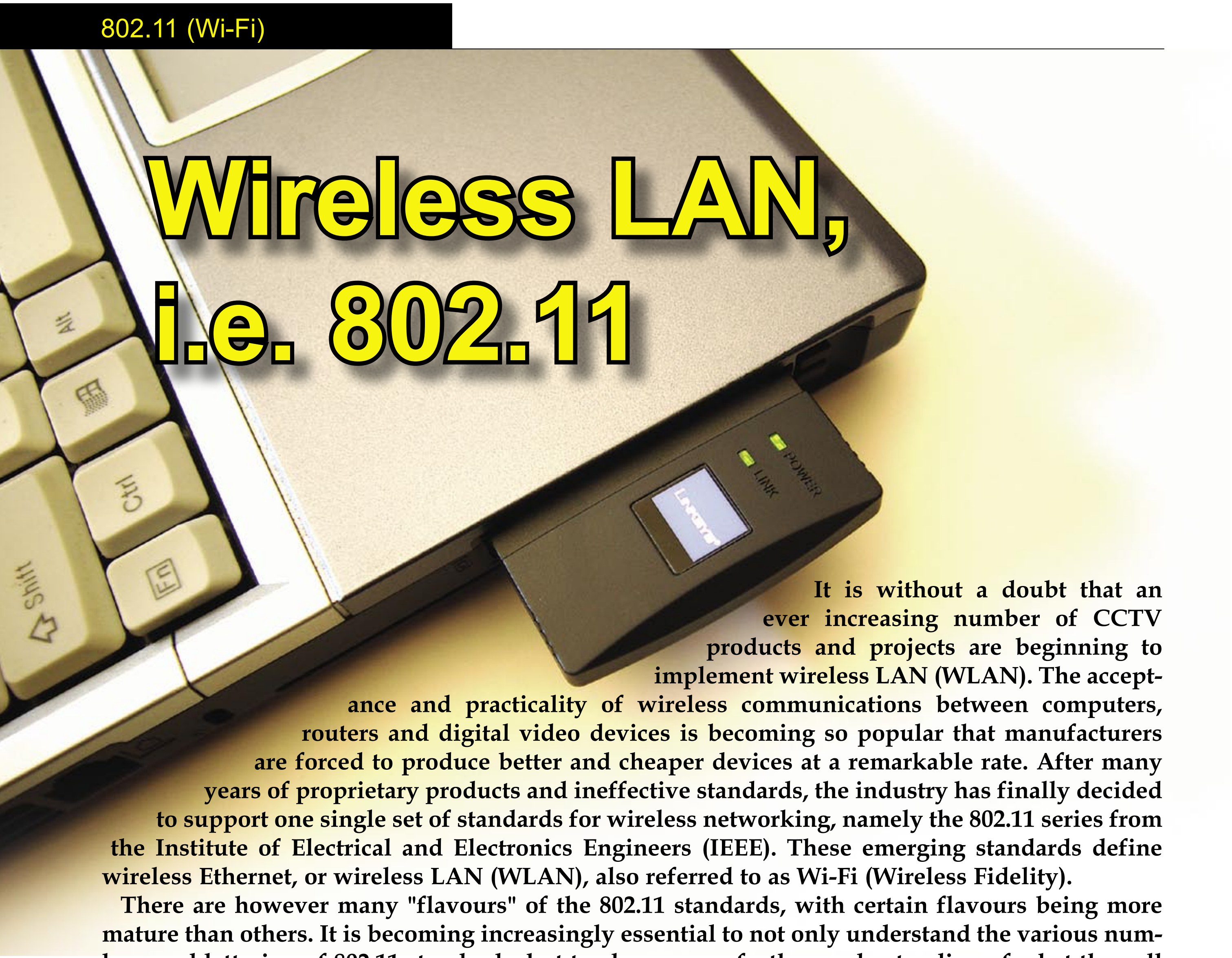
# Wireless LAN, i.e. 802.11



It is without a doubt that an ever increasing number of CCTV products and projects are beginning to implement wireless LAN (WLAN). The acceptance and practicality of wireless communications between computers, routers and digital video devices is becoming so popular that manufacturers are forced to produce better and cheaper devices at a remarkable rate. After many years of proprietary products and ineffective standards, the industry has finally decided to support one single set of standards for wireless networking, namely the 802.11 series from the Institute of Electrical and Electronics Engineers (IEEE). These emerging standards define wireless Ethernet, or wireless LAN (WLAN), also referred to as Wi-Fi (Wireless Fidelity).

