Chapter 1
Introduction to Wireless Design

Chapter 1 introduces technical and business concepts related to wireless design. The importance of quality, speed, environment, and aesthetics is discussed. Also identified are the costs, security, risks, and liability. An overview of wireless services and applications is also presented.
# Table of Contents

**General Wireless Design Considerations** ..................................... 1-1

- Technological Considerations .................................................. 1-1
  - Scalability ............................................................................ 1-1
  - Compatibility ....................................................................... 1-1
  - Standardization .................................................................... 1-1

- Business Considerations ............................................................. 1-1
  - Applications ........................................................................ 1-1
  - Coverage ............................................................................. 1-2
  - Flexibility ............................................................................ 1-2
  - Long-Term Growth ................................................................ 1-2
  - Security ............................................................................... 1-2

- Quality ....................................................................................... 1-2
  - Customer Satisfaction versus Investment ............................ 1-2
  - Quality of Service (QoS) ....................................................... 1-2

- Reliability .................................................................................. 1-3
  - Accessibility ......................................................................... 1-3
  - Continuity ............................................................................. 1-3
  - Consistency .......................................................................... 1-3

- Speed/Throughput ...................................................................... 1-3
  - Application Requirements ................................................... 1-3
  - Number of Users ................................................................... 1-3
  - Future Requirements .............................................................. 1-4
  - Product Quality .................................................................... 1-4

- Aesthetic Considerations ............................................................ 1-4

- Environmental Considerations .................................................. 1-4
  - Material Effects ..................................................................... 1-4
  - Indoor Environment ............................................................... 1-5
  - Outdoor Environment ............................................................. 1-5

- Potential for Revenue Generation .............................................. 1-6
  - Contributors to Revenue Generation .................................... 1-6
  - Case Studies in Mobile Revenue Generation ....................... 1-6

- Initial Cost .................................................................................. 1-7
  - Technology ........................................................................... 1-7
  - Coverage/Distance ............................................................... 1-7
  - Bandwidth ............................................................................. 1-7
Chapter 1: Introduction to Wireless Design

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>1-7</td>
</tr>
<tr>
<td>Return on Investment</td>
<td>1-8</td>
</tr>
<tr>
<td>Identifying Costs</td>
<td>1-8</td>
</tr>
<tr>
<td>Identifying Benefits</td>
<td>1-8</td>
</tr>
<tr>
<td>Realizing Return on Investment</td>
<td>1-8</td>
</tr>
<tr>
<td>Security</td>
<td>1-9</td>
</tr>
<tr>
<td>Hardware and Freeware</td>
<td>1-9</td>
</tr>
<tr>
<td>Forms of Attack</td>
<td>1-9</td>
</tr>
<tr>
<td>Future Defenses</td>
<td>1-10</td>
</tr>
<tr>
<td>End User Benefits and Fears</td>
<td>1-10</td>
</tr>
<tr>
<td>Security</td>
<td>1-10</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>1-10</td>
</tr>
<tr>
<td>Health and Safety</td>
<td>1-10</td>
</tr>
<tr>
<td>Reliability</td>
<td>1-10</td>
</tr>
<tr>
<td>Rapid Deployment</td>
<td>1-11</td>
</tr>
<tr>
<td>Ease of Installation</td>
<td>1-11</td>
</tr>
<tr>
<td>Licensed versus Unlicensed</td>
<td>1-11</td>
</tr>
<tr>
<td>Technology</td>
<td>1-11</td>
</tr>
<tr>
<td>Temporary Network Coverage</td>
<td>1-11</td>
</tr>
<tr>
<td>Risk of Using Unlicensed Spectrum</td>
<td>1-11</td>
</tr>
<tr>
<td>Federal Communications Commission (FCC), Title 47, Part 15</td>
<td>1-12</td>
</tr>
<tr>
<td>Protocols</td>
<td>1-13</td>
</tr>
<tr>
<td>Public Liability</td>
<td>1-13</td>
</tr>
<tr>
<td>Core Responsibility of the Federal Communications Commission (FCC)</td>
<td>1-13</td>
</tr>
<tr>
<td>Current Regulations and Interference Definitions</td>
<td>1-13</td>
</tr>
<tr>
<td>Long-Term Strategy</td>
<td>1-13</td>
</tr>
<tr>
<td>Frequency Reform</td>
<td>1-14</td>
</tr>
<tr>
<td>Federal Communications Commission (FCC)</td>
<td>1-14</td>
</tr>
<tr>
<td>Legislative Reform</td>
<td>1-14</td>
</tr>
<tr>
<td>Anticipated Industry</td>
<td>1-15</td>
</tr>
<tr>
<td>Global Harmonization</td>
<td>1-15</td>
</tr>
<tr>
<td>Potential Technology Obsolescence</td>
<td>1-16</td>
</tr>
</tbody>
</table>

