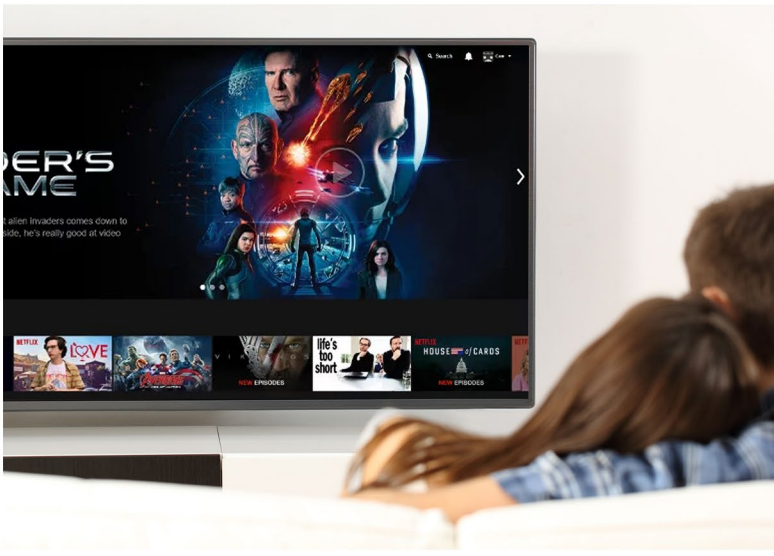
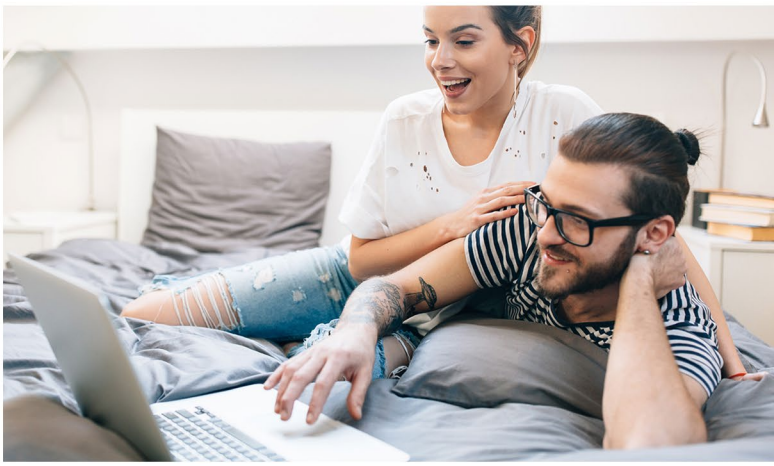
KITGURU

TECHNOLOGY **BUYER'S GUIDE** TO **ROUTERS**





CONTENTS

THE GUIDE TO ROUTERS

WIFI ROUTERS: THEN AND NOW

NOW that WiFi is considered a basic need along with air to breathe and food, it's easy to forget that the technology has only been in popular usage for less than two decades. The benefits of ubiquitous wireless networking at home and at work are so great that we now take it for granted, and our tempers rise when coverage is less than optimal.

It's clear that having the best wireless router at home and in your company is essential. In this technical booklet, we will be presenting a definitive guide to WiFi routers. We will trace the origins of WiFi and look at how to get the most out of wireless and your router's other networking capabilities whether in the domestic or business environments. We will focus particularly on the important area of keeping your WiFi secure, and ask a leading industry expert where the technology is headed.

Although we still call wireless networking WiFi and use the same Yin-Yang-style black and white logo introduced in September 1998, the technology itself has developed enormously over its 20 years.

This has been visible through the succession of 802.11 standards, starting with the original 1997 version and culminating in the current 802.11ac (so far...).

Most WiFi still operates on the 2.4GHz or 5-5.8GHz wavebands (with the latter normally abbreviated to 5GHz), although 60GHz 802.11ad WiFi was introduced in December 2012 for very high bandwidth at very short distances, and 900MHz 802.11ah in December 2016 for long range and low power for Internet of Things devices.

The first 2.4GHz WiFi operated at up to 2Mbits/sec, which then became the 802.11b that was the first popular standard, with up to 11Mbits/sec, followed by 802.11g with up to 54Mbits/sec. The 802.11n standard introduced MIMO technology over both 2.4GHz and 5GHz, where signals from multiple antennas could be combined to increase throughput.

Whilst 802.11n continues to be used today, it is being replaced in end-user devices by 802.11ac, which employs MIMO over 5GHz exclusively to provide theoretically up to 1.7 Gbps of bandwidth. But an even faster 802.11ax is on the roadmap for ratification by the end of 2018, promising up to 10.53Gbits/sec.

All of these are theoretical limits, however, and the true values depend on the products you use and how you set them up. In this guide, we will be looking at both home and business scenarios. But first let's run through some of the key terminology we will be using throughout this guide.

TAKE AWAYS

1 MIMO-capable WiFi such as 802.11n and 802.11ac increases bandwidth by sending data over multiple antennas and wavebands simultaneously.

2 Home WiFi is normally secured via a passphrase that goes with the SSID of the wireless network, but corporate WiFi usually adds a full login procedure on top of the SSID for further resilience.

3 The higher the frequency band, the shorter the range tends to be, which is why 2.4GHz 802.11n can often reach further than 5GHz 802.11ac, and 60GHz 802.11ad only operates in close proximity.

GLOSSARY

Networking used to be a dark art. There was no wireless and simply connecting 2 computers in the same room required expert knowledge. These days, most devices connect quickly and easily. That has been made possible by various standards that have been introduced over the past 40 years or so. We've broken down the most commonly used terms to help you better understand networking in general and routers in particular. The Institute of Electrical and Electronics Engineers (IEEE) were crucial in the formation of many of these standards – specifically those relating to 802.11 which describes a set of media access controls and physical layers necessary for wireless communications. The IEEE was also important in the creation and development of the WEP security standards.

CCMP – CTR Mode with CBC-MAC Protocol is a temporal key system like TKIP, but with stronger security. It uses AES encryption alongside message authenticity and integrity checking.

DSSS – Direct-sequence spread spectrum is a modulation system where a signal is spread across a wider waveband to improve resilience to interference. It's used by 802.11b WiFi and was an option for the original 802.11.

EAP – The Extensible Authentication Protocol is a framework for providing authentication methods so that users can login for access to a resource. It is used by 802.1x as an added level of security for WiFi networks.

FHSS – Frequency hopping spread spectrum is a modulation system where the signal is spread across a spectrum by rapidly hopping from frequency to frequency. It's used by Bluetooth and was an option for the original 802.11 standard.

OFDM - Orthogonal frequency-division multiplexing divides each channel into subchannels for greater robustness, because interference only knocks out one subchannel not the whole channel. It is used by 802.11a, 802.11g, 802.11n and 802.11ac.

MIMO-OFDM – Multiple-input, multiple-output OFDM is a process whereby the throughput is increased by transmitting an OFDM signal over multiple channels simultaneously.

MU-MIMO – Multi-user multiple-input, multiple output allows more than one MIMO-OFDM client to communicate with a base station at once.

RADIUS – Remote Authentication Dial-In User Service works alongside EAP to provide 802.1x login. A server supporting RADIUS provides the service to the client device.

SSID – The Service Set ID (SSID) is a logical network name, usually denoted by a natural language label. They can be left visible to WiFi client devices in the neighbourhood, or hidden from detection for added security.

TKIP – Temporal Key Integrity Protocol, which uses the SSID and passphrase or 802.1x server to generate a new 128-bit RC4 key for each packet of data sent over the WiFi network.

WEP – The Wired Equivalent Privacy algorithm was an initial attempt to bring the natural security of cabled Ethernet to a wireless network using encryption. It was superseded by WPA.

WPA – Introduced to provide a much more robust security for wireless networks compared to WEP. It uses a SSID and passphrase like WEP but introduces TKIP to prevent cracking of the encryption key via packet sniffing.

WPA2 – An enhancement of WPA that further strengthens security by replacing TKIP with CCMP for its per-packet encryption.

While computers work in bits internally, when it comes to sending data over a network, it's more common to bunch a block of bits together into a packet. Typically, the front of the packet will have an address, something to say what kind of data is being carried and an idea of how big the packet is. The back of the packet will hold checking information - to help confirm that it arrived OK. The forerunner of modern packet switched networks was set up in 1971 to help connect the islands of Hawaii. It was called ALOHAnet and it ran on UHF radio waves. Ethernet and 802.11 would follow years later.

IEEE 802.11

802.11ac – Unlike 802.11n, this standard only operates at 5GHz. It arrived in 2013. Using channels up to 160MHz wide, the maximum bandwidth with four spatial streams is 3,466.8Mbits/sec, although up to eight spatial streams are theoretically supported.

