



WIRELESS STANDARDS UPDATE Issue 3/2002

Ever read an article about wireless networking and getting totally confused in all the 802.11-extensions? Within this issue we will try to create some clarification in the WLAN standards- jungle.

Read about the ideal combination of the new Microsoft XP operating system and wireless LAN networks on page 4.

CONTENT

<u>Page</u>	<u>Title</u>
1	WLAN basic standards
2	802.11 standard extensions
3	Windows XP is 802.11 savvy



✓ WLAN basic standards

802.11 is a family of specifications for wireless local area networks (WLAN) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.

802.11b

The 802.11b standard - often called Wi-Fi - is backward compatible with 802.11. The modulation used in 802.11 has historically been phase-shift keying (PSK). The modulation method selected for 802.11b is known as complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference.

802.11a

The 802.11a standard operates in the license free 5 GHz frequency-band. It uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that makes possible data speeds as high as 54 Mbps, but most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps, depending on distance.

802.11g

The most recently approved standard, 802.11g, offers wireless transmission over relatively short distances at up to 54 Megabits per second (Mbps) compared with the 11 megabits per second of the 802.11b standard. Like 802.11b, 802.11g operates in the 2.4 GHz range and is thus compatible with it.



✓ 802.11 standard extensions

The various IEEE 802.11 standards can be confusing, to say the least. In addition to the three main specifications that define complete wireless LAN systems (802.11a, 802.11b, and now 802.11g), the IEEE is working on enhancements that mitigate weaknesses in the existing protocols. These aren't new wireless LAN systems, but rather extensions that will eventually be applied to one or all of the existing three.

- **802.11d** aims to produce versions of 802.11b that work at other frequencies, making it suitable for parts of the world where the 2.4GHz band isn't available. Most countries have now released this band, thanks to an ITU recommendation and extensive lobbying by equipment manufacturers. The only holdout is Spain, which may follow soon.
- **802.11e** will eventually add QoS capabilities to 802.11 networks. It replaces the Ethernet-like MAC layer with a co-ordinated Time Division Multiple Access (TDMA) scheme, and adds extra error-correction to important traffic. The technology is similar to Whitecap, a proprietary protocol developed by Sharewave and used in Cisco's 802.11a prototypes. A standard was supposed to be finalised by the end of 2001, but has run into delays thanks to arguments over how many classes of service should be provided and exactly how they should be implemented.
- **802.11f** tries to improve the hand over mechanism in 802.11 so that users can maintain a connection while roaming between two different switched segments (radio channels), or between access points attached to two different networks. This is vital if wireless LANs are to offer the same mobility that cell phone users take for granted.
- **802.11h** attempts to add better control over transmission power and radio channel selection to 802.11a. Along with 802.11e, this could make the standard acceptable to European regulators.
- **802.11i** deals with 802.11's most obvious weakness: security. Rather than WEP, this will be an entirely new standard based on the Advanced Encryption Standard (AES), the U.S. government's "official" encryption algorithm. The Task Group in charge hasn't yet chosen an authentication protocol: Some members want to use a new system called Offset Code book (OCB), but this is covered by three separate patents; other members would prefer one that everyone can adopt royalty-free.
-



- **802.11j** is so new that the IEEE hasn't officially formed a task group to discuss it, let alone produced a draft standard. It's supposed to cover how 802.11a and HiperLAN2 networks can coexist in the same airwaves.

Source : www.networkmagazine.com

✓ **Windows XP is 802.11-savvy**

When technologies start getting embedded into notebooks and operating systems, they are likely to ramp up in use by default. We can now see that most of the major notebook vendors are shipping IEEE 802.11b network interface cards with their business-class products, often in both "fixed" form factors and as slide-in PC Cards. The premium for the wireless connectivity is about \$100 to \$150, depending on the manufacturer.

As these notebooks ship with the Windows XP operating system, they will become even more wireless LAN (WLAN)-savvy. Windows XP is the first operating system able to recognise wireless devices. If you are hanging around a public hot spot with your notebook running, for example, XP will detect an 802.11 access point. It can even identify the wireless service provider associated with that access point, based on the access point's IP address. So don't be surprised if you are sitting in an airport and find yourself suddenly being asked by your PC whether you want to buy a day's connection to a WLAN service. This is a bit Big Brother-ish for some people, but can certainly be useful if you happen to need wireless, broadband Internet connectivity with a minimum of hassle.

In addition to the auto-detection of an 802.11 LAN, XP comes embedded with 802.1x capabilities. 802.1x is a near-complete standard for authenticating users between 802.11b access points and RADIUS servers. 802.1x also allows for the rotation of encryption keys, so that encoded data is more difficult for hackers to decipher. The advantage of 802.1x running in the operating system rather than on the NIC, notes Dan Park, a board member of the Wireless LAN Association and a product manager at WLAN maker Intermec, is that "someone can't take your NIC, put it in another device, and get access to a network." Rather, he explains, authentication happens at the user level, usually via a RADIUS server, which passes back a user confirmation to the access point. From that point on, the access points manage the encrypted session.◆

Source: Article posted on Network World By Joanie Wexler (21/2/2002)