**Services and Applications** .................................................. **1-17**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leased Line Alternative and Local Loop Bypass</td>
<td>1-17</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>1-17</td>
</tr>
<tr>
<td>Total Network Ownership</td>
<td>1-17</td>
</tr>
<tr>
<td>Redundancy</td>
<td>1-17</td>
</tr>
<tr>
<td>Limitations</td>
<td>1-17</td>
</tr>
</tbody>
</table>
Comparison with Cabled Infrastructure .......................................... 1-17
Cost Comparison ................................................................. 1-18
Ease of Installation .......................................................... 1-18
Performance ................................................................. 1-18
Wireless Data Applications .................................................. 1-18
Warehouse Data Collection .................................................. 1-19
Retail Service ........................................................................ 1-19
Office Environments .......................................................... 1-19
Education .............................................................................. 1-19
Health Care ........................................................................... 1-20
Emergency Notification Systems ......................................... 1-20
Voice over Wireless LAN (VoWLAN) ......................................... 1-20
Quality of Service (QoS) .......................................................... 1-21
Roaming ................................................................................ 1-21

Tables

Table 1.1 Expansion to unlicensed spectrum .................................... 1-12
General Wireless Design Considerations

Numerous factors must be considered before designing a wireless system. While all design considerations may not apply in every instance, they should be addressed for each project. Many of these considerations should be discussed with the client before making any formal recommendations for a wireless solution.

Technological Considerations

Technological considerations in the design of a wireless network include:

- Scalability.
- Compatibility.
- Standardization.

Scalability

The scalability of the network always should be addressed in the initial design. This includes analyzing the number of current users and considering any potential future users. Consider any potential system upgrades, and design a plan for growth.

Compatibility

Overall network compatibility should be addressed. Ensure that the proposed system integrates with the current network. Consider other nearby wireless systems and their potential for interference.

Standardization

A wireless network based around standards is preferable to a proprietary system that ties the design to any one vendor or technology. Because there are many wireless standards from which to choose, consider backward compatibility as well as present and future acceptance.

Business Considerations

Business considerations in the design of a wireless network include:

- Applications.
- Network coverage.
- Network flexibility.
- Long-term growth.
- Network security.

Applications

Because wireless applications can have many different uses on a network, first determine the various applications involved. These can include data collection, point of sale (POS), wireless local area networks (WLANs), building-to-building connectivity, wireless voice, and wireless video services.
Chapter 1: Introduction to Wireless Design

Business Considerations, continued

Coverage

Consideration must be given regarding what it will take to implement a wireless system within a facility or campus environment.

Flexibility

While also a technological consideration, the flexibility of the wireless network should be addressed from a business perspective. Questions to consider include:

- What applications will run on this network?
- Who can access the network?
- Can existing systems integrate with this network?

Long-Term Growth

The long-term growth of the wireless system should be considered. This includes sustained growth, compatibility with future applications, and operational growth issues.

Security

The security of the network must be considered. While all wireless networks should be designed for the secure transfer of information, the degree of security should be determined for each individual organization. This normally is dictated by how much the organization is willing to invest to protect the information. Additional security factors include who is allowed access, where they are allowed access, and what level of access is allowed.

Quality

Customer Satisfaction versus Investment

Customer satisfaction and the investment level of the wireless network should be balanced to achieve optimum quality.

The high demands of a wireless network require more services than ever before. If rapid growth is not managed correctly, excessive investment could result in higher costs and lower profits with no visible customer benefit in quality.

Quality of Service (QoS)

A clear quality of service (QoS) program can effectively create the balance between the end user and the wireless network performance. Network management tools should be considered for proper utilization of bandwidth on a per user per application basis. Prioritization for services (e.g., voice and video over a wireless Internet protocol [IP] network) can be handled via hardware or software for QoS. Ensure that the latest QoS standards are supported in the system design.
Reliability

The reliability of a wireless network can be defined by the system’s accessibility, continuity, and consistency of service.

Accessibility

The customer’s ability to immediately access the network is the desired service level. However, remote locations (e.g., underground parking garages, moving trains) can degrade or block access to the wireless network.

Acceptable access is sometimes a compromise between the user’s demand for access and the wireless network’s ability to expand services to these and other remote locations.

Continuity

Continuity reflects the network’s ability to continuously provide service. As dropped calls or dropped network sessions increase, the overall system reliability decreases. The system design should include roaming between wireless cells with few or no gap areas.

Consistency

Reliability also is measured by the wireless system’s consistency in maintaining voice or video quality from one session to the next.

Consistency in the minimum data rate as well as minimizing the bit error rate (BER) with each transmission is another measure of a wireless system’s reliability.

Speed/Throughput

Speed or throughput is of great concern in a wireless design. Examine the application requirements, number of users, future requirements, and quality of the product in the design.

Application Requirements

The numerous services and applications that run over a standard cabled network also apply to a wireless environment. Different services and applications require differing amounts of bandwidth and response speed to run at optimum efficiencies. This is an important aspect to include when planning a wireless network.

Number of Users

In addition to the applications being run, the number of users on either side of the wireless link or wireless network often determines the speed or throughput of the desired connectivity method. This is because many wireless services are sharing bandwidth at limited capacities.
Chapter 1: Introduction to Wireless Design

Speed/Throughput, continued

Future Requirements

There are also future issues to address regarding throughput. While 11 megabits per second (Mb/s) was considered adequate for many instances several years ago, a data rate of 54 Mb/s is now considered the minimum, with upcoming standards promising 300 to 600 Mb/s as the new standard for WLAN design. High-bandwidth applications (e.g., wireless video, voice over IP [VoIP] over wireless, database distribution) are being deployed now and will continue to be a factor.

Product Quality

In the wireless industry, many products vary in their throughput performance. The quality of the product specified has a large impact on the quality of the network. This affects not only the throughput in wireless but also the reliability of the network.