There are however many "flavours" of the 802.11 standards, with certain flavours being more mature than others. It is becoming increasingly essential to not only understand the various numbers and lettering of 802.11 standards, but to also grasp a further understanding of what they all offer, and what practical uses they offer in CCTV, as well as in general.

Sales are expanding rapidly as an increasing number of enterprises realise the value of WLANs. Growth has been helped by the Wireless Ethernet Compatibility Alliance (WECA), which provides conformance and interoperability testingand thus far, this group of more than 130 companies has granted its “Wi-Fi” label of approval to more than 185 products conforming to the 802.11b standard.

Globally, other standards bodies have also worked to standardise wireless data networking, The European Telecommunications Standards Institute (ETSI) is an example of one, which has developed "HyperLAN/2" for wireless LANs working at 5GHz which met regulations for working in a radio band traditionally used for radars in Europe although it not achieved the market momentum of the IEEE series.

In Japan, the Multimedia Mobile Access Communication (MMAC) Systems Promotion Council group is developing specifications for advanced types of wireless systems, however the IEEE is implementing additional standards to meet Japan's regulatory guidelines, severly reducing MMAC"s chances of acheiving similar widespread market acceptance.

Within the IEEE’s 802.11 series there are several specifications, some complete and some still under development. Users need to decide which are important; manufacturers need to decide which to include in products; resellers need to select which products to support and recommend; and service providers need to decide which to deploy in services.

## What is 802.11?

IEEE 802.11 or Wi-Fi denotes a set of Wireless LAN standards developed by working group 11 of IEEE 802. The term is also used specifically for the original version; to avoid confusion that is sometimes called “802.11 legacy”.

The 802.11 family currently includes three separate protocols that focus on encoding (a, b, g); security was originally included, but is now part of other family standards (eg, 802.11i).

Other standards in the family (c-f, h-j, n) are service enhancement and extensions, or corrections to previous specifications.

802.11b was the first widely accepted wireless networking standard, followed, paradoxically, by 802.11a and 802.11g.

The frequencies used by the 802.11 are in the microwave range and most are subject to minimal governmental regulation. Licenses to use this portion of the radio spectrum are not required in most locations.

## 802.11 (legacy)

The original version of the standard IEEE 802.11 released in 1997 and sometimes called “802.1y” specifies two data rates of 1 and 2 Megabits per second (Mb/s) to be transmitted via infrared (IR) signals or in the Industrial Scientific Medical frequency band at 2.4 GHz.

IR has been dropped from later revisions of the standard, because it couldn’t succeed against the well established IrDA protocol and has had no actual implementations. Legacy 802.11 was rapidly succeeded by 802.11b.

## 802.11b

802.11b has a range of about 50 metres with the low-gain omnidirectional antennas typically used in 802.11b devices. 802.11b has a maximum throughput of 11 Mbit/s, however a significant percentage of this bandwidth is used for communications overhead; in practice the maximum throughput is about 5.5 Mbit/s. Metal, water, and thick walls absorb 802.11b signals and decrease the range drastically. 802.11 runs in the 2.4 GHz spectrum and uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as its media access method.

With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometres (although some report success at ranges up to 80-120 km where line of sight can be established). This is usually done to replace costly leased lines, or in place of very cumbersome microwave communications gear. Current cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1, if signal strength becomes an issue.

Extensions have been made to the 802.11b protocol (eg, channel bonding and burst transmission techniques) in order to increase speed to 22, 33, and 44 Mbit/s, but the extensions are proprietary and have not been endorsed by the IEEE. Many companies call enhanced versions “802.11b+”.

