

makeuseof

Everything You Need to Know About **HOME NETWORKING**



by James Bruce

Everything You Need to Know About Home Networking

Written by James Bruce

Published March 2015.

Read the original article here: <http://www.makeuseof.com/tag/everything-need-know-home-networking/>

This manual is the intellectual property of MakeUseOf. It must only be published in its original form. Using parts or republishing altered parts of this guide is prohibited without permission from MakeUseOf.com.

Image credit: [Cabling behind router via Shutterstock](#)

Read more stories like this at MakeUseOf.com

Table of contents

The Big Picture – What Can You Do With a Home Network?	4
Multiplayer LAN Gaming	5
Stream Your Media	5
Set up a Home Server	5
Share Files	5
Control Your Computer Remotely	6
Game Sharing and Streaming	6
Routers, Modems, and Switches	7
Types of Network Connection	9
Ethernet / LAN	9
Wi-Fi / Wireless LAN	9
Power Line	10
Which Should You Use?	11
Expanding Your Wired Network	12
Dealing with Wi-Fi Issues	13
Wi-Fi “Blind Spots”	13
Wi-Fi Interference	14
Extending the Range of Your Wi-Fi	15
Choosing an Internet Connection	16
Required Speeds	16
Dial-Up	16
ADSL	16
Fibre to Cabinet (“Cable” Internet)	16
Fibre to Home / Fibre to Premises	16
3G/4G Dongle	17
Satellite	17
What are IP Addresses?	18
How Do I Do That? Home Networking Scenarios	21
You have a non-networked printer, and you want to share it to every computer	21
You want to print from your iPad or iPhone	22
You have a USB storage drive, and you want to share it to everyone without leaving your computer on all the time	22
You want to set up a web server to host a website	23
Endless Possibilities	24

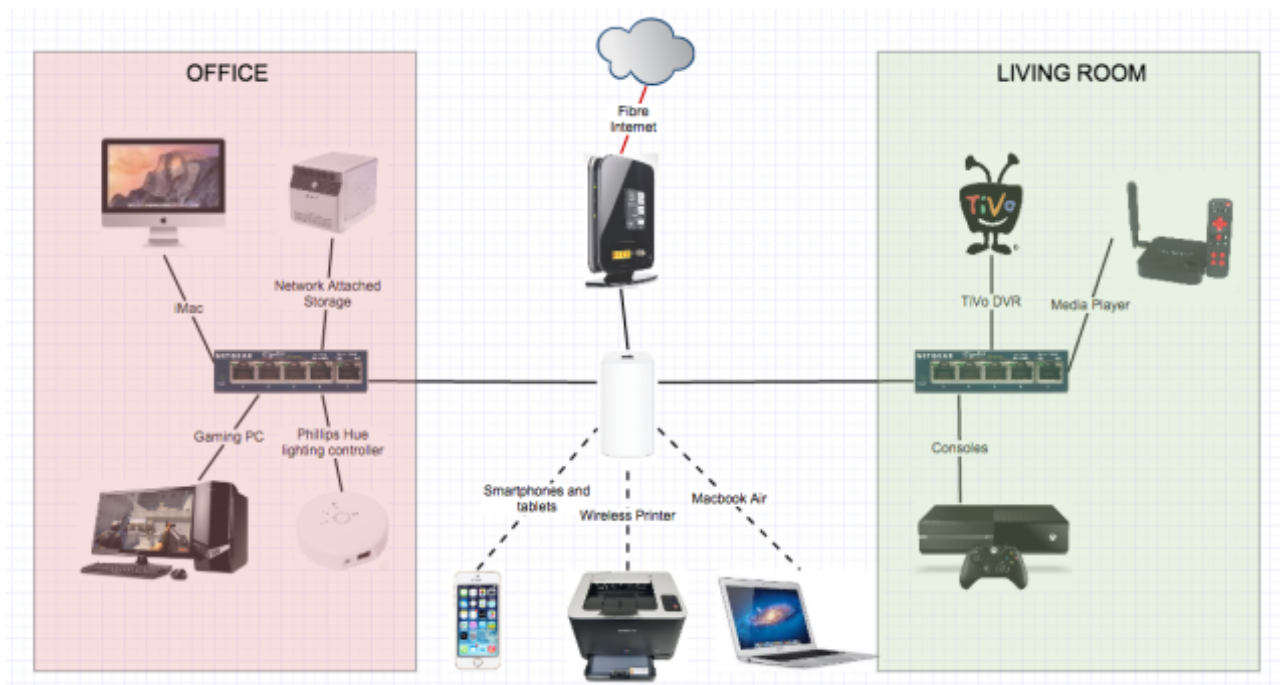
Setting up a home network is not as hard as you think it is. In fact, if your Internet Service Provider (ISP) gave you a router when you signed up for their services, you probably already have a home network.

In this guide, we're going to explain the fundamentals of home networking; look at expanding your network to handle more devices; consider the different types of Internet connections; and guide you through some exciting scenarios.

The Big Picture – What Can You Do With a Home Network?

Before we get into the technical details of setting up a home network, let's look at the big picture. A home network is a private collection of devices – computers, mobile phones, gaming consoles – which are all connected to a router or switch. This is also called a **local network**. Every device on your home network can “talk” to every other device, which opens up possibilities for media streaming, network backup, multiplayer gaming – and so much more.

Here's an example of a home network – mine, in fact.



I've augmented the router my ISP provided (by placing it into *modem mode*) with an Apple Airport Extreme, which provides better wireless performance to some devices. From there, I've extended the wired part of the network into two parts of the house using 5-port Ethernet switches – my office and living room, each with 4 devices. In the office, I have a Network Attached Storage (NAS) device, which provides shared data folders to every device, for movies and TV streaming anywhere in the house, as well as backups. In the living room is a range of gaming consoles, a TiVo box and an Android media player (our [ProBox EX2 review](#)). Despite owning a smart TV ([What is a smart TV and do you need one?](#)), it's not hooked into my network, simply because the devices we own do a far better job of anything the smart TV offers.