Aesthetic Considerations

The design of a wireless network must include its impact on the aesthetics of the environment. Although radio communications towers have a limited impact on the physical environment (e.g., footprint), the towers themselves may have a high impact on the visible environment. While location is crucial for most wireless transmission mediums, the wireless designer must consider scenic and historic sites when planning tower locations, thereby preserving the integrity of sensitive areas.

Building rooftops are another available alternative to a tower. However, even high-rise buildings have specific aesthetic requirements for mounting antennas and other external equipment.

For indoor wireless networks, consider low-profile antennas and plenum-rated equipment mounted above the drop ceiling. Power over Ethernet (PoE) can provide the flexibility to minimize the visual exposure of wireless equipment.

Environmental Considerations

When deploying wireless networks, thoroughly evaluate the environment in which it will be used. This evaluation can be performed through a site survey, propagation analysis, or modeling. Materials, objects, local geography, and atmosphere can affect wireless communications. These factors should be considered when designing a wireless system to help ensure it functions properly.

Material Effects

Different materials can affect wireless communications to varying degrees. Depending on the material composition and frequency being used, wireless signals can be reflected, inhibited, or altogether blocked.
Environmental Considerations, continued

Wireless communications use electromagnetic waves. Generally, lower frequency radiation will penetrate objects better, and higher frequency ranges tend to require line of sight (LoS). The material through which the electromagnetic waves must travel can affect somewhat the effective range. Knowing the characteristics of the wireless medium and how it will interact with the local environment is vital.

**Indoor Environment**

The indoor environment can be challenging for wireless network installation due to the wide variety of materials and objects present.

Everything from the walls of the structure to the contents of the space and the people occupying the space can affect wireless systems. These obstacles should be accounted for in the wireless design, and appropriate steps should be taken to minimize their effect.

The building structure is the basic concern in any indoor space. Solid structural materials like steel and reinforced concrete tend to be less permeable to wireless signals. Specific locations where these building elements are almost always present include stairwells and elevator shafts. Lighter materials like drywall and wood generally cause less signal attenuation.

The contents of the indoor spaces (e.g., furniture, bookshelves, miscellaneous room materials) also may adversely affect wireless communications. Items like steel filing cabinets or metallic cubicles can block and reflect wireless signals. Large shelves filled with books, particularly in library type environments, can cause severe signal attenuation in some wireless systems.

The intended use of the space and number of people it will hold should be taken into account when designing a wireless system. Not only is the number of people important for capacity planning, but the density of the population also can inhibit wireless signals.

**Outdoor Environment**

Outdoor wireless systems, although not bound by the same concerns as the indoor environment, carry their own unique concerns. Trees, buildings, and weather can affect signal propagation and quality. The outside environment should be evaluated for any potential problems.

Trees, bushes, and other organic growth can affect outdoor wireless communications to varying degrees depending on the frequency being used. They can inhibit signal propagation by causing attenuation and signal scatter. Their presence should be accounted for in areas where wireless installations are planned. A site survey should be performed to determine their effect on signal strength and integrity.

The potential for seasonal growth also is a consideration. A survey conducted in the fall may be drastically different from a survey performed in the spring or summer. The presence of rain or snow is a consideration as trees and bushes holding a quantity of water can have a greater negative impact on wireless systems.
Chapter 1: Introduction to Wireless Design

Environmental Considerations, continued

In the higher frequency ranges, a building obstructing the LoS to the wireless transmitter can completely block wireless signals. At lower frequencies, the same building may reflect the signal. Building windows can have various effects on wireless signals. Tinted windows in particular can reflect, attenuate, or completely block a wireless signal from passing through. This is especially important to keep in mind when implementing a wireless transmitter that will be located inside but is intended to cover outside areas (or vice versa).

Environmental conditions (e.g., rain, snow, fog) can affect wireless communications. The degree to which they can affect the signal depends on the frequency of the wireless system being used and the distance the signal must travel. High winds also may affect antennas and should be accounted for when mounting antennas in areas prone to high wind.

Potential for Revenue Generation

With the unprecedented deployment of wireless networks throughout a variety of industries, the potential for revenue generation can be different for each company.

Contributors to Revenue Generation

The most notable and best-documented contributor to revenue generation is the increase in sales productivity. The more freedom and access to information a mobile sales force has the greater the potential for sales in the field.

Improved customer care service also is realized because wireless communications in the field enable quicker responses to customer demands.

Increased operational efficiency lends to revenue generation as well, for the processes involved ensure prompt delivery of products to complete a user’s order.

Case Studies in Mobile Revenue Generation

Many white papers published recently from diverse industries document how a wireless network has improved sales and customer service. A few examples include the following:

- One of the largest supermarkets deploys handheld devices to its large-volume customers, allowing them to place grocery orders via a wireless connection.
- A hospital places orders through use of a wireless network to restock its operating rooms and labs with lifesaving equipment as it is used and pulled from the shelves.
- Several major airlines are competing for repeat business travelers by providing them with up-to-the-minute travel information, departures/arrivals, and gate information through a wireless network to the traveler’s handheld device.

It can be difficult to predict how much revenue wireless technology will generate, but it is clear that many industries have already begun to embrace, challenge, and meet their customers’ demands with new conveniences to improve quality of life.
Initial Cost

Many factors affect the initial cost of a wireless system. Areas that must be considered are technology, coverage/distance, bandwidth, and security.

