

Lemon Computing Ltd

Wireless systems - What are the pros and cons?

Wednesday 8th January 2007



Table of Contents

Purpose of this document.....	2
The pros and cons of wireless.....	2
Standards and compatibility.....	3
The 802.11b Standard.....	3
The 802.11a Standard.....	3
The 802.11g Standard.....	3
Frequencies and regulations.....	4
Congestion and interference.....	4
Performance, speed and range.....	5
Deployment and expansion.....	5
Keeping secure.....	5
Appendix A.....	7

Purpose of this document

This document aims to describe the pros and cons of using a wireless system.

The pros and cons of wireless

Few technologies in recent times have generated quite as much interest as wireless networking, and justifiably so. During a period of overhyped technologies, it's refreshing to find one that genuinely delivers unique and compelling services to both consumers and businesses at every level. Like all technologies though, wireless networking isn't perfect. While deserving much of its recent backslapping, there are a number of important issues every existing or potential wireless user should be aware of.

Beyond the most common issues of standards, compatibility and security, there are increasing concerns over interference and congestion with other networks or devices sharing the same radio frequencies. Head out on the road, and a whole raft of additional issues arise, including the safety of public hotspots, and whether your kit will operate or even be legal while abroad.

Then there's raw performance. Building a wireless network may be as easy as fitting an Access Point, but where should it be located for the best results, and what happens if you want to extend your coverage? Theoretical speeds may also look sufficient on paper, but in practice is wireless really suitable for applications such as streaming high-quality audio and video?

There are certainly plenty of issues to consider, but rest assured we've got the answers to these and more. We'll explain what to look out for and, most crucially, how to solve both common and obscure wireless worries, allowing you to relax and make the most of this impressive and enjoyable technology.

Standards and compatibility

Before worrying about performance, security and interference, the first wireless issue you may experience is plain and simple incompatibility. Over a few short years, the original 802.11 wireless Ethernet standard has enjoyed a raft of extensions, each identified by a lower-case letter tagged on the end. Some refer to entire physical layers designed for networking, while others specifically enhance security, quality of service and interoperability.

The crucial thing, though, is that certain combinations may work together, while others won't. Third-party certification may aim to simplify compatibility concerns, but introduces additional terms and branding. Finally, manufacturers eager to gain a competitive edge may release products based on a new standard while it's still in draft form. It's potentially confusing, so here's a brief compatibility overview of the main standards and certifications in common use.

The 802.11b Standard

There are currently three physical layer standards for wireless networking called 802.11a, 802.11b and 802.11g. The first, and most widespread, is 802.11b, operating on a frequency of 2.4GHz and delivering a maximum speed of 11Mbps.

In theory all devices conforming to the 802.11b standard should work together, but offering additional reassurance is the independent Wi-Fi Alliance with its own compatibility and certification process. Products sporting the Wi-Fi badge are assured to work together.

NB: 802.11b+ refers to a technology which claims to double data rates to 22Mbps. For this to work, the relevant devices must all support 802.11b+.

The 802.11a Standard

The second wireless physical layer standard is 802.11a, operating at a frequency of 5GHz and offering speeds up to 54Mbps. Since 802.11a operates on a different frequency to 802.11b, they are simply incompatible. 802.11a devices won't work on an 802.11b network and vice versa.

Again, while all devices conforming to the 802.11a standard should work together, the Wi-Fi Alliance has also begun certifying them, with a new extended badge differentiating products designed for different frequencies.

Offering some relief to those wanting to use both types of networks though, dual-band equipment is now available, supporting both 802.11a and 802.11b.

The 802.11g Standard

The third and latest wireless physical layer standard is 802.11g, matching the 54Mbps speed of 802.11a, but operating on the same 2.4GHz frequency of 802.11b - this gives 802.11g the unique advantage of being backwards compatible with 802.11b.

In theory, an 802.11g device should work on an 802.11b network and vice versa, although to enjoy 54Mbps, both the device and network need to support 802.11g. The official 802.11g standard was completed in June 2003, but numerous products based on an earlier draft specification have already been on sale for some months.

