An Introduction into WLANs

Executive Overview

Wireless LANs (WLANs) have managed to achieve a rapid growth since their introduction only two years ago and there are good reasons for that. The empowerment of the majority of today's workforce and an increasing amount of team-based work has resulted in an increasing mobility of many employees, both within the same enterprise and also within different geographical locations of the same enterprise. Hence, more and more employees are equipped with portable computers especially since the prices of notebooks and PDAs have fallen dramatically in the last years. This new class of mobile workforce is the primary target of wireless networks since their work requires them to be connected to the enterprise most of the time. WLANs are the ideal choice to provide them with a convenient and affordable access to the enterprise network in offices and conference areas.

Application Scenarios

In general, WLANs are the ideal means if portable devices are to be connected to an enterprise core network. Typical application scenarios include:

- Conference and meeting rooms in enterprises and hotels which allow notebook users to attach to the enterprise network or to the internet (in hotels)
- University campuses which allow students and staff to access the university resources on the whole area
- Department stores and warehouses where employees with small portable terminals like PDAs can roam around and request and input data affecting the inventory
- Restaurants where waiters can be equipped with portable terminals to send orders and print out bills without having to walk to the kitchen or the central cash
- Households where several users want to use a common internet access with their notebooks or desktop PCs
- Locations where cabling would be too expensive or where it is merely impossible
- Public internet access which is typically offered at airports or special "hotspots" in a city. In Singapore, Pacific Internet offers WLANs in many of the popular cafés and shopping malls in the city.

System Components

A typical WLAN architecture for enterprises consists at least of the following components:

- *NIC* (*Network Interface Card*): The most common model is a PCMCIA card that can be used with portable devices like notebooks or PDAs
- *Access Point*: This device connects the wireless LAN to a cables network and thus serves as a bridge between the mobile users and the immobile users like desktop PCs, printers, etc.

In enterprise scenarios, WLAN networks operate in the so-called *Infrastructure Mode*, with one or even more access points. One Access Point is sufficient if a conference room has to be equipped, but large areas such as university campuses require several Access Points that then allow the mobile users to roam from one point to another without losing the connection. Careful network planning ensures that there are no dead spots on the whole area and that there is sufficient capacity on spots with a high density of mobile users.

System Costs

802.11b WLANs have dropped significantly in their price, and PCMCIA NICs are already available at prices at about 155 S$. Access Points start at 300 S$ and can range until 1200 S$. The difference in their price refers to their ability to accommodate more simultaneous users in a WLAN, to additional interfaces, to the possibility of a fast WEP encryption and additional configuration possibilities like Web-based configuration or SNMP agents for network management software. Typically, a home user will opt for the cheaper variant, but when equipping an enterprise WLAN, the higher performance of the more expensive models may be a strong requirement.

Technology

In WLANs data is transmitted by means of radio waves, similar to TV or radio. Currently, there are two frequency bands specified for WLANs: the 2.4 GHz ISM Band, whose exact frequency range is shown in [1][2] and the 5 GHz Band [2]. The 2.5 GHz ISM Band is available throughout the world with minor differences for unlicensed operation in the industrial, scientific and medical field (hence: ISM) which actually means that there is a wide range of equipment besides WLANs that operates in this frequency band and that the installation of equipment does not require any registration with the telecommunication authorities in the respective country. The drawback of this is that interference between different devices is possible. The 5 GHz Band is only targeted at high-speed WLANs but it is not available throughout the world.
In order to transmit data on radio waves, the radio waves have to be formed in a special way that represents the data. This process is called modulation, and most people probably know the modulation schemes AM and FM from their radio receivers. WLANs can use different sophisticated modulation technologies which are listed in Table 1:

Standard	Frequency Band	N° of non-overlapping Channels	Modulation Technology	Data Rates in Mbit/s	Remarks
802.11a	5 GHz	12	OFDM	54, 48, 36, 24, 18, 12, 9, 6	high capacity (12 channels), but frequency band not available all over the world
802.11b	2.4 GHz	3	DSSS	11, 5.5, 2, 1	most used standard, well introduced and widely available
802.11g	2.4 GHz	3	DSSS, OFDM	54, 36, 33, 24, 22, 11, 9, 6, 5.5, 2, 1	backwards compatible to 802.11b