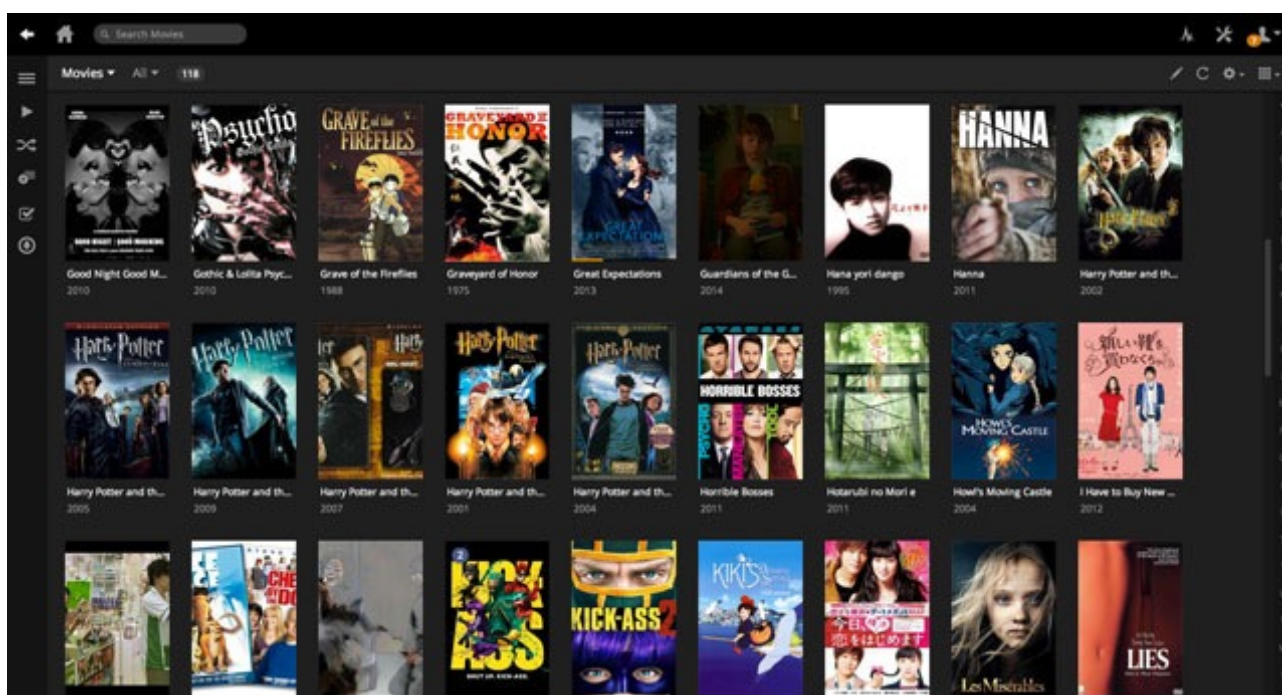
Many people think that getting a router is only about providing an Internet connection for all their tech toys, but it can be so much more. Here are a few ideas of what you can do with a home network – check out the last part of this guide for other home networking scenarios.

Multiplayer LAN Gaming

For the youth of today, multiplayer is synonymous with “online” gaming, but most games actually allow you to play multiplayer with other devices on your home network. It’s unlikely you’ll have 4 Xbox consoles, but you might have a few old computers that are capable of playing Minecraft. If you have friends with a laptop, you can invite them round and have a LAN party. Here’s my pick of [7 classic games to get your LAN party going](#), and our [ultimate guide to running a LAN party](#).

Stream Your Media

“Streaming” doesn’t need to be from Netflix – if you have a collection of movies stored on your computer, you can use an application like [Plex](#) to share them across your home network. Plex has a beautiful interface, identifies your movies automatically, and runs on every platform – so you can start watching on your TV and finish watching in bed on your iPad. Here’s our [full guide to Plex](#), and you might also want to consider a premium [Plex Pass](#) for even more great features.



If you’d like a more extensible media centre with plugins, [XBMC/Kodi](#) is a great choice too. (We have a guide on [setting up XBMC](#) too, but it’s a little out of date).

Set up a Home Server

At a basic level, a home server can act as a shared file store and perhaps shared printing, but you can also leave it open to the world as a web server to host your own website for free; or as a PBX call management system; or run your own Minecraft server... the possibilities are endless. Later in the scenarios section, we’ll talk specifically about setting up a web server that’s open to the public.

Share Files

The most common thing task on many home network is to simply to send a file from one computer or device to another. You can set up a shared folder on another machine, then access that folder from within Explorer or Finder like you would for any other folder on your local computer. This functionality is built into every operating system, but for even greater flexibility you might consider buying a NAS

drive – a dedicated network file storage device with features like redundant hard drives in case one fails. (Read our review of the [ASUSTOR 7004T NAS](#) for an example of features)

Control Your Computer Remotely

Sitting at the sofa, but still need access to your main computer? With a home network, you can. Try these [free remote desktop apps](#) for the iPad.

Game Sharing and Streaming

If you're a keen gamer with a Steam account and a good gaming rig, you no longer need to be tied to that machine to play your games: using [Steam In-Home Streaming](#), you can harness the power of your gaming machine, but play somewhere else. It's a great way of sharing your Steam library with the whole house, so you don't need to buy yet another gaming PC. Valve recently announced a \$50 [Steam Link](#) device due to launch November 2015, which hooks up to your TV to enable streaming games to a big screen (with a very small price tag). There's never been a better time to be a gamer!



PLAY YOUR GAMES ANYWHERE IN YOUR HOME WITH STEAM IN-HOME STREAMING

When you log into Steam on two computers on the same network, they automatically connect, allowing you to remotely install, launch, and play games as though you were sitting at the remote PC.

When you play a game using In-Home Streaming, video and audio are sent through your home network from your high-end gaming PC to another device in your home.

From here, your keyboard, mouse, and controller input is sent back to the remote computer.

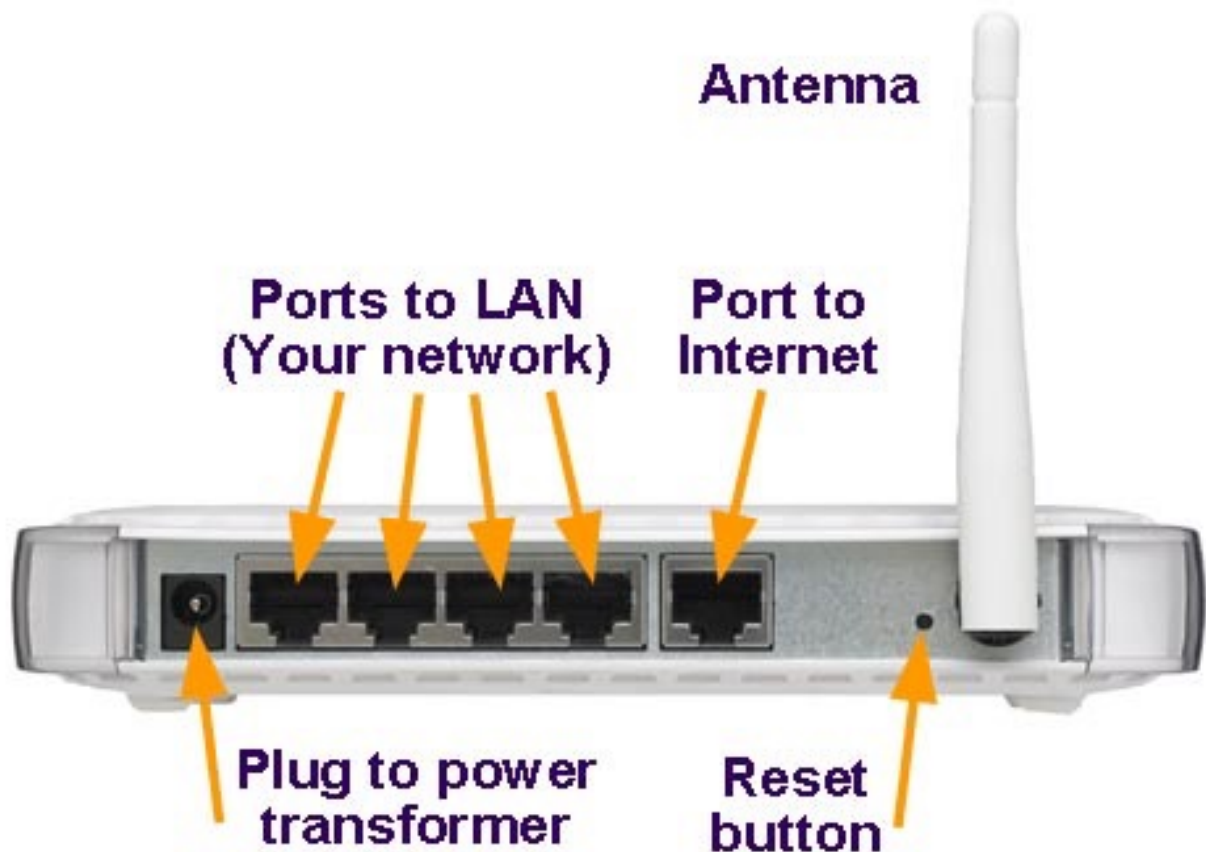
The diagram illustrates the Steam In-Home Streaming process. It features a dark blue background. On the left, a small monitor displays a game scene from 'DARK SOULS II'. To its right, a larger monitor also displays the same game scene. A white game controller is positioned in front of the larger monitor. A dotted line connects the two monitors, representing the network connection. Text boxes provide details about how video and audio are sent from the high-end PC to the other device, and how input is sent back to the remote computer.