Technology

A wireless solution can incorporate many current technologies. Some require licensing and are guaranteed interference free, while others are free to use but have interference issues that need to be considered. Unlicensed products built around standards (e.g., Institute of Electrical and Electronics Engineers, Inc.* [IEEE®] 802.11) provide a more economical solution where cost will continue to decrease over time.

Coverage/Distance

Generally, the greater the coverage or distance, the more expensive the system. More powerful equipment, higher-gain antennas, and higher-grade cables will be required for longer distances. Additionally, large towers may be required to provide extended range. Whether leasing space on an existing tower or building one, the additional cost is a factor in the design. Local zoning issues also may need to be considered.

Bandwidth

Like most networking systems, wireless networks become more expensive in direct relation to the amount of bandwidth provided. However, the price of wireless networking equipment has dropped dramatically due to standardization and the increased usage of the technology.

Security

Security is a major concern with wireless. Depending on the wireless technology involved, the security features built into the product may or may not be adequate. For example, wireless fidelity (WiFi) equipment comes with these security features deactivated, leaving it up to the individual or customer to establish their own security policy. While these standard features included with the equipment have improved over recent years to address weak encryption schemes, they still may not provide adequate security of the wireless network by themselves for many organizations.

To institute higher levels of security, third-party products are often required, which add to the overall project cost. New standards are now being adopted for security, which will drive down cost. However, the cost will always increase incrementally with the level of security desired.

There are security services that can provide added value to the owner of a WLAN installation. Software and hardware solutions are available that require authentication prior to obtaining access to the WLAN. These solutions also can require adherence to predefined policies such as minimum operating system patch level and minimum antivirus software versions and virus definitions. Another value-added hardware and software solution is wireless intrusion detection and prevention. These systems can detect and even disable rogue access points (APs) on the network.
Return on Investment

A major concern of any organization before implementing a wireless network or infrastructure is the ability to realize a return on investment.

Identifying Costs

Costs can be separated into two categories—direct costs and indirect costs.

Direct costs are items usually found in a traditional information technology (IT) budget, including:

- Hardware/software.
- Operations.
- Administration.
- Installation/construction.

Indirect costs are generated from forces external to the traditional IT budget, including:

- Network downtime.
- Initial disruption to end user operations.

Identifying Benefits

Like identifying costs, benefits also are separated into two categories—hard benefits and soft benefits.

Hard benefits (e.g., lower networking costs) will be realized if the wireless network is planned thoroughly and implemented properly.

Soft benefits can include intangible items, such as greater flexibility allowing employees to work where and when they want. This can lead to other benefits, including greater employee satisfaction, increased productivity, and faster decision making.

Realizing Return on Investment

In some cases, it may not take many users to pay for the infrastructure, and the breakeven point occurs relatively early in a wireless deployment.

As a company adds users to the wireless network, the cost per user drops. In turn, however, the benefit per user may drop as more users are added to the network. This inverse relationship occurs because wireless technology is usually deployed first to the users who will gain the most benefit from their new mobility.

However, each organization, regardless of its industry, will realize a return on investment with the productivity and flexibility the wireless network will provide its end users.
Security

Volumes of information on security within and for a wireless system are available not only to the IT management looking to secure the network but also to hackers.

WLAN is the most commonly victimized system due to its standardized nature and affordable equipment. At times, it appears that no sooner is a new wireless security standard released than hackers are quickly breaking the barriers and gaining access to the networks. While there are many ways to build security into a wireless network, the wireless designer should understand the various methods of intrusion and forms of attack.

Hardware and Freeware

Hardware and readily available freeware and techniques make intrusion easy for even novice hackers.

Freeware

New WLAN hacking tools (e.g., software, instructions) are introduced daily and are widely available on the Internet for free. These simple tools are commonly used with the intent to attach to the network as an entry point for free high-speed Internet access but also can be a means to vandalism, network disruption, or corporate espionage.

Antennas

A hacker can attach a commercially available long-range antenna to a wireless network interface card (NIC) to pick up IEEE 802.11 signals up to 610 meters (m [2000 feet (ft)]) away while sitting in a concealed parking lot or out of sight.

War Driving

A hacker driving around a city with a laptop, a wireless NIC, and packet sniffing software can discover unprotected airwaves that broadcast the wireless network identification information and offer an easy way into the network.

Forms of Attack

Four major forms of published attacks indicate the susceptibility of a vulnerable network that even an unsophisticated hacker can easily perform after downloading the right tools:

- Malicious association—The unsuspecting station is forced or tricked into connecting to a malicious AP or eavesdropping station.
- Identity theft—An authorized network user’s media access control (MAC) address is easily identified by a hacker, who then assumes the identity and connects to the WLAN.
- Man in the middle—A malicious station is inserted between a station and an AP, tricking each station into correctly identifying the other station.
- Denial of service—Hackers access the network through a vulnerable point and transmit a dissociation command, causing the shutdown of a portion or the entire network.
Security, continued

**Future Defenses**

From man in the middle to identity theft, each new attack presents the wireless industry with new challenges to make this ever-emerging technology more secure, allowing freedom of use without the worries of intrusion.

As standards evolve and vulnerabilities are identified, the ratio of attacks could dramatically decrease. However, hackers will always find more sophisticated means of intrusion and ways to break through the latest barriers, forcing new approaches to security. A wireless design consultant should be aware of the latest attacks and vulnerabilities to advise clients on how to defend against them.

