



Understanding Wi-Fi™

January 2002

Table of Contents

Table of Contents	1
Executive Summary	2
Introduction	3
Wireless LANs and Wi-Fi™	4
Benefits of Wireless LANs	4
802.11 Basics	4
The Evolving 802.11 Standard	5
RF Fundamentals for WLANs	8
Propagation Characteristics Must Be Considered	8
Data Rate and Range are Related	9
Regulations	9
Sharing the Airwaves	9
Allocated Spectrum	9
Mandated Use of Spread Spectrum Techniques	10
Appendix	12
Acronyms	12
References on the Web	13

Executive Summary

The IEEE 802.11 working group published the 802.11 standard for wireless LANs in 1999. 802.11b is a supplement to 802.11 that specifies a higher data rate and is currently the industry-accepted standard for WLANs. 802.11b products that meet a base standard of interoperability are certified by the Wireless Ethernet Compatibility Alliance (WECA) with the Wi-Fi™ logo.

Several IEEE 802.11 working groups are creating standards for improvements in data rates, quality of service, and security. Options for higher data rates will soon be available as 802.11a and 802.11g products begin to appear on the market. The 802.11e working group will be publishing recommendations for adding quality of service features to 802.11 as well.

An understanding of some basic radio frequency (RF) principles will help ensure a successful network design. Range is limited by the physical nature of RF energy to disperse as the distance from the transmitter increases, as well as its tendency to be absorbed by materials such as walls and furniture. Range also decreases as data rate is increased.

WLANs are unregulated in the sense that users are not required to be licensed. However, characteristics of the equipment itself, such as transmitter power and how the signal is transmitted, are governed by the FCC.

Introduction

This paper is targeted at individuals who are already familiar with traditional wired networks and who wish to become familiar with wireless networks and some of the issues concerning their development.

Once confined only to specialty niches, wireless networks are now beginning to proliferate in the form of IEEE 802.11b (Wi-Fi™) wireless LANs, allowing users to roam throughout a building with a laptop while still remaining connected to their network.

Wi-Fi™ networks are described, as well as how the 802.11 standard is evolving to supply higher data rates and better quality of service.

The reader is introduced to the concept of radio frequency propagation and how it affects wireless networks, as well as the FCC regulations that govern their use of the spectrum, and what technologies are utilized to meet these requirements.

Wireless LANs and Wi-Fi™

Benefits of Wireless LANs

Originally employed to free network elements to roam in manufacturing and warehouse facilities, wireless LANs (WLANs) are now deployed throughout the enterprise as a cost-saving measure. They can be used to replace wired LANs, or as an extension of a wired infrastructure.

It costs far less to deploy a wireless LAN than to deploy a wired version. The savings isn't just in the falling cost of wireless components; it's in the installation of the infrastructure as well. A major cost of installing and modifying a wired network is the expense to run network and power cables, all in accordance with local building codes. For this reason, WLANs are being installed even when the network is comprised only of non-roaming desktops. Examples of additional applications where the decision to deploy WLANs results in large cost savings include:

- Additions, moves, and changes within an organization
- Installation of temporary networks
- Installation of hard-to-wire locations
- Elimination of costly leased lines

Wireless LANs give the enterprise more mobility and flexibility by allowing workers to stay connected to the Internet and to the network as they roam from one coverage area to another. This increases efficiency by allowing data to be entered and accessed on site.

Besides being very simple to install, WLANs are easy to understand and use. With few exceptions, everything to do with wired LANs also applies to wireless LANs. They function like, and are commonly connected to, wired Ethernet networks. They not only free the networked laptop to roam, but dramatically simplify and lower the cost of network deployment.

802.11 Basics

Wireless LAN Product Certification

The Wireless Ethernet Compatibility Alliance¹ (WECA) is the industry organization that certifies 802.11 products that are deemed to meet a base standard of interoperability. The first family of products to be certified by WECA is that based on the 802.11b standard. These products are stamped with the Wi-Fi™ logo and referred to as Wi-Fi devices. 802.11a products will be stamped with the Wi-Fi5™ logo. The Wi-Fi logos certify that the product will work with any other Wi-Fi certified device, regardless of manufacturer.

