Wireless Local Area Networks (WLANs)

Wireless Local Area Networks (WLANs)

Wireless local area network solutions comprise one of the fastest growing segments of the telecommunications industry. The finalization of industry standards, and the corresponding release of WLAN products by leading manufacturers, has sparked the implementation of WLAN solutions in many market segments, including small office/home office (SOHO), large corporations, manufacturing plants, and public hotspots such as airports, convention centers, hotels, and even coffee shops.

In some instances WLAN technology is used to save costs and avoid laying cable, while in other cases it is the only option for providing high-speed Internet access to the public. Whatever the reason, WLAN solutions are popping up everywhere.

To address this growing demand, traditional networking companies, as well as new players to the market, have released a variety of WLAN products. These products typically implement one of the many WLAN standards, although dual-mode products that support multiple standards are starting to emerge as well. When evaluating these products, some key areas should be considered, including:

- **Range/coverage.** The range for WLAN products is anywhere from 50 meters to 150 meters.
- **Throughput.** The data transfer rate ranges from 1 Mbps to 54 Mbps.
- **Interference.** Some standards will experience interference from standard household electronics and other wireless networking technologies.
- **Power consumption.** The amount of power consumed by the wireless adapter differs between product offerings, often depending on standards they implement.
- **Cost.** The cost of a solution can vary significantly depending on the requirements of the deployment and which standard is being implemented.

In this section we provide some insight into typical WLAN configurations, as well as the leading WLAN standards.

WLAN Configurations

Wireless LAN configurations range from extremely simple to very complex. The simplest WLAN is an independent, peer-to-peer configuration where two or more devices with wireless adapters connect to each other, as depicted in Figure 3.2. Peer-to-peer configurations are often called ad hoc networks since they do not require any administration or preconfiguration. They also do not require the use of an access point, as each adapter communicates directly to another adapter without going through a central location.

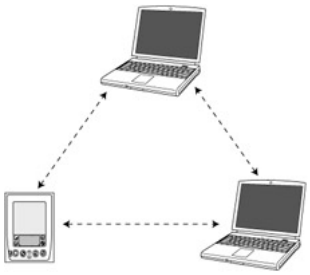

Figure 3.2: Peer-to-peer WLAN configuration.

Peer-to-peer networks are very useful when a group of users need to communicate with one another in an unstructured way. These networks can be extended by adding a wireless access point (AP) to the configuration. The AP can act as a repeater between the devices, essentially doubling the range of operation. In addition, access points can provide connectivity to a wired network allowing wireless users to share the wired network resources. Figure 3.3 illustrates this configuration.

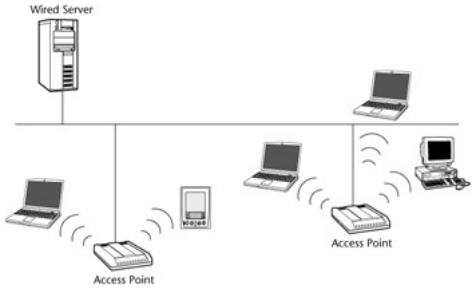

Figure 3.3: WLAN configuration with access point.

In a SOHO environment, access points can be used to provide multiple users access to a single high-speed connection without having to run Ethernet wires to each computer. In a corporate environment, many access points can work together to provide wireless coverage for an entire building or campus. The coverage area from each access point is called a microcell. To ensure coverage over a large area, the microcells will overlap at their boundaries, allowing users to freely move between cells without losing connectivity. This movement between a cluster of access points in a wireless network is called roaming. Roaming is made possible by a handoff mechanism whereby one access point passes the client information to another access point. This entire process is invisible to the client.

In more advanced configurations, extension points (EP) may be used in conjunction with access points. These EPs extend the range of the network by relaying signals to client devices, other EPs, or to an access point. They do not have to be tethered to the wired network, making it possible to service far-reaching clients. One other piece of WLAN equipment is a directional antenna. It allows a signal to be extended to locations many kilometers away. At the second location, the antenna is then connected to an access point, which provides wireless LAN connectivity for the rest of the facility.