802.11ad – Also known as WiGig, this is not a replacement or evolution of mainstream WiFi, but a specific wireless standard for very high bandwidth short-range connections. It operates at 60Hz, which is unlikely to penetrate walls, but provides up to 6,756.75Mbits/sec data rate.

802.11ah – This is not a replacement or evolution of regular WiFi either, but a low-power variant introduced in 2016 primarily in support of the Internet of Things. It operates at 900MHz and provides a theoretical maximum 347Mbits/sec bandwidth with 16MHz wavebands and three spatial streams.

802.11x – This IEEE standard provides authentication control for wired and wireless networking devices, so uses must login via EAP before they can get access to the network.

802.11-1997 – The original WiFi standard released in 1997 and clarified in 1999. It provided 1 or 2Mbits/sec over 2.4GHz, a bandwidth too low for widespread adoption.

802.11b – The first evolution of 802.11-1997, arriving in 1999 and offering a raw 11Mbits/sec over 2.4GHz, although in practice the maximum was 5.9Mbits/sec using TCP and 7.1Mbits/sec using UDP.

802.11a – A parallel evolution of 802.11-1997 to 802.11b, but shifting to 5GHz with OFDM, allowing a maximum throughput of 54Mbits/sec. It was ratified in 1999. The higher frequency gave slightly shorter range than 2.4GHz 802.11b.

802.11g – Arriving in early 2003, this standard copied the OFDM system of 802.11a to the 2.4GHz waveband, providing the same 54Mbits/sec theoretical maximum bandwidth. Included in Intel's first Centrino specification, 802.11g was when WiFi came of age.

802.11n – Although draft versions preceded it as far back as 2006, this standard arrived in final form in 2009. Operating over 2.4GHz and 5GHz, its main innovation was MIMO, allowing up to 600Mbits/sec with 40MHz channels and four spatial streams.

Wi-Fi **TCP/IP** **Packets** **Hashing** **Ethernet** **DNS** **Fibre** **RJ45** **Port** **NIC** **Bandwidth**

HOME USER

THE ability to have WiFi in the home has been a huge liberation (and maybe a new problem for those with teenage kids). If your broadband is supplied with a WiFi router, it's very tempting just to leave things at that and stick with what came with your subscription, particularly if it was included in the monthly subscription.

But this could mean you end up with a very basic router that can't supply the fastest WiFi, has a limited range, and only offers a few management features.

Most routers come with some form of firewall to protect your internal network, but there is a huge variation in the strength and configurability provided. You may benefit from features to enhance your gaming experience (see page 10), or there could be useful interoperability with voice control systems like Alexa. Or you may need to control how your kids access the Internet.

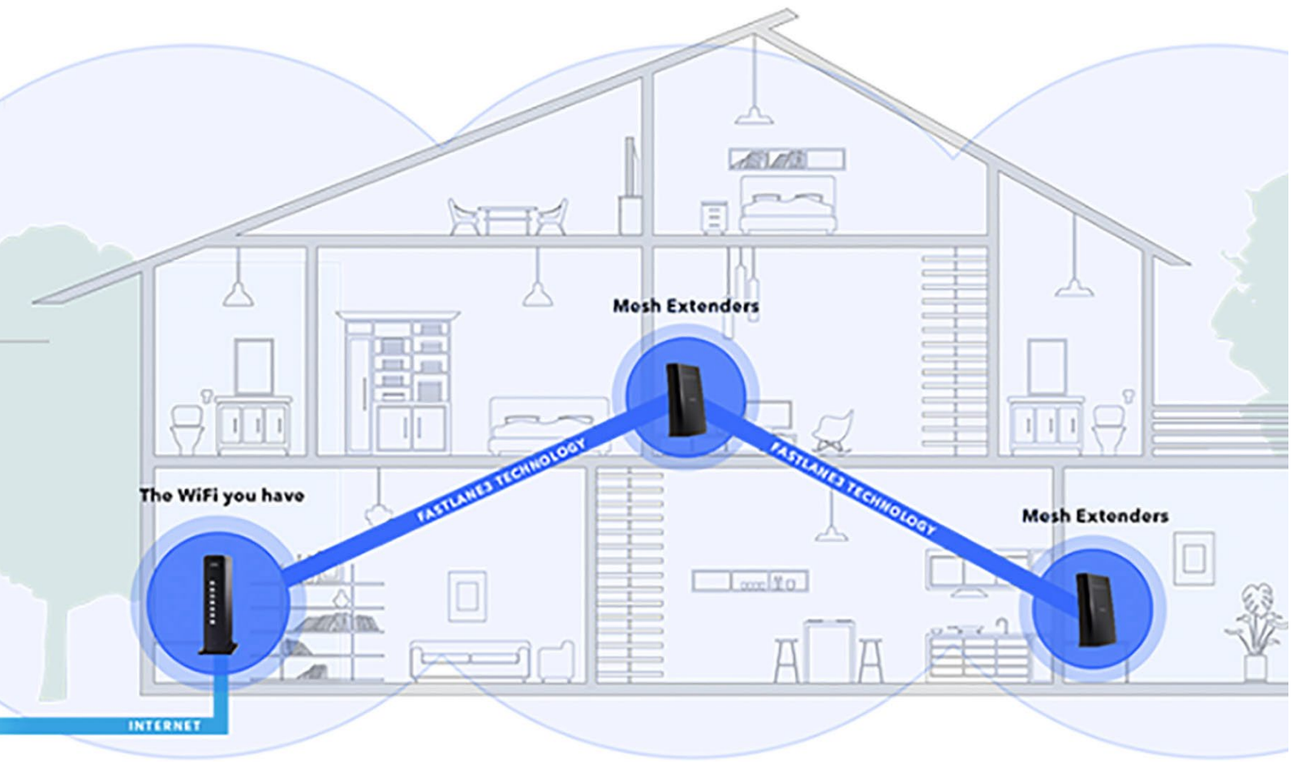
AC RATINGS AND ANTENNAS

ONE basic feature to look out for is the AC rating of the router (see page 7 for a listing of the options), which is an indication of the aggregate performance possible across all the available radio wavebands in Mbits/sec, usually rounded up. This makes the AC figure a bit of a marketing gimmick, because it doesn't tell you directly how much bandwidth an individual device will receive. But it does provide a very broad idea of the WiFi throughput you might expect.

For example, AC2600 usually refers to 1,733Mbits/sec over the 5GHz radio plus 800Mbits/sec over 2.4GHz. This will entail four streams of 80MHz apiece at 5GHz and four streams of 40MHz apiece at 2.4GHz. However, things get even more complicated with triband routers, which might not have symmetrical bandwidths even if two of the radios are at the same frequency. Mesh networking routers, in particular, may be configured like this (of which more shortly). If a router offers an exotic frequency like 60GHz 802.11ad, it may even have an AD rating instead, which really won't make much sense as a comparison to an AC rating.

Of course, not all routers with the same AC rating will have the same performance in the real world, and that is something we analyse on pages 12 and 13. There are many factors that can affect this. The client device you're using is one factor. Even if your router has a 4x4 aerial configuration, giving it up to four spatial streams, your client device may not have this. In fact, most notebooks are still 2x2 or 3x3, giving them two or three spatial streams. Nevertheless, we have found this doesn't affect performance as much as you would expect, with 3x3 only slightly faster than 2x2.

Range can really affect performance, and the power of the radio signal will influence how far the signal gets. However, few manufacturers will divulge the power output of their routers' radios. There are also factors such as how MU-MIMO is managed, or whether beamforming is utilised, which affect performance. Real-world testing is really the only way to know, and that should include range testing. This is something very few online publications do adequately, merely publishing the short-range performance results, which won't tell you much about how fast your WiFi will be upstairs or in the next room.



EXTENDING YOUR WIFI RANGE

MAXIMUM performance is only part of the picture, because that is usually only available in close proximity. Nevertheless, you want at least acceptable WiFi to extend around your entire premises. The best routers can provide a reasonably signal up to 15m or 20m inside a building with walls and floors in the way, after which the signal will deteriorate to an unusable level. A really good WiFi router might reach further, but probably not with great bandwidth, and most mid-range devices or lower are at their best at 10m or under.

Companies with built-in wired Ethernet infrastructure at their premises get around this by placing access points strategically around the building so that all the main areas have good WiFi coverage (in theory). But very few domestic users have houses that boast built-in wired Ethernet, so you can use your AC power cabling instead via powerline networking kit.

Powerline networking will usually have a power plug on one side, one or more wired Ethernet ports, and some even have a built-in WiFi hotspot. The networking is encoded into an encrypted signal that is transmitted along the ring main of your house, which usually connects all the power plugs in the house into one wiring loop, although some houses have separate circuits, and some streets have multiple houses on one wiring system, hence the need for an encrypted networking signal.

