

IFMA FOUNDATION

## Wireless Systems in the Facility



*This report sponsored by*

**Allsteel<sup>®</sup>**

*and the*

IFMA Foundation Corporate Circle of Contributors

This report was written by:



**BAKER ROBBINS & COMPANY**  
TECHNOLOGY CONSULTANTS

***About the authors:***

**Steve Falkin** has over twenty years of experience in IT and infrastructure consulting, design and implementation. He has diverse background and experience in the areas of system design and development, automation planning, system assessment and infrastructure design. In addition, he has considerable expertise in the areas of hardware configuration, data communications, cable plant design and computer facility design. His other areas of expertise include application selection, design and implementation and development of practice area procedures. Mr. Falkin is a member of International Facility Management Association and Building Industry Consulting Services International. He has a bachelor's degree in information systems from Northeastern Illinois University.

**William Sellers** has managed and conducted a wide range of projects including long and short range information system planning; software development; software selection and implementation; hardware and software acquisition through competitive bidding; business process reengineering; large scale desktop implementations; network audits; network design and analysis (LAN and WAN); data analysis; financial analysis; design of audiovisual, telephone and security systems; design of training programs; disaster recovery planning; Internet planning; RFP preparation and management of competitive bid procedures. He has had extensive involvement with data center design, from multi-room mainframe centers to small network installations. He has a master's degree in planning from Governor's State University, Illinois.



**IFMA FOUNDATION**  
Research • Scholarships • Education

*This paper was made possible by the support of the IFMA Foundation. Established in 1990 as a 501(c)(3) corporation, the Foundation funds research, education and scholarships. By increasing the body of knowledge available to facility professionals, the Foundation advances your profession and career potential.*

---

Additional copies of this report are available for sale from the IFMA Foundation,  
1 E Greenway Plaza, Suite 1100, Houston, TX, 77046-0194; (281) 974-5600;  
also available on line at <http://www.ifmafoundation.org>.

# Table of Contents

---

<b>Introduction</b> .....	<b>1</b>
<b>1. OVERVIEW OF MODERN WIRELESS SYSTEMS</b> .....	<b>2</b>
<b>Types of Wireless Systems</b> .....	<b>2</b>
Wireless Ethernet Network or Wireless Local Area Network .....	2
PDA Systems (e.g. Blackberry and Palm Pilots) .....	2
Cellular Phones .....	2
Microwave and Point To Point Systems .....	3
Satellite .....	3
Satellite Telephones .....	3
Bluetooth .....	3
Infrared .....	3
Wireless VOIP .....	4
Audiovisual Systems .....	4
E-mail .....	4
<b>Factors in Wireless Use</b> .....	<b>5</b>
Bandwidth .....	5
Reliability .....	6
Frequency .....	6
Mobile vs. Stationary Users .....	6
Wired Systems .....	6
Wireless .....	7
IP Devices .....	7
Hybrid Systems .....	7
Future Systems .....	7
Psychology And Market Factors .....	8
Standards .....	8
<b>2. WIRELESS IN THE FACILITY</b> .....	<b>9</b>
<b>Facility Manager Relationship with IT</b> .....	<b>9</b>
<b>Wired Infrastructure for Wireless Systems</b> .....	<b>9</b>
<b>Wireless Interaction with the Facility</b> .....	<b>11</b>
Office Buildings .....	11
<i>Conference Rooms</i> .....	11
<i>Raised Office Floors</i> .....	11
<i>Wiring Rooms</i> .....	11
<i>Computer Rooms</i> .....	11
<i>Systems Furniture</i> .....	12
<i>Ceilings</i> .....	12
<i>Workspace Requirements</i> .....	13
Schools .....	13
Medical Facility .....	13
Public Facilities .....	13
Restaurants .....	14
Building Management Systems .....	14
New Facility Construction .....	14
<b>IT Infrastructure</b> .....	<b>14</b>

## Table of Contents (cont.)

---

<b>3. WIRELESS SYSTEM IMPLEMENTATION</b> .....	<b>15</b>
System Planning .....	15
Vendors/Installer.....	15
WLAN.....	16
PDA.....	17
Wireless or Satellite Antenna .....	17
Cellular Repeater Systems.....	18
Maintenance Operations and Support .....	19
<b>4. OTHER WIRELESS CONSIDERATIONS</b> .....	<b>20</b>
Installed Life Cycle Costs .....	20
Capital Costs .....	20
Services.....	20
Operational and Soft Costs .....	21
Security Issues .....	21
Health Effects .....	22
Conclusion.....	22
<b>Appendix 1: Wireless Standards</b> .....	<b>23</b>
<b>Appendix 2: Glossary of Terms and Definitions</b> .....	<b>24</b>

## Introduction

---

Wireless technology is the transmission of information via radio frequency waves. The term wireless is one of the original terms for radio. Marconi, inventor of the first practical radio in 1895 which operated via Morse code, called his invention the wireless. This was wireless telegraphy, not requiring the hard wires of the traditional telegraph system. Today we talk about systems that do not require the hard wires of traditional data networks as wireless. The first wireless voice transmission occurred in 1906. Wireless data transmission began in the 1960s and wireless LAN transmission in the 1980s, but has gained widespread popularity since 2000. The company that Marconi founded in the 1890s still provides wireless services today. While wireless is predominantly radio based, some systems are based on infrared light transmission.

This document addresses the impact of modern wireless technology on the facility. It differs from the many other articles about wireless in that it is focused on what the facility manager needs to know when dealing with wireless systems within the facility. It provides a general non-technical introduction and information to assist the facility manager.

This report will introduce the facility manager to the common systems, but will not go into great technical depth about how wireless systems work, security protocols, network administration or other detailed technical information. Most of the technical detail is the responsibility of the Information Technology (IT) department. While some technical information is necessary to accomplish the goals of the paper, it is assumed that the reader is not an IT professional. Rather, the paper focuses on how such systems interact with the facility.

There are four major sections to this report:

1. ***Overview Of Modern Wireless Systems*** discusses types of wireless systems and some of the factors that affect their use. There are many different types of systems that the facility manager will encounter. This section provides an overview of the various types on the market. This section also discusses factors that are involved with wireless use such as reliability, bandwidth and market forces.
2. ***Wireless In The Facility*** covers how wireless works in the facility. There are several factors affecting wireless use in the facility and some facility changes that may occur due to wireless. Will wiring and computer rooms be downsized because of wireless, or will they get bigger? Will wireless profoundly change the way we work in the facility? Will phones become wireless? This section introduces the facility manager to those issues.
3. ***Wireless System Implementation*** provides guidance to the facility manager called upon to install wireless LANs, satellite antennae, cellular repeater systems or to link two buildings together and select vendors.
4. ***Other Wireless Considerations*** covers costs, security and health issues.

This paper assumes that a change to wireless systems will be gradual throughout many years, but it's hard to forecast the future. There are those that think that the transition from wired to wireless systems will be rapid.

# OVERVIEW OF MODERN WIRELESS SYSTEMS

---

## Types of Wireless Systems

There are many different technologies that are referred to as wireless which leads to considerable confusion in discussing such technology. Wireless can refer to telephone systems, computer systems, personal digital assistants (PDAs) – almost any type of electronic device. Wireless is simply a communication and delivery system from one device to another. This paper primarily focuses on wireless voice and data and does not include traditional wireless radio.

### **Wireless Ethernet Network or Wireless Local Area Network**

Wireless LANs are sometimes referred to as WLAN or Wi-Fi (wireless fidelity). WLAN is wireless connections to a local area network (computer network) which are internal to most organizations. It can also mean a wireless connection to the Internet via a service provider, as in a wireless hot spot like those found in coffee shops. Similar technology is involved for both systems. Wireless LANs in an office or home are typical of what many people mean when they talk about wireless systems.

