b compliant equipment from Cisco Systems, Inc., and Global Positioning System (GPS) equipment from Trimble Technologies, Inc. Aether Systems, Inc., supplies the mobile application software that enables the mobile office applications for the ruggedized Panasonic Toughbook notebook computers.

The system allows police officers to accomplish a multitude of activities from their vehicle without the intervention of a dispatcher or the need to return to a station. Some of the available functions include—

- Transmission and reception of various field report information
- Access to various local, state, and federal criminal information databases
- Transmission and reception of large data files
- Access to criminal history profiles
- Access to driver's license and vehicle registration records
- Access to persons imagery
- Internet access
- Real-time messaging.

The wireless mobile routing system automatically detects when a vehicle enters or exits the proximity of an 802.11b compliant AP. If information is waiting at the server for the unit, or if the unit has information to be uploaded, the mobile data device automatically transmits the information without any user intervention. When the vehicle moves out of range of the AP, the system automatically and seamlessly directs any data traffic to the alternative CDPD network for transmission to the unit.

The Baltimore solution is also purported to provide a potential migration path for future applications and new technologies. The network platform supports use of the GPS to provide information regarding the location and status of field resources, which can provide tactical advantages in providing more expedient and appropriate responses.

The security concerns surrounding 802.11b compliant equipment are mitigated using the Cisco equipment, which supports enhanced proprietary security capabilities and incorporates client-to-server encryption using DES or AES.

5.3.5 Lawrence, Kansas, Police Department

The Lawrence, Kansas, Police Department (LKPD) has deployed an 802.11b compliant WLAN to support wireless communications to 14 of its police vehicles and 4 vehicles from the University of Kansas. Lawrence is located in Northeast Kansas, west of Kansas City and east of Topeka, the state capital. The city has a reported population of 80,000 and is home to the

University of Kansas and Haskell Indian Nations University. The city's land area covers approximately 20 square miles.

Originally, the police department sought a cost-effective solution to provide WAN connections to a new police facility when the department was split between two locations. This original project was expanded and now provides the same network connectivity to the police vehicles as is found in the station.

The wireless network consists of eight sites located throughout the city. Each of these sites supports a Cisco Systems Aironet 340 wireless bridge, 42-inch omnidirectional 12 decibel antenna, 1 watt amplifier, cabling, and uninterruptible power supply. Each equipped police vehicle incorporates a Panasonic notebook computer with WLAN PC card to make the connection to the wireless AP. The infrastructure is purported to provide ¼-to½-mile radial line-of-sight coverage from the AP site. The entire system is composed of off-the-shelf components.

The network and its components support and are configured to use the integrated WEP that is commonly found with 802.11b compliant equipment. The department has also deployed firewall technology to enhance network security capabilities due to the known limitations of WEP. The wireless network infrastructure is configured as an external resource to the department and city's wired networks, and officers must also provide password authentication for access.

The police department is using the 802.11b compliant WLAN to allow officers to submit various field-completed reports and access case files and other information databases, the Internet, and mug shots.

5.3.6 Toronto Police Service

The Toronto Police Service in Toronto, Ontario, Canada, is updating its wireless data infrastructure to incorporate 802.11b technology. Toronto is located on the northwest shore of Lake Ontario and covers approximately 632 square kilometers. The city has combined seven area municipalities and represents the fifth largest municipal government in North America. The city employs 40,100 personnel and has a population of 2.48 million.

The Toronto Police Service has undertaken a technology expansion and upgrade project called eCop, implementing new technologies and services throughout the department. One of the projects within eCop is the provision of enhanced wireless mobile data services to facilitate more streamlined reporting and inquiry processes from field-deployed units when near a 802.11b compliant AP.

The wireless infrastructure incorporates the IBM Everyplace Wireless Gateway product, which allows laptop PCs in the police vehicles to communicate with multiple wireless data networks. The gateway allows the wireless devices in the police vehicles to roam between WLANs and wireless WANs because the software automatically and seamlessly detects when the vehicle is nearing or leaving a WLAN AP and nearing or leaving the wireless WAN environment. The gateway supports the department's existing private RF mobile data system, will support

cellular and packet-switched WANs, and will be capable of supporting commercial 2.5-generation wireless networks in the future, should the department decide to do so.

The gateway and network components incorporate enhanced security protocols in addition to the extremely vulnerable WEP standard for WLANs. The gateway product allows customers to choose the level of encryption support desired as it supports, DES, Triple DES, RC4, and AES.

The police department is using the 802.11b compliant WLANs to allow officers to submit various field-completed reports and to access new IBM DB2 database information applications and other departmental information assets.

6. FUTURE IMPACT

Users across business sectors should consider 802.11 technologies as an emerging standard. The wireless network market continues to rapidly advance and change with interesting developments occurring frequently. For instance, open wireless 802.11b compliant networks that are free to the public, coined "hotspots," can be found in a variety of locales including homes, businesses, airports, and conference centers. Building on this development, users have adopted various techniques for identifying non-secure, non-advertised wireless networks using detection software or locating chalk marks[15] on walls. These networks serve as a free path to the Internet. However, Wireless Internet Service Providers (WISPs), a developing industry, are preparing to combine hotspots into a nationwide network and charge for the service. Several major wireless services vendors have formed an alliance and are examining the possibilities of offering WISP services. Service providers will need to attract a large user base and offer a desirable service at acceptable prices. Due to the potential of interference caused by large numbers of users operating in the unlicensed bands, this and other developments should be monitored for potential impact on existing or impending deployments.

With reliable and stringent security features in place, WLANs may become an important communications medium used by the public safety community to transfer data in real time. This technology meets the flexible, fast requirements of the demanding and rugged environment within which these users operate. As WLANs become more commonplace, the overall costs for deployment, use, and maintenance will likely become more competitive with other existing wireless solutions.

[15] Chalk marks serve as a visual indicator for locations where wireless networks are available.

APPENDIX A—ACRONYMS

ACA	Australian Communications Authority
AES	Advanced Encryption Standard
AP	Access Points
ARF	Alternative Regulatory Framework
ATM	Asynchronous Transfer Mode
CAISI	Combat Service Support Automated Information System Interface Project
CAT5	Category 5
CCK	Complementary Code Keying
CDPD	Cellular Digital Packet Data
CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
GHz	Gigahertz
GIS	Geographic Information Systems
GPS	Global Positioning System
HiperLAN	High Performance Radio Local Area Network
ICV	Integrity Check Value
IEEE	Institute of Electrical And Electronics Engineers, Inc.
IP	Internet Protocol
IPSec	Internet Protocol-Security
ISM	Industrial, Scientific and Medical
IV	Initialization Vector
LAN	Local Area Networks
LKPD	Lawrence, Kansas, Police Department
LVWPSN	Lower Valley Wireless Public Safety Network
MAC	Media Access Control
Mbps	Megabits per Second
MHz	Megahertz
MT	Mobile Terminals
mW	Milli Watts
OFDM	Orthogonal Frequency Division Multiplexing
OSA	Open Systems Authentication
PBCC	Packet Binary Convolution Coding
PC	Personal Computer
PCI	Personal Computer Interconnect
PCMCIA	PC Memory Card International Association
PDA	Personal Digital Assistant
QoS	Quality of Service
RF	Radio Frequency

SNMPv3	Simple Network Management Protocol Version 3
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
UNII	Unlicensed National Information Infrastructure
USB	Universal Serial Bus
VPN	Virtual Private Networks
WAN	Wide Area Networks
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Encryption Privacy
WISP	Wireless Internet Service Provider
WLAN	Local Area Networks