The first widespread commercial use of the 802.11b standard for networking was made by Apple Computer under the trademark AirPort.

## 802.11a

In 2001, 802.11a, a faster related protocol started shipping even though the standard was ratified in 1999. The 802.11a standard uses the 5 GHz band, and operates at a raw speed of 54 Mbit/s, and more realistic net achievable speeds in the mid-20 Mbit/s. The speed is reduced to 48, 36, 34, 18, 12, 9 then 6 Mbit/s if required. 802.11a has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point.

Different countries have different ideas about regulatory support, although a 2003 World Radio-telecommunciations Conference made it easier for use worldwide. A mid-2003 FCC decision opened more spectrum to 802.11a channels as well.

802.11a has not seen wide adoption because of the high adoption rate of 802.11b, and because of concerns about range: at 5 GHz, 802.11a cannot reach as far as 802.11b, other things (such as same power limitations) being equal; it is also absorbed more readily.

Most manufacturers of 802.11a equipment countered the lack of market success by releasing dual-band/dual-mode or tri-mode cards that can automatically handle 802.11a and b or a, b and g as available. Access point equipment which can support all these standards simultaneously is also available.

## 802.11g

In June 2003, a third standard for encoding was ratified: 802.11g. This flavour works in the 2.4 GHz band (like 802.11b) but operates at 54 Mbit/s raw, or about 24.7 Mbit/s net, throughput like 802.11a. It is fully backwards compatible with b and uses the same frequencies. Details of making b and g work together well occupied much of the lingering technical process. However, the presence of an 802.11b participant reduces an 802.11g network to 802.11b speeds.

The 802.11g standard swept the consumer world of early adopters starting in January 2003, well before ratification. The corporate users held back and Cisco and other big equipment makers waited until ratification. By summer 2003, announcements were flourishing. Most of the dual-band 802.11a/b products became dual-band/tri-mode, supporting a, b, and g in a single card or access point.

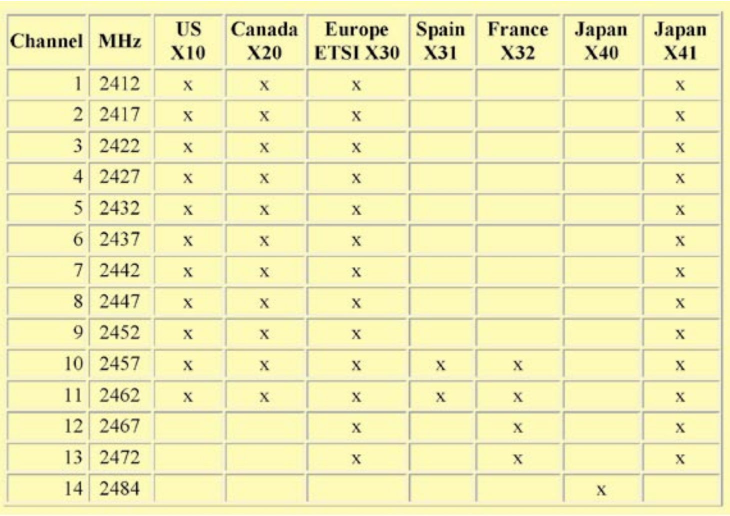
A new feature called Super G is now integrated in certain access points. These can boost network speeds up to 108 Mbit/s by using channel bonding. This feature may interfere with other networks and may not support all b and g client cards. In addition, packet bursting techniques are also available in some chipsets and products which will also considerably increase speeds. Again, they may not be compatible with some equipment.

The first major manufacturer to use of 802.11g was Apple, under the trademark AirPort Extreme.

## Channels and international compatibility

802.11b and 802.11g divide the spectrum into 14 overlapping, staggered channels of 22 megahertz (MHz) each. Channels 1, 6, 11 and 14 have minimal overlap and those channels (or other sets with similar gaps) can be used where multiple networks cause interference problems.