### **PDA Systems (e.g. Blackberry and Palm Pilots)**

These systems provide information to handheld personal digital assistants, Blackberry being one of the most common. Typically, they use the cell phone network. Some companies implement PDA systems for their mobile work force. PDA systems transmit information to mobile workers and allow those workers to send information back to the facility. Such systems often require custom applications for such things as service dispatch, time entry and expenses.

### **Cellular Phones**

Everyone is familiar with wireless phones and we will not discuss them in depth. What is of concern for the facility manager is how well cell phones work within the facility. Because some building structures can interfere with cell signals, systems have been developed to essentially put a cell antenna inside of the building. Such systems are expensive and complex for the facility manager to deal with. Because they can transcend an individual tenant, they are best implemented by the base building in multi-tenant buildings. Since the systems are expensive, base building management is often reluctant. Also, multiple service providers are usually involved.

There is a development to use Wi-Fi hot zones as cellular systems called Vo-Fi. This would allow Wi-Fi systems in public places such as coffee shops to function as phone systems. People would use cell phones with additional circuitry for this function. These systems are expected to emerge in the next few years.

## **Microwave and Point To Point Systems**

Microwave communication has been available for a long time, but there are also many newer technologies that provide point to point communication. These systems are useful for organizations that need to connect buildings that are some distance apart. The facility manager could be called upon to install antennae in the facility. Point to point systems are convenient for a small out-building in a campus or industrial complex, where connectivity is required, yet a wired connection would be expensive.

There are point to point systems sometimes called Ethernet bridges that will create connections up to several miles. Although generally reliable, these systems can be affected by weather. Many of these systems operate on extremely high radio frequencies that are not regulated by the government. In the U.S. the Federal Communications Commission regulates wireless. Many of these systems are proprietary, but there is a new standard emerging for these systems called WiMAX.

## **Satellite**

There are a variety of communication methods including television and satellite data services where systems in the facility connect to service providers via a satellite antenna. Often these are installed as backup to wired connections. The facility manager is likely to be called upon to install an antenna on the roof or facility grounds.

## **Satellite Telephones**

Another type of satellite system is hand-held telephones that operate like cell phones, but communicate with satellites instead of cell towers. These systems have much greater coverage than regular cell phones and are used by organizations whose workers go to remote places. These systems have little impact on the facility, as the handheld phone connects directly to a satellite.

## **Bluetooth**

This is a short-range system for connecting local electronic devices such as keyboards, mice and other devices to a computer. It has a range of approximately 30 feet.

## **Infrared**

This is transmission via infrared light instead of radio waves. It must be line of site and there is a short-range system for connecting local devices, such as wireless remotes in home electronic equipment, and a longer- range point to point system for connecting building to building.

## **Wireless VOIP**

Voice over Internet Protocol (VOIP) is a telephone system that operates on the computer network, rather than separate proprietary telephone wiring. In order to operate correctly, such systems require that the wireless network equipment have features that give priority to voice over data traffic, referred to as quality of service. While wired VOIP systems are gaining considerable market share, the wireless versions are just beginning to emerge and are not yet in widespread use.

It is important to understand that wireless VOIP is not the same as a cellular phone system, nor is it the same as a wireless phone used at home. A wireless VOIP system offers all the features of an internal PBX type system such as voicemail, conferencing and call forwarding without wires. When such systems are reliably available in the coming years, they have potential to revolutionize the facility.

## **Audiovisual Systems**

Audiovisual control systems available with wireless control pads and wireless microphones are common. However, most audiovisual equipment is still wired.

## **E-Mail**

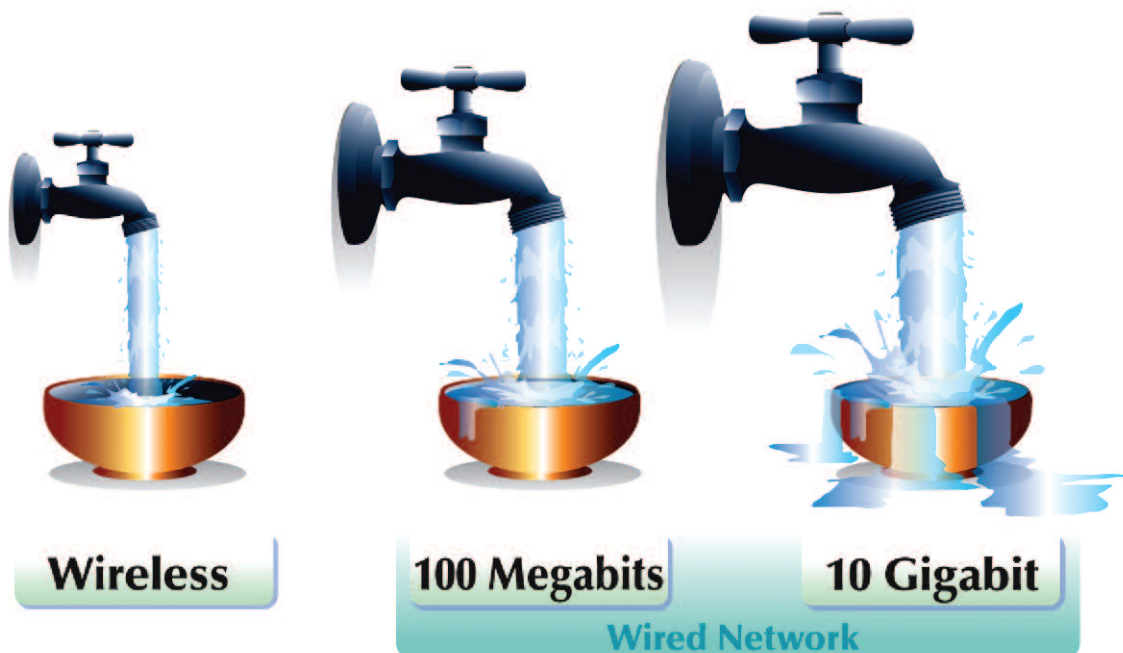
E-mail can be done through wireless Internet connections via a laptop or dedicated e-mail devices such as the wireless Blackberry and other PDAs.

## Factors in Wireless Use

### Bandwidth

Bandwidth is a technical concept that actually has two meanings in this context. One is the amount of radio spectrum that a wireless application uses. The other meaning is the amount of data that can be transmitted in a unit of time.

Bandwidth in terms of quantity of data transmitted is an important concept. Wired networks can transmit large amounts of information; 100 million bits<sup>1</sup> of data per second (100 megabits), 1 billion bits per second (1 gigabit) or 10 billion bits per second (10 gigabits). Most wireless networks transmit at only 11 million bits per second, although some now transmit at 54 million bits. Thus, wired systems can supply significantly greater bandwidth, by a large factor. While bandwidth is increasing for wireless systems, it is increasing for wired systems also. The following graphic shows the relative relationships. The amount of water represents the amount of bandwidth.



The result of the bandwidth limitation is that wireless networks can process much less information per unit of time possibly causing the wireless-connected computer to wait in order to execute a given task. Many applications have been particularly designed for wireless use to minimize the amount of data that is being transmitted.

The demand for bandwidth is growing as more and more services are being moved to the LAN such as physical security systems, building management systems, voice and audiovisual signals. It will be years until wireless can handle all of the bandwidth demands that are developing. Some applications such as video transmission require so much bandwidth that even today's wired networks are still stressed to provide adequate transmission. Consequently, wireless systems will not fully support video for some time. Bandwidth and reliability are two factors that may limit the deployment of wireless systems for certain environments.

<sup>1</sup> A bit is the smallest unit of information (1 or 0) involved in data processing.

## **Reliability**

Reliability can be an issue for wireless systems. The basic connection is a radio signal and is therefore subject to interference from other signals, including some building structures, electromagnetic fields and even the weather. Consequently, where high reliability is critical, a wired connection is much more predictable and stable.

## **Frequency**

Wireless devices operate at extremely high frequencies in the radio spectrum. Many operate above the area that is regulated. Sometimes there are multiple devices operating in the same frequency range in the same area of the facility and these devices can clash with each other. Many devices have multiple channels to adjust for this interference. Wireless frequencies, number of channels and the amount of radio spectrum allocated to these systems varies from country to country.