Routers, Modems, and Switches

These devices are at the heart of a home network, so it's important you understand what each one does and why you'll need them.

A **modem** is supplied by your ISP, and is used to turn their proprietary network signal – running through a phone line, copper coaxial, or glass fibre – into a standard computer network signal. In times gone by, you could actually hear the modem dialling a telephone number to establish a connection over the phone; but today they operate silently, often over a different infrastructure to your landline telephone.

A **router** acts a central point of contact between every device on your network, and the Internet connection provided by your modem. All modern routers will include Wi-Fi connectivity, plus a number of LAN ports – usually up to 4. In some cases, the modem will be built into your router, so the ISP only supplies you with a single device. It's also usually possible to configure these modem routers into “modem only” mode, in which only a single network port is enabled and all Wi-Fi features disabled – this is great if you want to buy a router more suited to your needs. If you have a separate router and modem, your router will plug in to the modem through an Ethernet cable, using the WAN (Wide Area Network) port on the router.



The image above was taken from Netgear's support page, showing the ports on the back of a typical router. Although the WAN port is physically identical to the local network ports, the router will have a built-in firewall for traffic entering that port only – while the internal network is trusted fully.

Switches (and **hubs**) are used to extend a network, taking one port of your router and turning it into many more ports. Consumer switches can typically be bought in sizes of 4, 8, 12, 24-port models. Though the terms *hubs* and *switches* are used interchangeably, historically there was a difference in the way that they would relay the signal: hubs would blindly repeat any incoming signal to every other

machine on the network; switches are intelligent enough to take an incoming signal, look at where it was going and only relay it to the relevant outbound port. Today, they mean the same thing.

Most switches you'll find in a home network are **unmanaged**, which means there's nothing for you to configure – just plug them in and they work. **Managed** switches are more expensive, and can be set up with features like Quality Of Service (which means you can give priority to data-packets from Skype, for instance, so you always have the best call quality).



Types of Network Connection

There are various ways you can connect devices in your home network, which offer vastly different performance and have their own pros and cons. Be informed before you purchase.

Ethernet / LAN

A LAN or Ethernet network refer to physical cables which plug into your router or switch through one of the available LAN ports. You are limited by this number, but can expand the network using additional switches (see the next section, *Expanding Your Wired Network*). LAN cables can achieve speeds of up to 1,000 Mbps (“Gigabit”) easily, though some older computers may be limited to 100 Mbps. In addition, LAN cables can be run up to 100 meters without any degradation in performance, so the only real limiting factor is how many holes in your walls you’re willing to make. If the answer is “none at all”, and you don’t like messy cabling between doorways, read on for alternatives.



Wi-Fi / Wireless LAN

Wireless networking works over radio waves and doesn’t require any wires at all. Although this sounds great in theory, wireless connections often suffer from limited range due to structural elements of a building and interference from other devices.

The latest Wi-Fi standard is 802.11ac (or just AC for short), which promises up to gigabit speeds, though this requires both a compatible router, compatible Wi-Fi devices (the iPhone 6 was the first Apple device to support AC, for instance, so you may find a lot of your devices won’t support it), and ideal conditions. Rather than blindly radiating the same signal out in every direction, 802.11ac (and 802.11n to a lesser degree), allows the router to focus the signal into a beam centred on the remote device – resulting in a faster, more reliable connection.

This terrifying device is the Nighthawk X6 - the latest Wi-Fi router from Netgear, capable of 3.2Gbps combined Wi-Fi speed.



With a higher latency, more prone to interference and errors, Wi-Fi should only be used when absolutely necessary – such as mobile devices. Cabled connections are always preferable for full size desktops, gaming consoles, and media centers.

Power Line

Power Line networking involves piggybacking a network signal on top of mains power electrical distribution, by manipulating frequencies not used for the AC current. All that's needed are some inexpensive adapter plugs (such as [this model for around \\$30](#)) which can then be connected to devices by standard Ethernet cable – you don't need any special drivers.

The network signal itself is carried all over your house through the existing wiring, so it's a great solution where installing traditional network cabling isn't possible but you want better performance than wireless.



Though the technology got off to a shaky start when it was first launched, things have improved to the point that you now get half-gigabit speeds with optimal conditions – though will vary depending on the age of your household wiring, the distance between the points, radio interference, and whether it's a full moon that night (*Okay, I'm kidding about that last bit*). The Netgear range features a special test LED which indicates whether the plug is suitable, so you can try out a few sockets without running your own performance tests – though if none of the sockets pass, you're out of luck.