Channels 10 and 11 are the only channels which work in all parts of the world, because Spain and France haven't licensed channels 1 to 9 for 802.11b operation. The full frequency list from IEEE STD 802.11b-1999/Cor 1-2001 is:



| Channel | MHz | US X10 | Canada X20 | Europe ETSI X30 | Spain X31 | France X32 | Japan X40 | Japan X41 |
|---|---|---|---|---|---|---|---|---|
| 1 | 2412 | x | x | x | | | | x |
| 2 | 2417 | x | x | x | | | | x |
| 3 | 2422 | x | x | x | | | | x |
| 4 | 2427 | x | x | x | | | | x |
| 5 | 2432 | x | x | x | | | | x |
| 6 | 2437 | x | x | x | | | | x |
| 7 | 2442 | x | x | x | | | | x |
| 8 | 2447 | x | x | x | | | | x |
| 9 | 2452 | x | x | x | | | | x |
| 10 | 2457 | x | x | x | x | x | | x |
| 11 | 2462 | x | x | x | x | x | | x |
| 12 | 2467 | | | x | | x | | x |
| 13 | 2472 | | | x | | x | | x |
| 14 | 2484 | | | | | | x | |

## 802.11n

In January 2004 IEEE announced that it will develop a new standard for wide-area wireless networks. The real speed would be 100 Mbit/s (even 250 Mbit/s in PHY level), and so up to 4-5 times faster than 802.11g, and perhaps 50 times faster than 802.11b. As projected, 802.11n will also offer a better operating distance than current networks. The standardization progress is expected to be completed by the end of 2005.

## To be merged:

IEEE 802.11a, which operates around the 5 GHz band, enjoys relatively clear-channel operation in the United States and Japan. In other areas, such as the EU, 802.11a had a longer wait for approval, and European regulators were considering the use of the European HIPERLAN standard. 802.11a was cleared for use in Europe around mid 2002. 802.11a also provides for up to 54 Mbit/s operation, but is not interoperable with 802.11b, except in the case of equipment implementing both standards.

## Certification

Because the IEEE only sets specifications but doesn't test equipment for compliance with them, a trade group called the Wi-Fi Alliance runs a certification program that members pay to participate in. Virtually all companies selling 802.11 equipment are members. The Wi-Fi trademark, owned by the group and usable only on compliant equipment, is intended to guarantee interoperability. Currently, 'Wi-Fi' can mean any of 802.11a, b, or g. By fall 2003, Wi-Fi also includes the security standard Wi-Fi Protected Access or WPA. Eventually 'Wi-Fi' will also mean equipment which implements the 802.11i security standard (aka WPA2). Products that say (they are) Wi-Fi are supposed to also indicate the frequency band in which they operate in, 2.4 or 5 GHz.

## Community networks

With the proliferation of cable modems and DSL, there is an ever-increasing market of people who wish to establish small networks in their homes to share their high speed Internet connection.

