White Paper

Wireless LANs vs. Wireless WANs

White Paper	2130273
Revision	1.0
Date	2002 November 18
Subject	Comparing Wireless LANs and Wireless WANs
Supported Products	Wireless data cards and modules, including 802.11

Kevin Chaplin, B.Sc. (Eng.)
Marketing Engineer
Sierra Wireless, Inc.

SIERRA WIRELESS
HEART OF THE WIRELESS MACHINE®

1: Defining Wireless LANs and WANs

- Wireless LAN
- Wireless WAN
- Bluetooth™

For users who want to access data and information wirelessly, the two main options available are a wireless LAN (Local Area Network) or a wireless WAN (Wide Area Network). These technologies are similar in that they both allow users to access data on their PCs or PDAs without using network or modem cables. These technologies are also rather different in their uses and applications.

This paper discusses the differences between wireless LAN and wireless WAN, and the two technologies are explained in detail, including: coverage, speeds, security, costs and the different uses of each. Also discussed is the possible use of these technologies together and how they compliment each other for wireless data access.

What is a Wireless LAN?

A wireless local area network (Wireless LAN) is a computer network that allows a user to connect without the need for a network cable. A laptop or PDA equipped with a wireless LAN card lets a user move around a building with their computer and stay connected to their network without needing to “plug in” with a cable. The most popular wireless LAN today is called an 802.11b network; the type of wireless LAN referred to in this paper.

Wireless LANs require an access point that all the wireless devices connect to, which then connects the users to the wired network. The coverage of a wireless access point can be up to 100 m (330 feet) indoors.

Wireless LANs are used in office buildings, on college campuses, or in houses, allowing multiple users shared access to one Internet connection. Some airports also plan to, or already offer wireless LAN access. Starbucks® coffee shops are beginning to equip their coffee shops with wireless LANs, which will allow laptop users to connect to the Internet in some of their stores.

Other names for wireless LANs are “802.11”, or “Wi-Fi”. There are also different versions of wireless LANs: 802.11b transfers data at speeds of up to 11 Mbps in the 2.4 GHz radio band. The next version, 802.11a, is supposed to transfer data at even higher speeds of up to 54 Mbps in the 5 GHz band. Wireless LANs are a successful and popular technology, which is widespread and being incorporated into many new laptops as standard equipment.

What is a Wireless WAN?

A wireless wide area network (Wireless WAN), covers a much more extensive area than wireless LANs. Coverage is generally offered on a nationwide level with wireless network infrastructure provided by a wireless service carrier (for a monthly usage fee, similar to a cellular phone subscription).

While wireless LANs are used to allow network users to be mobile within a small fixed area, wireless WANs are used to give Internet connectivity over a much broader coverage area, for mobile users such as business travellers or field service technicians. Wireless WANs allow users to have access to the Internet, e-mail, and corporate applications and information even while away from their office.

Wireless WANs use cellular networks for data transmission and examples of the cellular systems that are used are: CDMA, GSM, GPRS, and CDPD. A portable computer with a wireless WAN modem connects to a base station on the wireless networks via radio waves. The radio tower then carries the signal to a mobile switching center, where the data is passed on to the appropriate network. Using the wireless service provider’s connection to the Internet, data communications are established to an organization’s existing network.

Wireless WANs use existing cellular telephone networks, so there is also the option of making voice calls over a wireless WAN. Both cellular telephones and wireless WAN PC Cards have the ability to make voice calls as well as pass data traffic on wireless WAN networks.

What about Bluetooth™?

Bluetooth™ is sometimes referred to as a wireless PAN (Personal Area Network). Bluetooth is a low power, short-range, two-way wireless communication. Bluetooth is essentially a cable-replacement technology allowing wireless data communication at ranges of approximately 10 m (30 feet). Applications of Bluetooth technology are devices such as a headset that communicates with a mobile phone, or paying electronically for movie tickets, parking meters, and so on.

Bluetooth is not a included in this comparison white paper.

Bluetooth™ is a trademark of The Bluetooth SIG, Inc.