## **Mobile vs. Stationary Users**

Wireless is compelling for mobile users. Police officers, salespeople in the field, roving maintenance staff, forklift truck operators in a warehouse, delivery truck drivers, students, doctors within a hospital, mobile consultants, workers moving from office to office within an organization – all can benefit from wireless technology. In most cases the advantages are obvious. If the bandwidth limitations can be addressed, it is these types of users that can most benefit from such systems. Many organizations provide wireless networks for visitors, which provide connectivity for guests in lobbies, conference rooms and cafeterias while keeping the visitors secure from the internal network.

Most users of typical office applications such as word processing and e-mail can work well with wireless. There is a particular issue when specialized applications are used on PDAs. For this purpose custom applications can be designed that minimize the transmission of data and therefore minimize bandwidth between the wireless device and the system.

For the stationary user, a wireless connection offers little advantage and significant disadvantage in reduced bandwidth. The main benefit of wireless is mobility but many desktop computers never move. Because of the lower bandwidth, there is little benefit for wireless connections to a desktop computer, except possibly cabling costs. Power is usually required in desktop computers, and this is delivered using cables.

## **Wired Systems**

While small offices may be able to implement wireless systems with very little wiring, wireless systems are typically implemented with a wired infrastructure. Wired connections are appropriate where high bandwidth and/or high reliability is required and where mobility is not important like most corporate workstations. Service entrance cables from service providers to the facility will usually be a wired connection. In larger and/or multi-floor facilities, backbone connections to wiring closets from the computer room will most often be wired for the foreseeable future.

## **Wireless**

Wireless is appropriate wherever mobility and portability is required and bandwidth requirements are low; for example laptops, PDAs and bar code readers for mobile workers. It is also relevant for small temporary installations, as it can be installed quickly. This should be considered for old facilities that do not have data wiring, such as old college dormitories. Wireless is useful for historic buildings where the interior cannot be changed for the installation of wiring, or for buildings where the landlord will not permit wall penetrations or the addition of cabling.

## **IP Devices**

Internet Protocol (IP) is used to identify devices on a network. Any IP addressable device could theoretically become a wireless network device. For example there are IP addressable video cameras. These could be used as security cameras in remote places where wiring is difficult. Cameras are frequently finding applications for mobile monitoring of traffic or for security monitoring in public areas such as outside of buildings where power is available, but data connections are sparse.

## **Hybrid Systems**

Hybrid systems are primarily wired systems that incorporate a wireless component. With hybrid systems some or all offices and workstations are wired. The wireless networks are supplemental, primarily for guests, but also for workers who want to be able to move their computers to different locations within the facility. Wireless systems in this case frequently focus on public areas such as conference rooms, reception areas and lunch rooms.

Some facilities that have an extensive outsourced workforce or a large number of guests have a wireless network throughout the facility for the outsourced workers, while the regular staff operate with a wired network. This allows security separation between the outsourced workers and the in-house network.

## **Future Systems**

Hybrid systems are the norm today. Facility network designers and network installers report that most large organizations are still installing fully wired networks with supplemental wireless networks. Until the bandwidth issue is resolved and wireless is more reliable, most major organizations are expected to install fully wired infrastructure for some time.

## **Psychology And Market Factors**

There is enormous enthusiasm for wireless in the market place. Television ads, wireless hot spots, billboards – everything is wireless. However, there is an aspect of irrational exuberance in this enthusiasm. One issue in talking about wireless systems is the widespread experience with consumer-oriented wireless – home networks, Internet hot spots at coffee shops and other public places. These systems give a distorted view because the demands of a serious organization are vastly beyond the scope of these individual systems. Yet it is difficult for the person who has just used a laptop at a coffee shop to understand the issues and implications of using wireless networks in the enterprise. Ads refer to high-speed wireless access, creating the incorrect idea in some that wireless is actually faster than a wired connection.

There are those who are so enthusiastic that they assume that everything can or should be wireless, often ignoring some of the limitations. Non-technical executives read about wireless in a magazine and assume that they should implement it. The result of these psychological and market issues is that there will be some inappropriate implementations of wireless systems.

## **Standards**

Like many other aspects of technology, standards are important, defining how various types of equipment connect so that equipment from diverse manufacturers will work together. Often vendors develop technology before standards are defined resulting in proprietary systems that work only with one vendor's equipment. It is widely felt that proprietary systems result in the organization being stuck with that vendor regardless of how good or bad they are. Standards-based systems provide more products, interoperability across vendors and cost competition.

Sometimes there are competing standards and it is not clear which one will prevail. Sometimes emotional rather than technical factors cause one standard to be adopted instead of another. The competing standards of consumer video between VHS and BETA is an example. It is somewhat of a gamble to adopt a standard when that standard is still competing with other standards.

It is not necessarily bad to buy a proprietary system. With new technology it may be the only choice. Wireless is such a fast moving technology that vendors are bringing out proprietary systems before standards are in place. If one needs a technology for which there is no standard, then it may be reasonable to implement a proprietary system. However, it is important to recognize the dangers in buying a proprietary system. Those dangers include high cost, no ability to switch vendors, and potentially having to replace equipment when standards eventually emerge. (See Appendix 1 for further information about standards.)

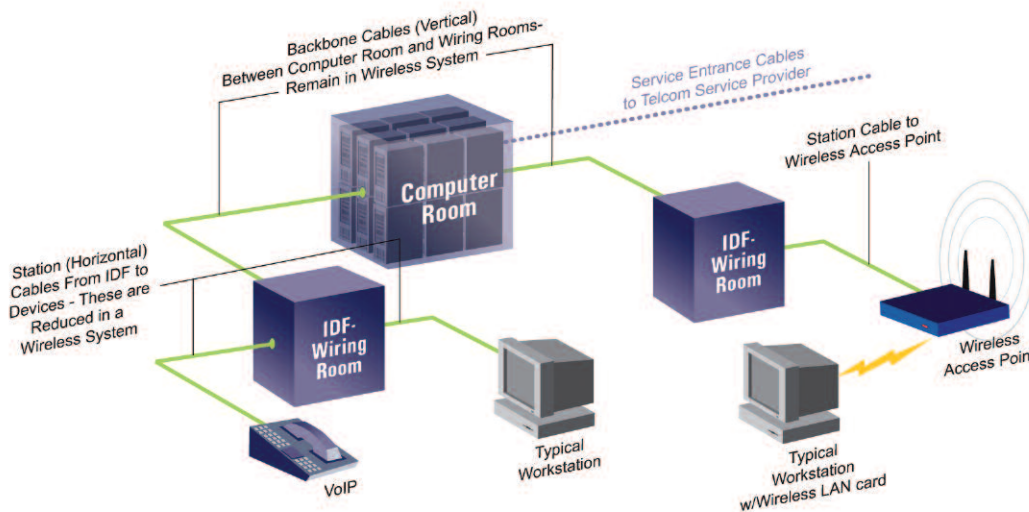
# WIRELESS IN THE FACILITY

## Facility Manager Relationship with IT

The relationship between the facility management department and the IT department is an important one. The IT department is responsible for delivery of services to the organization for the IT systems that exist within the facility. It is the wise facility manager who cultivates a good relationship with the IT director, and vice versa. Together IT and the facility management department can collaborate for the good of the enterprise, yet these two departments are often separated organizationally and sometimes IT and facilities are embroiled in turf wars. If there is a poor relationship between the facility management department and IT, the entire organization will suffer and both will be hampered in conducting their responsibilities. With good collaboration, IT can focus on the details of system administration and the facility management department can focus on how systems occupy the facility. Wireless projects will inherently be a collaboration of IT and the facility management department, as IT will be responsible for the technical system details, but the equipment will be housed in the facility.

