U.S.Robotics

Wireless LAN Networking
White Paper

Introduction

Wireless technology has helped to simplify networking by enabling multiple computer users to simultaneously share resources in a home or business without additional or intrusive wiring. These resources might include a broadband Internet connection, network printers, data files, and even streaming audio and video. This kind of resource sharing has become more prevalent as computer users have changed their habits from using single, stand-alone computers to working on networks with multiple computers, each with potentially different operating systems and varying peripheral hardware. U.S. Robotics wireless networking products offer a variety of solutions to seamlessly integrate computers, peripherals, and data.

Wireless networking enables the same capabilities and comparable speeds of a wired 10BASE-T network without the difficulties associated with laying wire, drilling into walls, or stringing Ethernet cables throughout an office building or home. Laptop users have the freedom to roam anywhere in the office building or home without having to hunt down a connector cable or available jack. Every room in a wireless home or office can be "connected" to the network, so adding more users and growing a network can be as simple as installing a new wireless network adapter.

Reasons to choose wireless networking over traditional wired networks include:

- Running additional wires or drilling new holes in a home or office could be prohibited (because of rental regulations), impractical (infrastructure limitations), or too expensive
- Flexibility of location and data ports is required
- Roaming capability is desired; e.g., maintaining connectivity from almost anywhere inside a home or business
- Network access is desired outdoors; e.g., outside a home or office building

Wireless LANs in the Office

An 802.11 network is the ideal solution for a network administrator in many respects. No longer is it a requirement that every workstation and conference room be wired up to hubs and switches with cables in hard-to-reach areas. Wireless networking allows for impromptu meetings in cafeterias, hallways, courtyards, or wherever inspiration strikes while providing real-time LAN connectivity for business applications such as sending e-mail, working on spreadsheets on shared drives, and conducting market research.

Wireless LANs in the Home

Wireless networking has become commonplace, and with prices reduced to a fraction of what they were, it is no wonder that wireless networking products have transitioned from the office and into the home. For the home user, a wireless network provides freedom in convenience and lifestyle to exchange words, data, and music or video with any computer – across the Internet, or around the world. Home users can create a wireless network out of an existing wired network and wirelessly extend the reach of the Internet throughout the home on multiple computers, making it more convenient for everyone to get online.

IEEE Wireless Networking Specifications

The IEEE (Institute of Electrical and Electronic Engineers) released the 802.11 specifications in June 1999. The initial specification, known as 802.11, used the 2.4 GHz frequency and supported a maximum data rate of 1 to 2 Mbps. In late 1999, two new addenda were released. The 802.11b specification increased the performance to 11 Mbps in the 2.4 GHz range while the 802.11a specification utilized the 5 GHz range and supported up to 54 Mbps.

Unfortunately, the two new specifications were incompatible because they used different frequencies. This means that 802.11a network interface cards (NICs) and access points cannot communicate with 802.11b NICs and access points. This incompatibility forced the creation of the new draft standard known as 802.11g. 802.11g supports up to 54 Mbps and is interoperable with 802.11b products on the market today. The concern is that the 802.11g specification is currently in development and products will not be available until a later date.

802.11 Specifications

The 802.11 specifications were developed specifically for Wireless Local Area Networks (WLANs) by the IEEE and include four subsets of Ethernet-based protocol standards: 802.11, 802.11a, 802.11b, and 802.11g.

802.11

802.11 operated in the 2.4 GHz range and was the original specification of the 802.11 IEEE standard. This specification delivered 1 to 2 Mbps using a technology known as phase-shift keying (PSK) modulation. This specification is no longer used and has largely been replaced by other forms of the 802.11 standard.

802.11a

802.11a operates in the 5 - 6 GHz range with data rates commonly in the 6 Mbps, 12 Mbps, or 24 Mbps range. Because 802.11a uses the orthogonal frequency division multiplexing (OFDM) standard, data transfer rates can be as high as 54 Mbps. OFDM breaks up fast serial information signals into several slower sub-signals that are transferred at the same time via different frequencies, providing more resistance to radio frequency interference. The 802.11a specification is also known as Wi-Fi5, and though regionally deployed, it is not a global standard like 802.11b.

802.11b

The 802.11b standard (also known as Wi-Fi) operates in the 2.4 GHz range with up to 11 Mbps data rates and is backward compatible with the 802.11 standard. 802.11b uses a technology known as complementary code keying (CCK) modulation, which allows for higher data rates with less chance of multi-path propagation interference (duplicate signals bouncing off walls).