Power Line networking – otherwise known as *Ethernet over Power* (EoP) – is not to be confused with *Power over Ethernet* (PoE), which enables small devices to be powered directly over the Ethernet

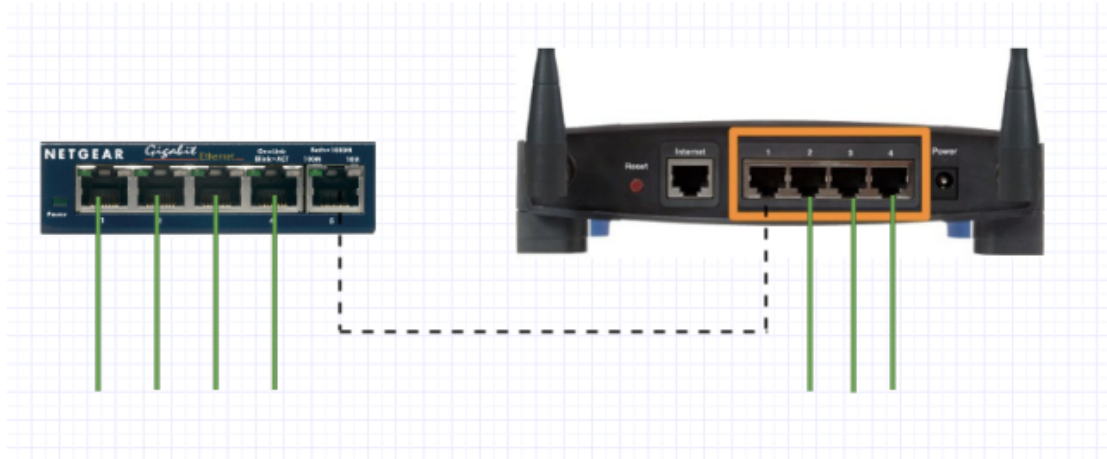
cabling, reducing wiring complexity and useful for things like IP cameras. It requires a compatible router/switch, and unless you need PoE for a specific device, it's safe to forget about it.

Which Should You Use?

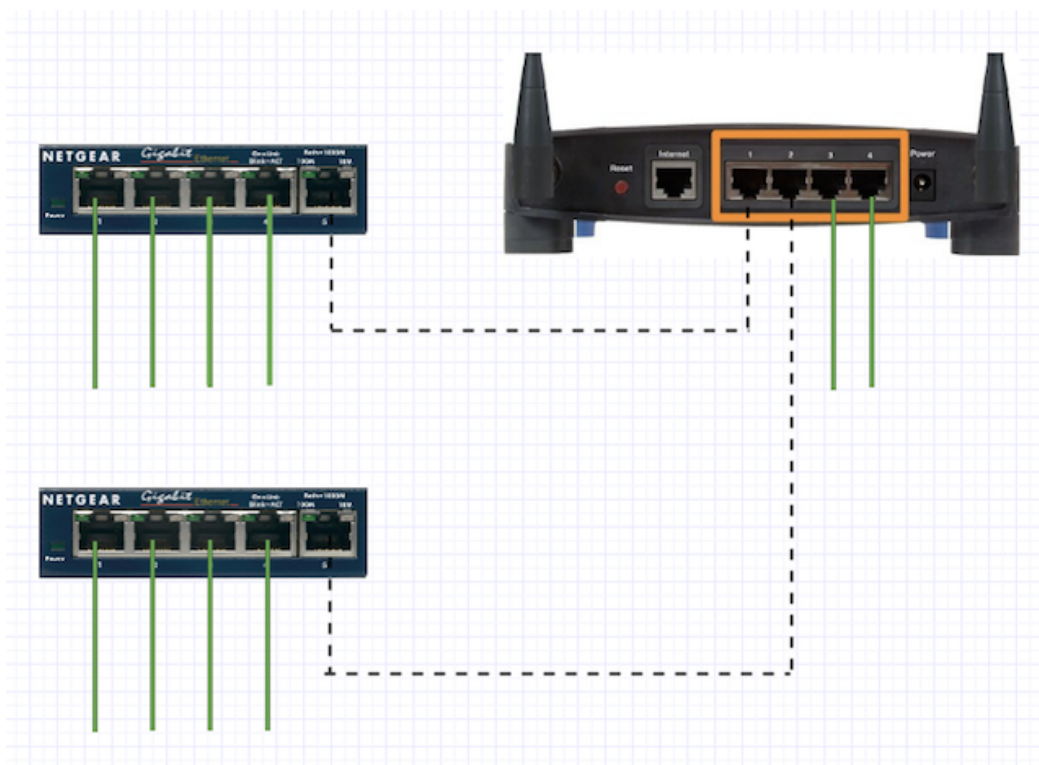
In short: using wired Ethernet connections is always preferable. It offers the fastest speed, the best reliability, and the lowest latency. Use wireless only for devices where you don't have the option, and don't buy waste money on a fancy wireless-AC router unless you know your devices support it ([our advice from 2013](#) about AC-routers is still relevant today, sadly). Power Line adapters are risky, but may be preferable to wireless if you can't run cables and aren't getting good wireless coverage in a specific area of your home – thankfully they're now relatively cheap ([less than \\$30-\\$50 for a starter pack](#)), so it's not a huge loss if they turn out to be useless.

Expanding Your Wired Network

Run out of Ethernet ports on your router? No problem: just buy a **switch** to add more ports. Switches come in a number of sizes and can cost as little as \$30 for a Gigabit 5-port switch. Note that one port on both sides will be used as an interconnection, so a 5-port switch actually only has 4 useable ports to connect more devices, and you'll be losing one of your router's ports too (so if your router has 4 ports which are currently in use, adding a 5-port switch will give you 3+4 ports in total).



If you need to expand again, it's best to use one of the original ports on the router – while daisy chaining switches together is possible, you will introduce a small amount of latency each time. If there's no other option though because the router is too far, daisy chaining one or two times is still preferable to other technologies like Wi-Fi or powerline.



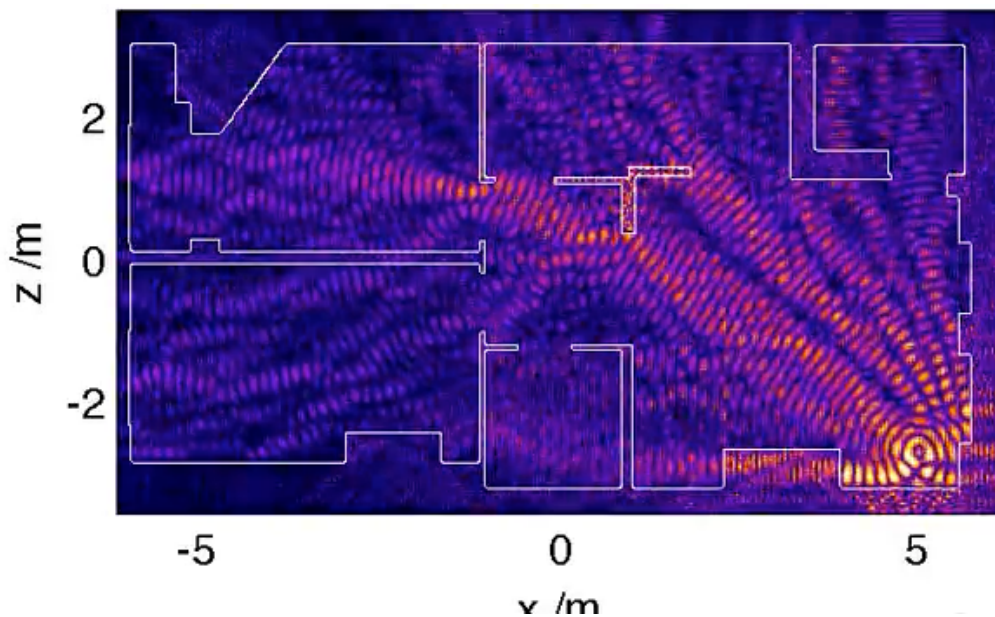
Do I need crossover cable? **No.** You may have heard that crossover network cables are used to connect things like switches and routers, but modern hardware is clever enough to do this crossover in firmware – there is no need to use special cabling. On some switches, you may still have a designated “uplink” port, or even a physical button to change modes – use this as the interconnecting port.