While each supplier has offered assurances of compatibility with the final 802.11g specification (or upgrades if they don't), it's too early to tell if there are any serious concerns for early adopters. In our own tests with draft 802.11g equipment, we measured similar speeds to 802.11a, and confirmed compatibility with 802.11b devices. Unfortunately, once an 802.11b device was connected to our draft 802.11g network though, it forced all draft 802.11g devices to operate at the slower 802.11b speeds.

Despite being a recognised problem, several 802.11g manufacturers now claim this has been fixed. One solution involves building access points with two antennas, but until such products or those conforming to the final specification are tested, we can't comment. Early adopters of draft 802.11g equipment may wish to contact

their supplier for information on possible updates, although if they're exclusively using 802.11g devices, they should be fine.

With the specification now finalised and officially ratified by the IEEE, we should soon know what 802.11g is truly capable of, warts and all; Wi-Fi certification will follow soon after. Suffice it to say we will keep you updated with all the news and test results. In the meantime, users interested in supporting the maximum number of standards should consider new tri-mode/dual-band products supporting 802.11a, b and g.

Finally we should mention Intel's Centrino brand, which can be applied to notebook computers featuring a Pentium M processor, Intel 855 chipset and an Intel integrated wireless network connection. The first Centrino notebooks employ 802.11b, although we can expect dual-band 802.11a /b in the near future, and 802.11g support probably added in the new year.

Larger enterprise users may additionally be interested in products with Cisco-compatible extensions, which assure compatibility with Cisco's wireless security suite. Centrino notebooks and products based on new Atheros chipsets already support Cisco-compatible extensions.

Frequencies and regulations

In the previous section we said all devices conforming to the same physical layer standards should work together - so one 802.11b device should work with another 802.11b device and so on. One potentially large fly in the ointment, though, is how radio resources have been split up worldwide, with countries often using different regulations or reserving certain frequencies for non-public use.

Consequently, while all devices conforming to the same physical layer standard and originating from the same country should work together, taking them abroad may be an entirely different matter. A wireless globetrotter could find themselves abroad with equipment that simply doesn't work or may even be illegal. This is clearly a big issue for anyone using corporate, domestic or public wireless networks, while on holiday or business travel.

To discover which products can work together and whether they're allowed in certain countries, you must delve into certified frequency ranges and radio channels. In doing so, the broader capabilities, potential congestion and ultimate capacity of various standards are revealed. 802.11b and 802.11g are described as operating on a frequency of 2.4GHz, but their range potentially runs from 2.412 to 2.484GHz. This range defines 14 radio channels, but the full number are only certified for use in Japan.

ETSI (European Telecommunications Standards Institute) regions in Europe have certified 2.412 to 2.472GHz for 802.11b and g, allowing channels 1 to 13 to be used. North America and Spain are the most restrictive, allowing a range of 2.412 to 2.462GHz with channels 1 to 11. Consequently you can use channels one to 11 in any of these regions, but 12 and 13 are only certified for ETSI Europe and Japan, while 14 is for use in Japan. Wireless kit bought in various regions should conform to that region's regulations, but check the specs to see if it was designed for use elsewhere. We've recently reported US-spec cards being sold in the UK, for instance.

In practice for 802.11b and 802.11g, channel selection is rarely a problem. The channel is set on an access point, after which all clients configure themselves. The only potential problem is if, say, a European access point has been set to channel 12 or 13, preventing a US client from connecting. The worst case scenario is a Japanese access point set to 14, blocking everyone apart from local clients. We can only hope that public hotspot and corporate network administrators stick to channels one to 11 for international compatibility. There are additional issues with 802.11b and 802.11g channels in terms of congestion, which we'll discuss later.

Congestion and interference

Perhaps the biggest technical issue facing day-to-day wireless networking is interference, either from nearby wireless networks or devices sharing the same radio frequencies. The 2.4GHz frequency is particularly congested, with 802.11b and 802.11g networks sharing the same radio resources as Bluetooth, microwave ovens, cordless phone systems, baby monitors and wireless video senders.

One solution is to try changing the channel on which your access point or device is operating, but if this

doesn't work, you will either have to switch off the conflicting device or swap it for one operating at a different frequency. Careful channel selection is also essential to avoid interference between nearby Wireless Access Points. While you may believe the 11 to 14 channels of 802.11b and 802.11g provide plenty of scope, each one overlaps with the next.