U.S. Robotics 22 Mbps 802.11b

Recent developments to 802.11b have seen numerous improvements to this well-established and widely-deployed wireless standard. New U.S. Robotics 22 Mbps products are designed to support Packet Binary Convolutional Coding (PBCC) in addition to CCK modulation. This not only increases performance but also maintains complete 802.11b compatibility with both 11 Mbps and 22 Mbps products. The overall benefits include:

- Up to twice the data rate of conventional 11 Mbps 802.11b standard products
- Greater WLAN coverage: up to 70% greater than standard 11 Mbps 802.11b products
- Full interoperability with all 802.11b products: works with 802.11b 11 Mbps, 802.11b 22 Mbps, and upcoming 802.11g products
- Improved security over standard 802.11b: 256-bit WEP encryption and MAC address authentication*

802.11g

802.11g is the most recent IEEE 802.11 draft standard and operates in the 2.4 GHz range with data rates as high as 54 Mbps over a limited distance. It is also backward compatible with 802.11b and will work with both 11 and 22 Mbps U.S. Robotics wireless networking products. 802.11g offers the best features of both 802.11a and 802.11b, but as of the publication date of this document, this standard has not yet been certified, and therefore is unavailable.

** MAC address authentication available with U.S. Robotics 22 Mbps Wireless Access Point and U.S. Robotics 22 Mbps Wireless Cable/DSL Router.*

All four standards are based on the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) Ethernet protocol for path sharing. The most significant contribution of the 802.11 specification is that it allows for interoperability among different vendors' equipment. Thanks to the Wireless Ethernet Compatibility Alliance (WECA), 802.11 standard equipment will work together interchangeably, regardless of the manufacturer.

Different WLAN Technologies

As various wireless networking technologies have advanced over time, several WLAN technologies have emerged, including: narrowband, spread spectrum, frequency hopping spread spectrum, and direct sequence spread spectrum.

Narrowband

As the name suggests, narrowband technology uses a specific radio frequency (in the range of 50 cps to 64 Kbps) for data transmission.

Spread Spectrum

Originally developed for military use, spread spectrum technology allows for greater bandwidth by continually altering the frequency of the transmitted signal, thus spreading the transmission across multiple frequencies. Spread spectrum uses more bandwidth than narrowband, but the transmission is more secure, reliable, and easier to detect.

Frequency Hopping Spread Spectrum (FHSS)

Frequency hopping spread spectrum (FHSS) technology synchronizes the changing frequency of both the transmitter and receiver (using a narrowband carrier) to, in effect, produce a single transmission signal. This frequency "hopping" can occur as often as several times a second; it is constantly changing from one frequency to another, transmitting data for a certain period of time before changing frequency again. Like spread spectrum technology, FHSS technology consumes additional bandwidth, however, this is over the course of multiple carrier frequencies.

Direct Sequence Spread Spectrum (DSSS)

Direct sequence spread spectrum (DSSS) technology breaks down the transmitted stream of data into small pieces across a frequency channel. A redundant bit pattern (known as a chipping code) is generated for each bit transmitted. Generally, the longer the chipping code, the more likely it is that the original transmitted data will be properly received. DSSS technology uses more bandwidth than FHSS, but DSSS is considered more reliable and resists interference. Because of the chipping code, data can still be recovered without retransmission of the signal, even in the case of damaged data bits. U.S. Robotics wireless networking products utilize DSSS technology.

Wireless LAN Frequency Usage

The 802.11b standard defines 14 frequency channels for use with this technology. Depending on the country a user lives in and where he or she will be installing a WLAN, there are certain governmental restrictions for companies offering these products and consumers or businesses deploying these products.

In North America, the FCC (Federal Communications Commission) and IC (Industry Canada) allow manufacturers and users to use channels 1 through 11, per ETSI approval (European Telecommunications Standards Institute); most of Europe can use channels 1 through 13, while in Japan, users have all 14 channels available.

Channel	Freq. (GHz)	US FCC	Canada IC	Europe ETSI	Spain	France	Japan
1	2.412	√	√	√			√
2	2.417	√	√	√			√
3	2.422	√	√	√			√
4	2.427	√	√	√			√
5	2.432	√	√	√			√
6	2.437	√	√	√			√
7	2.442	√	√	√			√
8	2.447	√	√	√			√
9	2.452	√	√	√			√
10	2.457	√	√	√	√	√	√
11	2.462	√	√	√	√	√	√
12	2.467			√		√	√
13	2.472			√		√	√
14	2.484						√

Figure 1 – 802.11b channels and frequency per region

Even though there are 14 channel frequencies available for use, it should be noted that the actual channel frequency indicates the "center frequency" used by the transmitter and receiver for communication. An 802.11b radio signal consumes approximately 30 MHz of frequency spectrum, leaving a 5 MHz separation between center frequencies. This means that the signal extends out 15 MHz of the center frequency spectrum.

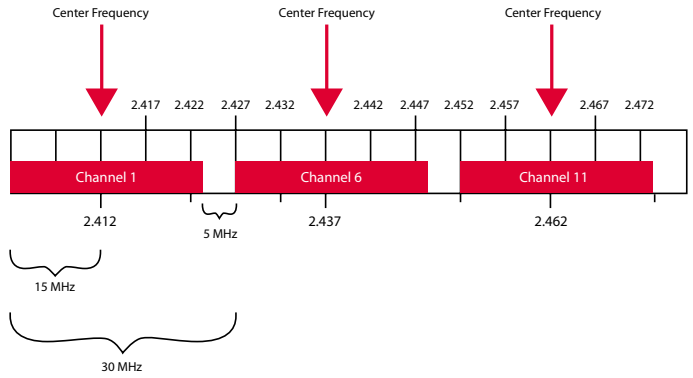

Figure 2 – Bandwidth required for each 802.11 channel (also demonstrates the 5 MHz between each frequency)

As a result, the bandwidth required for each channel signal overlaps several adjacent frequencies. This leaves the typical U.S. user with three channels available for use by access points (channels 1, 6, and 11) that are within radio range of adjacent access points.