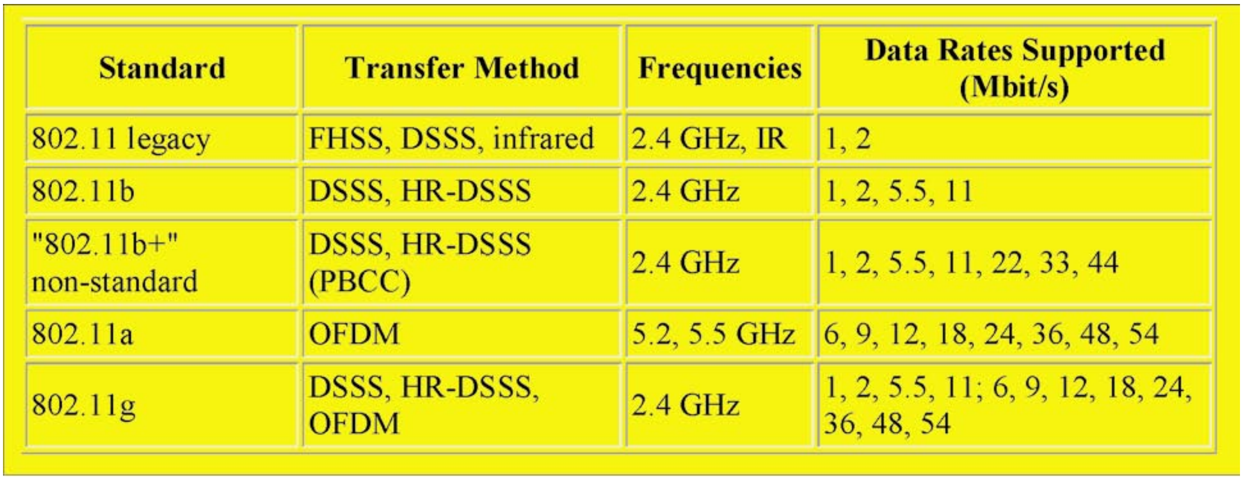
Wireless office networks are often unsecured or secured with WEP, which is easily broken. These networks frequently allow "people on the street" to connect to the Internet. There are also efforts by volunteer groups to establish wireless community networks to provide free wireless connectivity to the public.

## Security

In 2001, a group from the University of California at Berkeley presented a paper describing a weakness in 802.11b described by Fluhrer,

**The following standards and task groups exist with the IEEE 802.11 working group:**

- *IEEE 802.11 - The original 2 Mbit/s, 2.4 GHz standard*
- *IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)*
- *IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)*
- *IEEE 802.11d - New countries*
- *IEEE 802.11e - Enhancements: QoS, including packet bursting*
- *IEEE 802.11f - Inter-Access Point Protocol (IAPP)*
- *IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)*
- *IEEE 802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) and Transmit Power Control (TPC) for European compatibility*
- *IEEE 802.11i (ratified 24 June 2004) - Enhanced security*
- *IEEE 802.11j - Extensions for Japan*
- *IEEE 802.11n - Higher throughput improvements*



| Standard | Transfer Method | Frequencies | Data Rates Supported (Mbit/s) |
|---|---|---|---|
| 802.11 legacy | FHSS, DSSS, infrared | 2.4 GHz, IR | 1, 2 |
| 802.11b | DSSS, HR-DSSS | 2.4 GHz | 1, 2, 5.5, 11 |
| "802.11b+" non-standard | DSSS, HR-DSSS (PBCC) | 2.4 GHz | 1, 2, 5.5, 11, 22, 33, 44 |
| 802.11a | OFDM | 5.2, 5.5 GHz | 6, 9, 12, 18, 24, 36, 48, 54 |
| 802.11g | DSSS, HR-DSSS, OFDM | 2.4 GHz | 1, 2, 5.5, 11; 6, 9, 12, 18, 24, 36, 48, 54 |

Mantin, and Shamir entitled "Weaknesses in the Key Scheduling Algorithm of RC4". This presentation was soon followed by Adam Stubblefield and AT&T publicly announcing the first verification of the attack. In the attack they were able to intercept transmissions and gain unauthorized access to wireless networks.

The IEEE set up a dedicated task group to create a replacement security solution, 802.11i (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an interim specification called Wireless Protected Access (WPA) based on a subset of the current IEEE draft. These started to appear in products in mid-2003. 802.11i (aka WPA2) itself was ratified in June 2004, and uses the Advanced Encryption Standard, instead of RC4, which was used in WEP and WPA.

## What about Bluetooth?

If asked to construct a wireless local area network (WLAN), most IT managers would think of 802.11b wireless Ethernet technology. Few would consider using another short-range radio technology, Bluetooth, on its own or in combination with 802.11b-based equipment.

The reason for its neglect is that Bluetooth has been marketed as a technology for linking devices such as phones, headsets, PCs, digital cameras and other peripherals, rather than as a technology for LANs.

However, Bluetooth could become a serious WLAN option, partly because a lot more Bluetooth devices will be released over the next 12 months. But IT managers may think twice before supporting this technology ¬ because 802.11b and Bluetooth use the same 2.4GHz spectrum to transmit data, interference is a real possibility.