Although the latest powerline networking kit claims throughput up to 2,000Mbits/sec, in reality you will never see even close to this. Poor quality wiring and extension leads can significantly reduce the real bandwidth. And, of course, to use powerline to extend your WiFi you will need adapters with hotspots built in, or extra access points placed strategically around the house.

For greater WiFi range, a popular option has been a WiFi extender or repeater. This kind of device is meant to be placed within the range of your primary router. It sits on the WiFi as a client, and then provides another WiFi network that will extend further. The problem with an extender like this is that it will usually create a separate WiFi SSID of its own, whilst piggybacking off your primary WiFi. If you're well out of range of the primary WiFi, it will work reasonably well, but if the primary WiFi is still detectable, you may have to switch over manually on your client device.

This is where mesh networking comes in. A mesh network uses a hidden WiFi link as a "backhaul", a bit like the way wired Ethernet is used in corporate networks to stitch together multiple access points. Some mesh networking kit can also use wired Ethernet when available as backhaul. But as most houses don't have this, the WiFi option is the most likely. The best mesh WiFi kit will have a tri-band radio, so that it can offer 2.4GHz and 5GHz connections, whilst using its third radio (usually another 5GHz one) to connect the base unit to its satellites.

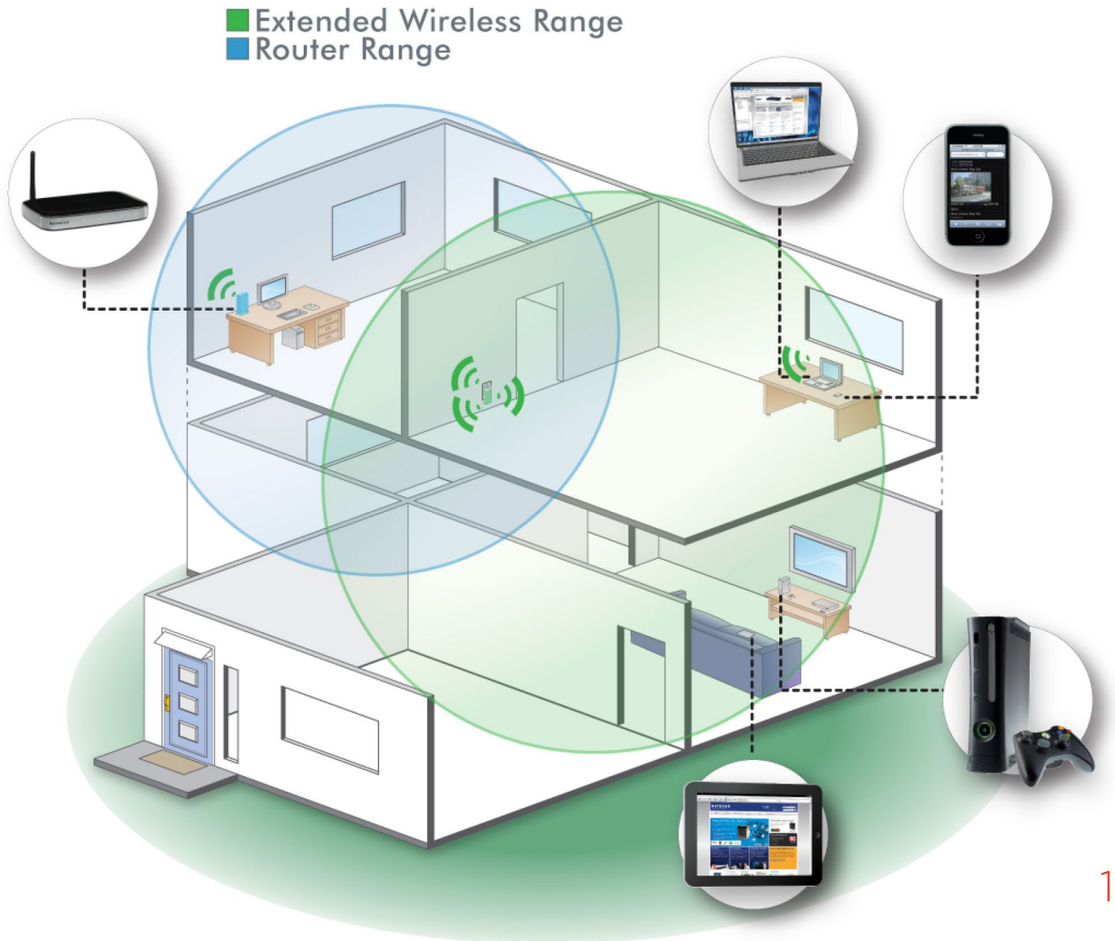
There are a couple of advantages that a system like this has compared to an extender. First of all, the same SSID is used across the whole network, so devices can move around the zone without having to change any settings. They will be switched seamlessly to the closest access point with the strongest signal as they move. The user shouldn't even realise which satellite they're connected to.

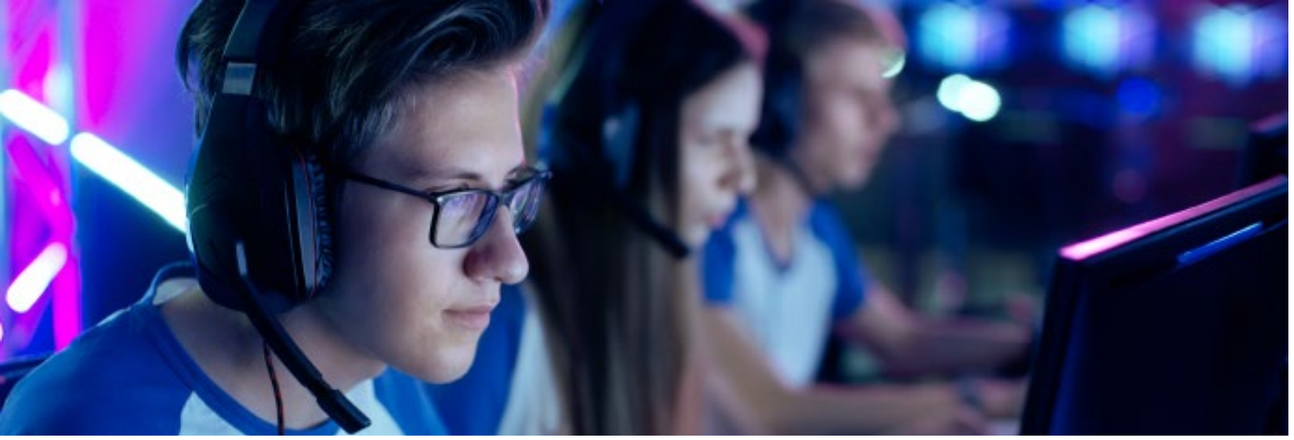
The other primary benefit is when tri-band mesh units are used, the "backhaul" WiFi is kept completely separate from the WiFi that client devices connect to, so it will only be used for communication between base station and satellite. This means that you get the fastest WiFi possible from the local satellite, without clients and mesh satellites competing for the same block of bandwidth.

The one downside of a dedicated mesh network is that it is designed to replace your existing WiFi. This means that if you already have an expensive, feature-rich router, you will at least have to turn off its WiFi radios or even stop using it to gain use of all the mesh base unit's functionality.

The answer to the latter problem is a mesh WiFi extender, which a few manufacturers are beginning to introduce. These use mesh WiFi technology, but via the radios on your existing router alongside those on an extender device. The latter sits on the primary WiFi like a regular range extender, but presents the same SSID, so devices don't need to be connected to a different network to use the added range.

With a dual-band router, these mesh extenders aren't going to be quite as fast a mesh system with tri-band units and a dedicated backhaul. You will also generally need to match the brand of router with your mesh extender to use the full feature set including a single SSID. However, there are mesh extenders on the market such as NTGR Nighthawk which are designed to operate with any 3rd party brand of router But they're a great compromise that saves you from having to decommission a powerful, feature-rich router that you've set up just the way you want.





GAMERS

GAMING may seem like just one amongst many home entertainment activities. But it makes very specific requirements from your network. Game content files are usually huge and downloading them can take ages. But once these are installed, the actual bandwidth most games require can be pretty small compared to, say, watching video online.

However, games are very sensitive to latency, also known as ping. If your broadband connection takes even a few tens of milliseconds longer to respond during an online game than your competitors, it could mean the difference between a monster kill rampage and sitting the rest of the round out.

With most generic routers, if one or two people are playing games over the broadband, and then a few more decide to download large files or stream high-bandwidth video, the gamers are likely to suffer. Even if their own bandwidth requirements are minimal, there could be momentary drops that will be experienced as "lag", and could completely ruin the experience, making it impossible to win a tightly contested match.