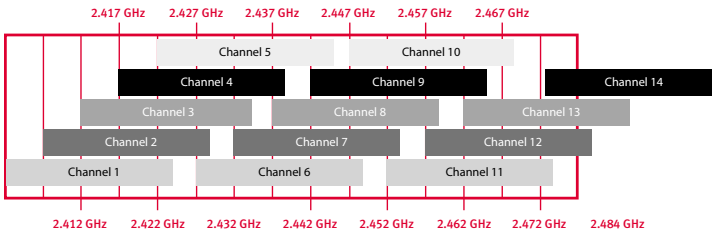

Figure 3 – Shows an example of overlapping frequencies — 802.11b bandwidth allocation

Ad Hoc (Peer-to-Peer) Mode vs. Infrastructure Mode

The 802.11 specification defines two types of operational modes: ad hoc (peer-to-peer) mode and infrastructure mode. In ad hoc mode, the wireless network is relatively simple and consists of 802.11 network interface cards (NICs). The networked computers communicate directly with one another without the use of an access point. In infrastructure mode, the wireless network is composed of a wireless access point(s) and 802.11 network interface cards (NICs). The access point acts as a base station in an 802.11 network and all communications from all of the wireless clients go through the access point. The access point also provides for increased wireless range, growth of the number of wireless users, and additional network security.

Ad Hoc Mode

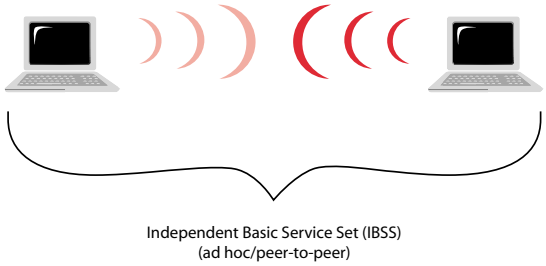

Figure 4 – Ad hoc mode

In ad hoc mode, also known as Independent Basic Service Set (IBSS) or peer-to-peer mode, all of the computers and workstations connected with a wireless NIC card can communicate with each other via radio waves without an access point. Ad hoc mode is convenient for quickly setting up a wireless network in a meeting room, hotel conference center, or anywhere else sufficient wired infrastructure does not exist.

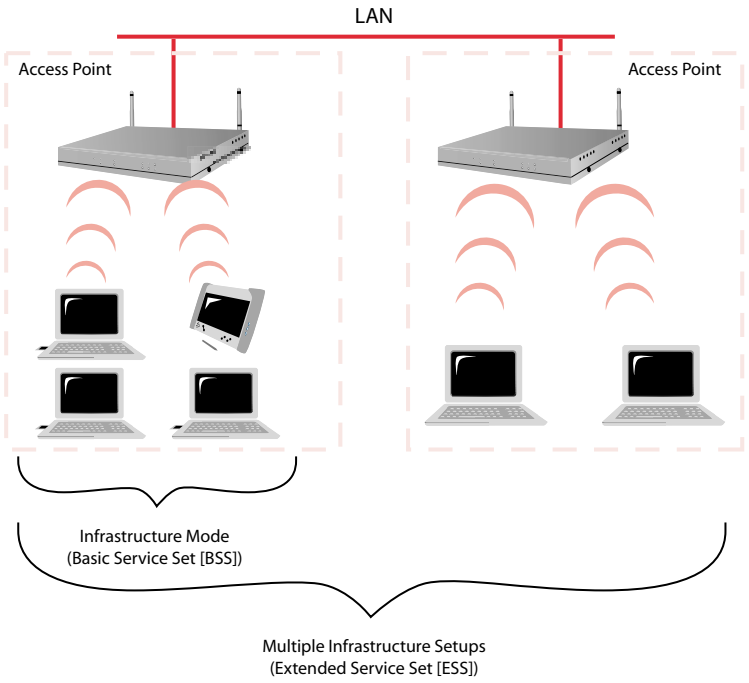

Figure 5 – Basic Service Set (BSS) and Extended Service Set (ESS)

Infrastructure Mode

In infrastructure mode, all mobile and wireless client devices and computers communicate with the access point, which provides the connection from the wireless radio frequency world to the hard-wired LAN world. The access point performs the conversion of 802.11 packets to 802.3 Ethernet LAN packets. Data packets traveling from the LAN to a wireless client are converted by the access point into radio signals and transmitted out into the environment. All wireless clients and devices within range can receive the packets, but only those clients with the appropriate destination address will receive and process the packets.