Network Topology

Each component of a WLAN requires a radio transceiver and antenna. Components are either stations or access points. *Stations* (STAs) are wireless LAN client radios. They can be

incorporated into a LAN card installed in a desktop, a USB adapter, a PCMCIA or PC card, or can be integrated into the notebook or handheld device itself. *Access Points* (APs) form a bridge between wireless and wired LANs.

A Basic Service Set (BSS) is formed when two or more stations have recognized each other and established a network. The network can be configured in two basic ways:

- *Peer-to-peer (ad hoc mode)* – This configuration is identical to its wired counterpart, except without the wires. Two or more STAs can talk to each other without an AP. When two or more stations form an ad hoc network, this is referred to as an *Independent Basic Service Set* (IBSS).
- *Client/Server (infrastructure networking)* – This configuration consists of multiple stations connected to an AP, which acts as a bridge to a wired network. A BSS in this configuration is referred to as being *in infrastructure mode*.

An *Extended Service Set* (ESS) is formed when multiple overlapping BSSs (each containing an AP) are connected together by means of a distribution system, usually a wired Ethernet LAN. BSSs whose ranges overlap must transmit on different channels to avoid interference.

Range between STAs and APs is up to 100 m (depending on data rate), but the overall range of an ESS is limited only by the range of the wired distribution system. Also, ESSs can be further extended with wireless links up to several miles by the use of directional range extender antennas.

The Evolving 802.11 Standard

The IEEE

The IEEE 802 LAN/MAN Standards Committee² produces the series of standards referred to as 802.x³, which originally encompassed LANs and MANs and now includes PANs such as Bluetooth™. IEEE 802 is confined to standardizing processes and procedures that take place in the bottom two layers of the OSI Reference Model⁴, the Media Access Control (MAC) or link layer and the Physical (PHY) layer.

The committee is currently divided up into Working Groups (WGs) numbered 802.1 through 802.17. Each working group deals with different issues and develops standards that are then given the same number as the working group which produced them. 802.1 (security and other issues) and 802.2 (logical link control) are standards that apply to both wired and wireless LANs. 802.11⁵ WG creates standards for WLANs and 802.15⁶ WG creates standards for wireless PANs. WGs are further divided up into smaller Task Groups (TGs) that work on various supplements and enhancements to the standards.

The Original Standard

The original 802.11 standard was published in 1999 and provides for data rates at up to 2 Mbps at 2.4 GHz, using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS).

Since that time many task groups have been formed to create supplements and enhancements to the original 802.11 standard. At present there are task groups “a” through “i” (the 802.11 WG refers to task groups by lower case letter), which are working on various methods to standardize improvements to the 802.11 standard.

Some of the supplements are considered optional from an IEEE point of view and may never become an industry accepted standard.

The Current Standard

802.11b

The 802.11b TG created a supplement to the original 802.11 standard, called 802.11b, which has become the industry standard for WLANs. It uses DSSS and provides data rates up to 11 Mbps at 2.4 GHz. 802.11b will eventually be replaced in the marketplace by products built to standards with higher data rates, more quality of service (QoS) features, and better security.

The Battle for Higher Data Rates

The same evolution that increased the speed of wired Ethernet is now being played out in the wireless realm. There are presently two options for higher data rates in the near future - one clearly defined in a published standard, and the other currently being developed. Market forces will decide which wins. Either option means big gains for the user beyond seeing just faster data throughput rates, as more stations can now be added to an Access Point without noticeable performance degradation.

802.11a

The 802.11a supplement to 802.11 was published in 1999. It uses Orthogonal Frequency Division Multiplexing (OFDM) to provide data rates to 54 Mbps in the 5 GHz U-NII bands.

In addition to being uncrowded, more spectrum in the U-NII bands allows room for 12 non-overlapping channels, compared to just three in the 2.4 GHz ISM bands. Both of these factors make operating in the U-NII bands far less prone to interference.

However, at 5 GHz, more path loss occurs due to increased absorption of the RF energy by walls and other solid objects. This, combined with a decrease in range due to the higher data rates, may require that more access points be installed to effectively cover an area comparable to that of 802.11b.