This is where Quality of Service (QoS) settings come in. These allow you to reserve a minimum level of bandwidth to a particular application or specific systems on the network. By ensuring that these applications or systems always get at least the minimum bandwidth they need to run smoothly, this potentially disastrous lag can be prevented.

This means purchasing a router that has QoS abilities you can use to give games the guaranteed bandwidth they need and keep everyone in the house happy. However, even routers that claim to have QoS features may not have the right options for this task. They may have QoS that is geared towards activities like Skype and IP telephony rather than games.

What you need is the ability to give nominated systems on the network a fixed minimum bandwidth, and / or do the same for specific applications. This means finding the port numbers used by the games you wish to use and giving those a priority. Finding the right ports may not be so easy. Player Unknown Battleground, for example, allegedly uses a random UDP port from 7,000 to 7,999, so all of these will need to be prioritised. You will need to do some searching on games forums to find these for other games.

One company that specifically focuses on software aimed at making this a whole lot easier is NetDuma. The company's DumaOS includes an automatic QoS system for games, plus the ability to give each device on the network a fixed minimum bandwidth. You can also give systems specific priority for particular games, with a number of popular titles supported, or you can add unlisted titles via port number range as described above for PUBG.

The DumaOS also provides facilities to limit the servers and players to within a geographical distance. This in theory means they will have lower latency, as the two are directly related thanks to the time it takes for electrical signals to travel down a wire.

Of course, you can use a sledgehammer to crack a nut and simply get the fastest Internet connection available. You can also ban other people from using the broadband when gaming is happening. But purchasing a router with strong QoS capabilities means different users of your home broadband can coexist, sharing the connection without anyone ruining anyone else's experience.

MANAGEMENT FEATURES

ASSUMING you have adequate performance and coverage for your needs, another important consideration is the features best suited to how you want to use your network and the Internet. Plans are afoot to make this side of WiFi routing much easier (see page 18), but for now you will be faced with a complicated Web browser interface, or maybe a smartphone app.

The management interface will usually provide facilities for configuring your broadband connection if necessary. However, it can be useful to have modes other than routing, for example access point mode - where the device connects to a separate router - or bridge mode, where the device uses its WiFi to connect to another router, and then you can connect to the wired Ethernet ports.

Other useful features include monitoring tools, that allow you to see how much data is passing through the router and which client devices are using the most bandwidth. This might also include a metering system, where you can limit the amount of data allowed over a certain period, which is handy if your Internet connection has a monthly cap.

As a final general feature worth looking out for, many routers will come with a USB port or two, so it's best to make sure yours has USB 3.0 rather than 2.0. This can be used for USB storage and printer sharing, both of which are handy if you don't have a NAS device or network printer. It's worth checking how far the USB storage abilities go, too. This might just be a Windows network share, but it will probably also provide a DLNA-compliant media sharing server, and possibly even cloud-style external access. The USB port may also support a mobile data dongle, which could be useful as a backup in case your main broadband goes down.

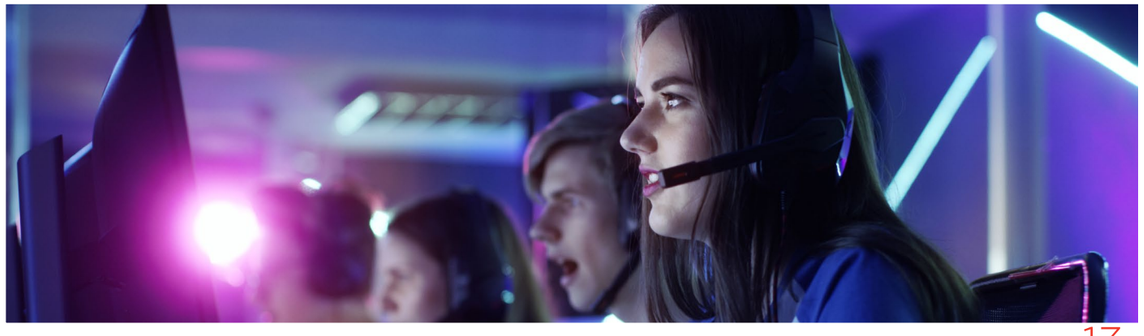
You may also want virtual private network (VPN) capabilities, so you can connect with external devices over an encrypted link, but we will discuss this in more detail when we turn to professional scenarios on page 18. And if you're gamer, there will be other specific features to consider, which we cover on page 12.

KEEPING CONTROL OVER THE KIDS

INSTEAD of just monitoring and filtering data throughput, it's also useful to do this for the type of content as well. This can include the ability to block websites, keywords, and IP addresses from being accessed by client devices on the network. However, this may mean typing each URL or keyword into the system directly. There are third-party services like OpenDNS that you can use, but this usually requires pointing your router at their external system. Some routers have a facility like this built in, but usually as part of a parental control system.

A good parental control system will include the ability to control when a router allows specific clients to have Internet access by day of the week and time of day. So you can limit someone's online time to a specific time period during the week, and a longer period at the weekend. More sophisticated systems like those from Trend Micro or Circle from Disney can also filter content by category or age group. Circle is available in a standalone device or built into some routers.

Finally, if you've invested in a voice command enabled system like Google Home or Amazon Echo, check out routers that support that technology. Then you can avoid complicated interfaces and control some aspects of your router verbally instead.



PERFORMANCE TESTING

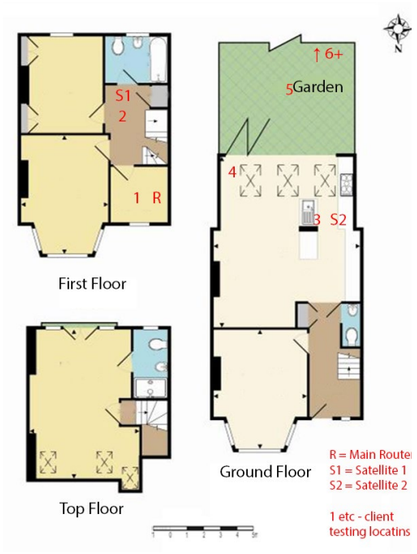
HOW WE TESTED

We tested all the router configurations exhaustively from eight different positions with three different WiFi clients. The clients used were an HP Spectre 13 Windows 10 notebook with 2×2 802.11ac WiFi, and an older HP Folio 13 which maxes out at 3×3 802.11n WiFi. Read our full testing report on KitGuru.net

In each case, we used the freely available iPerf 3.1.3 software, which stresses a network by sending packets of random data and measures the throughput. One system acts as a server, and the other as a client, as data is sent between them. In all cases, we used a Windows 10 workstation connected to the routers via Gigabit Ethernet as the server, so that the WiFi was always the slowest connection.

iPerf commands used: Server: iperf3 –s –i 1 Mesh clients: iperf3 –c <IP Address> –P 4 –i 1 –t 60 Standalone router clients: iperf3-c<IPAddress>-i1-t60

Note that with mesh systems the client command sends four streams of data simultaneously, simulating a multi-client connection as closely as possible with just one client. It takes 60 throughput readings at one second intervals and then averages the result. The above diagram shows the layout of the house we used for testing. Note that we didn't test on the top floor of the house because this was directly above the first floor and wouldn't have provided much of a range test compared to the lower floor. Instead, we used two locations on the same floor as the router (the first floor), then more distant locations on the ground floor extending out the back of the house into the garden.