**End User Benefits and Fears**

End users have many benefits and fears associated with employing wireless technology as opposed to a traditionally cabled solution, which should be considered when designing the wireless system.

**Security**

Security is a great concern of end users that should be considered when designing wireless solutions. Generally, there is a trade-off between the level of security and the ease of use to end users. The wireless designer must determine the degree of security necessary that will still provide ease of use for end users.

**Bandwidth**

End users are accustomed to the bandwidth and high speed of the cabled network and are generally unwilling to sacrifice network speed for mobility. A wireless system should be designed to provide equivalent or greater bandwidth to end users than their current cabled system.

**Health and Safety**

The safety of wireless equipment is a concern of end users, especially with the advent of ever-stricter health and safety polices demanded at commercial, national, and international levels. In addition to manufacturer specifications, design the wireless system in accordance with the Federal Communications Commission (FCC) or local codes and regulations to minimize health concerns.

**Reliability**

Reliability is another end user concern associated with wireless technology. This likely stems from the lack of a tangible connection, as found in a cabled solution. Designing a wireless system with an intuitive graphical user interface on the client device will minimize trouble calls that are due to network problems outside the wireless infrastructure.
Rapid Deployment

Virtually all wireless systems offer rapid deployment. However, some equipment and technologies can be deployed faster and easier than others.

Ease of Installation

Some wireless equipment may require a secure mast for mounting, while others may simply be positioned on the side of an existing structure. The location of the wireless equipment with regard to existing infrastructure (e.g., power and data connection points) will impact the ease of installation for a wireless solution. This in turn will affect the time of deployment for a solution.

Licensed versus Unlicensed

Depending on the country, various radio frequency (RF) bands either are required by law to be licensed or reside in the license-free spectrum. The frequency chosen along with the country of deployment’s regulations therefore determine whether a wireless link can be established without notice. Unlicensed systems can be deployed in a matter of hours or days as opposed to a licensed solution that, in most cases, is subject to approval prior to installation.

Technology

As mentioned, technology is a factor in the speed of deployment, as the wireless solution may or may not need to be licensed before installation. Different technologies may require different mounting procedures, antenna types, cable accessories, and placement considerations. These factors can either speed up or slow down the deployment process.

Temporary Network Coverage

A wireless solution often can be used as an alternative to a cabled solution for temporary network coverage. These include hotel conventions and conferences, workshops, seminars and lectures, festivals and fairs, concerts, and many other short-term events.

They also can replace a leased line alternative for building-to-building connectivity. Portable classroom buildings, construction sites, and emergency tents are all examples of temporary wireless links, which can be set up quickly and moved as needed.

Risk of Using Unlicensed Spectrum

Within the United States, by definition, unlicensed spectrum devices are permitted to emit RF without any specific authorization, registration, or grant to guard against harmful interference. Rules for the unlicensed use of RF are contained in the FCC Code of Federal Regulations, Title 47, Telecommunication, Part 15: Radio Frequency Devices.
Risk of Using Unlicensed Spectrum, continued

Federal Communications Commission (FCC), Title 47, Part 15

The basic premise of Part 15 unlicensed operations is that unlicensed devices cannot cause interference to licensed operations, nor are they protected from any interference they receive.

Three types of unlicensed devices exist under Part 15:

- Intentional radiators—These devices, by design, intentionally generate and emit RF energy by radiation or induction. They include cordless telephones, remote control toys, and WLAN equipment.
- Unintentional radiators—These devices generate RF energy within the device but are not intended to emit RF energy by radiation or conduction. They include PCs, printers, disk drives, and other digital devices with internal clocks or circuitry for timing.
- Incidental radiators—These devices generate RF energy during the course of their operation but are not intentionally designed to generate or emit energy. They include motors and generators.

Part 15 rules have been amended to provide new opportunities for unlicensed operations, including additional frequency bands for unlicensed use.

Table 1.1 depicts the expansion to the unlicensed spectrum within the past two decades.

### Table 1.1
Expansion to unlicensed spectrum

<table>
<thead>
<tr>
<th>Bands</th>
<th>Year Authorized</th>
<th>Frequencies (MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial, scientific, and medical/spread spectrum</td>
<td>1985</td>
<td>902–928, 2400–2500, and 5725–5875</td>
</tr>
<tr>
<td>Unlicensed personal communications system</td>
<td>1993</td>
<td>1910–1930 and 2390–2400</td>
</tr>
<tr>
<td>Millimeter wave</td>
<td>1995</td>
<td>59,000–64,000</td>
</tr>
<tr>
<td>Unlicensed National Information Infrastructure (U-NII)</td>
<td>1998</td>
<td>5150–5350 and 5725–5825</td>
</tr>
<tr>
<td>Millimeter wave expansion</td>
<td>2001</td>
<td>57,000–59,000</td>
</tr>
<tr>
<td>U-NII expansion</td>
<td>2003</td>
<td>5250–5450</td>
</tr>
<tr>
<td>World Radio Conference</td>
<td>2003</td>
<td>5470–5725</td>
</tr>
</tbody>
</table>
Risk of Using Unlicensed Spectrum, continued

Protocols

There are currently mandatory protocols in Part 15 that many industry analysts have attributed to as causing the limitation of growth in certain areas. However, industry groups such as the IEEE have developed, and continue to develop, voluntary protocols for certain types of unlicensed devices. These changes will evolve as the market is enhanced by the FCC’s new approach to the unlicensed spectrum regulations. Further, the new market-based approaches on spectrum management are a result of the FCC’s Spectrum Policy Task Force (SPTF) recommendations to be flexible and encourage technological solutions that optimize the efficient use and sharing of the spectrum.