A basic wireless infrastructure with a single access point is called a Basic Service Set (BSS). When more than one access point is connected to a network to form a single sub-network, it is called an Extended Service Set (ESS).

The 802.11 specification includes roaming capabilities that allow a client computer to roam among multiple access points on different channels. Thus, roaming client computers with weak signals can associate themselves with other access points with stronger signals. Alternately, by setting up multiple access points to cover the same geographic area and by using different non-overlapping frequencies, client workstation networking loads can be better balanced. A wireless LAN NIC may decide to "reassociate" itself with another access point within range because the load on its current access point is too high for optimal performance. These capabilities can have a positive impact on overall network performance.

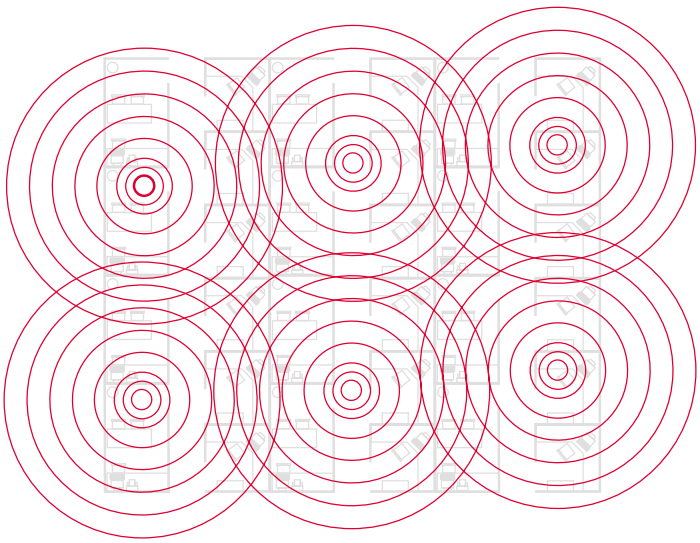

Figure 6 – Roaming among access points with non-overlapping frequencies allows for virtually unlimited coverage range

Wireless Network Components

Much like a traditional wired LAN, a WLAN is a grouping of computers and peripheral devices that share a common communications backbone. As is implied by the name, a WLAN allows users to connect to the LAN wirelessly via radio transmission. The following are the most common components of a WLAN.

Access Point

The access point is a device that links a wireless network to a wired LAN. It increases the effective range of a wireless network and provides additional network management and security features. Wireless networks of three or fewer PCs do not require an access point for ad hoc networking. Access points are useful for larger networks, and they are particularly well-suited for adding wireless capability to an existing wired network.

The U.S. Robotics 22 Mbps Wireless Access Point connects via an RJ-45 cable to a LAN and can support up to 20 wireless users at an effective range of up to 1500 feet in open spaces. It also enables additional security features such as MAC address authentication.

PC Card

A wireless PC card enables laptop users to connect wirelessly to the LAN. U.S. Robotics 22 Mbps Wireless PC Cards allow for ad hoc networking of up to three computers at an effective range of up to 1000 feet in open spaces

PCI Adapter

Just as a wireless access PC card allows portable and laptop computers access to the LAN, a wireless access PCI adapter allows desktop PC users access to the LAN. U.S. Robotics 22 Mbps Wireless PCI Adapters allow for ad hoc networking of up to three computers at an effective range of up to 1000 feet in open spaces.

Router

A router is a device used for sharing a single Internet connection across multiple computers. This is ideal in the home or office where multiple computers and devices can be online at the same time with only a single Internet connection. The U.S. Robotics 22 Mbps Wireless Cable/DSL Router includes built-in wireless access point capabilities.

Wireless networking users should keep the following in mind:

- One wireless PC card (U.S. Robotics 22 Mbps Wireless PC Card, model 2210) is needed for each laptop and one wireless PCI adapter (U.S. Robotics 22 Mbps Wireless PCI Adapter, model 2215 or 2216) is needed for each desktop computer to be wirelessly networked.
- An ad hoc network of up to three computers can be created with wireless PC cards or PCI adapters. To connect more than three computers, include an access point or router (U.S. Robotics 22 Mbps Wireless Access Point, model 2249, or U.S. Robotics 22 Mbps Wireless Cable/DSL Router, model 8022) in the network design.
- Ad hoc wireless networks using U.S. Robotics 22 Mbps wireless networking products have an effective range of up to 300 feet in any direction, indoors or out, and even on different levels of a building. As with any wireless product, ad hoc networks work best when closer together and in an open environment.
- Wireless networks that use either a U.S. Robotics 22 Mbps Wireless Access Point or a U.S. Robotics 22 Mbps Wireless Cable/DSL Router have an effective range of up to 1500 feet, with the same considerations as ad hoc networks.
- Sharing Internet access among multiple computers or laptops requires a router. The U.S. Robotics 22 Mbps Wireless Cable/DSL Router is capable of supporting up to 253 clients (with additional hardware) for wired and wireless Internet sharing.