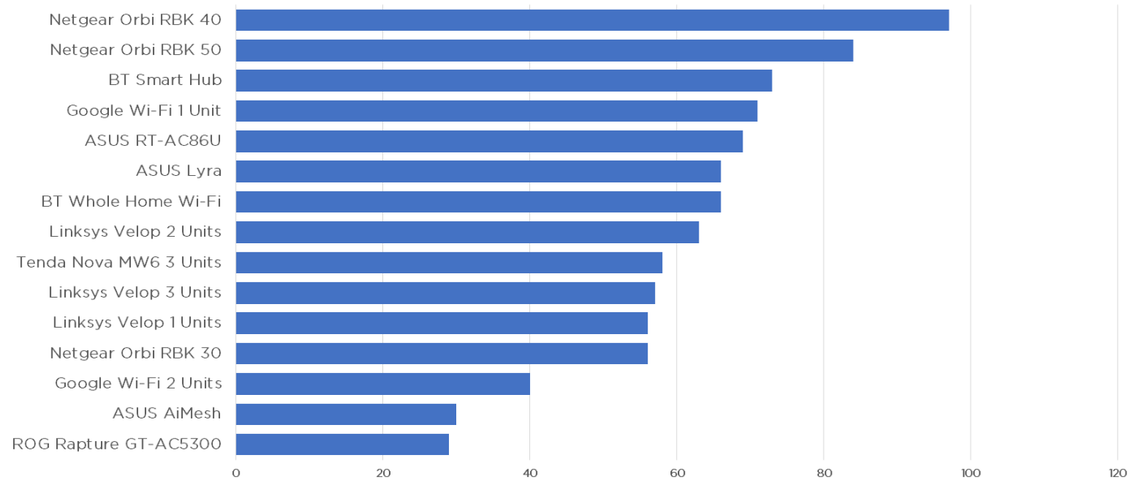


When KitGuru tests routers, we do so extensively, across a broad range of distances. For the purpose of this guide, we have chosen 5 metres, 15 metres and 30 metres. These distances will give you a good idea of how the more popular routers behave 'in the room', 'between floors' and 'at some distance'. When comparing the numbers for 2.4GHz and 5GHz, it helps to think of them as AM and FM radio. You get a much clearer, brighter signal on FM – but it rapidly falls off with distance. The AM signal is not great, even when you are close to the source, but it will carry over a very long distance – helping to keep you connected. In our testing set up, the 30m readings are taken from the foot of the garden, with a signal that is generated at the front of the house. This 30m signal has to cope with multiple walls, floors and even a shed at the end of the garden. If you have a larger property, then these test results will be most important to you. The 15-meter test will give you a good idea of the 'whole home' data rates and tests at 5 metres will give you a good idea of speeds inside an apartment.

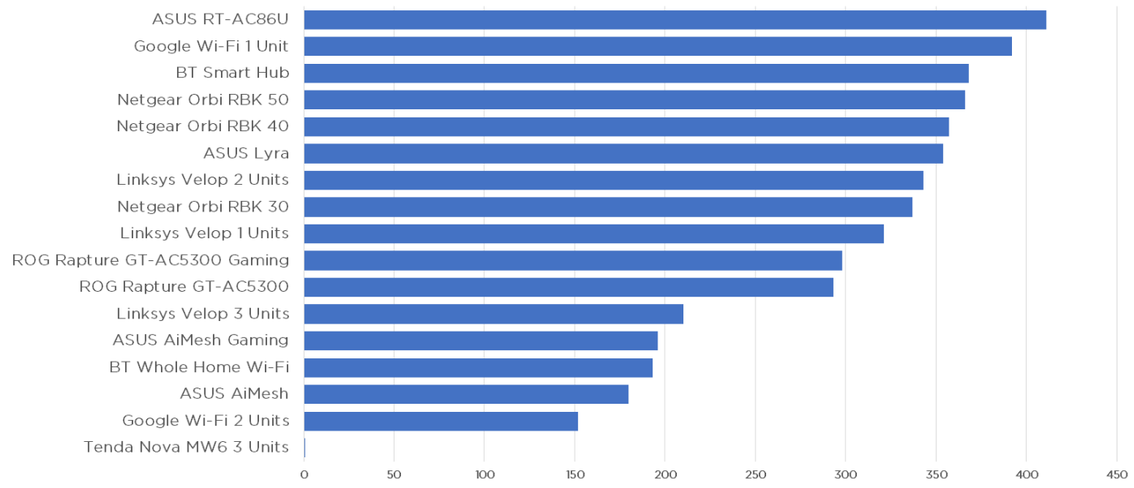
5M TEST

This is a typical 'across the room' or 'just next door' distance. At this kind of range, data transfer from the weakest of routers is likely to be impressive. It's where the higher frequencies come into their own. In our testing, even the slowest of the popular choices (Google WiFi in a 2 unit set up) managed to deliver 150Mbps at a distance of 5 metres.

2.4 GHz

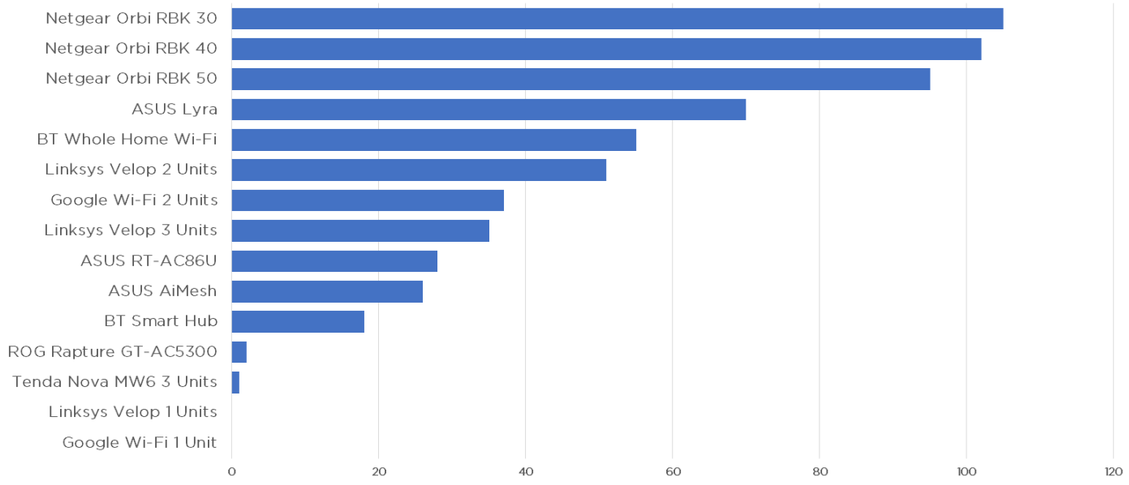


5 GHz



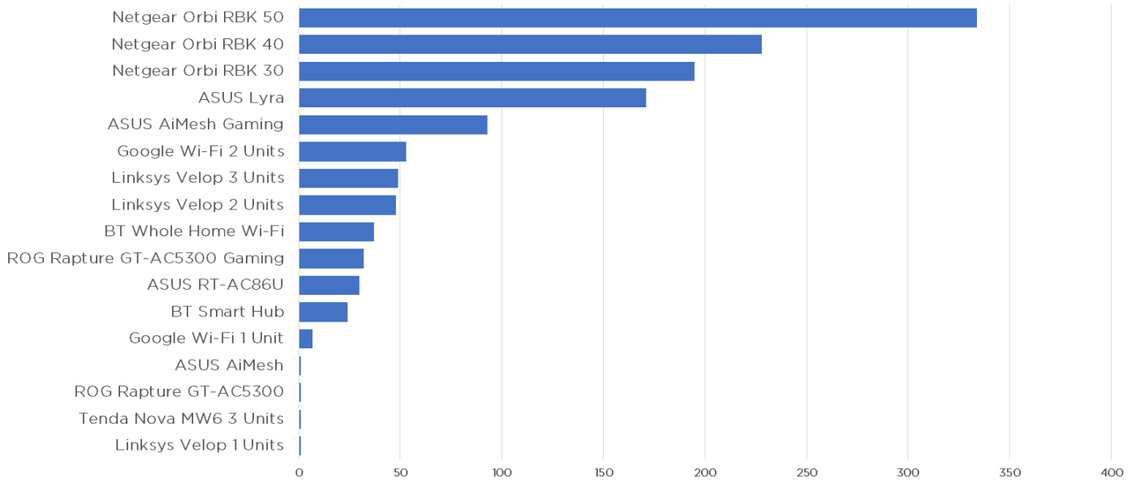
15M TEST

2.4 GHz



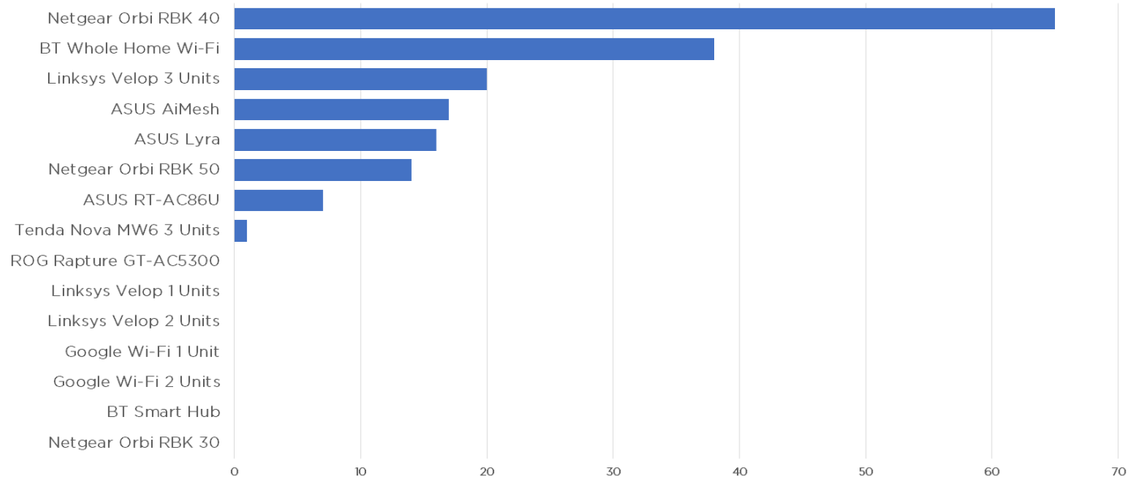
Many suburban houses will have a garden that's 15 metres long. Similarly, it's the kind of distance that you might find when measuring from your router in the sitting room to the back of your kitchen. Lastly, remember that signals radiate in all directions, so the 15-meter test also gives you an idea of the data rate you can expect on different floors.