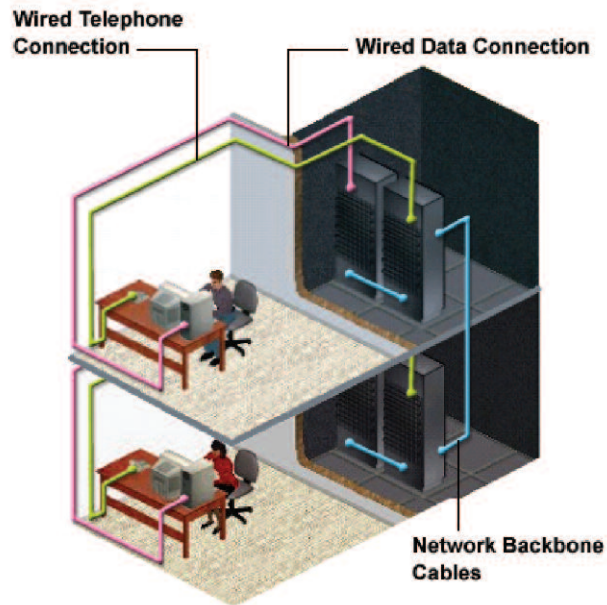
## Wired Infrastructure for Wireless Systems

An important thing to understand about wireless network systems, in all but the smallest facilities, is that in most cases wires are required. There are still network backbone cables that connect the computer room to the wiring rooms (IDF) and there are wires (horizontal station cables) from the wiring room to access points<sup>2</sup> or antenna throughout the facility. The following drawing shows how wiring rooms connect to the computer room. The wiring room on the left shows a traditional wired network. The wiring room on the right shows a wireless network. The wireless system eliminates the wire from the wall to the computer. A rule of thumb is that a fully wireless network requires 40 percent of the cabling of a fully wired network. Small offices may not require backbone cables and can use a minimal cable plant from the central equipment to the access points.



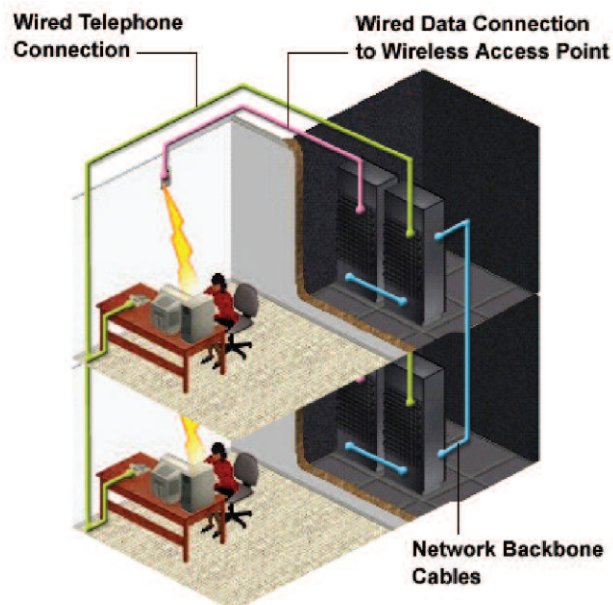
<sup>2</sup> The radio device that transmits between the wired network and wireless devices is called an access point.

The following drawing shows a typical wire infrastructure:



**Example of Wired Infrastructure**

Thus far, wireless networks have been weak at supporting office telephone systems, so wire has still been required to the telephone instrument, even where the computer connection has been eliminated. The ability of wireless LANs to support telephones is expected to grow in the coming years. The following diagram shows the wiring associated with a wireless data network and wired phones.



**Example of Wireless Data Network with Wired Phones**

## Wireless Interaction with the Facility

It seems likely that most new construction of large facilities in the next three to five years will have fully-wired systems in conjunction with wireless systems of growing sophistication. It will be some time until major organizations do not have wired networks at all. Some organizations will experiment with all wireless, particularly smaller and start-up organizations. Consequently, the impact on workplace configuration and furniture design will be slow and gradual.

Many of the remarks in this section relate to typical office environments. Factories, warehouses and industrial locations have unique requirements and situations. Wireless has been particularly effective in warehouses where wireless bar code readers on fork lift trucks transmit inventory data to a central system. In these situations wireless access points are typically installed on columns and girders, with the wire running along the girders. Wireless can be difficult in heavy industrial sites. Heavy industrial equipment can generate significant interference to today's wireless systems. Installation in such areas requires extensive testing.

### Office Buildings

#### *Conference Rooms*

Conference rooms and conference centers are often intensive areas for technology. This is the area where there is most likely to be a wireless LAN in an office today to provide guests with Internet access. There are often complex audio visual systems in conference rooms for presentations and these systems are mostly wired today. While there are wireless AV control systems, video over wireless is very difficult for the foreseeable future

#### *Raised Office Floors*

Raised office floors serve several purposes: AC power, voice and data cable, and sometimes air conditioning distribution. Most facilities will still have voice and data cables to workstations in the next three to five years. Even as the voice and data cables phase out over time, raised floors will continue to have value for power and air distribution.

#### *Wiring Rooms*

Distributed wiring rooms (IDF or TR) in larger facilities have been growing in size and complexity for the last 20 years. Newer wireless LANs locate additional equipment in these rooms. Emerging voice technology (VOIP) is adding equipment to these rooms for providing power to telephones. Ethernet switches, traditionally located in these rooms are getting larger. Wiring rooms will be getting larger during the coming years and will require additional power and cooling. They will be treated more like miniature computer rooms with UPS systems, security, environmental monitoring and anti-static floors – all of the features of a computer room.

#### *Computer Rooms*

Computer rooms hold voice and data servers and as such are little changed by wired vs. wireless distribution systems. Because backbone cables from the computer room to wiring closets are still required in a wireless system, there is little change in the wiring entering the computer room. VOIP phones reduce traditional telephone wiring in the data center, but this is unrelated to wireless.

### *Systems Furniture*

Systems furniture has evolved significantly with regard to supporting technology. Interactive whiteboards, sensors for lighting controls, sound masking, cable management and distribution and flexible power circuiting are just some of the features that have become available. In terms of wireless networks, there will be some continued evolution of systems furniture, but it may not be as dramatic as might be seen in other aspects of the facility.

Power to the user area will continue to be a key requirement, even for wireless devices. As a result, the wiring raceways that commonly occur in systems furniture panels will remain for some time. More user area equipment will require small power supplies and transformers<sup>3</sup> that plug into traditional electrical outlets and then supply low voltage (i.e. “DC electricity”) to a device like a laptop or PDA. Systems furniture could evolve to build these power supplies into the wiring raceway for easier distribution and/or provide better management for the transformers and power supplies.

Telephones may be hard wired in some cases even when computers are wireless, causing continued need for low voltage cable raceways. Bluetooth-type technology will likely minimize the local wiring for keyboards and mice and will clean up the workspace. The grommets in the tops of desks for wires will be less needed in the coming years, but will still be used to manage lamp, calculator and similar type cords. There could be situations where wireless access points and antennae are built into systems furniture in the future. Antennae could be inside the furniture panels and the wiring raceways will be needed for the antenna cables.

Wireless may encourage greater use of laptops in place of desktop computers, because the primary benefit of wireless is mobility. The use of laptops may reduce the amount of equipment at the user area and systems furniture work surfaces. Storage may be redesigned to specifically accommodate the growing number of devices associated with the mobile user, such as a laptop, a docking station or a PDA.

Moving people around and reconfiguring systems furniture to support changing business requirements (churn) has and will continue to be a challenge. While wireless technology can greatly facilitate this (by reducing the volume of low voltage cabling), there will still be power wiring for the foreseeable future, so the process of reconfiguring systems furniture will not change much.

Fabric covered cubical walls can affect wireless signals, and wireless coverage should always be studied after cubicles and other furniture and finishes are installed. One study indicated that cubicles could negatively affect wireless signals more than just about anything in an office other than a concrete wall. The materials in future systems furniture construction may change to minimize this impact. The facility manager needs to be mindful of the potential impact on existing wireless systems when reconfiguring systems furniture.