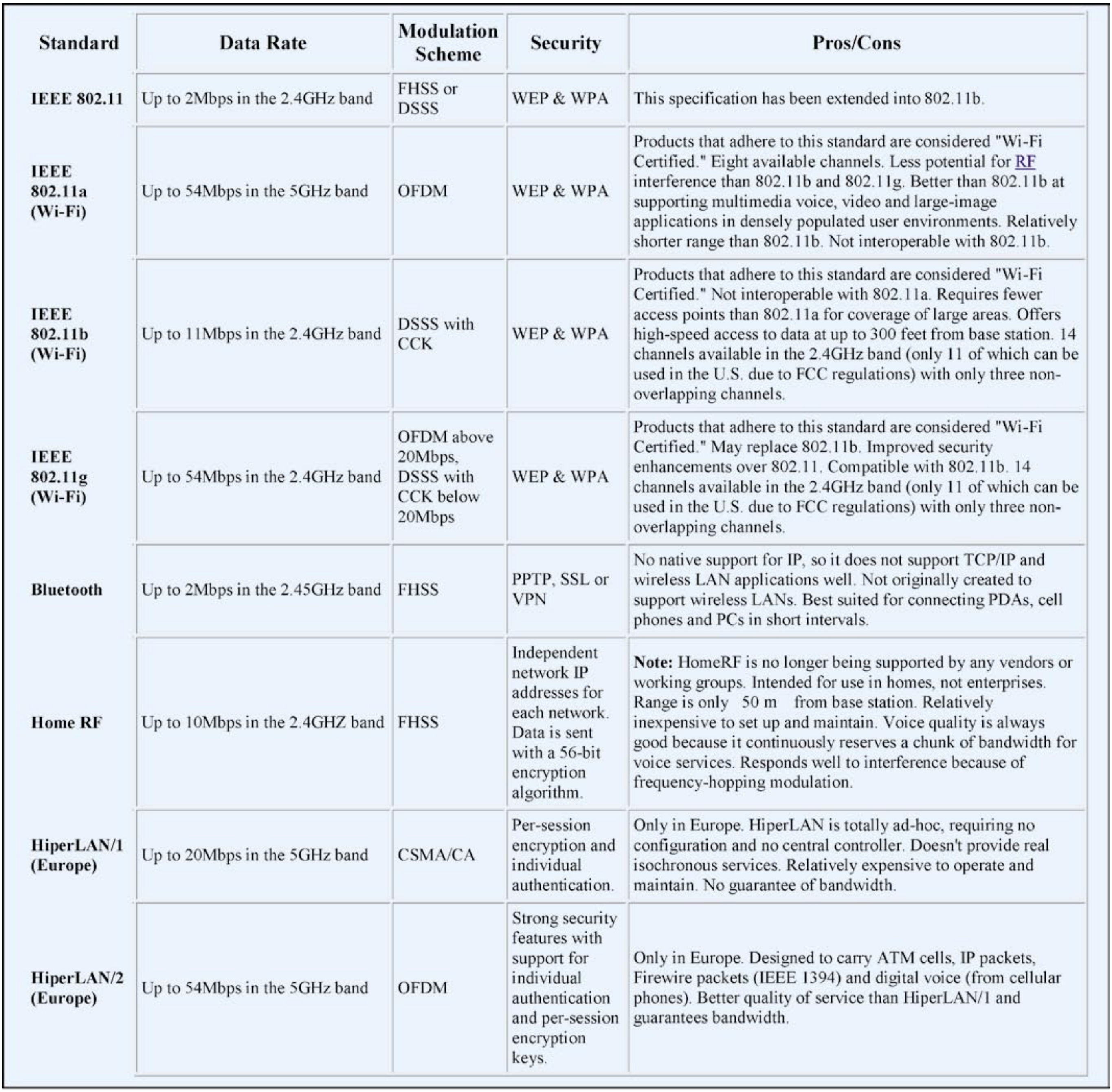
This conflict may lead some IT managers to adopt a cautious approach to Bluetooth on their wireless networks until the standard is better established, said Peter Judge of analyst company Infonetics. "The imminent arrival of Bluetooth is not something that the WLAN suppliers counted on. It must be making a lot of IT managers think twice about installing and relying on 802.11b equipment in areas where there are likely to be lots of Bluetooth devices," said Judge.