WLAN Performance

Much the same way a cordless phone works better when it is close to its base, wirelessly networked computers function best when located relatively close together and in open sight of each other. The level of performance of an 802.11 WLAN is dependent on a number of important environmental and product-specific factors. Access points will automatically negotiate the appropriate signaling rate based upon environmental conditions, such as:

- Distance between WLAN devices (AP and NICs)
- Transmission power levels
- Building and home materials
- Radio frequency interference
- Signal propagation
- Antenna type and location

Depending on environmental specifics, automatic downshifting by the access point or client allows compatibility adjustment to prevailing radio frequency conditions. At any one moment, an 802.11b network can be running at 11 Mbps, 5.5 Mbps, 2 Mbps, or 1 Mbps 22 Mbps wireless networking products). And depending on where each wireless device is in a home or office, each of those devices can be transmitting at any one of these speeds. Typically, the software applications that ship with an 802.11 NIC adapter are capable of reporting current connection speeds and also allow users to perform site surveys for the best location of an access point.

The diagram below shows how distance and building materials can impact the performance of an 802.11 network.

Distance Between WLAN Devices

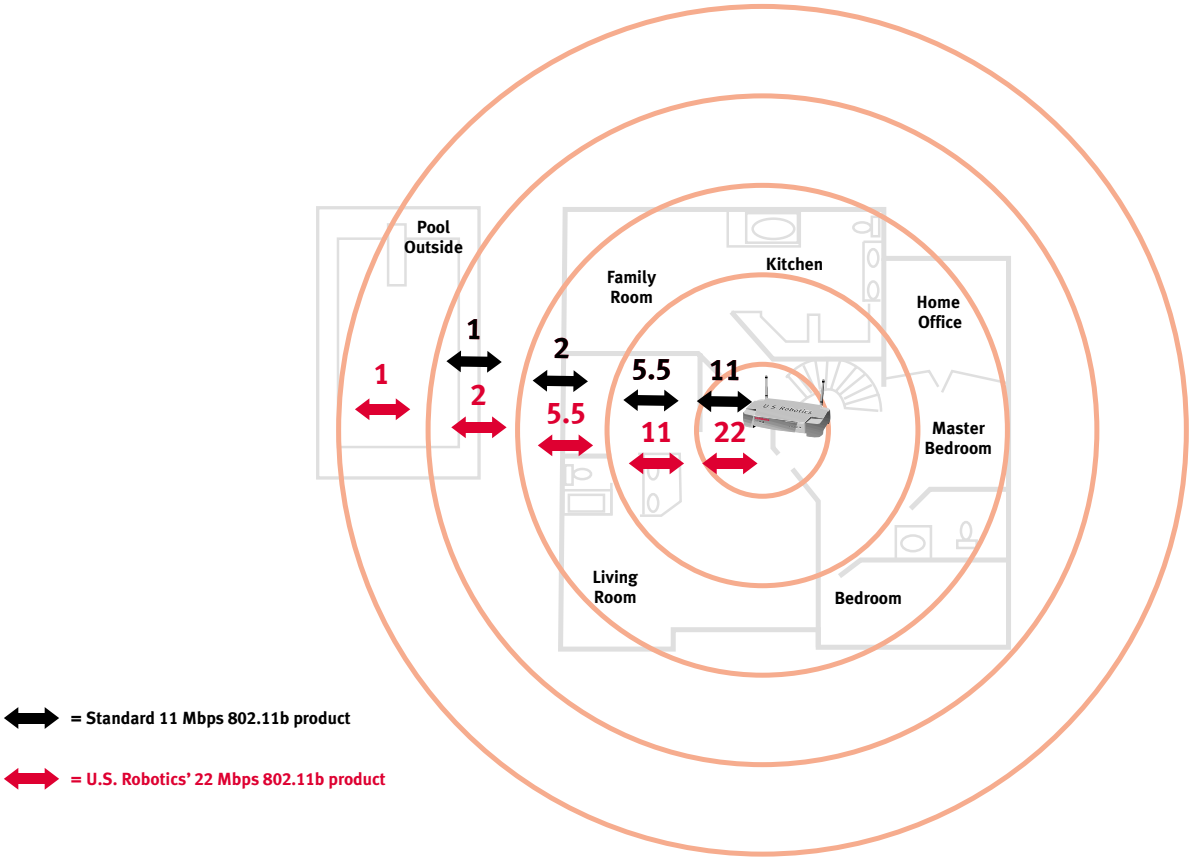

Figure 7 – Effects of distance on the 802.11 signal

(Access Points and NICs)

Typically, published wireless range claims are for line-of-sight or open area environments such as cafeterias, auditoriums, or other areas that lack interference-causing obstacles. The following chart provides a quick comparison of conventional 802.11b wireless products against U.S. Robotics 22 Mbps wireless products in a real-world application with typical levels of interference and common obstructions, such as walls and other physical barriers. U.S. Robotics 22 Mbps maximum sustainable throughput is clearly superior to that of standard 11 Mbps 802.11b.