WLAN Standards

Two standards bodies, IEEE and European Telecommunications Standards Institute (ETSI) and one technology alliance (HomeRF) promote WLAN standards. In the IEEE 802.11 family of WLANs, three standards deserve individual attention, and a handful of others are worth a quick mention. The leading standard is 802.11b, or Wi-Fi, short for Wireless Fidelity. The clear challenger is 802.11a, which provides increased throughput at a higher, less cluttered frequency; the outside contender is 802.11g, which just completed the final stage of IEEE approval at the time of writing. Other WLAN standards that are worth consideration are HIPERLAN/1 and HIPERLAN/2. We will provide information on each of these standards to give you a firm understanding of their technical and business advantages.

802.11

The IEEE 802.11 specification was approved in July 1997, making it the first wireless LAN standard to be defined. It uses the same switching protocols as wired Ethernet, but allows communication to happen without wires, instead using unlicensed 2.4-GHz frequency radio communication. Two frequency modulation techniques are supported in 802.11: FHSS and DSSS. 802.11 products are not commonly sold anymore, as updated versions (802.11a and 802.11b) have taken its place, providing higher bandwidths at a lower cost.

Note We are starting with 802.11b before 802.11a because it has achieved a higher level of commercial adoption. The letter after the name represents the time at which the specification was first proposed, but not necessarily which one was first adopted.

802.11b/Wi-Fi

802.11b is the most popular standard in the 802.11x family. The specification was approved at the same time as 802.11a in 1999, but since then has achieved broad market acceptance for wireless networking. 802.11b is based on the DSSS version of 802.11, using the 2.4-GHz spectrum. Since DSSS is easier to implement than orthogonal frequency division multiplexing (OFDM), as used in 802.11a, 802.11b products came to market much sooner than their 802.11a counterparts. In addition, the 2.4-GHz spectrum is available globally for WLAN configurations, while the 5-GHz spectrum that 802.11a uses is for limited uses in many countries.

802.11b is able to reach a maximum capacity of 11 Mbps. This surpassed the 10 Mbps speed that is part of the original Ethernet standard, making 802.11b a practical alternative to, or extension of, a wired LAN. To help foster interoperability between 802.11b products, the Wi-Fi Alliance [formerly the Wireless Ethernet Compatibility Alliance (WECA)] has set up certification the aforementioned Wireless Fidelity, or Wi-Fi. Obtaining Wi-Fi certification ensures that 802.11b products will be able to interoperate with other Wi-Fi products globally. This certification, combined with the release of 802.11b products by leading networking companies such as Cisco, Lucent, Agere Systems, Proxim, and 3Com, has made 802.11b the leading WLAN standard.

The use of the 2.4-GHz band for communication has advantages and disadvantages. On the plus side, the 2.4-GHz spectrum is almost universally available for WLAN configurations. Initially, a few countries did not allow for its usage, but this has changed thanks to lobbying by industry groups. Additionally, 2.4-GHz signals are able to penetrate physical barriers such as walls and ceilings more effectively than higher frequencies can. The downside of using the 2.4-GHz spectrum is congestion. Since it is unlicensed, meaning anyone can use it without obtaining a special license, other electronic products also use this frequency for communication. Two common examples are cordless phones and microwave ovens. With the widespread use of this spectrum, there is a possibility that it will become overcrowded, resulting in too much interference for effective data communication. Hopefully, this will not be the case since any manufacturer of any product that uses the 2.4-GHz band is required to take interference into account in its product design.

One interesting point about the 802.11b specification is how it handles roaming between access points. The specification requires a method for roaming, but leaves the implementation up to the AP manufacturer. This will make roaming between different vendors' access points difficult, as it is unlikely that manufacturers will employ the same handoff routines.