There are now chip sets appearing that include both 802.11a and 802.11b capability, and technology is being developed to allow the seamless handoff of communication between overlapping 802.11a and 802.11b networks.

802.11g

The 802.11g task group is working on a supplement to the 802.11 standard that defines a technology for operation at 2.4 GHz that offers higher data rates (up to 22 Mbps) using OFDM, while remaining backwards compatible to 802.11b. In addition, the supplement

will specify even higher data rates using two different methods (up to 33 Mbps using PBCC-DSSS and up to 54 Mbps using CCK-OFDM) which manufactures can optionally incorporate.

When compared to 802.11a, 802.11g offers the advantages of lower cost, backwards compatibility to existing 802.11b equipment, and less path loss than 802.11a. This translates into higher data rates for a given range, or increased range for a given data rate.

The Need for Addition of QoS

802.11e

The 802.11e task group is working to enhance the current 802.11 MAC to expand support for applications with quality of service requirements. (Note: Security issues formerly being considered by the 802.11e task group are now being considered by the 802.11i task group.) The intent is to make 802.11 fully capable of supporting applications from both business and home environments, including multimedia.

Data transmission is relatively immune to interruptions caused when packets are resent or shuffled in transmission. However, these interruptions and time delays can wreak havoc on information that must be streamed across in a continuous fashion, such as voice or video. 802.11e has created a QoS Baseline Document (eventually to become a draft) that proposes methods for handling time-sensitive traffic. Among other things, it guarantees collision avoidance and provides mechanisms for scheduling transmissions and improving channel robustness. 802.11e expects to publish a draft supplement in 2002.

Higher data rates and QoS will be welcome additions to the evolving 802.11 family of standards. However, the most pressing and immediate need for 802.11 is an improvement in security.

RF Fundamentals for WLANs

Though WLANs are easy to deploy, the network administrator or IT professional will benefit from some basic knowledge about radio wave propagation. Although it is possible to utilize infrared technology (which always requires line of sight between elements of the network), this paper deals only with Radio Frequency (RF) wireless networks, which have become the industry accepted standard for WLANs.

The reason for using RF is simple. It can pass through solid objects such as office walls. However, radio waves do not go on forever in all directions without weakening or being affected by physical barriers. The user needs to have some understanding of their propagation characteristics, as well as the relationship between power levels and data rates, before a wireless network can be designed.

Propagation Characteristics Must Be Considered

Reflection - Radio waves can be reflected by some materials. This phenomenon is often used to steer microwave signals between stations that are not line-of-sight, but in an office environment it can create multipath (see below).

Absorption - Radio waves can be absorbed by many materials such as water, plastic, sheetrock, and carpet.

Geometric Spreading loss - Radio waves, like light waves, get weaker as they expand outward away from their source. This loss grows as the square of the distance. This means that if a device is moved twice as far away, the signal power drops by one fourth.

Path loss - The above phenomena lead to path loss, or an unavoidable weakening of the signal's power as it propagates outward. In an office environment, the placement of furniture and walls, and even the movement and location of people, will contribute to the amount of path loss.

Multipath - If a received signal is made up of radio waves from the same signal that has dispersed and arrived from different paths, i.e. some of the original energy was reflected off an object before arriving at the receiver, then the effects of multipath are seen. Television sets connected to antennas often exhibit this as ghosting. Network users may likewise experience its digital counterpart - referred to as **intersymbol interference**. This is caused when the difference in time between radio waves arriving from the same signal, referred to as **delay spread**, is enough to cause symbol overlap in the digital data. As the data transmission speed gets faster, the time between received data bits get smaller and more susceptible to intersymbol interference, so multipath places an upper limit on data transmission speed.

Propagation characteristics are frequency dependent:

At lower frequencies (longer wavelengths), less RF energy is absorbed by obstructions. Signals can pass through solid objects (walls) more readily.

At higher frequencies (shorter wavelengths), smaller antennas can be used. However, if antennas are scaled down proportionately with wavelength, the received signal power will decrease as a function of frequency squared, due to less signal energy being intercepted by the smaller antenna. This shortcoming can be overcome by using higher gain antennas.