11 Mbps Products	U.S. Robotics 22 Mbps Products
~8 Mbps @ 200 ft	~13.5 Mbps @ 200 ft
~4.5 Mbps @ 250 ft	~8 Mbps @ 250 ft
~2 Mbps @ 300 ft	~6 Mbps @ 300 ft
~1 Mbps @ 325 ft	~4.25 Mbps @ 325 ft
N/A	~4 Mbps @ 350 ft

Products designed to work with the 802.11a standard have a faster data rate, but the signal is limited in distance and susceptible to environmental conditions like rain and fog. Because of these limitations, 802.11a products are more practical for indoor applications, will most likely require additional access points for proper area coverage, and will achieve lower data rates than the maximum allowed.

Transmit Power Levels

Most WLAN devices have a power output of only 30 mW, which is far less then a typical cellular phone or walkie-talkie.

Power Consumption Levels

Most 802.11b NICs allow the user to customize the power modes in the software drivers in order to optimize WLAN performance versus battery life for a notebook system.

Building and Home Materials/Signal Propagation

The contents of a home or office building can have a dramatic impact on the quality of the signal obtained with an 802.11 wireless network. The wood, metal, and other building materials have a direct impact on signal propagation and absorption. Other factors include:

- Multi-path interference: This occurs when signal strength and timing are altered due to the signal reflecting off walls, filing cabinets, beams, and other objects. This results in a device receiving two or more identical signals.
- Fading: Fading is the reduced amplitude of a signal as a result of passing through radio-transparent objects such as walls and ceilings.
- Dead zones: Locations where radio signals never reach due to reflections, obstructions, or other environmental conditions.

The new 22 Mbps line of U.S. Robotics wireless networking products are specifically designed for optimal use in the home with minimal degradation in signal quality due to environmental conditions; U.S. Robotics wireless products are designed to work through walls instead of around them.

Radio Frequency Interference

Varying amounts of radio interference exist all around us. A savvy wireless user can minimize this interference to maximize the performance of his or her WLAN. But before a user can begin to minimize these points of interference, he or she must begin to recognize the more common causes.

The 802.11b standard uses the unlicensed radio spectrum that is commonly shared by a variety of consumer devices: baby monitors and cameras, 2.4 GHz cordless phones, microwave ovens, and Bluetooth-enabled devices like cellular phones or personal digital assistants (PDAs). These devices transmit in the 2.4 GHz range and can impact WLAN performance. DSSS technology, as used in U.S. Robotics 22 Mbps wireless networking products, is very effective at minimizing these types of interference.

A quick scan around a user's home or business will tell if there are any potential problems. Using products designed to work in the 900 MHz frequency can help minimize any interference and maximize the performance of any WLAN.

Antenna Type and Location

There are two general types of antennas used for 802.11: directional and omnidirectional. A directional antenna concentrates energy in a narrow conic path when sending and rejects signals outside a single direction when receiving. An omnidirectional antenna transmits in a 360° arc and is capable of receiving signals from any direction. Most 802.11b devices implement an omnidirectional antenna. The antenna type and location are important factors when setting up a wireless network. Users should experiment with several locations for their access point and antenna in order to determine the optimal location for maximum performance.

Aggregating Bandwidth

For businesses looking to increase performance and for supporting dozens of devices in close proximity, it is possible to overlap access points to provide an aggregate bandwidth to all of the wireless clients. This can be achieved by setting the access points to non-overlapping frequencies for the covered area.

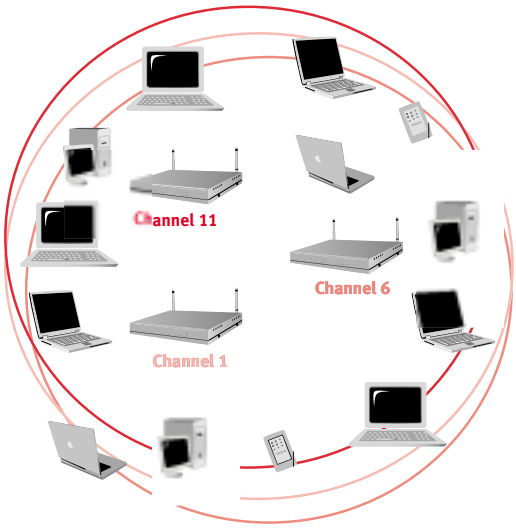

Figure 8 – Aggregating access points to provide more available bandwidth

Bluetooth vs. 802.11b

Those unfamiliar with wireless technology commonly confuse 802.11b and Bluetooth technologies. Both technologies use the 2.4 GHz radio frequency for wireless communications; however, the goal, focus, and concept of Bluetooth is different from 802.11b wireless networking.

Bluetooth technology is focused on replacing the short cables used to connect consumer electronic devices such as keyboards, mouse devices, personal digital assistants (PDAs), computers, printers, and cellular phones. This type of close proximity connectivity is often referred to as a Wireless Personal Area Network (WPAN).