2: Comparing LANs and WANs

Coverage

Wireless local area networks by definition operate over a small, “local” coverage area, normally about 100 m in range. They are typically used in buildings to replace an existing wired Ethernet, or in a home to allow multiple users access to the same Internet connection. Other wireless LAN coverage areas can include public hotspots in coffee shops or some city neighborhoods.

Wireless wide area networks cover a much “wider” area, such as wherever the cellular network provider has wireless coverage. Typically this is on a regional, nationwide, or even global scale. Using a wireless WAN usually gives the user access to data wherever they go and is one of the biggest advantages of a wide area network.

Speed

The 802.11b wireless LAN standard transfers data at speeds of up to 11 Mbps, with typical rates of between 1–4 Mbps, decreasing as more users share the same wireless LAN connection. The next version, 802.11a, is supposed to transfer data at speeds of up to 54 Mbps. However, a potential problem for throughput is overcrowding of the bandwidth. Many people or businesses using wireless LANs in the same area can overcrowd the frequency band on which they are transmitting. Problems with signal interference are already occurring and airwaves may become overcrowded.

Wireless WAN speeds differ depending on the technology used. GPRS networks offer a maximum user data rate of over 115 kbps if all eight timeslots in a cell are allocated for data transmission, (one timeslot can provide between 9 and 21 kbps). However, a realistic and consistent user data throughput rate of 30–50 kbps is expected and seen in practice, when 4 timeslots are used, as currently supported by most networks. This may be increasing in the future. These timeslots are shared with the voice traffic on the GPRS network.

Data speeds on CDMA networks were initially available at speeds of 14.4 kbps, but have increased to a maximum throughput of 153 kbps as carriers have implemented CDMA2000 1X (1xRTT) networks. This gives the user typical throughput speeds of 40–70 kbps, in addition to doubling the voice capacity of the carriers network.

Future wireless WAN technologies, like CDMA2000 1xEV-DO, provide peak data rates of up to 2.4 Mbps in a standard 1.25 MHz CDMA channel. UMTS, also known as WCDMA (Wideband CDMA) is another approved next generation standard which utilizes one 5 MHz channel for both voice and data, offering data speeds up to 2 Mbps.

Data Security

Security is one of the most important features when using a wireless network. Security is one of the biggest strengths for cellular wireless networks (WWANs) and one of the biggest weaknesses in 802.11 networks (WLANs).

802.11b networks have several layers of security, however there are weaknesses in all of these security features. The first level of security is to have wireless LAN authentication done using the wireless adapter’s hardware (MAC) address. However, this alone is not secure because the MAC address of a wireless client can easily be falsely created.

Security can be increased on wireless LANs by using shared key authentication. This shared key must be delivered through a secure method other than the 802.11 connection. In practice, this key is manually configured on the access point and client, which is not efficient on a large network with many users. This shared key authentication is not considered secure and is not recommended to ensure security.

Another weakness in an 802.11 network is the difficulty in restricting physical access to the network, because anyone within range of a wireless access point can send, receive, or intercept frames. WEP (Wired Equivalency Protocol) was designed to provide security equivalent to a wired network by encrypting the data sent between a wireless client and an access point.

However, key management is a significant problem with WEP. WEP keys must be distributed via a secure channel other than 802.11. The key is normally a text string that needs to be manually configured on the wireless access point and wireless clients, which is not practical to a large network. There is also no mechanism to change the WEP key regularly or periodically, so all wireless access points and clients use the same manually configured WEP. With several wireless clients sending large amounts of data, without changing the WEP key, it is possible to intercept data traffic and determine the WEP key. This would allow a hacker to intercept and decrypt the data traffic.

Another problem that has been reported with wireless LANs is that when the security features are turned on, there are problems with interoperability between wireless LAN modules from one vendor and wireless LAN access points from another vendor.

Wireless LANs were designed specifically to operate in the 2.4 GHz band, which is a globally allocated frequency for unlicensed operation. This means that there is no requirement to be a licensed operator to run a wireless LAN in this frequency. A wireless WAN however operates in tightly regulated frequency spectrums and all operators must be licensed to operate in this frequency. This implies much better data security and protection, since licensed operators have to follow government regulations for wireless access.

In contrast to the security weaknesses in 802.11 networks, cellular wireless WAN networks are extremely secure. These networks incorporate military technology and sophisticated encryption and authentication methods.