Data Rate and Range are Related

The signal strength at the receiver is often stated in reference to the noise level as the signal-to-noise ratio (S/N ratio or SNR). Information theory defines a relationship between the SNR of a received signal, and how much information can be reliably transmitted over that channel. The result for the user is that for a given SNR (and corresponding transmitted power level), the bit error rate (BER) increases as the data rate increases. Thus there exists a tradeoff between data rate and range. All things (transmitter power, encoding method, antenna gain, etc.) being equal, if a wireless network is operated at a higher data rate, the effective range will decrease. Conversely, if it is operated at a greater range, the data rate may need to be dropped to obtain an acceptable BER. The only way to increase range without decreasing data rate is to increase power – and the FCC puts a ceiling on power levels.

It is not difficult to get a wireless network up and running, but it is often advantageous, especially for large corporate LANs, to have a specialist do an RF site survey first. The site survey will assist in the network design process by providing details about how particular conditions in a building contribute to path loss and multipath, and thus to data rate and range.

Regulations

Sharing the Airwaves

While wired networks send traffic over a dedicated line that is physically private, WLANs send their traffic over shared space – the airwaves. This brings new challenges in the form of *interference* from other traffic and the need for *additional security*.

Allocated Spectrum

WLANs and Bluetooth™ both operate under Federal Communications Commission (FCC) Part 15 rules. They share portions of their spectrum with the globally allocated Industrial, Scientific, and Medical (ISM) bands in the 2.4 GHz region, and, in the case of 802.11a WLANs, the Unlicensed National Information Infrastructure (U-NII) bands in the 5 GHz region. These portions of the spectrum have been set aside specifically for largely unregulated use, in the sense that the individual user does not require a license. Wireless devices using the ISM bands include portable phones, microwave ovens, garage door

openers, security devices, etc. Within the ISM bands, all users share the airwaves and must tolerate interference from one another.

Mandated Use of Spread Spectrum Techniques

Radio transmission of information relies upon the concept of superimposing information on, or modulating, a carrier wave. Traditional narrowband radio transmission centers this carrier at a specific frequency. As the carrier is modulated, its power is confined to a relatively narrow band around the carrier's center frequency. The listener must then tune his receiver to that frequency to receive the transmission.

For those bands becoming crowded with users, the FCC is embracing a different philosophy, that of spreading or smearing a signal's power over a very large band of frequencies. At any one frequency the signal's average power over a given period of time will be very low – in many cases down in the noise level. Signals that use the same spreading technology can still interfere with one another, but the interference presented to all other signals is much reduced, allowing more users to occupy the same band.

To minimize interference in this crowded spectrum, the Part 15 rules specify that all transmissions with a power level exceeding 0 dBm (1 mW) must utilize either frequency hopping or direct sequence spread spectrum techniques. The FCC is in the process of modifying the Part 15 rules to allow Orthogonal Frequency Division Multiplexing (OFDM) as well. All of these techniques serve the same purpose, to spread the signal's power over a wider range of frequencies, thus reducing the average power density of the signal at any particular frequency and minimizing interference to other signals occupying the same band. A brief explanation of these signal-spreading techniques follows:

Frequency Hopping Spread Spectrum (FHSS)⁷ was originally conceived as a means to hide a transmission from unwanted listeners. It is now utilized for another purpose - the reduction of interference. Frequency hopping works by transmitting the signal carrier for a short period of time on one narrow band, then hopping to another, and so on. Over a period of time, the average signal power is thus spread over a very wide band of frequencies.

The frequency hops appear random to anyone who doesn't know the pre-arranged hop pattern. Fifty years ago this made it impossible to tune in and listen to a transmission, because the signal carrier never stayed on one frequency long enough for the listener to locate it and retune the receiver to the new frequency. Today, wireless LANs or PANs that incorporate FHSS do so on predetermined hopping sequences that are not secret, and the technology to follow the hopping pattern and retrieve the signal is available for the cost of a wireless card. Thus, FHSS, as employed by wireless LANs and PANs, no longer offers any inherent security. It does, however, serve to reduce interference to and from other devices.