Bluetooth devices differ from 802.11b in a number of ways. Bluetooth is not a "true networking" standard in the manner that Wi-Fi is, and its range is limited to approximately 10 to 30 feet (3 m to 9.1 m) with a raw data rate of 1 Mbps/723 Kbps available. Bluetooth also limits the maximum number of separate 1 MHz simultaneous connections (devices) to seven at a single time.

Since Wi-Fi was designed for higher throughput and a multi-user environment, the two technologies have their own unique places in home and office environments. Technical details about Bluetooth are beyond the scope of this document, and additional information can be found at http://www.bluetooth.com.

Wireless Security

Security is an obvious concern with any network, wired or wireless. Because communication over a traditionally wired network is, by its very nature, over physical wires, security is often built into the physical environment itself. WLANs operate over radio signals, so the same security measures cannot be assumed. For many wireless users, the enabling of the built-in security known as Wireless Equivalent Privacy (WEP) is sufficient for their home or small to medium office WLAN. WEP uses 64- and 128-bit encryption and is the cipher scheme designated for use in 802.11b networking. U.S. Robotics 22 Mbps wireless products include enhanced 256-bit WEP encryption that is not commonly

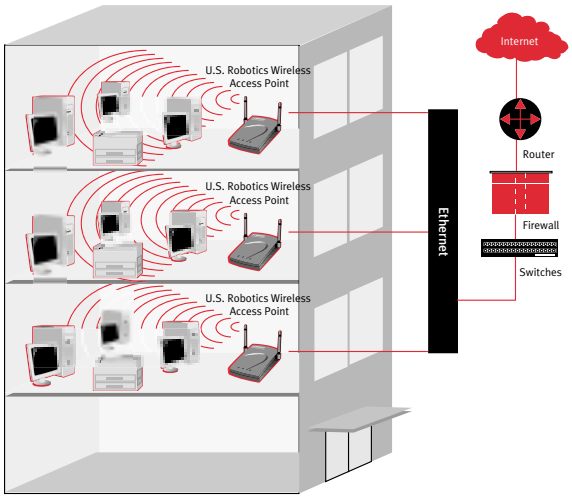

Figure 9 – Locating an access point off of a corporate LAN

available in the 802.11b standard. WEP encrypts the data transmitted over a WLAN, protecting the once vulnerable communication between the client and access point. When combined with traditional security measures (password protection, authentication, encryption, virtual private networks), WEP can be very effective.

For business and enterprise users, network and data security is of the utmost concern. To address this, there are a number of common precautions that a WLAN user can take to limit a network to hacker attacks, vandalism, and corporate espionage.

Change Common Passwords Frequently: Most of the top manufacturers have default passwords for all of their equipment. Users should be diligent in changing any default passwords and to change them on a regular basis in order to avoid detection.

Limit MAC Addresses: Some access points allow users to specify exactly which Media Access Control (MAC) addresses can communicate with the network. A MAC address is a hardware address that uniquely identifies each node of a network. Every network adapter in the world has a unique MAC address. By strictly specifying only those MAC addresses that can attach to a network, unauthorized users can be denied access.

Disable DHCP: By default, some access points respond directly to Dynamic Host Configuration Protocol (DHCP) requests or allow the forwarding of DHCP requests from clients. DHCP is a protocol for assigning IP addresses dynamically on a network. However, with DHCP enabled on a WLAN, and without proper security measures enabled, a user can connect automatically to the network.

Change Subnet Default: Some access points default to the IP subnet of 192.168.x.x. When disabling DHCP and using static IP addresses, users should also change their default IP subnet value.

Move Access Point in Front of Firewalls or DMZs: The best solution for keeping prying eyes away from a corporate network is to move the access point off of the corporate LAN and in front of a firewall or on a DMZ (demilitarized zone) port. With the access point in front of a firewall, intruders will not have access to the corporate LAN. All corporate wireless users will require the installation and use of a virtual private network (VPN) client to create a secure tunnel into the corporate LAN. This may require additional administrative support from IT personnel, but the extra security is well worth the effort.

In addition to offering standard 64- and 128-bit WEP encryption, the U.S. Robotics family of 22 Mbps wireless products also offers the added security of 256-bit encryption for improved security over conventional 11 Mbps wireless products to protect against hackers while maintaining maximum performance. The U.S. Robotics 22 Mbps Wireless Access Point and 22 Mbps Wireless Cable/DSL Router also include the added security of built-in MAC address authentication for even more local network protection.