More detail on the various features of wireless WAN networks can be found in a Sierra Wireless White Paper entitled “Wireless Data Security”, available at www.sierrawireless.com

Hotspots

Hotspots are wireless LANs available to the public in a location, like an airport, coffee shop, or city neighborhood. These (hotspots) enable users to access the network either free of charge, or for a fee paid to the network operator. These networks are being deployed by individuals, wireless LAN operators, and even cellular operators as a way of complimenting their existing cellular networks for data users.

Although the coverage of hotspots is limited, they provide an alternative method of publicly accessing data wirelessly. Obviously security should be a major concern when using a wireless LAN in a hotspot, since there may be no security on the public, shared network.

Costs

Since wireless LANs operate in the unlicensed frequency range, there is no service cost for using a private wireless LAN (such as in a corporate office or home office). There will be a monthly Internet service provider cost for accessing the Internet through your wireless LAN access point (through broadband or cable connection). The other main cost involved is the cost of purchasing and installing the wireless LAN equipment and devices, and the cost of maintaining the network and the users. There are normally fees for using public “hotspot” access.

For cellular wireless WANs, the wireless network is acting as your Internet service provider by providing access to the Internet over their wireless network. The wireless provider therefore charges a monthly subscription rate to their network, similar to a wireless phone subscription. This may be a flat monthly fee, for time connected to the network, or per megabyte of data transferred.

3: Conclusions

- Working Together
- Summary

Can wireless WANs and wireless LANs work together?

Although wireless LANs and wireless WANs may appear to be competing technologies, they are far more useful as complementary technologies. Used together, a user would have the best of both technologies, offering high-speed wireless access in a campus area, and access to all their data and applications with high-speed cellular access from anywhere with wireless WAN network coverage.

A wired analogy of these complimentary technologies would be as follows: A user would plug their laptop (with built in network adapter) into a wired LAN connection while they are in the office. This gives them high-speed access to their e-mail, applications, data, and the web. When they leave the office and work from home, or on the road at their hotel, they would use their dial up modem to have remote access to their e-mail, applications, and the web.

In the wireless example, the same user has a laptop with built-in wireless LAN access. This wireless LAN access is used for high-speed access to applications while in the office. Once out of the office, travelling to a local customer site, completing a work order in the field, or accessing e-mail from a hotel or airport, there is no longer any access to an 802.11 network. The wireless WAN card is now used to access a cellular provider’s network and obtain secure, remote access to e-mail, applications, and the web.

Since many computers are now coming with wireless LAN devices built in, having a wireless WAN PC Card inserted into the computer would ensure that users can have high-speed wireless access where it is available, but still be able to access their important data with their wireless WAN card wherever there is cellular network coverage.

Summary

The following table summarizes the main differences between wireless LAN and Wireless WAN.

	Wireless LAN	Wireless WAN
Coverage	Office Buildings or Campus with some public hotspots	Available wherever there is cellular network coverage; nationwide and global
Throughput Speeds	1–5 Mbps (However the underlying Internet connection may yield a slower speed)	30–50 kbps (GPRS) 40–70 kbps (CDMA2000 1X)
Security	Security flaws	Secure encryption and authentication
Airtime Charges	Airtime charges exist for most Hotspot access. No airtime charges for office or home users (although ISP monthly service fee still exists).	Monthly subscription from wireless network provider
Uses	• Accessing a shared network within a building or across a campus	• Remote access to a corporate network for e-mail and applications • Web and internet access.
Voice	No	Yes
Wired analogy	Ethernet Network	Remote modem access
Advantages	• High speed • No airtime charges to set up networks (hardware costs and broadband internet connection fee still apply)	• Ubiquitous coverage • Secure Network • Access your data from anywhere
Disadvantages	• Localized coverage only • Security problems	• Data rates faster than dial up, but not at wireless LAN speeds yet

When considering wireless LAN and wireless WAN technologies, it is important to note the differences between them and ensure that you choose the right technology for your specific application. Both of these wireless technologies have great advantages when used in the right application, and can compliment each other when used together.

SIERRA WIRELESS
HEART OF THE WIRELESS MACHINE®