### *Ceilings*

Wireless access points are often installed above the ceiling. The electronic part of wireless systems may move into the distributed wiring rooms, but antennae will still need to be distributed throughout the facility. Plenum ceilings complicate installation. Special ceiling panels are already on the market to hold access points. Antennae do not have to be in the ceiling and we may see them built into walls or furniture in the future. Some ceilings tiles have a foil back that can interfere with a radio signal when the antenna is installed above the ceiling.

<sup>3</sup> Often called Wall warts or AC adapters, wall transformers or a power pack.

### *Workspace Requirements*

As wireless systems evolve in the coming years and achieve substantially more functionality than is available today, there could be major impacts on the facility. Wireless technology in the future could impact how people use office space. In particular if telephones within an office become completely wireless, people could become much more mobile within the office. This could change the ways in which people collaborate and meet. It could also change the typical scenario where every worker has a dedicated workspace. This is mitigated by the workers need for personal affects, paper files and a place to call home. The elusive paperless office long discussed as a consequence of computers, though not necessarily wireless, has never materialized. This connection to paper, keeps workers connected to their workspace.

There is a long standing concept called hoteling where workers do not have a dedicated workspace, but are assigned one for the day. This is often used where workers are frequently in the field, and occasionally in the office. Hoteling is often complex to implement, partly because of telephones and computers. Extensive evolution of wireless could make hoteling easier.

How the workplace will evolve as a result of wireless is not clear at this time. We cannot say there will be more hoteling, no dedicated workspace or more collaboration areas. These changes are not only a function of what technology makes possible, but corporate preferences, psychology, people and how they want to work. It is likely that there will be a lot of experimentation in facility design in the coming years as wireless matures. Architects will be following these trends closely as systems evolve. The facility manager is also advised to follow these trends closely and keep an open mind to the possibilities.

### **Schools**

Educational facilities are the ideal environments for wireless LANs. Students are highly mobile within the campus and many have laptops. Moving from class to class, dorms and public spaces, the student can connect throughout the wireless campus. Many schools have old buildings that do not have wired systems where retro-fitting wired data connections is difficult. Wireless is a good solution in such facilities. On the other hand many schools have high bandwidth requirements such as distance learning and AV and video applications. Educational buildings with high-end classrooms require a wired network. Colleges and secondary schools tend to have a greater amount of technology than primary schools.

### **Medical Facility**

Many hospitals and medical facilities have implemented wireless systems which are widely used. Patient monitors, bedside monitors and clinical tools have been in use for some time. Due to the need for high reliability, there are special radio frequencies being set aside for medical wireless networks, however regular wireless systems are also in use. Some systems allow doctors and intake workers to collect and enter data into wireless devices while consulting with the patient. Wireless in the hospital is a specialty area requiring considerable expertise as the systems involve life safety. Interference to the wireless signals can have serious consequences in medical applications.

### **Public Facilities**

Public facilities such as libraries are logical venues for wireless systems where customers may bring in laptops or PDAs and connect to a public network. Marinas, restaurants, coffee shops, cultural centers, museums and airports are also likely locations for such systems.

## Restaurants

Restaurant applications allow the server to take orders on a PDA and have those orders immediately transmitted to the kitchen from the table. Such systems are speeding up service delivery.

## Building Management Systems

It is possible for building management systems to have a wireless component. This is particularly useful for remote devices that may be difficult to wire. It is possible to read the output of a system on a wireless device, enabling the facility manager to be aware of the status of the systems even when not on site. In large facilities, service personnel could be dispatched and report service calls via wireless PDAs.

## New Facility Construction

When the facility manager becomes involved in new facility construction there is a great deal to consider. It would be wise to meet with management and IT very early in the process to determine what types of systems will be implemented. The requirements for wired and wireless systems, computer rooms, distributed wiring closets and special technology requirements, such as satellite antenna, conference rooms and unique areas, should be defined early in the process.

New construction design does not always provide sufficient space for distributed wiring rooms, computer rooms and communication cable pathways such as risers, cable trays and conduit. It is important for the organization to consider what systems it will implement, what systems will be wired and wireless, and what is required for IT spaces. This should be provided as programming information to the architect as early as possible, so that adequate space is programmed in the schematic design phase. Ideally the architect and wireless system designer would meet to discuss the impact of materials and design. If there are to be wireless systems and/or satellites, there is an opportunity to build these systems into the plan of the building if they are identified up front. When technology requirements are considered late in the design cycle, this often results in inadequate technology facilities.

Regardless of the foreseeable evolution of wireless systems, wired entrance cables or the connection to the telephone company in the street for telecommunications service are likely to be required indefinitely. Wireless can be used as backup to wired connections, but wired entrances are required for bandwidth and life safety considerations. In times of emergency, the telephone system is a lifeline to help. Conventional wisdom is not to rely on wireless communications for emergencies. Consequently, facilities will need entrance conduits which are usually underground, but sometimes aerial, NetPOP rooms in the basement and communication risers for distribution for the foreseeable future.

## IT Infrastructure

Sufficient space for distributed wiring rooms, computer rooms, NetPOPs and cable pathways, requires special consideration. In most cases wireless systems do not reduce the need for these facilities. Other factors such as the growth of computer applications, growth of data storage, disaster recovery, and the convergence of systems on the network that were not traditionally network-based, drive the need for good quality spaces for computer rooms, wiring closets and risers. Organizations and facilities that do not allocate adequate space for these functions will have ongoing problems. It was assumed that the downsizing of equipment would create more and more space in data centers and wiring rooms, however, there are now diminishing returns from this previous trend and the expansion of the number of devices going into these rooms is the bigger factor.

## WIRELESS SYSTEM IMPLEMENTATION

---

The facility manager will be called upon to assist with various types of installations

- **WLAN:** A wireless LAN is the most common installation for a facility manager in a general office environment.
- **PDA:** Some organizations with a mobile work force may implement a wireless system for handheld devices.
- **Satellite Antenna:** Organizations of all types are considering satellite systems, in many instances as backup to wired connections for disaster recovery purposes.
- **Cellular Repeater:** Facilities of all types and sizes might benefit from a cellular telephone repeater system.

### System Planning

The implementation of a wireless system requires up-front planning to be successful. Advance planning about the wireless application, the type of device, bandwidth, where devices will be located in the facility, costs, security and connection with the network is essential.

### Vendors/Installer

Often a system will be installed by a vendor who sells the equipment. The facility manager's role may be to find and select that vendor and oversee the installation. This is much like finding a vendor for any purpose in the facility. In seeking a wireless vendor, it is difficult to determine the skill of a potential vendor. Because the technology is so new, there are new vendors in the field. It is important to judge the skill and experience of a potential vendor to handle the proposed system. Ideally, the vendor will have already done a number of installations that will provide a reference. Some vendors may provide equipment from only one company and will push the brand that they provide. It is best to determine what equipment is desired before contacting vendors. The vendor should provide and configure the equipment and conduct any coverage studies that are needed. Be sure to include security configuration in the contract.

It is usually appropriate when contracting for the installation of these types of systems to define performance specifications in the contract. These specifications tie satisfactory system performance to the conclusion and payment of the contract. Performance will be expressed in the terms like, "the ability of the system to connect to a wireless device in certain areas of the facility with a certain signal strength or decibel level." The contract should require testing that proves that the performance is met.

## WLAN

The wireless LAN is installed within the facility. The first consideration in planning such a system is what the application will be such as e-mail, Internet connection, corporate database access, voice, data or audiovisual. A system must be chosen with adequate bandwidth to support the planned applications.

The number of users to be served by the system must also be determined. Some access points share the available bandwidth among multiple users. Depending on the number of users, this can result in slower performance, so the number of users per access point must be considered. More access points may need to be added as the user count increases. Design of the access point type and placement is a combination of the number of users, application requirements and building structure.