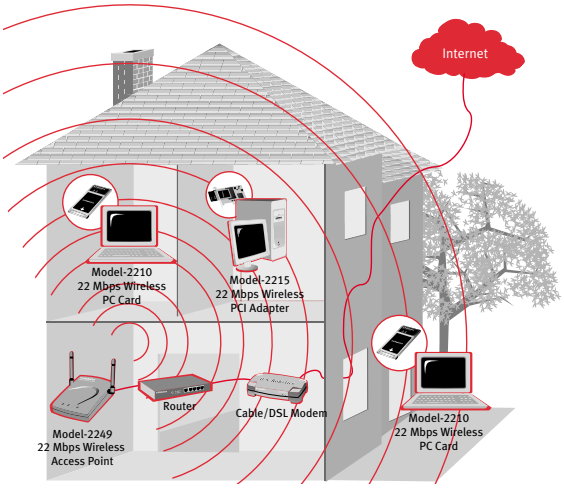

Figure 10 – Locating an Access Point off of a Home LAN

U.S. Robotics Wireless Solutions

With the world's number-one selling modem brand, U.S. Robotics has the most recognized product line in its category within the Internet access industry. Millions of computer users around the globe first connected to the Internet with a U.S. Robotics analog modem. U.S. Robotics has extended its reputation for providing quality, reliability, and technically innovative products to a new line of wireless networking solutions for home and office networking applications. These new products include a complete family of 22 Mbps wireless networking products that provide faster speeds, greater range, and better area coverage than conventional 11 Mbps products.

U.S. Robotics 22 Mbps wireless networking products are fully compatible with all IEEE 802.11b 11 Mbps and 22 Mbps wireless products and will automatically adjust to the fastest rate possible: 11 Mbps or 22 Mbps. This means that networks can easily incorporate a combination of both 11 Mbps and 22 Mbps wireless products. In fact, all U.S. Robotics 22 Mbps wireless networking products are forward compatible and designed to work with the upcoming 802.11g standard when it becomes available. So, whether a wireless client is using the latest 22 Mbps gear, a combination of 11 Mbps and 22 Mbps, or plans on adding the next standard when it becomes available, U.S. Robotics wireless networking solutions can continue to play an integral role in any network.

For simple ad hoc networking of up to three computers, a user simply installs the software, plugs a **U.S. Robotics 22 Mbps Wireless PCI Adapter (Model 2215 or 2216)** into each desktop PC or a **U.S. Robotics 22 Mbps Wireless PC Card (Model 2210)** into each laptop's available PC card slot, and starts sharing Internet access, files, and printers at speeds up to 22 Mbps. U.S. Robotics adapters can support any combination of up to three 22 Mbps Wireless PC Cards and 22 Mbps Wireless PCI Adapters when in ad hoc mode. Security is maintained through 64-, 128-, and 256-bit Wired Equivalent Privacy (WEP) encryption for improved security over 11 Mbps wireless products.

For larger networks (up to 20 computers for an Access Point or Wireless Router) and for enhanced security features like MAC address authentication, a **U.S. Robotics 22 Mbps Wireless Access Point (Model 2249)** or a **U.S. Robotics 22 Mbps Wireless Cable/DSL Router (Model 8022)** with built-in wireless access point can be added easily to an existing LAN – wired or wireless. To network more than 20 computers, include multiple U.S. Robotics 22 Mbps Wireless Access Points or 22 Mbps Wireless Cable/DSL Routers. These two products increase the effective range of a wireless network from 1000 feet to 1500 feet in any direction – even outside or on different levels of a building.

802.11 Committees	Standard Definition
802.11	1 to 2 Mbps using 2.4 GHz frequency
802.11a	Up to 54 Mbps using 5 GHz frequency
802.11b	Up to 11 Mbps using 2.4 GHz frequency with standard 802.11b equipment Up to 22 Mbps with U.S. Robotics Packet Binary Convolutional Code (PBCC) 22 Mbps technology
802.11c	Support for wireless bridge operations
802.11d	Support for improving operations in markets currently not served by the standard
	The IEEE 802.11 Committees below are still in the standard developmental stages.
802.11e	Developing an Ethernet quality of service over wireless
802.11f	Developing multi-vendor access point roaming features
802.11g	Developing >20 Mbps and up to 54 Mbps wireless using 2.4 GHz
802.11h	Developing a uniform standard for transmission and power usage
802.11i	Developing a new security protocol
802.11h	Developing spectrum managed 802.11a
802.1x	Developing a version of the extended authentication protocol (EAP) applicable to wireless networking

For additional information on IEEE wireless activity, standards, and development, visit the IEEE Web site at: http://standards.ieee.org/wireless/.

The U.S. Robotics 22 Mbps Wireless Cable/DSL Router not only includes the functionality of a 22 Mbps Wireless Access Point, but it also includes router capabilities for sharing high-speed Internet access among multiple users spread throughout a household or office building.

All U.S. Robotics 22 Mbps wireless networking products offer numerous benefits and conveniences that can be applied to SOHO (Small Office/Home Office) users, computing environments requiring flexibility, and even existing legacy networks. The IEEE 802 standard supports the same network configuration options of legacy Ethernet LANs, which allows for a variety of applications and solutions.

U.S. Robotics continues to develop solutions to provide data access to both business professionals and home users. U.S. Robotics wireless networking solutions are built upon proven technology and backed by an organization that is committed to the highest standards of product quality and customer satisfaction. These wireless networking solutions from U.S. Robotics represent just some of the latest developments in keeping people connected worldwide – with information, entertainment, and each other.