In typical indoor office configurations, an 802.11b access point can communicate with devices up to 100 meters (around 300 feet) away. The further away a terminal is from the access point, the slower the communication will be. Devices within about 30 meters can usually achieve a raw data transfer rate of 11 Mbps; beyond 30 meters, the rate drops to 5.5 Mbps, and then to 2 Mbps around 65 meters away, and finally, to 1 Mbps around the outer edge. These numbers represent the anticipated coverage area and transmission speeds, but the products from each vendor will differ in performance. If you are looking to implement an 802.11b WLAN, it is recommended that you do a site survey to obtain the actual operating range and associated bandwidth for your location.

802.11b Security

When the IEEE created the 802.11 specification, it implemented a feature called Wired Equivalent Privacy (WEP) with the intent of providing basic levels of authentication and data encryption. As the name suggests, the goal of WEP is to provide an equivalent level of security as normally present in an unsecured wired LAN. This is clearly important, as wireless networks do not have the physical protection that wired environments do. Both 802.11a and 802.11b specifications use WEP.

For authentication, an access point that has WEP enabled will send a text request to the client to verify the client's identity. The client uses RC4 encryption with a secret key to encrypt the text, then returns the encrypted text back to the access point. Once received, the access point decrypts the text using the same key. If the text matches the text that was sent, then the client is authenticated and granted access. For encryption, WEP provides a 24-bit initialization vector that augments the WEP key. This vector changes with each packet, thereby providing a basic level of data encryption.

Unfortunately, both forms of WEP security present some concerns. For authentication, WEP supports no more than four keys and provides no mechanism for refreshing those keys on a regular basis. The result is that the same keys are used by multiple clients and access points and are never changed. This means that malicious users can "listen" to the communication stream and, by using freely available software, very quickly authenticate themselves to the access point. For the encryption layer, WEP uses RC4 in what is called a one-time-pad manner. The security of a one-time-pad is only as secure as the pad being used, which for WEP is the 24 bits. This means that the onetime-pad is repeated at least every 2^{24} packets. For access points with moderate amounts of traffic, this is a matter of hours, hence, attackers monitoring the datastream could detect two messages encrypted with the same 24-bit initialization vector and be able to determine the keys and decipher the plain text.

Companies should realize that WEP was never designed to provide end-to-end security. It is intended for usage in conjunction with existing security mechanisms such as firewalls, virtual private networks (VPNs), and application-level security. The following are some suggestions for corporations that are using, or planning on using, WEP security as part of their WLAN:

- Use a firewall to separate the wireless network from the wired network.
- Have the wireless users authenticate with a VPN to access the corporate network.
- Incorporate security at the application level for highly confidential information.
- Implement dynamic key refreshing for the WEP keys.
- Do not assume that WEP guarantees absolute data privacy.

Not all of the 802.11 WLAN security issues can be attributed to problems with WEP. Many of these issues have resulted from companies not using the WEP for its original purpose or from not using it at all. By implementing additional security mechanisms as listed, corporations can ensure secure wireless communication. In addition, the 802.11i Task Group is working additional levels of security for 802.11 WLANs. The first component of the 802.11i draft is currently being implemented in the form of Wi-Fi Protected Access. Wi-Fi Protected Access offers increased security over WEP. (More information on mobile and wireless security can be found in Chapter 6 "Mobile and Wireless Security.")

802.11a

802.11a is a high-speed alternative to 802.11b, transmitting at 5 GHz and speeds up to 54 Mbps. Unlike 802.11 and 802.11b, 802.11a uses OFDM modulation technology. This, along with the difference in frequency, makes 802.11a networks incompatible with 802.11b networks. Due to the increased complexity of 802.11a, the first products did not reach the market until early 2002, with all the chipsets being provided by a single vendor, Atheros Communications. Since then other vendors have released 802.11a chipsets, helping 802.11a gain broader market acceptance and interoperability certification.