Direct Sequence Spread Spectrum (DSSS)⁸ is a more complex technique which spreads the signal's power across a wider bandwidth by spreading the carrier itself, instead of rapidly moving it around as FHSS does. It does this by directly modulating the carrier

with a high-speed code sequence which has the characteristics of pseudo-random noise (PN). The faster a carrier is modulated, the wider its bandwidth becomes.

The spreading sequence is produced by modulating the data stream with a PN spreading code, thus resulting in a signal which has a much higher bandwidth than the information bandwidth alone. For example, with 1 and 2 Mbps 802.11 DSSS, each bit of data is logically combined with an 11-bit Barker code. Because the bit-rate (chip-rate) of the spreading sequence is much higher than that of the data rate, the bandwidth is effectively spread over a much larger area than would otherwise be occupied if the carrier was modulated by the data stream alone. The result is that the signal power is spread over a much larger band and appears to other users as low-power noise.

Orthogonal Frequency Division Multiplexing (OFDM)⁹, which utilizes multiple carriers (referred to as subcarriers), is technically not a spread spectrum technique because the subcarriers remain stationary and are not spread, but it serves the same purpose of spreading the signal power over a large band. It does this by breaking the signal up into parts and transmitting each of the parts on a different subcarrier at a different center frequency. Thus a fast transmission is sent as many slow transmissions, simultaneously, on many different frequencies.

This effective slowing of the symbol transmission rate, without slowing the actual data transmission rate, makes OFDM resistant to intersymbol interference resulting from multipath. In theory, if higher data rates are required, then the signal can just be broken up into more parts and transmitted on additional subcarriers, each part still being sent at a slow enough rate to avoid intersymbol interference. In practice, the amount of bandwidth available for additional subcarriers is limited by the FCC.

These different techniques for spreading the signal's carrier, and the different digital modulation techniques employed to put information on the carrier, are central to defining the different wireless technologies and standards, as well as putting a perspective on interference issues among 802.11 LANs and Bluetooth networks.

Appendix

Acronyms

AP - Access Point
BER - Bit Error Rate
BSS – Basic Service Set
CCK - Complementary Code Keying
DSSS - Direct Sequence Spread Spectrum
ESS – Extended Service Set
FCC -Federal Communications Commission
FHSS - Frequency Hopping Spread Spectrum
IBSS – Independent Basic Service Set
IEEE - Institute of Electrical & Electronic Engineers
ISM - Industrial, Scientific, Medical
IT - Information Technology
MAC - Media Access Control
MAN - Metropolitan Area Network
Mbps - Megabits per second
MBps - Megabytes per second
OFDM - Orthogonal Frequency Division Multiplexing
OSI - Open System Interconnection
PAN - Personal Area Network
PBCC - Packet Binary Convolution Coding
PCMCIA - Personal Computer Memory Card International Association
PHY - Physical (Layer)
PN - Pseudo-random Noise
QoS - Quality of Service
RF - Radio Frequency
S/N ratio - Signal-to-Noise Ratio
SNR - Signal-to-Noise Ratio
STA - Station
TG - Task Group
U-NII - Unlicensed National Information Infrastructure
USB – Universal Serial Bus
WECA – Wireless Ethernet Compatibility Alliance
WG - Working Group
WLAN - Wireless LAN
XOR - exclusive OR (a mathematical logic operation)

References on the Web

- ¹ Wireless Ethernet Compatibility Alliance, <http://www.wirelessethernet.org/index.html>
- ² IEEE 802 LAN/MAN Standards Committee, <http://grouper.ieee.org/groups/802/index.html>
- ³ IEEE 802 standards, <http://standards.ieee.org/getieee802/>
- ⁴ A good explanation of the seven-layer OSI Reference Model, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#xtocid130454
- ⁵ IEEE 802.11 working group, <http://grouper.ieee.org/groups/802/11/index.html>
- ⁶ IEEE 802.15 working group, <http://grouper.ieee.org/groups/802/15/index.html>
- ⁷ FHSS, <http://www.sss-mag.com/ss01.html#other>
- ⁸ DSSS, <http://www.sss-mag.com/ss01.html#other>
- ⁹ OFDM, <http://www.sss-mag.com/ofdm.html>