The placement of wireless equipment has traditionally been in or on the ceiling, but sometimes wireless access points are mounted in or on the walls or even on desks. Special ceiling panels are available to house wireless equipment. There are plenum-rated access points and antennae, however these may not be acceptable in all jurisdictions due to fire codes.

Early access points were devices that had to be plugged into main power. These devices are still available. Consequently, the installation of an access point involved having an electrician run a new outlet. There is a system of supplying power to devices over the Ethernet data cable. Extra wires, within the data cable, but not used for data, are used to supply DC power to access points. This is referred to as power over Ethernet (POE). In addition to access points, POE is increasingly being used to power devices such as VOIP phones, web cameras, security devices and building management systems. In this system, there are power supplies in the wiring closet that power the distributed devices. The power supplies are either part of the network devices or external devices, eliminating the need for individual AC power circuits at the access points. This puts a large power load in the wiring closet.

Typically, a survey of wireless coverage must be conducted. Building steel, partitions, furniture and other electric equipment can affect the wireless signal in unpredictable ways. Some material can reflect radio waves and cause interference. There is no practical way to fully figure out the facility impact in advance. Normally, a survey is conducted by temporarily installing access points and then walking around with a test device to determine where there is adequate signal strength. The coverage of each point is mapped and additional points are added until the entire desired area is covered. One must be careful that there are no dead spots between access points. Typically the vendor/installer will perform this survey as part of the installation fee. The steps in this design process are:

1. Select initial positions for access points, based upon experience.
2. Test signal strength and move access points or adjust antenna direction as required.
3. Create map of how each access point covers area.
4. Consider number of users per point.
5. Determine if additional points are required.
6. Assign frequencies to access points.
7. Re-check coverage.

The actual installation may involve data wiring, electrical outlets, access points and antenna. It could also include the installation of wireless circuits or Network Interface Cards (NIC cards) in computers. This is typically an IT function. Thus, the installation may involve data wiring contractors, electricians, IT and a wireless vendor. The facility manager may be called upon to act as a project manager in such an installation.

It is important to configure security on the wireless system. Without good security, corporate data is at risk to easy access by hackers. This is normally an IT responsibility.

Training will likely be required for several groups. If the IT department has not worked with wireless before, then the network engineers will have to be trained to administer the system. The help desk will have to be trained to answer user questions and users will have to be trained in the use of the system.

## **PDA**

An organization with a mobile work force might give their field personnel PDAs or tablet devices to communicate to the office about the status of work orders, parts needed or jobs completed. Such an implementation would be a major project for the IT department and could involve the development of custom software. A PDA system installation may or may not involve the facility manager.

By the nature of a system for a mobile field work force, much of it is used outside of the facility. Usually, such a system would be implemented via the cell phone system, but there could be antennae at the facility in some cases. This antenna and associated transmitters and receivers could be located off-site or could be constructed at the central facility. A system of PDAs within a facility, such as a restaurant or maintenance system could have a central antenna or could be implemented via a series of wireless access points.

## **Wireless or Satellite Antenna**

The facility manager may be called upon to install an antenna or satellite dish. Such systems are usually on the roof, although in a campus setting a ground location may be possible. Mounting the antenna on the roof can be a challenge. Obviously, it must be very physically secure. Fortunately, satellite dishes are getting smaller and there is little need to install the six foot diameter dishes of past years. In multi-tenant buildings, the tenant should negotiate rights to install an antenna as part of the lease, even if none is planned upon move-in.

There are two basic methods to installing an antenna. On a flat roof a weighted sled is sometimes used. A sled simply sits on the flat roof and is sufficiently large to spread the weight out. The sled will have weights to keep it from being blown off of the building by the wind. The antenna is mounted to the sled. Engineering input is required on the design and weight of the sled. The advantage of the sled is that there are no roof penetrations involved, hence no opportunity for leaks. The other method is to clamp the antenna to a mast or pole or an existing part of the roof structure if there is any. Sometimes a short mast can be mounted to the parapet wall. For vertical or whip type antenna this is the preferred method of mounting. Point to point wireless antennas (i.e. WiMAX) are often boxes about a foot square and are usually mounted to poles.

Typically a satellite antenna must point to the equator, in North America most satellite antenna need to point south or southwest, but this must be confirmed with the satellite service provider. A suitable location must be found to give the correct line-of-sight to the satellite. Building owners are usually concerned about minimizing the visibility of antenna for aesthetic reasons. In many areas there are building code restrictions on permanent fixtures on the roof. A movable mount is sometimes preferred for this reason. In Europe, dish antennae cannot be permitted to break the skyline or to have a visual impact on an old or preserved building. Depending on the roof configuration, it is often possible to install an antenna that cannot be seen.

When an antenna is mounted on the roof some provision must be made for the antenna wires to enter the building. It is best not to penetrate the roof membrane if possible for waterproofing reasons. Often a conduit can be installed in the parapet wall or in the wall of a mechanical penthouse. If the antenna is installed on the ground, an underground conduit or aerial cable to the building may be required.

With some systems active electronics must be installed near the antenna. A room or closet may be needed near the roof to house this equipment. Whether or not there is active equipment, there must be a cable pathway for the antenna wire to reach the building communication riser to route it to its final destination, usually the computer room.

## Cellular Repeater Systems

Cellular service in certain facilities is poor or non-existent. In these cases a system may be installed to improve service. In multi-tenant buildings, it is often desirable for the repeater system to cover the entire building, rather than just a specific tenant space, although it is possible for an individual tenant to install a repeater system. These systems are fairly expensive and building owners are often reluctant to invest in the systems when no direct revenue will result. Sometimes they try to prorate the cost of the system to the tenants via the lease or a special charge. In these scenarios, the facility manager can become involved in complex negotiations. In single tenant or company-owned facilities the factors involved with installing this type of system are simpler.

There are a number of vendors that supply repeater systems in this rapidly evolving market. Some cell phone companies themselves supply repeater systems. It is usually necessary however, for the system to connect to multiple service providers. An exception might be if an organization has provided cell phones to all employees, in which case there would be a single service provider. Some providers' systems support more than cell phones including wireless LANs and repeaters for two-way radios, like those used for maintenance or security. With rapid evolution of suppliers, the facility manager must survey the alternatives when an implementation is planned.

The repeater system creates a cell within the building. There may be an antenna on the roof to connect to the service provider or there may be a hard-wired connection to the service providers in the basement NetPOP. In a high-rise building, the antenna typically runs up and down the communication riser to serve the core of the building and elevators. The antenna usually radiates out from the core to cover the floors, typically above the ceiling. Plenum ceilings can be complex and add cost. Active devices are banned in plenum ceilings in some jurisdictions.

There may be active equipment in the riser closets on some floors. This is usually not needed on every floor. If there is a hard-wired connection to the service providers in the NetPOP, there will likely be active equipment. If there is a satellite antenna on the roof, there may be a need for active equipment somewhere on the upper floors to connect the satellite to the internal system. Wherever active equipment is installed, the facility manager should expect to supply power and mounting space.

## Maintenance Operations and Support

Maintenance of wireless systems falls heavily on the IT department. Wireless LANs must be maintained in a way similar to other network systems. The IT department must pay particular ongoing attention to security administration. Support for users is generally a training and help desk function which is also typically the role of IT.

As discussed above, the number of users per wireless access point must be limited or bandwidth to each user may be unacceptably reduced. If more users are moved into an area served by wireless, then additional access points may have to be added. The facility manager overseeing the movement of employees within the office should consider the change in user load on the wireless system.

The facility manager needs to be aware that changes in the facility can affect the wireless system. Furniture, partitions, coatings on glass, steel and ceiling tile composition can affect the signal. If a section of the facility is remodeled or changed it is very possible for that remodeling to affect the wireless system. Putting up new partitions, adding heavy equipment, such as air conditioning, adding new furniture and other changes could affect the wireless signal. The facility manager should coordinate with IT before any remodeling begins, so changes to the wireless system can be planned. Although it may not be possible to determine what the impact will be in advance, IT or the wireless vendor should be staged for testing as construction occurs.