Dealing with Wi-Fi Issues

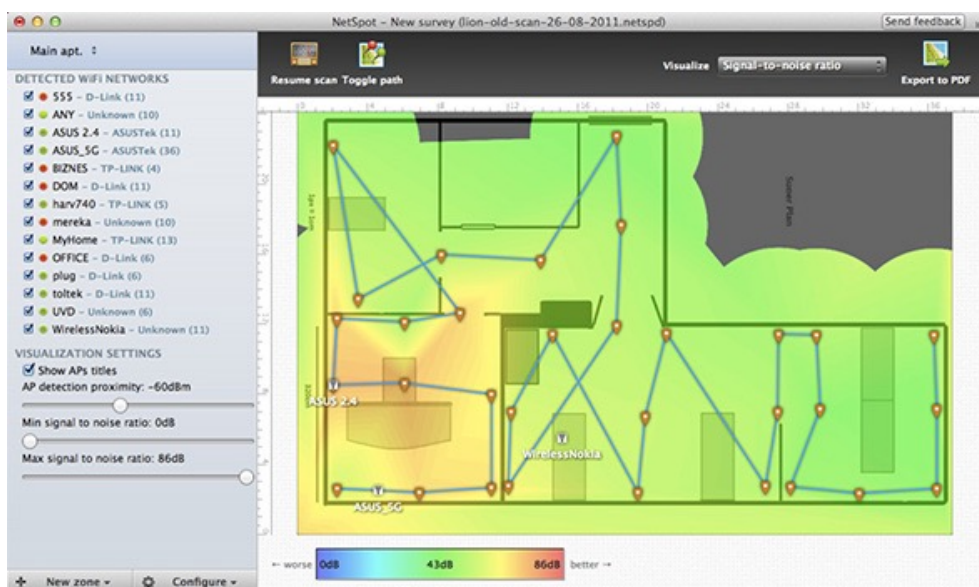
Wi-Fi “Blind Spots”

Ever held your phone up in the air to try and get another bar of signal? Wi-Fi is no different – there'll be some places around your home that just don't get a signal. Perhaps there's a mesh of metal somewhere, or just too many walls. Wi-Fi is quite fickle really; avoid issues by setting up your network correctly in the first place.

Jason Cole even went as far as to develop a reliable mathematical equation for calculating this, which confirmed his suspected wireless dead spots.



You can do something similar by walking around your home with a laptop, using an app like NetSpot for Mac or HeatMapper for Windows.



Of course, the app can't fix these, but you might then consider repositioning the router and testing again. Read our guide on Wi-Fi Feng Shui to learn all about the best positions.

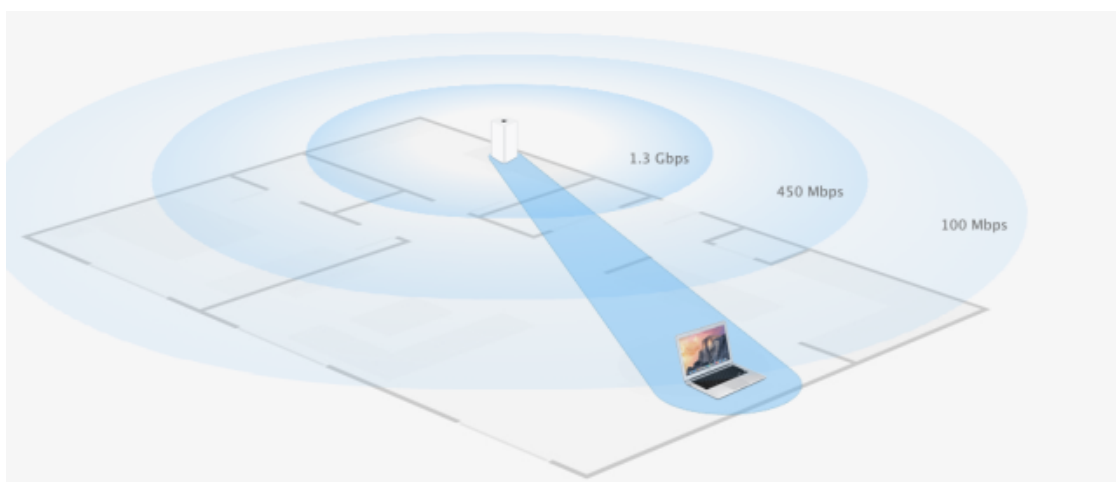
Wi-Fi Interference

The wireless spectrum is generally a busy place, particularly if you live in an urban environment. Sometimes you'll get bad wireless performance simply because you're using the same "channel" as everyone else. There are around 12 different Wi-Fi channels available (the exact number depends on where you live in the world), and you'll get better performance if you find a channel that no one else is using: [how to find a unique Wi-Fi channel](#). A modern router should do this automatically though.



There are also legally dubious options available to you: by replacing the firmware of your router with something like DD-WRT ([What is DD-WRT and how can it make your router into a super-router?](#)), you can "overclock" the Wi-Fi signal to transmit stronger than legally permitted, or to use channels that are not allowed in your country. These may land you jail time!

If your mobile devices support it, upgrading your router to one capable of 802.11ac can improve performance, as it introduces "beamforming" technology to focus the signal just where needed.

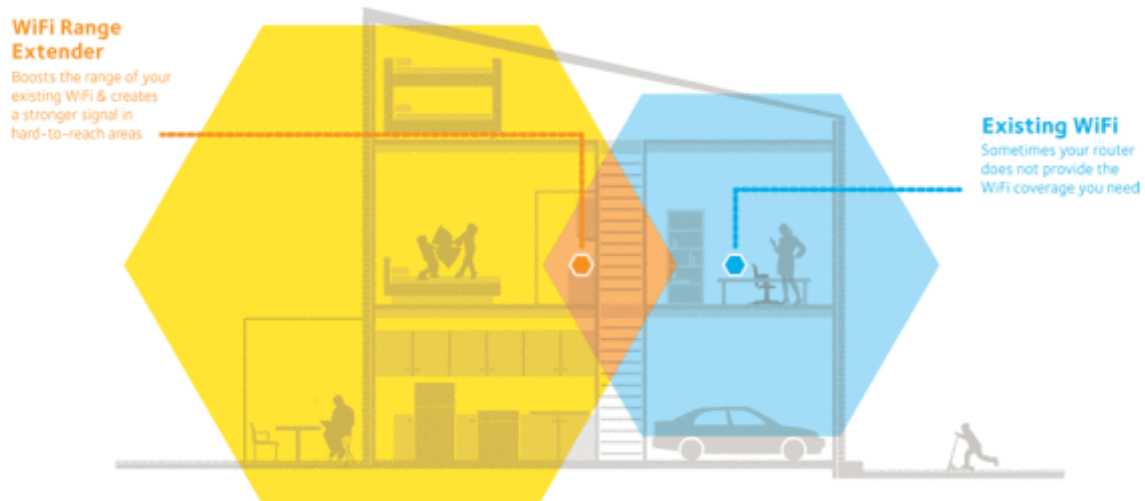


The image above was taken from Apple.com explaining the AirPort Extreme with 802.11ac "beamforming" technology.