The arrival of personal hubs able to handle both types of traffic may provide a solution. Such hubs would sit next to a desktop PC and manage the wired and wireless communication around it. 3Com has a hub system in development. Judge added that it is not yet clear whether Bluetooth will pose a problem. "It's possible that bubbles of Bluetooth activity will be small and therefore not interfere directly with a lot of 802.11b traffic," he said.

Bluetooth is also closing the gap in signal range. TDK Systems is testing a new ceramic antenna that will boost the range of Bluetooth to around 50 metres, up from the 10 metres currently specified and on a par with the maximum range offered by 802.11b components. But TDK, which also manufactures WLAN devices, is hoping it will not be seen as a threat to 802.11b. 'Range is a very emotive and woolly subject,' said Nick Hunn, director of research and development at TDK Systems Europe. 'What's important is throughput. At the moment WLAN easily has the edge, with around 3Mbit/s to 4Mbit/s in practice, compared with about 200kbit/s for Bluetooth. So I think we will start to see Bluetooth in the office for voice services primarily, and 802.11b for data.'

Hunn also stressed that there are options that allow interoperability and migration for the various technologies. He predicted that the huge number of telephone handsets now being sold will give Bluetooth enormous momentum and drive down the price of Bluetooth devices and chipsets faster than their 802.11b equivalents.

Spectralink, a vendor that specialises in voice products for WLANs, was adamant that Bluetooth is no threat. "The Bluetooth camp admit that it is not a network protocol," said Ben Guderian, director of marketing at Spectralink. "Data conflict will be sorted out by the industry bodies involved. IT managers have gone beyond wait-and-see because they know 802.11b WLAN solutions are here today." [•]



| Standard | Data Rate | Modulation Scheme | Security | Pros/Cons |
|---|---|---|---|---|
| IEEE 802.11 | Up to 2Mbps in the 2.4GHz band | FHSS or DSSS | WEP & WPA | This specification has been extended into 802.11b. |
| IEEE 802.11a (Wi-Fi) | Up to 54Mbps in the 5GHz band | OFDM | WEP & WPA | Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b. |
| IEEE 802.11b (Wi-Fi) | Up to 11Mbps in the 2.4GHz band | DSSS with CCK | WEP & WPA | Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels. |
| IEEE 802.11g (Wi-Fi) | Up to 54Mbps in the 2.4GHz band | OFDM above 20Mbps, DSSS with CCK below 20Mbps | WEP & WPA | Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels. |
| Bluetooth | Up to 2Mbps in the 2.45GHz band | FHSS | PPTP, SSL or VPN | No native support for IP, so it does not support TCP/IP and wireless LAN applications well. Not originally created to support wireless LANs. Best suited for connecting PDAs, cell phones and PCs in short intervals. |
| Home RF | Up to 10Mbps in the 2.4GHZ band | FHSS | Independent network IP addresses for each network. Data is sent with a 56-bit encryption algorithm. | **Note:** HomeRF is no longer being supported by any vendors or working groups. Intended for use in homes, not enterprises. Range is only 50 m from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Responds well to interference because of frequency-hopping modulation. |
| HiperLAN/1 (Europe) | Up to 20Mbps in the 5GHz band | CSMA/CA | Per-session encryption and individual authentication. | Only in Europe. HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Doesn't provide real isochronous services. Relatively expensive to operate and maintain. No guarantee of bandwidth. |
| HiperLAN/2 (Europe) | Up to 54Mbps in the 5GHz band | OFDM | Strong security features with support for individual authentication and per-session encryption keys. | Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth. |