5 GHz



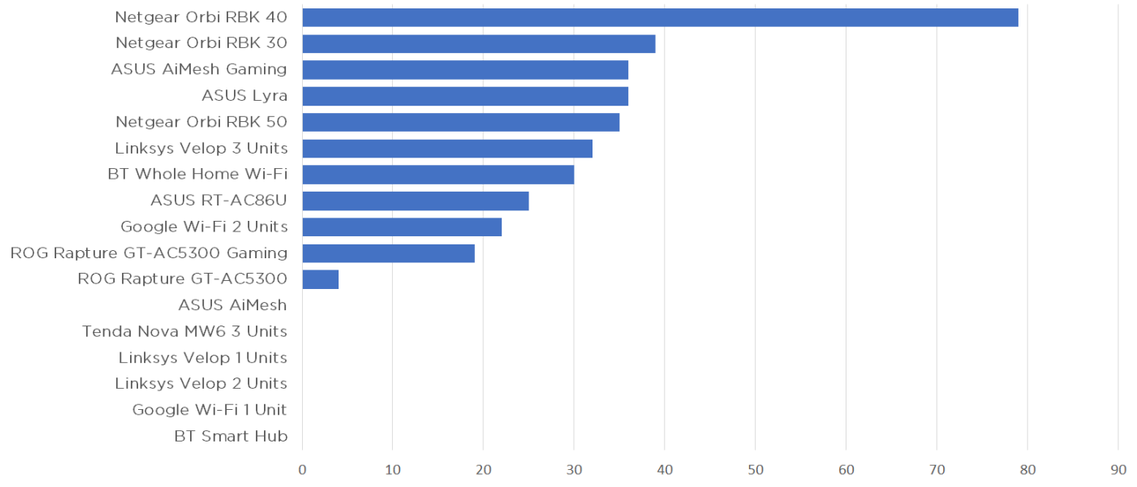
30M TEST

2.4 GHz



Here we are putting modern router technology to the test across a large distance. Especially if there are obstructions in the way. Still, with a large office, reasonably length garden of a 3-floor property, the test results at 30 metres should interest you. Also, worth bearing in mind that if you want to really extend a mesh network over a long distance, it's likely to be trying to carry the 'backbone' traffic (i.e. data packets between mesh routers) on a 5GHz signal.

5 GHz



PROFESSIONAL AND ADVANCED USERS

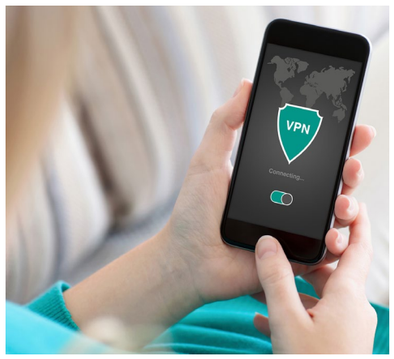
WiFi has become a mainstay of companies as much as it has for home users, if not more so. But whilst the features home users and companies need from their wireless networks overlap, there are a number of areas where business users will want additional capabilities from their routers. We already mentioned how Quality of Service settings can benefit gamers, but it's potentially even more important for professional users. For example, if your company uses IP telephony or videoconferencing regularly, this traffic should really take precedence over an employee Googling which restaurant to have dinner in this evening or checking Facebook.

Telephone and Virtual Private Networks

Some routers have direct support for IP telephony, maybe even including a built-in PBX, so you can plug regular phones into the router itself. Alternatively, or even in addition, there may be support for Ethernet or WiFi-based IP telephones. Either way, this will be enhanced if the router includes features like call forwarding, voicemail, and multiple recorded messages. The router will usually support SIP, the standard Internet telephony protocol, so you can sign up for any one of the many services that provide the SIP interface to the regular telephone network.

Although (as we discussed earlier) home users might want to use a virtual private network (VPN), businesses are the most likely to take advantage of this feature. A VPN creates an encrypted conduit over a public network that is supposed to provide the same sort of privacy as an internal wired LAN. The router itself might be able to act as a VPN server, conforming to standards such as OpenVPN or PPTP.

Alternatively, the router can act as a VPN client to connect your entire local network to the VPN system over an encrypted link. This will require a third-party account with a service like HideMyAss, IVPN, or Kaspersky, which will all require a subscription. It's best to avoid free services, as they usually come with a catch that could be more dangerous than not using a VPN at all. But the router will probably support a few VPN services, or even just one, so check whether this fits your needs before purchase.



A larger company will also want one WiFi network spanning an entire office space, which could consist of many rooms on one floor, or even multiple floors. The mesh WiFi systems we have already mentioned can extend wireless reach and could be a great choice for a small office, but might not be up to covering a company office spanning a large area or multiple floors.

Fortunately, purpose-built office space will usually benefit from wired infrastructure that includes Ethernet cabling. This can allow the placement of Ethernet-connected access points around the premises. A mesh WiFi system that supports a wired backhaul as an alternative to WiFi can stand in quite nicely for a fully corporate multiple access point setup. In practice, they're essentially the same thing. But routers with an access point mode will at least be able to be used as nodes.

There's also likely to be a lot more at stake if your professional WiFi gets broken into, making security a significantly more important factor. In fact, it's so important that we've devoted the whole next section to it (see page 20).

Dynamic DNS and Making Services Externally Accessible

A company with a permanent leased line Internet connection should have a fixed IP address and can therefore potentially supply services to the outside world. But a small business (or home user) on a regular broadband connection is likely to have an IP address that changes every few days, if not more frequently.

This makes providing external services – including remote management of the router itself – problematic. Fortunately, you can use a Dynamic DNS service to get around the issue. There are umpteen of these in existence, such as DynDNS or No-IP, and most of the larger router manufacturers have their own services too. What DDNS does is provide a memorable alphabetic URL, which remains static. But this directs the user to the service, which has a record of the current dynamically allocated IP address that your broadband connection is using.

Your router will need to support the DDNS service you are using, which will be an entry in the management system. Once you've provided your DDNS login credentials, the router will regularly keep your chosen DDNS service updated with the current broadband connection IP address.

However, without further configuration, if someone enters the DDNS URL, all they are likely to see is an error page. If your router firewall is any good, it will act like there's nothing there at all. In order for systems on the local network to provide services to the outside world, they need to be given a route through your router's firewall. This is where port forwarding and a "de-militarised zone" (DMZ) are essential.

Most routers will offer these facilities in some form. A DMZ makes a system on the local network visible to the outside world. It's a virtual process, where you can simply nominate a client connected to the router via wired Ethernet or WiFi as being in the DMZ. This could be a webserver, a mail server, FTP server, your IP telephony server, or a media streaming device.

Port forwarding is more selective, however. Every type of network application, from serving a website, to email delivery, FTP, and even games servers, uses a particular port to communicate. If the external IP address of the broadband router is like the main switchboard number, the port is like the extension.

With port forwarding, you can tell the router to redirect traffic from the outside to a client system on the local network that is running the application that uses the particular port. A single system could run multiple applications, or different systems could supply each one. But the beauty of port forwarding is that only the services provided via that port are externally accessible. Everything else on that system will remain invisible.

A router worth its salt will provide a list of common applications like webserver, FTP server, or mail server. You can choose one, select a system from the list of network devices, and set up the port forwarding. Consumer-oriented routers may also have a list of common game server ports as well, so that you can serve a game to your friends over the Internet (see gaming on page 12).

These are just the headline features to look for in a WiFi router aimed at more professional applications. A truly fully-featured router is likely to have an administration menu that is pages and pages long, with a daunting range of options. This is why the future could entail a different approach, where the router becomes part of a service provided by multiple devices that is configured in a more user-friendly and holistic manner. But before we get to that (on page 23), let's look at how WiFi routers and networks are kept secure.