Because of the rapid advances in wireless technology, the facility manager should expect to have to change or upgrade their wireless system every few years. It's somewhat difficult to say what the life cycle will be, but three years is the best estimate at this time. The architecture of the systems may also change. It's difficult to determine what the architecture may be three to five years from now.

When it is time to change out a system, the facility manager should expect a project that will be somewhat disruptive. This will probably mean a new coverage survey, selectively removing the drop ceilings, installing power, antennas, data cable, new access points and retraining.

## OTHER WIRELESS CONSIDERATIONS

---

### Installed Life Cycle Costs

The cost of a wireless system is a rapidly moving target, and it can't be said if costs are rising or falling because the equipment is getting more complex. Most people assume that a wireless LAN is less expensive than a wired LAN, yet this is not necessarily true, particularly if one considers the cost of delivering bandwidth that is equal to a wired system. Some of the costs to expect in implementing a wireless LAN system include:

#### Capital Costs

*Cabling:* Backbone cables from the computer room to the wiring room are still required with a wireless system. Some cables from the wiring rooms to wireless devices are also needed. In an existing facility, these components are likely already in place.

*Wireless Access Points:* The access points are the radio transmitters that are the primary components of the wireless system.

*Antennae:* Antennae may be part of the access point or may be separate devices.

*Mounting Devices:* Access points are often installed in the ceiling. Special ceiling tiles or wall mount boxes may be appropriate. In some jurisdictions there are limitations on the installation of active devices in a plenum ceiling or plenum-rated access points may be possible. The laws and building codes must be determined for each jurisdiction.

*Power:* The wireless access points require power. Some must be plugged into electrical outlets requiring the installation of a power outlet at each point. More commonly, the access points are powered through the Ethernet cable and power supplies are required in the wiring room. Power circuits may have to be installed for these power supplies. Individual access points do not draw much power and plug into a conventional outlet. When many pieces of equipment are installed in the wiring closet, the electrical load can accumulate from the multiple devices.

*Wireless Network Interface Cards (NIC Cards):* Individual computers require a circuit for connection to the wireless system called an NIC. Many laptop computers come with wireless NIC cards. If the computers do not have the cards, one will have to be purchased for each computer.

#### Services

*Planning Study:* A survey of wireless point coverage will have to be conducted to determine the number of points and their optimal placement. Typically, this is conducted by the vendor/installer of the wireless equipment, and is part of their overall fee.

*Installation:* Typically, an outside vendor will install the system, although some are installed by the IT department. Usually a vendor has a contract to conduct the planning study, provide the equipment, and install the system, including access points, antenna, power and NIC cards. The vendor also performs the initial configuration and testing, and provides training.

*Electrician:* An electrician may be required for the power and/or data cable installation.

## Operational and Soft Costs

*User Training:* Users of the system will have to be trained. A wireless LAN involves training users how to connect and log-in, otherwise computing is the same as a wired network. A PDA system with custom software could involve very elaborate training.

*IT Staff Training:* IT staff may need training in how to administer the system. In particular wireless LANs have unique security administration requirements that may have to be learned.

*IT Staff Administration Time:* The wireless network must be maintained, like all other parts of the network. In particular the security features must be diligently maintained. Staff must also monitor the system for unauthorized intrusion. The IT staff's ongoing time must be apportioned to the life cycle cost of the wireless system.

*Help Desk Training and Time:* Part of the life cycle cost is the training of the help desk staff with part of their ongoing time apportioned to the life cycle cost of the wireless system. They will get calls when users are unable to connect to the wireless network, or when their connections drop.

The evolution of wireless systems is so fast moving that each installation can be expected to have a short life cycle before demand for a replacement or upgrade occurs. Most of the cost components will occur again with the replacement system. If a proprietary system has been installed, the life cycle can be particularly short. Proprietary systems may have to be replaced as standards-based systems emerge.

## Security Issues

Security has been a weak spot in many wireless LANs, and these systems have a bad reputation for poor security. Hackers drive around and find corporate LANs to tap into from their cars. There is underground information about how to tap into free wireless networks. The unsecured networks of organizations do more than open the Internet to outsiders, they also open the organization's servers and data stores to outsiders as well.

Reasonably comprehensive security features are now built into many new wireless systems. But even the most secure wireless systems can still be broken into by a very skilled hacker. The biggest security problem traditionally is that organizations do not implement the security features that they have. The security features must be implemented, maintained and used. If a system with elaborate security features is purchased, and those features are not turned on, then the enterprise systems are at definite risk of intrusion. Such maintenance typically falls to IT as part of LAN administration and the facility manager has little involvement. A typical office worker today with a wireless card in a computer in a multi-tenant building can access one or more unsecured LANs of other tenants. One would think that all the publicity about underground access to wireless networks would make organizations more security conscious, but this has been slow to develop.

Another common type of problem occurs when employees install unauthorized wireless equipment on networks. Often, when this is done, the security features are not turned on, creating a large network security gap. It is not uncommon for networks to have wireless equipment that IT does not know about. Some IT departments now have technology for detecting unauthorized devices. The facility manager who often tours the facility more than IT staff may be in a position to be more aware of unauthorized systems. The facility manager would well serve the organization by having a collaborative relationship with IT and informing the department of unauthorized devices.

Bluetooth devices are not immune to security problems and it is possible for unauthorized devices to access Bluetooth equipment. PDAs are subject to security issues and viruses. PDAs are also easily lost or stolen and if unsecured, can provide a path into the network. A stolen PDA may have local unsecured data that could be accessed. PDA systems can use encryption and connect to the facility network via a Virtual Private Network (VPN) for added security.

## Health Effects

Wireless is the transmission of information via electromagnetic waves. Are these fields harmful to health? Research is inconclusive, but little impact has been found. We are all subject to low-level electromagnetic fields every day. Our local AM and FM radio stations are bombarding us with a wireless signal all the time. Standing next to a refrigerator or large electric motor subjects one to a greater electromagnetic field than a wireless LAN.

Cell phones are a particular concern, because the phone is held right next to the brain for a prolonged period of time. Research is inconclusive on this matter. Still the possibility of a problem with cell phones exists and radio waves were recently announced as a treatment for some brain problems, so there can be an impact. Radio frequency energy at higher levels than is found in wireless systems can be dangerous. Some argue that since we are unsure about the impact, exposure should be limited, particularly in children.

The preponderance of evidence since 2000 shows no adverse health effects from low level radio frequency waves. However the possibility of some impact particularly from cell phones, has not been completely ruled out. Direct exposure to high power microwave radiation may be a problem, and a microwave transmitter should not be installed close to occupied space. Both the Federal Communications Commission and OSHA in the United States have formulas to calculate the safe distance.

## Conclusion

The biggest challenge with wireless is to look ahead. Wireless technology is developing quickly and there are many complex forces shaping its future. The facility manager must be prepared for the future, yet the future evolution of wireless systems is not clear. We have made educated projections about how it will impact the facility, but this could change rapidly. Facility managers should keep up with new developments in this area. It is also important to not get caught up in the hype involved with wireless.

Wireless can be a fantastic business asset, but its limitations must be admitted. There will be a role for wired infrastructure for some time. Keeping up with the evolution of wireless standards is also important, as organizations are always better off with standards based-systems.

## Appendix 1: Wireless Standards

---

There are a number of standards for wireless systems that the facility manager may hear about in dealing with the systems. There are several standards groups, but the Institute for Electrical and Electronic Engineers (IEEE) has developed many of the wireless standards. Following is a brief overview of some of those standards:

Standard	Bandwidth (Theoretical Maximum, not Always Achieved)	Frequency Band	Note	Status
802.11	2 Mbps	2.45 GHz		
802.11a	54 Mbps	5.8 GHz	Limited implementations. Frequencies vary across the world.	Standard Ratified in 1999.
802.11b	11 Mbps	2.45 GHz	Most common installation. Most Internet hot spots use this installation.	Standard Ratified in 1999.
802.11e			Addresses quality of service for wireless VOIP.	
802.11g	54 Mbps	2.4 GHz	Backward Compatible with 802.11b.	
802.11i			Enhanced Security.	
802.11n	108 Mbps			In Development. Products expected in 2007.
802.16 (WiMAX)	70 Mbps		Range of up to 30 miles.	