Extending the Range of Your Wi-Fi

Sometimes, your Wi-Fi just won't reach far enough. If that's the case, you've got a couple of options:

- Commercial Wi-Fi extenders: running from \$40-\$100 and up, these simple devices can take your existing signal and “repeat” it. However, there is an overhead to doing this – expect speeds to roughly halve.



- Repurpose an old router to do the same job. This may involve replacing the router firmware with DD-WRT.
- Try some DIY methods that focus the antenna in a specific direction using some kind of metal can.

Alternatively, consider Power Line networking instead (see the section on types of network earlier in this guide).

Choosing an Internet Connection

Required Speeds

To give you an idea of what your speed requirement may be – or conversely, what's possible using your available Internet connection – here are Netflix's recommended minimum speeds:

- SD quality (DVD) – 3 Mbps
- HD quality (720p/1080p) – 5 Mbps
- Ultra-HD (4K) – 25 Mbps

Megabits vs Megabytes: This can confuse the best of us, so before you complain to your ISP that you're not getting the quoted speed, let's take a moment to examine the difference between **Megabits** and **Megabytes**. File sizes are quoted in Megabytes or MB – notice the uppercase B, which means Bytes; network speeds are quoted in Megabits, or Mb (and the larger Gigabit, which is 1000 Megabits). Crucially, **a bit is 1/8th of a byte**. So, if you have Gigabit internet speeds (1000 Mbps), this means you can achieve a theoretical maximum throughput of 125 Megabytes per second.

Dial-Up

The slowest and worst kind of Internet available, mostly restricted to extremely rural areas. Dial-up requires your computer to literally make a phone call to your ISP's server. Top speed of 0.056 Mbps. Avoid if at all possible, because even loading the simplest of web pages will be tedious.

ADSL

Also done using a phone line, but technological advances mean speeds of up to around 30 Mbps (downstream) / 5 Mbps (upstream) are possible – more than enough for the average home user. ADSL connections can be quite unreliable though, since it uses the same antiquated infrastructure as telephones. Speeds are not guaranteed, and will vary greatly depending on local conditions, other users, and distance from the telephone exchange cabinet. Avoid if possible, but for most consumers not living in a built-up area, ADSL is your only choice.

Fibre to Cabinet ("Cable" Internet)

The most common type of fibre-Internet available in which glass fibre cable is used as the backbone of the network, but the final leg of the journey from the provider's cabinet to your house is done using traditional copper cabling. Speeds on this type connection currently max out at around 120 Mbps, though this may improve in future. You will be limited by how far you are from the cabinet – the further the signal has to travel over copper, the worse the speed you'll be getting.

Fibre to Home / Fibre to Premises

The fastest Internet currently available involves bringing the glass fibre cable directly into your home. These provide anywhere up to 1,000 Mbps (or "1 Gigabit"), though again this may improve in future and could be enabled simply with a new router or firmware upgrade. If you want the best of the best, ask for fibre to your home. Read more about the [differences between fiber connections to your home](#).

3G/4G Dongle

Where a fixed line isn't available, you may also have the option of using a mobile connection – 3G or 4G/LTE – via a USB dongle. You'll need a suitable router (such as [this one from D-Link](#)), as very few will support a USB internet connection.

Mobile connections come in a variety of flavours: [4G+](#), [4GX](#), [XLTE](#), [LTE-A](#), and [VoLTE](#); click on the link to read more about their differences.

Satellite

For extremely remote areas, broadband speeds can also be obtained using satellite communications. There are typically restrictions on the amount you can download each month, though speeds will be comparable to a good quality ADSL line or fibre-to-cabinet connection. They involve high setup costs, and monthly fees are more expensive than regular broadband. Satellite connections are high latency, which means that although they're fast once the download request has been established, the initial request can be quite slow, making them unsuitable for things like online gaming and video chat.

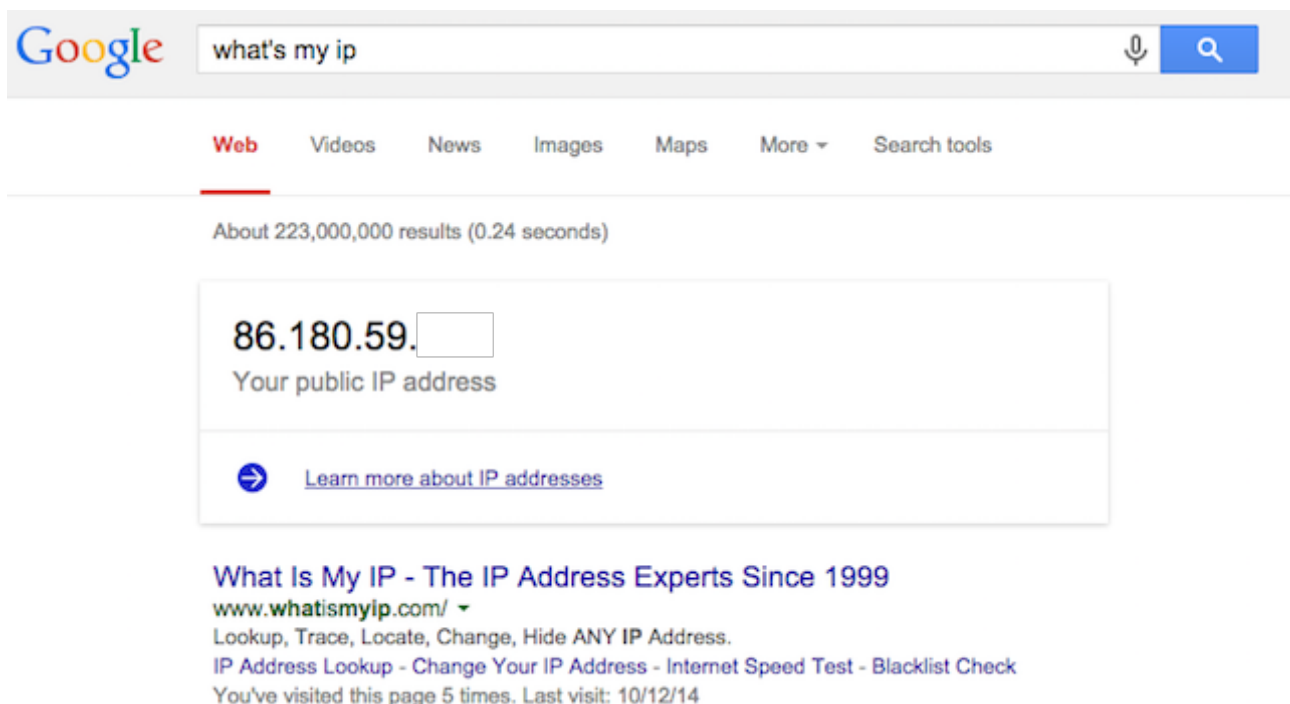
Confused about the different ways of accessing the Internet? Guy McDowell broke it down even further in his article:

What are IP Addresses?