SECURITY

Securing Your WiFi

If someone can get onto your WiFi illicitly, it's not just a matter of them accessing your Internet connection for free. They will be on your local network and can potentially access all your computers and other systems. This is why wireless security is such a big issue. To get onto your wired network, an invader would have to be physically connected to your network, or have broken through your Internet router (of which more later). But a WiFi interloper just needs to be within radio range, and could even be in another building or out on the street.

The process of travelling around looking for easily hacked WiFi used to be called wardriving, and almost reached sport status a decade or so ago. Participants would find an open WLAN or hack into a secure one using packet-sniffing software, and then use chalk to mark the security details on the pavement nearby, which was known as warchalking. More powerful WiFi security has made this mostly a sport of the past, but only if you take care to ensure your wireless network actually uses the security options available.

WEP, WPA and WPA2

The original WEP security system was very insecure, particularly the standard 64-bit version. The Shared Key authentication system made it relatively easy to capture the frames in the handshaking process and derive the key. Fortunately, WEP has been deprecated in favour of WPA and WPA2, with WPA3 announced at the beginning of 2018 as well. WPA3 is a major leap forward that aims to provide robust security for next generation devices and will be a mandatory feature for 11ax platforms moving forward.

WPA (WiFi Protected Access) implements most of the 802.11i standard, including the Temporal Key Integrity Protocol (TKIP). This is a very different system to WEP. Where the latter uses a 64-bit, 128-bit or (sometimes) 256-bit key that is the same for every packet, TKIP dynamically generates a new 128-bit RC4 key for every packet. So even if a hacker manages to crack one key, it will only work for that one key and is then useless, which effectively eradicates the packet sniffing compromises associated with wardriving and warchalking. There's also a message integrity check built into WPA that prevents packets from being captured, altered, and sent onwards with a malicious payload.

However, WPA2 is stronger still, implementing all the mandatory portions of 802.11i. In particular, it replaces TKIP with Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol. Thankfully, the latter has been shortened to CCMP. It uses 128-bit AES encryption and a complex data unit with five sections, including a message integrity code section, which is more secure than TKIP.

Both WPA and WPA2 still use a pre-shared key (PSK) or 802.1x exchange (see below). Most routers will only provide WPA-PSK, which is the passphrase you will be familiar with entering when accessing a particular WiFi network. The PSK is used for initial authentication, and then for generating a

shared secret key called the pairwise master key (PMK) via a cryptographic hash. This is a 256-bit key, and the 128-bit pairwise transit keys (PTK) for TKIP and CCMP are derived from it dynamically.

Although the PMK is very strongly encrypted, and the PTKs change so often their 128-bit keys are nearly impossible to crack too, all this relies on the passphrase you use for PSK. If you use a short, easily guessed word for your PSK, a brute force system of trying lots of passwords until one matches could compromise your WiFi. So WiFi passwords should be similarly complex to other passwords. Even when you are careful about the passphrase you use with your SSID, if you have guests regularly on your network, any one of them could provide a weakness. If their device is stolen with access credentials saved, it can provide a doorway into your local network. Or it might be possible to extract SSID and passphrase from a device that has been left unattended.

Some routers offer an alternative system that can protect against this situation, via a Guest Network. This allows the creation of a secondary WiFi SSID, or one each for 2.4GHz and 5GHz, which you hand out to visitors, whilst keeping the primary credentials for permanent users only. You can change this every day or at the end of an event, so that none of the guest devices can get on anymore and they won't be able to be used as a beachhead into your local network.

An additional level of security can be added with MAC address control. A MAC address is the unique serial number ID that every networking device has. It can be spoofed, but you would need to know the address to spoof; it can't be derived by cracking or packet sniffing. By only allowing known MAC addresses on your network, you can prevent any other devices from connecting. The downside is that you will usually need to enter each MAC address individually using its unique 12-character alphanumeric code, which will be laborious for lots of devices.

RADIUS and 802.1x

As we mentioned earlier, there is an alternative authentication system for WPA2. On your router, you may see WPA-Personal and WPA-Enterprise options. The WPA-Personal is WPA-PSK as described above. WPA-Enterprise, on the other hand, adds another layer called 802.1x, which in turn uses Extensible Authentication Protocol (EAP) for authentication, with a number of different sub-types available.

Essentially, you will still have a PSK from your SSID and passphrase, but this is only for the initial stage of authentication with the access point or router. After this stage, 802.1x will reveal another login interface, where a completely different username and password will be required before the WiFi device is properly on the network. Unlike with WPA-PSK, the dynamic PTKs are being supplied by the authentication server instead.

This makes WPA-Enterprise considerably more secure than WPA-Personal. Even if a brute force attack manages to guess the PSK, that will only provide initial access, and then

the 802.1x-supplied login must be cracked as well, which will be much harder to do. However, WPA-Enteprise requires a RADIUS server to supply the authentication, so is more complicated to set up and manage. This is why you will usually only find it in businesses beyond the small to medium level.

Wi-Fi Protected Setup - Cloned Access Points

Connecting to WiFi can be a laborious process, particularly if you've been sensible and selected a complex SSID and passphrase combination. Fortunately, there's a system called WiFi Protected Setup (WPS) to help you. This is a protocol where the SSID and passphrase are configured for you automatically.

This can be performed via a PIN that you enter on the client device, via pushing buttons on both router and client simultaneously, via NFC (so the client needs to be brought close enough to the router), or in the past via a USB thumb drive containing the necessary data. Obviously, there is a short period of vulnerability when a new client is being added, and if you're near the router with a push-button device you can simply press both buttons. A PIN is also not a very secure code. But generally there has not been widespread exploitation of WPS, since it is only vulnerable when being used, which won't be that often.

As a final note of caution, a popular method that hackers use to compromise client devices, particularly in public WiFi spaces, is to clone a SSID. People don't tend to check what they've connected to if they've used a WiFi network before. The cloning method involves copying a SSID but without security, in the hopes that unsuspecting users will connect to it without checking. They will then be able to read your unencrypted WiFi traffic, with potentially dangerous consequences if you were connecting to WiFi to check your bank balance online.

THE FUTURE OF WIFI ROUTERS

LIKE everything else in tech, WiFi routers are constantly developing. The barely-usable original 802.11 became the just-about-usable 802.11b, then the entirely-usable 802.11g and 802.11a. With 802.11n, WiFi came of age, and 802.11ac has become a standard for both homes and businesses. There's much more to come. We asked John McHugh, Senior Vice President and General Manager of the Business Unit at NETGEAR, what lies in store for WiFi routers over the next five to ten years.

"The next big thing for WiFi is 802.11ax," explains McHugh. "This will mean a fourfold increase in performance, which will really push the wired infrastructure." Although 802.11ax on paper is only about a third faster than the nominal speed of 802.11ac, its more efficient use of the spectrum is expected to make 802.11ax around four times faster than 802.11ac in terms of real-world throughput. "It's doing a lot of spatial and quadrature encoding to use the same ecosystem but puts lots of concurrent data streams in it," explains McHugh.

McHugh sees 802.11ax making current 60GHz products using 802.11ad even more of a niche than they are already. "802.11ad is making some pretty hard trade-offs," he explains. "You're getting high throughput, but only at really short distances. You'll get something comparable out of 802.11ax over a much wider range." Whilst 802.11ad has a theoretical maximum bandwidth of 4,620Mbits/sec, KitGuru's testing with the NETGEAR Nighthawk X10 R9000 saw 754Mbits/sec, around twice the result with 802.11ac at the same range. If 802.11ax can quadruple the performance over 802.11ac, it might even be faster. So there really won't be any reason to use 802.11ad when 802.11ax is the more mainstream option and has similar range to 802.11ac. There is an 802.11ay update for 60GHz imminent promising up to 20Gbits/sec, but this is still likely to remain specialised for very short, unobstructed indoor distances and outdoor backhaul. There's also a 45GHz 802.11aj variant, but this will have similar limitations to 60GHz WiFi.

"The biggest challenge is balanced networks, not making investments that are wasted money,"

"The biggest challenge is balanced networks, not making investments that are wasted money," continues McHugh. Even with 802.11ac, WiFi is offering internal networking speeds ten times that of even quite fast broadband. So the major benefactor of faster and faster WiFi is internal traffic.

For this reason, although more people are turning to mobile data as their primary Internet connection, McHugh doesn't see faster standards such as 5G offering a significant challenge to the broadband-router-WiFi combination. Whilst 4G data contracts offering high monthly usage can cost a similar fee to wired broadband, providing comparable throughput as well (assuming you have a good signal), there's still value to fast local WiFi. "There are certain things that will always be local traffic, like streaming videos from your NAS", argues McHugh.