Public Liability

Core Responsibility of the Federal Communications Commission (FCC)

The core responsibility of the FCC and its SPTF has been interference protection, which is critical in effectively managing the spectrum. The vital issue is electromagnetic interference (EMI) that, if not properly managed, could affect spectrum users from simple annoyance to harm, whether economic or life safety.

Current Regulations and Interference Definitions

Current regulations define limits in band transmitter power and out-of-band emission for the majority of the spectrum. There is much debate whether the current definitions of interference are still valid in this ever-increasing spectrum marketplace.

The FCC defines four rules of interference:

• Interference—The effect of unwanted energy due to one or a combination of RF emissions, radiation, or induction upon reception in a radio communications system, manifested by any performance degradation, misinterpretation, or loss of information that could be extracted in the absence of such unwanted energy

• Harmful interference—Any emission, radiation, or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio communications service

• Permissible interference—Observed or predicted interference that complies with quantitative interference and sharing criteria contained in specific radio regulations

• Accepted interference—Interference at a higher level than that defined as permissible interference and that has been agreed upon between two or more administrations without prejudice to other administrations

Long-Term Strategy

Long-term strategy involves the quantification of acceptable interference within the unlicensed spectrum, along with an interference management plan. This will be vital as consumer demand grows within the spectrum.
Chapter 1: Introduction to Wireless Design

Frequency Reform

Federal Communications Commission (FCC)

The FCC is an independent U.S. agency directly responsible to Congress. It was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite, and cabling.

The FCC’s Office of Engineering and Technology (OET) and Office of Strategic Planning and Policy Analysis (OSP) are continuously studying the frequency spectrum and proposing recommendations for an orderly approach to its growth.

Office of Engineering and Technology (OET)

The core mission of the OET is to manage the spectrum and create new opportunities for competitive technologies through its leadership and expertise. The OET also advises the FCC on engineering matters.

Office of Strategic Planning and Policy Analysis (OSP)

The OSP works with the FCC Chairman, Commissioners, and bureau offices to develop a strategic plan for policy objectives, both long and short term.

The OSP is responsible for monitoring the trends and issues within the communications industry. In addition, the OSP reviews legal matters (e.g., e-commerce and intellectual property issues).

Legislative Reform

Government legislation regarding frequency and spectrum reform spans the White House to Capitol Hill.

In May 2003, an Executive Memorandum issued by President George W. Bush recognized the spectrum as an “important economic engine,” stressing a commitment to “putting spectrum to its highest and best use for the American people.”

In the United States, numerous bills (e.g., Boxer-Allen bill, Intelligence Reform and Terrorism Prevention Act of 2004) have been introduced on Capitol Hill in an effort to allocate RF spectrum for wireless broadband devices. The reallocation is meant to stimulate innovation development within the information transport systems (ITS) industry.
Frequency Reform, continued

One such frequency band is the 700 MHz spectrum currently allocated to television broadcast. This spectrum will become available in February 2009. The available spectrum will prove valuable to RF carriers looking to expand their service portfolios. It should be noted that the 700 MHz frequency band is noncontiguous as parts of the spectrum are occupied by agencies representing life safety initiatives (e.g., law enforcement, emergency medical service [EMS], homeland security, first responders).

Special interest groups (e.g., Wi-Fi Alliance, Worldwide Interoperability for Microwave Access [WiMAX] Forum, Wireless Communications Association International [WCA]) are actively involved with the FCC and legislators in issuing comments, questions, and concerns regarding proposed legislation or initiatives.

Anticipated Industry

With the unprecedented growth in the wireless industry, legislators and industry groups agree that a forward-looking approach is necessary to ensure the best performance and management of the spectrum for the future.

Global Harmonization

In addition to a strong emphasis on how the spectrum is administered in the United States, the spectrum must be coordinated with the international community to ensure a global harmonization policy. The FCC staff already participates in the international allocations processes and study group to promote technical compatibility both domestically and abroad.

To maintain this relationship, the International Bureau of the FCC participates in the following organizations:

- International Telecommunication Union (ITU)—Headquartered in Geneva, Switzerland, the ITU is an international organization within the United Nations where governments and the private sector coordinate global telecommunications networks and services.
- Organisation for Economic Co-operation and Development (OECD)—The OECD comprises 30 member countries sharing a commitment to democratic government and the market economy. The OECD produces internationally agreed upon instruments, decisions, and recommendations to promote rules in areas where multilateral agreement is necessary for individual countries to make progress in a global economy.
- Asia-Pacific Economic Cooperation (APEC)—APEC is an organization for facilitating economic growth, cooperation, trade, and investment in the Asian Pacific region. Its 21 members are referred to as member economies. It was founded in 1989 to further enhance economic growth and prosperity for the region and to strengthen the Asian Pacific community.
- Inter-American Telecommunication Commission (CITEL)—CITEL is an entity of the Organization of American States (OAS). It is the main forum in the hemisphere in which governments and the private sector meet to coordinate regional efforts. The primary focus of these regional efforts is to develop the global information society according to the mandates of the OAS General Assembly and the mandates entrusted to it by the heads of state and government at the Summits of the Americas.
Frequency Reform, continued

