A Guide to the Wireless Standards

The 802.11 Alphabet

The IEEE 802.11 standards are at the center of the wireless revolution. The wireless alphabet starts with 802.11a and extends to 802.11n. Linux Magazine helps you get your wireless spelling right.

BY JÖRG LUTHER

www.sxc.hu

Networking is in, and wires are out. But owners of WLAN-capable laptops are not the only ones who prefer to do without wires. Many households need to connect more than one computer to the Internet; and consumer electronics devices such as stereos or personal video recorders rely increasingly on LAN connectivity. Wireless connectivity is preferable of course, unless you really want to lay network cable across your living room carpet.

This trend for wireless is reflected by skyrocketing sales in wireless network equipment. Business is booming for WLAN chip and device manufacturers. In Europe alone, wireless turnover is expected to hit the magical billion dollar mark by 2007. This trend is good for customers, too, as increasing quantities mean rapidly falling prices for WLAN equipment.

Instead of a single, and thus reliable standard (IEEE 802.11b), there is a whole alphabet soup of wireless variants for users to choose from. 802.11a, b, g, and h compete for the user's favor as basic technologies, with 802.11n waiting in the wings. And 11c, d, e, f, and i add a little spice to the mix.

Potential customers are typically confused by the variety of options: 11 or 54 Mbps? 2.4 or 5 GHz? WEP, WPA or 802.11i? This article helps you find your way through the WLAN alphabet.

Technology Overview

Wireless networks fall into two major classes, with the frequency band as the decisive factor. Legacy technologies use the 2.4 GHz band, whereas later variants use the wider 5 GHz band. The first class includes The Institute of Electrical and Electronics Engineers (IEEE) 802.11b (11 Mbps) standard and its downwardly compatible successor, 802.11g (54 Mbps). This first class is the most common option at this time of writing.

On the other hand, 802.11a and 802.11h, both of which achieve a nominal throughput of 54 Mbps, operate in the 5 GHz band. 802.11h, which is referred to in the USA as a "compatibility issue in Europe," is the European variant of the US standard. Its two major features are dynamic frequency selection and variable transmitter power, which The European Telecommunications Standards Institute (ETSI) mandates for the European market to ensure that systems have a reasonable transmitter power.

IEEE 802.11c specifies approaches to wireless bridging, that is, methods of connecting different network topologies by wireless means. The 802.11d is typically referred to as "World Mode": it refers to regional differences in technologies – such as how many and which channels are available for use in which regions of the world. As a user, you only need to state the country in which you want to use the WLAN card, and the driver takes care of the rest.

IEEE 802.11e defines Quality-of-Service and streaming extensions for 802.11a/h and g. The aim is to enhance 54 Mbps networks for multimedia applications and Voice over IP – that is, telephony over IP networks and the Internet. The network needs to support guaranteed data rates for individual services, or minimal propagation delays, to be useful for multimedia and voice. 802.11f describes standard handover approaches ("Roaming") for mobile clients between access points, with IAPP, the Inter Access Point Protocol, handling the details.

Security Standards

802.11i was designed to solve the security problems that had troubled wireless LANs up to that point. It integrates everything the world of security has to offer. The major features of 802.11i include IEEE 802.1x authentication, with the Extensible Authentication Protocol (EAP), RADIUS, and Kerberos, as well as encryption based on the Rijndael AES

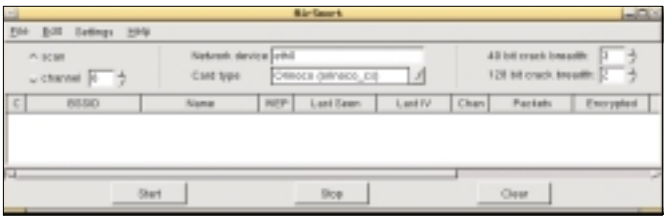

Figure 1: Airsnort is capable of cracking WEP encryption after sniffing a large enough number of packets.

algorithm. The complexity of the 802.11i standard made it extremely difficult to complete: the standard was finally released by the IEEE after a difficult process of negotiations in the late summer of 2004.

The scope and duration of the standardization phase for 802.11i indicate just how aware of security issues manufacturers and organizations now are. The reason for this care is the almost total debacle surrounding the first standardized encryption technique for WLANs, which was known as the Wireless Equivalent Privacy (WEP) standard. WEP is based on a RC4 stream cypher with static keys and an Initialization Vector (IV), which is modified for each packet within a transmission. WEP demonstrated major weaknesses in IV implementation that allow hackers who can sniff a sufficiently large number of data packets to reconstruct the key. In fact, there are analysis tools [2] that handle this task automatically.

Prior to the introduction of 802.11i, WLAN manufacturers attempted to compensate for the inherent weaknesses of WEP using an interim solution known as Wi-Fi Protected Access (WPA), which was developed under the aegis of the Wi-Fi Alliance [3]. WPA's major features are Weak Key Avoidance ("WEPplus"), EAP-enabled authentication, and the Temporal Key Integrity Protocol (TKIP). TKIP is designed to avoid WEP's major weaknesses by replacing the static key with dynamically modified keys and implementing vastly improved integrity checking. For reasons of downward compatibility, TKIP still uses the weak RC4 stream cipher. WPA2 is the term the Wi-Fi Alliance uses to refer to the implementation of all mandatory components of the 802.11i standard.