Each device on your internal home network is assigned a **private IP address**, of the form **192.168.x.x** or **10.0.x.x** (*Why these particular numbers? No reason, it was just decided that these were the numbers that would be reserved for private networks*).

When your computer asks to browse a website, it's the router's job to send requests out to that website, then direct the replies back to the appropriate device on your network. Your router will have also have a **public IP** address, through which Internet services and websites will know where to send their data back to your house, at which point the router examines the data packet and says, "*Oh, this was meant for that PC in the bedroom, I'll send it there.*"

To find out your public IP address, the easiest thing to do is literally just ask Google, "What is my IP?" For a detailed report including a rough location, use whatsismyipaddress.com.



The screenshot shows a Google search interface. The search bar contains the text "what's my ip". Below the search bar, the results show "About 223,000,000 results (0.24 seconds)". The main result is a box displaying the IP address "86.180.59." followed by a small empty box. Below the IP address, it says "Your public IP address". There is a link "Learn more about IP addresses" with a right arrow icon. Below this, there is a link "What Is My IP - The IP Address Experts Since 1999" with the URL "www.whatismyip.com/". Below the link, it says "Lookup, Trace, Locate, Change, Hide ANY IP Address." and "IP Address Lookup - Change Your IP Address - Internet Speed Test - Blacklist Check". At the bottom, it says "You've visited this page 5 times. Last visit: 10/12/14".

This is a great time to bring up an important security issue you need to be aware of. As far as the Internet is concerned, your house has a single IP address and potentially just a single computer. It doesn't know the private IP addresses of each device on the network – it only knows the public IP address of your router. That means that if you live in shared accommodation, or if you allow your neighbours to use your Wi-Fi connection, it is impossible for the outside world to tell from which computer any activity occurred. Or in other words, you (the account holder with the Internet Service Provider) are held responsible for everyone in your household (and neighbours, if you share your connection) and anything they do online. **It's important to educate every member of the household to use the Internet responsibly, and not to share your Internet connection with the neighbourhood!**

You may also have heard that the world is running out of IP addresses, and everything needs to be fixed by upgrading to **IPv6**. This is true, but you needn't worry about it. When your ISP upgrades to IPv6, they will replace your router to one that's compatible. Your home network can continue to operate on IPv4, with the router handling the address translation between the Internet and locally.

Most of the time you can forget all about IP addresses: computers and devices will appear automatically on the Windows or OS X network browser. But sometimes it's useful to know the IP

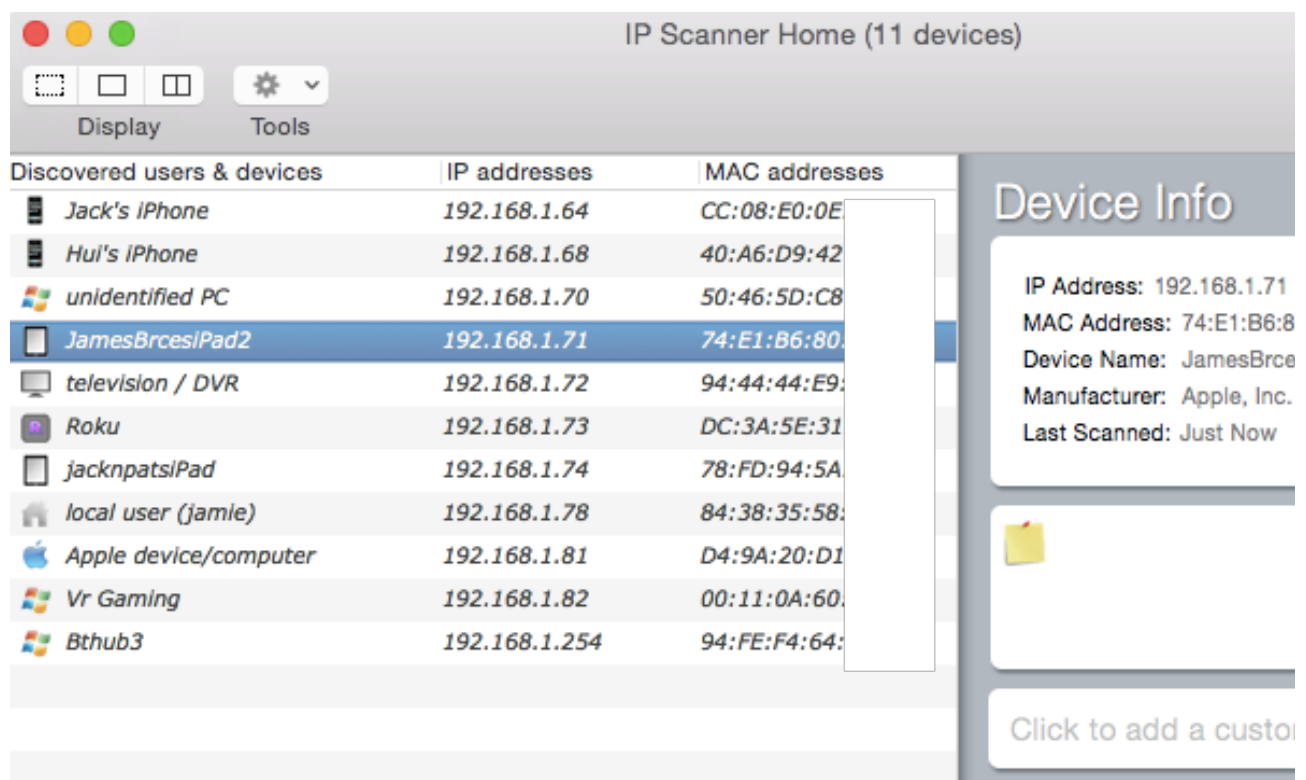
address if something needs to be configured manually, and there are couple of ways to go about doing this.

On a Windows PC, open up the command prompt and type **ipconfig** – you'll find your IP somewhere in the output. On Linux and OS X, open a terminal and type **ifconfig** instead.