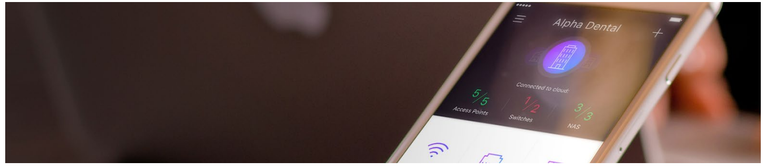
However, the infrastructural needs of faster mobile data networks would be the biggest issue. "What is the real refresh rate of the ecosystem that gives us 3G, 4G, 5G?" asks McHugh. "It's very complicated. Infrastructure has to be built and monetised. Telcos have been talking about eliminating local area networks for years, but it has never materialised because the costs didn't close enough. Also, virtually every business application is designed to sit behind a protective gateway, rather than communicating directly with the Internet."

Despite this, McHugh does see an increasing role for LTE, 4G and 5G as a failover. More and more routers have the facility to have a secondary mobile data broadband connection, which only kicks in if there's an outage in the primary wired broadband. "Companies buy a pack of mobile data and this only gets spent if it's used," explains McHugh. Another current problem that McHugh is already addressing at NETGEAR is the issue of managing WiFi and wired networking devices. "The notion of thinking about device by device management is going away," argues McHugh. "Network protocols and so on are going away. Management is going to be in business language – how do you deliver value for business activities."

"There needs to be a revolution in the way facilities are delivered"

Right now, if you look at the management interface of virtually any WiFi router, unless you're a networking expert, you will understandably feel a bit daunted. There will be numerous sections you won't go near during the lifetime of the device because you're not really sure what they do. But in many cases, there will be settings in these admin menus that really could improve your online experience, either by optimising performance or providing additional security.

McHugh reckons that there needs to be a revolution in the way these facilities are delivered via WiFi routers and other network-connected devices. Usually these devices have to work together to provide the services in question, such as an internal NAS device requiring configuration in line with the router's firewall to make its contents securely accessible from outside over the Internet. So it makes sense to look at this as a service you want to set up as a whole, and provide an administrative system that deals with the individual devices for you, seamlessly behind the scenes.



NETGEAR is aiming to kick-start this move towards user friendliness with its Insight management system. "The breakthrough for user experience with Insight is that it sits in the cloud," explains McHugh. "We can reskin Insight for a specific business, or we can strip it for the expert. It allows you to say what you want to do with your network and it sets it up for you."

Essentially, once you register an Insight-compatible NETGEAR device, it becomes available to be managed remotely as part of a whole that provides a service, rather than just a standalone device with lots of confusing features. As a taster of this, NETGEAR's Arlo surveillance cameras provide an entirely cloud-based management system that allows the user to configure cameras and base station as a whole, from anywhere in the world.

From a consumer perspective, the rise of devices like Google Home and Amazon Echo have made ubiquitous WiFi even more part of everyday life, and the need for user-friendly, voice operable interfaces a necessity. Systems you speak to like Alexa and Siri are being used to manage Internet of Things devices, which are already being managed in this more wholistic way, because you wouldn't want to configure every single radiator or temperature sensor in a smart home. You just want to set a few rules about how warm you want your house to be at different times of the day. Routers are already available with built-in support for Internet of Things devices, centralising control in this way, and this can often be connected to services like Alexa.

Overall, then, the WiFi router will be with us for a good deal longer. In a few years, 802.11ax will provide faster than ever WiFi four times the speed of current 802.11ac. But equally importantly, WiFi routers will fit into business and home activities much more seamlessly, alongside other networked devices, from storage to Internet of Things sensors and security devices. You'll be able to manage your whole, super-fast network of devices with one user-oriented cloud interface, or even just tell it how you want it set up with your voice.

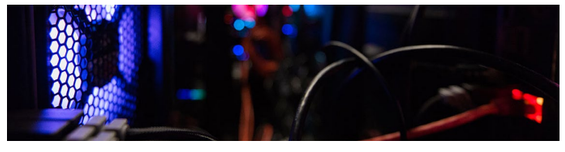
WIFI ROUTER **MUST HAVE**

DON'T rely on the router provided by your ISP. You can gain performance and features by upgrading to a premium model with more aerials and better software.

GIVE the positioning of your router plenty of thought to get the most out of its WiFi signal and avoid the positioning gotchas on page 10.

Dr. WiFi

USE a WiFi analyser app on your smartphone (e.g. Dr WiFi) to measure the signal & performance around your premises, then try altering your router position to eliminate weak spots.



RESTART your router regularly by cycling the power or turn it off at night. When your router hunts for the best channel on startup, it will be more likely to avoid your neighbour's WiFi.

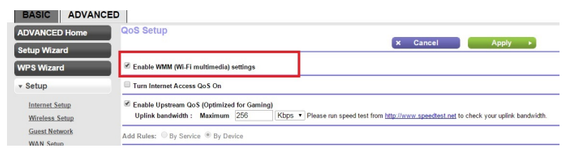
WiFi WiFi WiFi

IF your WiFi regularly finds interference from neighbours' WiFi, use a WiFi analyser app to check the channels being used and set your router up to avoid these.

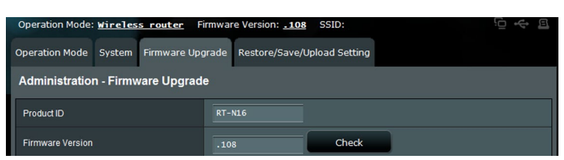
CONSIDER hiding your WiFi SSID to avoid prying neighbours. Some routers offer several SSIDs to help keep your traffic secure and separated.

SSID SSID

IF your WiFi regularly finds interference from neighbours' WiFi, use a WiFi analyser app to check the channels being used and set your router up to avoid these.



IF your router has Quality of Service options, consider using them to improve the experience for your network users. You can prioritise gaming etc for maximum response speeds.



KEEP your router firmware up to date. The latest firmware will contain performance enhancements and security patches to ensure your WiFi runs fast and stays hacker-free.

IF you have large premises, consider investing in mesh WiFi instead of just a standalone router, or add a mesh-based extender if your existing router brand offers that option.

WIFI ROUTER **MUST AVOID**

DON'T put your router near large, solid metal objects, as these can dissipate the radio waves and prevent WiFi transmission.

THICK concrete and brickwork block WiFi transmission, so try to avoid putting your router close to a wall, although ceilings and floors are usually made of wood so less obstructing.

YOUR Microwave oven operates at a frequency close to 2.4GHz WiFi, so avoid placing your router near it, as it could knock out your wireless networking when it's operating.

manufacturer Default

CHANGE your SSID and password from the manufacturer default options.

MAKE sure you position the router with its antennas pointed upwards, as this is likely to be the optimum orientation for best radio signal.

More homes now have multiple devices requiring strong, steady WiFi signals. Avoid buying too quickly. Evaluate a range of options - there's a product out there to meet every type of home & office networking need.

admin password

DON'T leave your router's admin login and password on default settings. Create more complex values for both to avoid giving hackers an easy time.

PLACING your router on a higher shelf or upper floor can help with the range of your WiFi. Avoid metal shelves where possible.

GETTING a new installation? Central locations are best for WiFi distribution - but make sure your router is close to devices that need a direct connection. Your installer can help.

IF you have cordless phones in your house, use DECT-compatible models. These operate at 1.9GHz, whereas some non-DECT models use 2.4GHz or 5.8GHz, which may cause WiFi interference.

CONCLUSION

OVER all the preceding pages, we looked at the history of WiFi routers, and how the wireless aspect has developed over the years. We have provided some tips about what to look for in a router for home usage, from performance to features. You may not get everything you want in one package, particularly as standalone routers and mesh WiFi systems develop in parallel, with mesh providing the best coverage but a standalone router still offering the most features. But weighing up the pros and cons should deliver what your home or office needs.

Gamers will have some specific requirements, and fortunately there are now routers arriving on the market that are specially designed with this kind of user in mind, offering features to optimise the gaming experience online. Professional users have yet another set of requirements, including support for IP telephony and providing network services from internal systems to devices connecting via the Internet.

Security is a key consideration with all networking devices, and the WiFi router is the gateway between the internal network and the outside Internet. So it's your frontline defence, and care should be taken to configure your router properly to perform this job as capably as possible.

Although the AC rating of a router will give you some idea of its performance capabilities, always check real-world tests to see if it lives up to its billing. As you will see from our tests of a selection of popular options, routers with the same rating can have quite different performance in real scenarios.

Over just a couple of decades, WiFi routers have become an essential device for every home or office. They now provide fast, secure and feature-rich Internet connectivity and local networking across your entire house or business, and even out into your garden. But they will continue to get faster, and potentially easier to configure so you get more from the features available. The WiFi router's future destiny is to become even more the central hub of your digitally connected world.

[Read KitGuru's latest router reviews here.]