The Wi-Fi Alliance has included certification for 802.11a products within the Wi-Fi certification program. They are using the same name for both 802.11b and 802.11a to help reduce confusion in the market and to foster growth of the emerging 802.11a products. The Wi-Fi Alliance are hoping that Wi-Fi certification will have the same effect on the 802.11a market as it did on the 802.11b market. Certification gives consumers confidence that the products they are purchasing will work with other products based on the same specification.

The move to the 5-GHz band and OFDM modulation provides two important benefits over 802.11b. First, it increases the maximum speed per channel from 11 Mbps to 54 Mbps. This is a tremendous boost, especially considering that the bandwidth is shared among all the users on an access point. The increased speed is especially useful for wireless multimedia, large file transfers, and fast Internet access. Second, the bandwidth available in the 5-GHz range is larger than available at 2.4 GHz, allowing for more simultaneous users without potential conflicts. Additionally, the 5-GHz band is not as congested at the 2.4-GHz band, resulting in less interference.

These advantages come with some downsides. The higher operating frequency equates to a shorter range. This means that to maintain the high data rates, a larger number of 802.11a access points are required to cover the same area, versus 802.11b. While 802.11b access points have a typical range of 100 meters, 802.11a access points are often limited to between 25 and 50 meters. In addition, OFDM requires more power than DSSS, leading to higher power consumption by 802.11a products. This is definitely a disadvantage for mobile devices that have limited battery power. Another downside is that 802.11a and 802.11b products are not compatible. With the large number of 802.11b products on the market, this will have a negative effect on the adoption of 802.11a products. That said, both standards can coexist, and products are now on the market that support both 802.11a and 802.11b in a single chipset. This dual-mode approach is very attractive for users who want the advantages of 802.11a, with the backward compatibility and market penetration of 802.11b.

One final item to note about 802.11a is that the 5-GHz frequency is not universally available for WLAN products. Many European countries, as well as Japan, are resisting the adoption of 802.11a as a standard, leaving some doubt as to whether it will become a global standard as 802.11b has.

802.11g

IEEE 802.11g brings high-speed wireless communication to the 2.4-GHz band, while maintaining backward compatibility with 802.11b. This is accomplished on two layers. First, 802.11g operates on the same 2.4-GHz frequency band as 802.11b, with the same DSSS modulation types for speeds up to 11 Mbps. For 54 Mbps, 802.11g uses the more efficient OFDM modulation types, still within the 2.4-GHz band. In practice, an 802.11g network card will be able to work with an 802.11b access point, and 802.11b cards will work with an 802.11g access point. In both of these scenarios, the 802.11b component is the limiting factor, so the maximum speed is 11 Mbps. To obtain the 54-Mbps speeds, both the network cards and access point have to be 802.11g compliant. In all other aspects, such as network capacity and range, 802.11b and 802.11g are the same.

Since 802.11g offers the same speed as 802.11a, comparisons between them are inevitable. And because they both use OFDM modulation, the main differences result from their frequency ranges and corresponding bandwidth. The total available bandwidth at 2.4 GHz remains the same as with 802.11b. This results in lower capacity for 802.11g WLANs when compared to 802.11a. In addition, fewer channels are available, leading to a higher potential of conflicts. When we take into consideration the backward compatibility that 802.11g has with 802.11b, 802.11g becomes an attractive option for companies that have 802.11b installations.