Other multinational organizations dedicated to the international maintenance of RF spectrum usage include the following:

- Telecommunications Regulators Association of Southern Africa (TRASA)
- Common Market for Eastern and Southern Africa (COMESA)
- African Telecommunications Union (ATU)
- Southern African Development Community (SADC)
- Commonwealth Telecommunications Organisation (CTO)
- National Association of Regulatory Utility Commissioners (NARUC)

Potential Technology Obsolescence

As the uses and capabilities of wireless technologies advance, the obsolescence of some current technologies is inevitable. Traditional telephone services, for example, are being replaced by cellular and VoIP services in many areas. The widespread use of these new services may eventually cause landlines as we know them to become obsolete.

The demand for bandwidth will continue the evolution of higher-speed wireless technology with increased capacity and distances. These new wireless products will make older wireless systems obsolete.

In planning for the future, consider a standards-based solution with a future migration path. For example, products based on IEEE 802.11g are backward compatible with products based on IEEE 802.11b. In other words, IEEE 802.11b devices communicate with IEEE 802.11g devices. This allows for a migration strategy to the latest technology by eliminating the design and purchase of an entire new system.

As new standards are ratified (e.g., IEEE 802.11n, IEEE 802.11y), backward compatibility issues will need to be reviewed.
Services and Applications

Leased Line Alternative and Local Loop Bypass

A wireless point-to-point (PTP), point-to-multipoint, or mesh system can be a cost-effective alternative to expensive monthly leased lines. Wireless can provide greater bandwidth, total network ownership, and backup if the leased line system goes down. However, the following limiting factors should be considered.

Bandwidth

Compared with a 1.5 Mb/s leased line, the bandwidth available from a wireless link is significantly higher. This allows networks to operate at much higher speeds and reduces existing bottlenecks in network performance. Additionally, when comparing the cost of a wireless link with the cost of a leased line beyond 1.5 Mb/s, wireless becomes even more attractive.

Total Network Ownership

The installation of a wireless link between buildings as an alternative to a leased line eliminates the need for the service provider. This allows the organization to pay for the network over a number of months as opposed to an unending lease agreement in which the organization owns nothing. It also provides the organization the same amount of control over their wide area network (WAN) as their LAN.

Redundancy

In addition to using a public switched telephone network (PSTN) to provide connectivity between sites, wireless can be used to augment or back up existing WAN links and provide fault tolerance and network stability. Wireless also can be used to back up a wireless system with alternative routing and redundant equipment and antennas.

Limitations

The main limitations with wireless as a leased line alternative are distance and LoS. Typically, wireless links can only be achieved at a maximum distance of 32 kilometers (km) to 48 km (20 miles [mi] to 30 mi) with a clear LoS. Accomplishing this requires ideal rooftop and elevation conditions with no pathway obstructions. A professional site survey should always be performed to determine feasibility.

Comparison with Cabled Infrastructure

WLANs are quickly becoming an additional means of providing network access. While cabling is typically installed in every office, cubicle, and conference room, wireless provides the ability to move freely without having to reconnect to the network. When comparing wireless systems with cabled systems, areas to look at include cost, ease of installation, and performance (cabling to the network is still required for wireless transmission equipment).
Comparison with Cabled Infrastructure, continued

Cost Comparison

When comparing the cost of a wireless system with that of a cabled system, a simple formula can be developed.

On the wireless system, this should include the wireless transmission equipment (i.e., an AP), client receivers (if applicable), cabled infrastructure (which connects the wireless transmission equipment back to the network), and all necessary labor. For PTP connections between buildings, external antennas, and towers, mounting accessories should be considered. This should be compared with cabled system components, which at a minimum include the entire cabling infrastructure, networking switches, and NICs (if applicable).

Ease of Installation

Installing cabling is usually more challenging and time consuming than mounting wireless equipment and antennas. This is especially true in an occupied environment where cabling will need to be installed while people are working.

However, a wireless installation normally requires a cabling installation to connect the wireless transmission equipment back to a cabled network. While this does not present a direct cabling drop to user correlation, it can be extensive depending on the number of devices required for a given wireless application.

Other factors that might make a wireless installation more challenging than a cabled installation include:

• Wireless site survey and engineering.
• Wireless security planning and setup.
• Outside interference from neighboring wireless systems.

Performance

From a per user bandwidth perspective, a cabled system frequently will outperform a wireless system. There are two primary reasons for this. First, the RF technology to transmit and receive the data has not caught up with that of a cabled system. Secondly, RF is frequently a shared medium between the users, whereas the cabled system is frequently dedicated per user. However, for most business applications, the bandwidth provided from a wireless system is substantial.

Wireless Data Applications

Wireless data applications have traditionally been used for warehouse data collection and retail services. With the advent of the IEEE 802.11 standard, these applications are rapidly expanding into the office, medical facilities, the home, and beyond. WLANs and wireless WANs continue to grow at an accelerated rate.
Wireless Data Applications, continued

Warehouse Data Collection

Proprietary wireless equipment has been used in warehouse environments for many years. Wireless barcode scanners are used for inventory, order entry, and shipping and receiving. While warehouse personnel will continue to use wireless for applications such as these, the proprietary systems are being phased out with standards-compliant equipment that can be integrated more easily with the rest of the network. This also allows various devices and applications to be run over the same wireless network.