In fact to eliminate interference, you should select 802.11b/g channels numbered as many as five apart. Consequently 802.11b and 802.11g are limited to just three non-overlapping channels: 1, 6 and 11. If you have an 802.11b/g network with more than one access point, ensure each is set on a different non-overlapping channel. The same applies to other 802.11b/g networks in range, such as a neighbour or adjacent office. Consequently to maximise your performance and range you must co-operate with neighbouring networks to avoid using conflicting channels.

Performance, speed and range

The prospects of cable-free networking open up all manner of possibilities, but to avoid disappointment it's important to understand any performance limitations. In terms of speed, most Ethernet networks tend to perform at roughly half their quoted maximum due to protocols and other overheads, and wireless is no different.

802.11b may be described as offering 11Mbps, but from our tests you should expect around 4.5Mbps at best. Similarly, the 54Mbps maximum of 802.11a and 802.11g works out nearer 20Mbps in real-life apps, although we've measured it operating as slow as 10Mbps even under good conditions. Depending on your wireless kit, you may also experience a further reduction in performance with Wired Equivalent Privacy (WEP) encryption activated.

In tests with some 802.11b access points, we've experienced 10 to 20 per cent performance hits using 64 and 128bit encryption respectively. Additional users accessing the network will share the available bandwidth, reducing your personal allotment.

In terms of range, figures are dependent on surroundings and normally work out much lower than theoretical maximums. Each installation varies, but during indoor tests with budget 802.11b access points we've measured ranges of around 10m while maintaining maximum speed, or 20m at half speed.

Deployment and expansion

In theory you can place an access point anywhere to build a wireless network, but some locations work much better than others. For the best range, position your access point roughly in the middle of the desired coverage area and high on a wall away from any physical obstructions.

Also consider hidden joists and what's behind walls, as nearby metal sheets, tanks or girders can impact wireless range. If your access point is built into a wireless router, you may not have to mount the entire thing on a wall - many support external antennas which can be easily positioned.

Every access point has a maximum operating range and number of simultaneous users, but if you need to increase either, simply add extra access points to your network. The use of multiple access points on a single network is known as roaming. Multiple access points on the same network must share the same SSID name, but be set to different non-overlapping channels to avoid interference.

Keeping secure

The radio waves that transport wireless networking data can easily penetrate walls and be received by snoopers. Consequently, unless you live in the middle of nowhere or don't care about your data, then security is in order.

802.11a, b and g all offer encryption using the WEP system. While reasonably effective at keeping out basic snoopers, WEP is widely considered to be inadequate against anything more serious; indeed many believe it's

discouraging larger corporates from adopting wireless.

During the next year WEP will be replaced by a security amendment known as 802.11i. In the meantime the Wi-Fi Alliance has taken a subset of 802.11i and created Wi-Fi Protected Access (WPA), which offers better security than WEP and is being offered on new products or as firmware updates on others - a WPA update is already available for Centrino notebooks.

Worried corporates can, however, implement additional security measures by connecting users through Virtual Private Networks (VPNs). This seems the safest way to use public hotspots, many of which do not use encryption.

Cautious users of non-encrypted wireless networks may wish to avoid submitting sensitive data such as personal or credit card details until they return to a known cabled environment. Finally, if you're connecting to someone else's network, it's probably wise to have anti-virus software running.

Appendix A

The table below outlines the wireless standards discussed in this document.

Attribute	Wireless A	Wireless B	Wireless G	Wireless N
Wireless standard	802.11a	802.11b	802.11g	802.11n
Maximum speed	54 MBit/s	11 MBit/s	54 MBit/s	100 Mbit/s – 540 MBit/s
Approximate speed in use	20 MBit/s	4.5 MBit/s	20 MBit/s	At least 100 MBit/s
Theoretical range outdoors at top speed	30m	120m	50m	Further than current standards
Theoretical range indoors at top speed	12m	60m	20m	Further than current standards
Operating frequency	5 GHz	2.4 GHz	2.4 GHz	Not yet known
Total channels in UK	8	13	13	Not yet known
Non-conflicting channels	8	3	3	Not yet known
User per wireless router/access point	64	32	32	Not yet known
Compatible with	802.11a	802.11b, 802.11g	802.11b, 802.11g	Not yet known
Official standard	Yes	Yes	Yes	Expected during 2006