Other 802.11 Standards

Just as 802.11g improved upon 802.11b, other 802.11 task groups are in place to improve upon the exiting 802.11x standards. The areas of concentration are security, quality of service, compliance, and interoperability. All of these are still in the task group stage of the specification process:

- **IEEE 802.11e.** Aimed at providing quality of service (QoS) capabilities to enable reliable voice communication to complement 802.11b systems. 802.11e will also provide enhanced security and authentication mechanisms. It is expected to receive final IEEE approval in 2003.
- **IEEE 802.11f.** Aimed at developing the recommended practices for an Inter-Access Point Protocol (IAPP) to achieve multivendor access point interoperability.
- **IEEE 802.11h.** Aimed at enhancing the 802.11a High-Speed Physical layer in the 5-GHz band to make IEED 802.11a products compliant with European regulatory requirements.
- **IEEE 802.11i.** Aimed at enhancing the 802.11 MAC layer to increase security and authentication mechanisms.

HomeRF

As the name suggests, HomeRF is a wireless LAN technology aimed at home wireless networking. It is based on the 802.11 FHSS standard, but enhancements have been made to meet the unique needs of the average consumer. HomeRF uses the Shared Wireless Access Protocol (SWAP). One of the major enhancements of SWAP is its support for high-quality voice communication. Additionally, the HomeRF specification incorporates the Digital Enhanced Cordless Telephony (DECT) standard. This allows cordless phones to use the same home networking infrastructure as PCs and appliances while providing advanced telephony features, including call waiting, caller ID, call forwarding, and personal ringtones.

The HomeRF specification has been designed for ease of use and price rather than bandwidth and performance. HomeRF networks provide a range of up to 50 meters (around 150 feet) with maximum speeds at 10 Mbps. The first generation of HomeRF products provided throughput of 1.6 Mbps. HomeRF uses the 2.4-GHz frequency band so it will experience similar interference as 802.11b from household appliances such as microwaves.

With wide industry adoption of 802.11b, HomeRF products have not been able to reach critical mass. The major advantages of HomeRF over 802.11b are ease of use, cost, and telephony support, all areas being addressed by 802.11b products and upcoming 802.11x specifications. For this reason among others, the HomeRF Consortium disbanded in early 2003, making HomeRF a defunct standard.

HIPERLAN/1 and HIPERLAN/2

The European Telecommunications Standards Institute (ETSI) proposed the High-Performance Radio Local Area Network (HIPERLAN) standard in 1992 to address the need for high-speed short-range wireless communication. This first version is commonly referred to as HIPERLAN/1. It is based on Ethernet standards, with its radio transmission taken from GSM. It uses the 5-GHz frequency band. The operating range and bandwidth is difficult to determine since HIPERLAN/1 did not experience commercial success. According to the specification, HIPERLAN/1 has data rates approaching 23.5 Mbps.

HIPERLAN/2 is the next-generation WLAN specification from ETSI Broadband Radio Access Networks (BRAN). It continues to use the 5-GHz frequency band, but with OFDM technology. It is able to achieve peak speeds of 54 Mbps with an approximate range of 150 meters (450 feet).

HIPERLAN/2 has been designed to address the various market segments where WLANs are used: enterprise networking, SOHO, and 3G wireless hotspots. To this end, it has incorporated QoS for real-time multimedia communication, efficient power consumption for portable devices, strong security and interoperability with Ethernet, IEEE 1394 (Firewire), and 3G mobile systems. The specification also permits roaming between HIPERLAN/2 access points, making it suitable for corporate environments. As of late 2002, HIPERLAN/2 still has not seen any meaningful adoption in either the consumer or corporate space.

WLAN Summary

The market demand for WLAN solutions is growing at a rapid pace across several market segments, including the home, office, and public hotspots. Deciding which technology is appropriate to use is not a trivial task, as all three WLAN specifications have strengths and weaknesses and because each WLAN deployment is unique. When evaluating a WLAN solution, make sure you take into consideration future needs, since the technology upgrade paths depend upon the original choice. The following are some key criteria for selecting the right high-speed WLAN solution for you:

- **Capacity requirements.** If you are installing a WLAN for a large number of users, and population density is a concern, then 802.11a may be a good choice since it provides larger bandwidth to accommodate more users per access point. If not, 802.11b/g might be more appropriate.
- **Interoperability of wireless devices.** Wireless LAN solutions from different vendors may not be interoperable, perhaps because of the frequency band used, the frequency modulation technology (FHSS, DSSS, or OFDM), or just due to the implementation of a particular vendor. Wi-Fi certification helps to ensure that 802.11b and 802.11a products will work with products using the same standard. (The first 802.11g products became available in January 2003.)
- **Timing of high-speed requirement.** If high-speed access is needed immediately, a WLAN technology such as 802.11a or HIPERLAN/2 is probably the right choice. If it can wait, then 802.11b with an upgrade to 802.11g might be suitable.
- **Migration plan.** If a WLAN solution is already in place, or if you are looking to take advantage of proven technology such as 802.11b, keep in mind the migration plans for incorporating higher speeds or, possibly, other frequencies. A range of dual-mode WLAN products are available that support both 802.11a and 802.11b.
- **Interference concerns.** If interference is expected on the 2.4-GHz frequency band from products such as Bluetooth, cordless phones, or even microwave ovens, it might make sense to select a product that is using the less-crowded 5-GHz frequency band.
- **Range/penetration.** Higher-frequency signals have shorter range and worse penetration than lower-frequency signals. In some ways, these effects are mitigated by the system manufacturers, but it is still a worthwhile consideration. In some cases, you may prefer a solution that cannot penetrate walls, to prevent eaves-dropping from outside parties. For longer range and better penetration, the 2.4-GHz standards such as 802.11b and 802.11g are better choices than those using the 5-GHz frequency band.
- **Power requirements.** Does the device using the WLAN technology have a limited power source? If so, power requirements for each standard must be a factor. The rule of thumb is that higher frequencies require more power to transmit the signal the same distance as lower frequencies. This may not apply in all cases, but it is a safe guideline to go by.
- **Regulatory factors.** Are there limitations imposed by your geographic location that you have to consider when choosing a technology? How about the availability of products in your region? These should be taken into account before making any decision.

Table 3.3 provides an overview of the characteristics that you need to evaluate when determining which solution is best for your situation.

Table 3.3: Comparison of WLAN Technologies

STANDARD	FREQUENCY	BANDWIDTH	RANGE	POINTS OF INTEREST
802.11	2.4 GHz	1–2 Mbps	100 meters (300 feet)	The first approved specification in the 802.11 family.
802.11a	5 GHz	54 Mbps	50 meters (150 feet)	Uses OFDM modulation to achieve high data rates; first commercial products became available in 2002.
802.11b	2.4 GHz	11 Mbps	100 meters (300 feet)	Largest market penetration of any WLAN standard, with commercial products available since 1999.
802.11g	2.4 GHz	54 Mbps	100 meters (300 feet)	Approved by the IEEE-SA in the fall of 2002. Backward-compatible with 802.11b.
HomeRF	2.4 GHz	10 Mbps	50 meters (150 feet)	HomeRF did not achieve commercial success.
HIPERLAN/1	5 GHz	Theoretically 20 Mbps	-	HIPERLAN/1did not achieve commercial success.
HIPERLAN/2	5 GHz	54 Mbps	150 meters (450 feet)	Designed for integration with other networks, including wired LANs, IEEE 1394 (Firewire), and 3G mobile networks. Unlikely to achieve commercial success.

One of the most exciting uses of WLAN technology is for providing high-speed Internet access to public hotspots such as hotels, airports, school campuses, and coffee shops. In this scenario, WLAN technologies are being incorporated to wireless wide area network (WWAN) deployments to provide more reliable connectivity at a lower cost. As we discuss WWAN technologies in the next section, we will take a closer look at how WLAN technology is playing a role in the third-generation (3G) wireless deployments.

Remember the name: eTutorials.org

Advertise on eTutorials.org (mailto:admin@etutorials.org)

Copyright eTutorials.org 2008-2018. All rights reserved.