Retail Service

Retail is another industry that has long used wireless for data transfer. Uses include scanning inventory, POS, and order entry. As with warehouse applications, retail wireless equipment has traditionally been proprietary. Migrating to IEEE 802.11 technology allows the applications to expand to customer use. Providing wireless Internet access to customers and real-time customer tracking services can create an enhanced customer experience and increase sales.

Office Environments

WLANs have been readily available in offices since 1997, when the IEEE 802.11 standard was ratified. However, most use has been limited to small groups of individuals in a limited geographic capacity. Now that security concerns by corporate IT managers have been adequately addressed, total wireless office coverage is accepted as an alternative network connectivity option.

Wireless chip sets imbedded in electronics are a standard feature for laptops and some personal digital assistants (PDAs). This helps fuel the need for wireless infrastructure throughout offices. Additionally, more people are now using WiFi in their homes and demanding the same mobility in their offices. While uses typically include Internet, e-mail, and file transfer applications, WLANs are increasingly being used for all standard office network applications.

Education

Wireless systems in the education environment are of tremendous benefit for student mobility. IEEE 802.11-enabled PDAs and laptops provide students with access to the Internet, as well as assignments, event calendars, and reference materials, while moving about freely through the building or campus. Wireless also is a benefit in older buildings with hard-to-access walls, frequently changing lab locations, and classroom setups that constantly require new drops to be run.

Other wireless applications used in education include PTP and point-to-multipoint wireless for interbuilding network connectivity. This is typically used as an alternative to optical fiber cabling in a campus environment or leased line replacement for buildings on separate properties.
Chapter 1: Introduction to Wireless Design

Wireless Data Applications, continued

Additionally, because of the fluctuation of students from year to year, schools are often required to add portable buildings to meet growing populations. With wireless technology, it is possible to quickly and easily connect new portables, which may be moved between campuses or to different locations on the same campus. Wireless provides the flexibility to network these buildings by simply moving or realigning antennas in most cases. This provides an alternative to a permanent connection (e.g., fiber), which will be of no value once the building is moved.

Health Care

The health care industry requires wireless access networks due to constant mobility. Doctors were one of the first professionals to carry pagers and cordless telephones. With the advent of WLANs, doctors and nurses can move throughout a hospital using laptop, handheld, and tablet PCs to pull up charts without plugging into a data port, in many cases replacing a clipboard and paper system.

By equipping staff with laptops or PDAs, they not only free up valuable desktop space but also can be moved to the patient’s location. Doctors can write prescriptions and notes directly into the system while in the exam room, eliminating the need to input this data at a later time.

Wireless systems in health care also are being deployed to provide mobile videoconferencing services to connect doctors and patients in emergency situations. With a videoconference terminal on a cart, which is connected wirelessly using voice and video over wireless LAN (VoWLAN), doctors can connect to remote clinics or directly to patients anywhere in the world from wherever they are in the hospital. The mobility provided by a wireless system saves valuable time in cases that are life threatening.

Emergency Notification Systems

Organizations such as educational institutions are deploying or contracting with third-party vendors to provide emergency notification systems that can utilize multiple channels for communication. These systems can utilize both wired and wireless technologies. When an emergency notification is authorized, it may be distributed via short message service (SMS) to a mobile telephone, to a mobile or landline telephone via a voice call, and to clients with WLAN-enabled laptops via e-mail, RSS feeds, or Web site updates.
Voice over Wireless LAN (VoWLAN)

Wireless voice is most commonly associated with cellular technology and wireless video with satellite. However, because of the maturation of video and VoIP technology and the proliferation of WLANs, VoWLAN is a credible alternative or enhancement to traditional private branch exchange (PBX) and videoconference systems. The design of a VoWLAN should include a QoS mechanism, seamless roaming capabilities, and a migration path from the current telephone system.

Although some organizations make the investment in a VoIP system and WLAN at the same time, most prefer a slower migration path to phase out their existing voice and video systems while allowing more and more wireless users on the network. This approach normally requires proprietary third-party gateways, telephones, cameras, and in some cases APs. The third-party products chosen should be able to integrate easily with the existing network, PBX, video and VoIP system, and WLAN.

Quality of Service (QoS)

The most important element in a VoWLAN is QoS. Voice and video packets must be prioritized over the data packets to provide equivalent voice and video quality to that of traditional telephone and videoconference systems.

While retries for a data file are acceptable, broken audio or video is much less tolerable to end users. The IEEE 802.11e standard has a provision for the prioritization of voice, audio, and video signals on a WiFi network. While this standard is somewhat limited, it lessens the need to rely on third-party gateways and software enhancements to provide QoS on the network.

Roaming

One of the main benefits of a WLAN is the ability to move about the facility or campus while remaining connected to the network. While seamless roaming between APs is an important design element of a WLAN, it becomes even more critical for a voice and video network.

Voice users in particular tend to be more mobile and will not appreciate dropped calls as they move around the building. This is really a function of the WLAN design and a mandate of the IEEE 802.11 standard. Whether a new or existing WLAN, a professional site survey should be conducted to eliminate any coverage gaps or interference that could hinder roaming performance.