Table 1: The three 802.11 standards for WLANs [2]

DSSS (Direct Sequence Spread Spectrum) is a modulation technology where the user data is modified in a way (through a pseudo noise sequence) that the resulting spectrum is broadened significantly. With this technology, the transmission is resistant to narrow-band interference resulting from other applications in the ISM band. The origins of this technology are based in military data transmissions. The drawback is that it uses a very high data stream of so-called chips, and this high-rated data stream is very sensitive to *multipath propagation* which can result from signal reflections at walls of buildings. Therefore, *equalizers* and *channel estimators* have to be used in order to regenerate the original signal on the receiver side. *OFDM* (Orthogonal Frequency Division Multiplex) splits up the user data stream in several data streams of lower speed and modulates these streams on different radio frequencies. Each radio channel has a relatively low-speed transmission compared to DSSS and is thus less affected by *multipath propagation*. However, OFDM requires either many different transmitters or computationally intensive signal operations before feeding the data in a special transmitter, and this is the main reason why systems using OFDM like 802.11a and 802.11g just come up now, about two years later than 802.11b. DSSS and OFDM must not be confused with physical modulation schemes like QAM, PSK, BPSK, FSK, GFSK, GMSK, AM and FM. Details are highlighted in [2].

Similar to wired LANs like Ethernet (IEEE 802.3), WLANs use a method called *CSMA/CA* (Carrier Sense Multiple Access with Collision Avoidance) in order to administer the air traffic [5]. Like that, a LAN Card sends a short request to an Access Point and waits for a granted access time slot prior to sending a whole data package immediately. Special procedures ensure that simultaneous sending is avoided as far as possible and that retransmission of disturbed data packets occurs transparently for the application programs [5].

Security becomes more and more a critical issue in enterprise LANs, and the WLAN specifications offer several security features like MAC lists, SSID and WEP. A *MAC* (*Media Access Layer*) address is a 48 bit number that is (or should be) unique for each network interface card. If an *Access Point* only allows listed MAC addresses to access it, the users can be chosen individually. The *SSID* (*Service Set Identifier*) is a name for the WLAN network, and it can be configured that only users who know the name can access the WLAN Access Point. *WEP* (*Wireless Equivalent Privacy*) defines an encryption method with a 40 or 128 bits encryption key so that all the wireless data transmission is encrypted. However, all three methods are not a serious obstacle to hackers, and the only reliable way of securing a WLAN is to use a *VPN* (*Virtual Private Network*) and to separate the backbone wired network by the WLAN with a Firewall like it is done at the NTU campus.

Table 2 lists additional WLAN specifications that target some of these issues and intend to resolve them.

Standard	Remarks
802.11e	introduces QoS (Quality of Service) and thus enables VoIP (Voice over IP) services since some data streams can be preferred in their transmission and thus delay times are reduces for critical applications
802.11h	Enhancement to 802.11a which introduces DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) and thus allows the usage of 802.11a in the European Union
802.11i	deals with security enhancements since the WEP algorithms have some design errors which allow hackers to decipher WEP-encrypted WLAN sessions

Table 2: Three important addendums to the 802.11 standards [3][4]

Literature

[1] Jim Zyren and Al Petrick: *IEEE 802.11 Tutorial*
[2] Wireless LAN Association: *High-Speed Wireless LAN Options 802.11a and 802.11g*
[3] CNETAsia: *Digesting the 802.11 alphabet soup*
[4] c't 14/2002, Ernst Ahlers: *Netzen ohne Kabel*
[5] BreezeCom, Pablo Brenner: *A Technical Tutorium on the IEEE 802.11 Protocol*

Web Sites

http://www.ieee.org http://www.weca.net/ http://www.gartner.com http://www.heise.de/ct
http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/np1692-01.pdf
http://203.147.194.107/i802_11/tutorials.asp http://www.linksys.com/products/whitepaper.asp http://www.webopedia.com
http://www.mobileinfo.com/Education/white_papers.htm http://www.itpapers.com/cgi/SubcatIT.pl?scid=39