



WIRELESS TECHNICAL UPDATE Issue 1/2001

In this issue we will give a brief introduction into some issues concerning Wireless Local Area Networks (WLAN). We will also overview the latest information on IEEE802.11 Wireless Networks standards.

CONTENT

Wireless Networks to be or not to be?

<u>Page</u>	<u>Title</u>
1	Introduction
2	Security
3	Wireless standard evolutions

Wireless Networks, To be or not to be?

Introduction

Since the launch of the 802.11b (Wi-Fi) standard in 1999, this technology has walked a rough road and still has numerous obstacles to overcome.

Through the years it has mutually acquired enthusiastic supporters, there were others remain sceptical and reticent towards the whole concept of wireless networking.

The standard has strong market support through the WECA (Wireless Ethernet Compatibility Alliance), an alliance of over 50 wireless-equipment and technology providers spurring towards vendor-interoperability.

Enabling vendor interoperability will allow for market unification, and enables a greater application area for deployment in enterprises, airports and hotels...

Wireless Security

Since recently published reports on wireless security (or the lack of it) it is still hot topic n° 1 in technology discussions and networking articles.

The embedded wireless security called WEP (Wired Equivalent Privacy) is proven to be vulnerable and inefficient towards unauthorised attacks. Various researchers succeeded to successfully break the WEP algorithm, thereby gaining access to private corporate data travelling over the wireless enterprise network.

To enhance the security of wireless communication with the means at hand, start with enabling WEP (by factory-default switched off) and change keys frequently, also use MAC filters to restrict access to authorised users and block the MAC entries of lost or stolen NIC cards

The IEEE 802.11i task group which is addressing these security-issues within the WLAN standard, are doing great efforts to enhance security and strive to overcome the initial security flaws in the implementation of WEP. Enhanced features such as “per session, per user” encryption-key distribution, will provide a secure means for wireless users wanting to access the enterprise network. However, until these features are available and embedded in the standard, other higher layer security solutions can be proposed and are highly recommended.

For now, the most effective solution is to treat wireless clients as remote dial-up users, requiring a process of authentication and authorisation. The use of VPN-tunnelling solutions with IPsec or L2TP encryption provides high security for mobile users, keeping unauthorised users off the network. The benefit here is that most of the authentication takes place independently of the wireless network, keeping access point maintenance simple.

In the next issue we will take a closer look at the promising “port based” 802.1x standard within wireless networking.



Wireless standard evolutions

Another key-aspect in wireless networking is the evolution within the standards, constantly striving to provide higher speeds and greater performance. The current 802.11b (Wi-Fi) standard provides you with a theoretical shared bandwidth of 11Mbps and operates in the 2.4Ghz frequency band. Recently, the IEEE has finally approved the 802.11g standard, which will also work in the 2.4Ghz frequency band and promises speeds up to 54Mbps. Equipment availability for this technology is expected in Q4 2002.

This 802.11g technology has the advantage to be compliant with the widespread installed 802.11b base, eliminating the need for forklift network upgrades.

On the other hand, the license-free 2.4Ghz spectrum is getting crowded, as this is also the operational frequency for mobile phones, Bluetooth devices and even microwave ovens, creating increasing potential for collisions and performance decrease.

Therefore there is a great expectation towards the emerging 5Ghz technologies like 802.11a (baptised Wi-Fi5) and Hiperlan2.

These technologies operate in the license-free 5Ghz frequency spectrum and promise throughput-rates of 54Mbps, enabling the seamless use of bandwidth hungry programs over the wireless network. Some vendors have therefore already launched Access-Points which are 802.11a and Hiperlan2 ready, providing a seamless migration path towards these future wireless standards, creating a future- proof network solution with guaranteed return on investment.

Beware however, for now there are some regulatory differences that need to be addressed within the US version of 802.11a before this technology can be deployed in Europe, these issues are related to the available operational frequency spectrum and the maximum transmitted power level use by wireless equipment. Therefore features as DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) need to be embedded in the standard before European acceptance, within the IEEE, task group "h" is addressing these regulatory issues, leveraging the road towards global standardisation.

When setting priorities for now, most network managers and users are more focused on creating a secure wireless network environment than thinking about migrating to higher speeds. With the recently launched migration platforms you can actually focus on security now and install a future ready infrastructure.