## Appendix 2: Glossary of Terms and Definitions

---

**Access Point:** A radio transmitter and receiver that transmits and receives information between a wireless device, such as a wireless LAN card or PDA, and a wired network.

**Backbone:** A hard-wired network cable, usually copper or fiber, that connects a computer room to wiring rooms, sometimes called vertical cables. These cables carry the signal of many devices and usually operate at high transmission rates.

**Bandwidth:** The amount of information that can be transmitted in a unit of time.

**Bluetooth:** A short-range wireless network technology intended to replace cables between user devices such as a keyboard connection to a PC.

**Channel:** A section of the radio spectrum intended for a specific radio transmission purpose.

**Encryption:** The process of scrambling information so that it is not easily decrypted by third parties listening in on a transmission. Usually a code or key is used to encrypt and decrypt.

**Ethernet:** The standard protocol for data transmission on a network both wired and wireless.

**FCC:** (U.S. Federal Communications Commission) U.S. government agency that regulates most wireless technology.

**Frequency:** The radio or wireless spectrum is made of many frequencies. In order to create a wireless or radio signal, the transmitter creates a signal that oscillates or varies at a given frequency. Thus, the frequency of an AM radio station might be 89 kilocycles (899 thousand cycles per second) and an FM radio station might be 91 megacycles or (91 million cycles per second).

**Frequency Hopping:** The wireless device operates by rapidly changing frequencies, a technique to minimize interference.

**GHz:** (Gigahertz) 1 GHz = 1 billion cycles per second; a measure of radio frequency.

**Gbps:** (Gigabits per second) A measure of bandwidth. 1 Gbps = 1 billion bits per second.

**GPRS:** (General Packet Radio Service) A standard for transmitting data via cell phones and other wireless devices.

**IEEE:** (The Institute of Electrical and Electronics Engineers) An organization that sets standards for network and wireless technology.

**MAC Address:** (Media Access Control) An identification number of a PC or other device used for security control in small WLANs.

**Mbps:** (Megabits per second) A common measure of bandwidth. 1 Mbps = 1 million bits per second.

**MHz:** (Megahertz) 1 MHz = 1 million cycles per second; a measure of radio frequency.

**NetPOP:** A room usually in the basement for termination of service entrance cables from a telecommunications service provider.

**PAN:** (Personal Area Network) A short-range computer network for connecting devices such as laptops, printers and cameras often via Bluetooth.

**PDA:** (Personal Digital Assistant) A handheld device that may have a wireless connection such as a Palm Pilot or Blackberry.

**Plenum Ceiling:** An interstitial space where the cavity above the drop ceiling is part of the ventilation system (air plenum). This is significant to the installation of cable and wireless devices in the ceiling, as there are fire codes in many jurisdictions about what can be installed in such a ceiling.

**Receiver:** A device for receiving a wireless transmission that may also amplify or process the signal.

**RF:** (Radio Frequency) Radio waves or wireless, a form of electromagnetic energy.

**Satellite:** A device launched and orbiting the earth. Satellites for wireless systems are designed to send and in some cases receive wireless signals from the earth.

**SMS:** (Short message service) A system for sending short text messages, up to 160 characters, on handheld wireless devices.

**Spread Spectrum:** A type of radio transmission that uses a wide section of the radio spectrum; a technique for minimizing interference.

**SSID:** (Service Set Identifier) A security technique for wireless LANs.

**Station Cables:** Hard-wired cable from wiring room to workstation, sometimes called horizontal cables. These cables carry the signal of one or two devices including wireless access points and usually operate at slower speeds than backbones.

**Tablet Device:** A type of wireless handheld device where the user can write, draw or select buttons on the screen with a stylus.

**Transmitter:** A device for transmitting wireless signals.

**UHF:** (Ultra High Frequency) A section of the radio spectrum from 300 MHz to 3 GHz.

**VHF:** (Very High Frequency) A section of the radio spectrum from 30 MHz to 300 MHz.

**VOIP:** (Voice Over Internet Protocol) Often confused with voice over Internet, VOIP is really voice over a local area network which uses Internet Protocol (IP). VOLAN would have been a clearer term. The confusion is additionally caused by the fact that the Internet is now often used for long distance rfvoice service.

**VPN:** (Virtual Private Network) A type of software for creating a secure connection from a mobile computer to a network via the Internet.

**WAP:** (Wireless Application Protocol)

**WEP:** (Wired Equivalent Protocol, also WEP2) A security encryption protocol for wireless networks.

**WLAN:** A Wireless Ethernet Local Area Network.

**WPA:** (Wi-Fi Protected Access) A Wi-Fi security protocol.

**Wi-Fi:** Short for wireless fidelity; this is a term for 802.11 wireless networks (originally for 802.11b). This is the most common wireless standard and is used in Internet hot spots. However, this term is now so wide-spread in the public that it is sometimes used to refer to any wireless network.

**Wi-Max:** New standard for wireless point to point system.

**WLAN:** (Wireless Local Area Network)

**WMAN:** (Wireless Metropolitan Area Network)

**WMTS:** (Wired Medical Telemetry Service) Area of the radio spectrum set aside for medical systems.

## **If you find this publication useful, there is something you should know...**

This publication was made possible by the support of people like you through the IFMA Foundation.

Established in 1990 as a non-profit, 501(c)(3) corporation, and separate entity from IFMA, the IFMA Foundation works for the public good to promote priority research and educational opportunities for the advancement of facility management. The IFMA Foundation is supported by the generosity of the FM community including IFMA members, chapters, councils, corporate sponsors and private contributors who share the belief that education and research improve the FM profession.

By increasing the body of knowledge available to facility professionals, the IFMA Foundation advances your profession and career potential.

**Contributions to the IFMA Foundation are used to:**

**Underwrite research – to generate knowledge that directly benefits the profession**

**Fund educational programs – to keep facility managers up-to-date on the latest techniques and technology**

**Provide scholarships – to educate the future of the facility management profession**

Without the support of workplace professionals, the IFMA Foundation would be unable to contribute to the future development and direction of facility management. That's why we need your help. If you are concerned with improving the profession and your career potential, we encourage you to make a donation or get involved in a fund-raising event. After all, isn't the future of facility management and your career worth your support?

To learn more about the good works of the IFMA Foundation, visit [www.ifmafoundation.org](http://www.ifmafoundation.org).



**IFMA FOUNDATION**  
Research • Scholarships • Education

**IFMA Foundation  
1 E. Greenway Plaza, Suite 1100  
Houston, Texas 77046  
(281) 974.5600  
[www.ifmafoundation.org](http://www.ifmafoundation.org)**

©2005 IFMA Foundation All rights reserved. ISBN 1-883176-61-1

Copyright and photocopying: Because this report is copyrighted, one must obtain permission to copy from the Copyright Clearance Center (CCC), 222 Rosewood Drive, Danvers, Mass. 01923. CCC's phone number is (978) 750-8400; fax number is (978) 750-4470. There is a nominal charge payable to CCC to photocopy any page herein for personal or internal reference use. Unauthorized duplication or use of the information and/or contents herein without express written authorization of IFMA Foundation is strictly prohibited.



IFMA FOUNDATION  
Research • Scholarships • Education

The IFMA FOUNDATION would like to thank all the members of the Corporate Circle of Contributors for their sponsorship of this research report. Their generous support help to make the Foundation's research initiatives possible.

**IFMA FOUNDATION  
CORPORATE CIRCLE OF CONTRIBUTORS**

Allsteel®

Designed to work. Build to last.

Antron®  
carpet fiber

Milliken Contract

**Steelcase**