Table 1: IEEE 802.11 Overview

Working group	Focus
802.11a	54 Mbps WLAN in the 5 GHz band
802.11b	11 Mbps WLAN in the 2.4 GHz band
802.11c	Wireless bridging
802.11d	"World Mode," adaptation to regional requirements
802.11e	QoS and streaming extensions for 802.11a/g/h
802.11f	Roaming for 802.11a/g/h (Inter Access Point Protocol IAPP)
802.11g	54 Mbps WLAN in the 2.4 GHz band
802.11h	802.11a with DFS and TPC, "11a Europe"
802.11i	Authentication and encryption (AES, 802.1x)
802.11j	802.11a with additional channels above 4.9 GHz, "11a Japan"
802.11k	Exchange of capability information between client and access point
802.11l	*not used because of danger of typographical confusion*
802.11m	"Maintenance", publication of standard updates
802.11n	Next Generation WLAN with at least 100 Mbps net

Compatibility Issues

Assuming you will not be setting up a completely new WLAN, you will probably need to give compatibility to existing 802.11b devices some thought. 802.11g has a few things going for it in this respect: 11b and g devices use the same frequency band, the same modulation technique, and the same range, so mixed operations are no problem.

However, compatibility does affect performance: if a single 11b component associates with an 11g network, the system throughput immediately drops from 54 to 11 Mbps.

Mixed operations with 802.11b and g components, but also with older and newer g devices, can cause a few issues. The WLAN 802.11i security standard was not introduced until the summer of 2004. Older wireless networks typically support only the far weaker WEP method and necessitate additional hardening of the network using VPN technologies. Some manufacturers of devices that support a subset of 802.11i **WPA** offer firmware upgrades to 802.11i/WPA2.

So-called Dual-Band/Triple-Mode products can help you avoid compatibility headaches right from the outset. These systems support 2.4 and 5 GHz waveband operations, and all three basic technologies: 11a, 11b, and 11g. From a radio technology point of view, there are no obstacles to interoperating with any other WLAN components. On the downside, these devices are a lot more expensive to buy.

The Wi-Fi Alliance has introduced the "Wi-Fi certified" label to ensure unproblematic interoperations between LAN systems from various manufacturers. Products are required to prove their conformity with current standards by going through a comprehensive test suite, and to demonstrate their interoperability with devices from other manufacturers, before they are given this seal of approval. The Wi-Fi Alliance assigns the certified logo to 2.4 GHz systems with speeds of 11 and 54 Mbps and to 54 Mbps 5 GHz systems for WPA, WPA2, and WMM. WMM stands for Wi-Fi Multimedia and indicates 802.11e conformity.

Figure 2: The certified logo by the Wi-Fi Alliance on the product packing indicates conformity to standards and compatibility with products by third party manufacturers.

Chipset specific and non-standardized transmission technologies with higher data rates fail completely in the compatibility stakes. More specifically, these are "802.11b+" with a speed of 22 Mbps, 108 Mbps modes for IEEE 802.11a products ("Turbo Mode"), and 802.11g ("Super G", "Extreme G"). The gross transfer rates promised by these systems are only achievable using equipment by the same manufacturer and product series.

WLAN 2006: 802.11n

The next generation of WLANs looks set to provide higher data rates, with the IEEE 802.11 committee task group currently working on drafting the standard. WLAN chip manufacturer

Agere has already produced a chip to demonstrate how the underlying technology works. The prototype uses simple means to accelerate the existing 802.11a technology to speeds of 162 Mbps. The system uses three parallel transmitter/receiver antennas to increase the transfer rate, using Orthogonal Frequency Division Multiplexing (OFDM), which 11a defines, to provide clean separation between the individual subcarriers within the frequency band. This trick, which is referred to as MIMO (Multiple Input / Multiple Output), allows the throughput to grow with the number of antennas used, says Agere.

The new 802.11n standard, which is scheduled for introduction in 2006, should achieve net data rates of at least 100 Mbps using MIMO technology. But that is all that we can say with certainty about the successor to today's wireless networks. Two competing industrial lobbies are currently battling it out over the technical framework of the future 802.11n standard.

The TGn Sync faction [4] – the abbreviation stands for "Task Group n Synchronization" – includes Agere and other major players such as Atheros, Intel, Sony, and Philips. The group aims to use 40 MHz channels in the 5 GHz band, and according to Agere, this will put them in a position to support net data rates of up to 500 Mbps.

Figure 3: Some manufacturers have already started to offer "Pre-N" systems based on the MIMO principle. The Belkin router shown here achieves transfer rates of over 300 Mbps in the 2.4 GHz band.

The WWiSE faction ("World Wide Spectrum Efficiency") [5] favors a more conservative approach using 20 MHz channels in the 2.4 GHz band; its most prominent members are Broadcom, Conexant, Texas Instruments, Airgo, and STMicroelectronics. The WWiSE approach promises downward compatibility with b/g systems and offers more conservative use of frequency resources, however, it does not support extremely fast transmission speeds.

Conclusion

The tried and trusted 802.11b standard has not reached the end of its useful life, despite competition from 54 Mbps successors. Versatility and low prices make 802.11b an ideal technology for newcomers. If your bandwidth requirements are moderate, and if you can do without multimedia support, 802.11b is still a good choice.

802.11g is the dedicated successor on the small office/home office market, and it has the advantage of being downwardly compatible.

In contrast, 802.11a/h WLANs are best suited to large networks with large numbers of users. ■

INFO

[1] Bluetooth: *http://www.bluetooth.com/*
[2] WEPCrack: *http://wepcrack.sourceforge.net/*, AirSnort: *http://airsnort.shmoo.com/*
[3] Wi-Fi Alliance: *http://www.wi-fi.net/*
[4] TGn Sync Proposal: *http://tgnsync.org/*
[5] WWiSE Alliance: *http://www.wwise.org/*