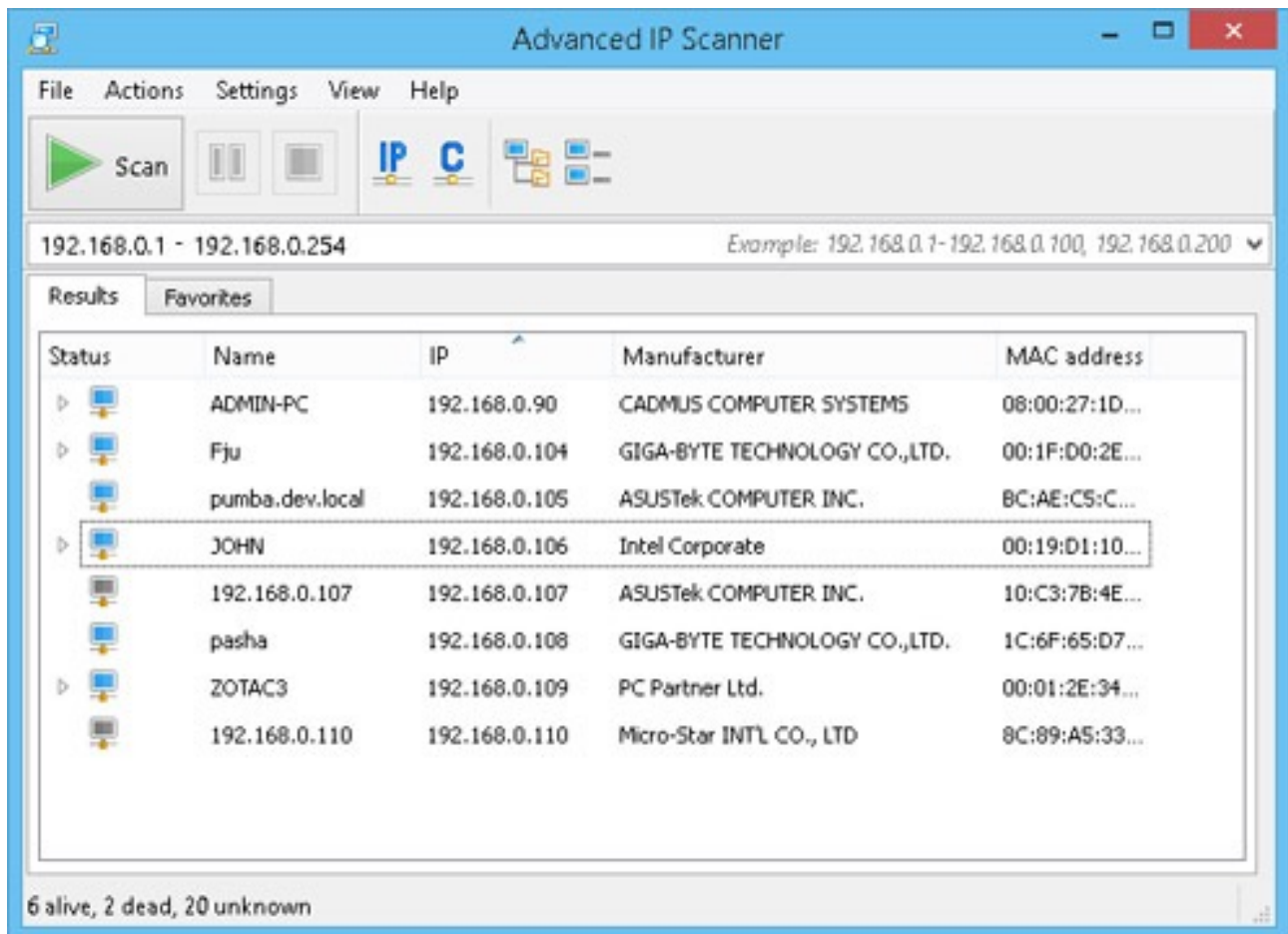
```
jamie — bash — 84x41
[Restored]
Last login: Mon Mar  9 17:57:40 on console
Jamess-Air:~ jamie$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=3<RXCSUM,TXCSUM>
    inet6 ::1 prefixlen 128
    inet 127.0.0.1 netmask 0xff000000
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=1<PERFORMNUD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 84:38:35:58:e7:44
    inet6 fe80::8638:35ff:fe58:e744%en0 prefixlen 64 scopeid 0x4
    inet 192.168.1.78 netmask 0xfffff00 broadcast 192.168.1.255
    nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
```

Your home network connection will be on en0, en1, wlan0 or wlan1

You might also prefer to use a graphical interface for browsing networked machines. For OS X, I recommend [IP Scanner Home](#). It has a built-in database of manufacturers, so having discovered a device, it probes to see if it can automatically identify the type of device (and assigns a cute little icon for easy identification).



On Windows, Advanced IP Scanner does a similar job.



At this point, you might be wondering – *What’s a MAC address?* It stands for “Media Access Control address”, but really it’s just a kind of serial number that’s encoded in the hardware itself. Each manufacturer has their own unique start number, so you can often tell who made the device by checking the MAC address. In theory, no two devices in the world should have the same MAC address, but this can’t be relied upon for secure purposes as some devices are able to reprogram their MAC address (and hence, they can “fake” being something else).

IP addresses are dynamically assigned by DHCP (*Dynamic Host Configuration Protocol*) – it’s your routers job to manage this, and ensure that no devices are given conflicting addresses. Devices must occasionally “check-in” with the router to say they’re still alive (powered on) and still need the address; if your router restarts or its configuration changes, it’s possible that machines on your network will be given a new address. This can sometimes be problematic – read the scenario on **how to set up your own web server** later in the guide for an example of how to overcome the problem of changing IP addresses.

How Do I Do That? Home Networking Scenarios

You have a non-networked printer, and you want to share it to every computer

Many new printers come with built-in networking capabilities – some are even wireless. But if you already own a printer, it's useful to share that printer on the network so that any computer can use it – not just the “host” machine that the USB cable is plugged in to. What are your options?

- If the host computer is running Windows 7, simply enable the **Homegroup** feature. Windows 8 users can follow this guide. If the host is off or sleeping, the printer will be inaccessible.
- Share your printer with anyone in the world via Google Cloud Print. Again, this requires the connected machine to be left running and will only work from within a Chrome browser session, but it does then open up possibilities to print from Google Docs or Sheets on a mobile device.
- Buy a print server. A wired print server can be bought for as little as \$30, allowing you to place it next to your network switch or anywhere you can get a network cable to; wireless ones are considerably more at around \$60.



- Use a Raspberry Pi to make your own wireless print server. The total cost is about \$45 including the wireless adapter, but if you've already got a Pi sitting on your network gathering sensor data, it would be cost effective to repurpose it as a print server too.
- Check your router – if it has a USB port, it's probably able to act as a print server. The Apple Airport Extreme can do this, for instance – but the one given to you by your ISP might not.

You want to print from your iPad or iPhone

AirPrint is a special protocol that enables you to print from Apple iPhone and iPad devices. Despite Apple Airport Extreme, AirPort Express and Time Capsule hardware having the capability to share a USB printer, it doesn't magically turn that printer into an AirPrint compatible device. There are however two ways you can go about adding AirPrint to a non-AirPrint device.

The first is by using the same Raspberry Pi hack described above; just install some additional software on the Pi, and your non-networked printer will be both shared on the network and AirPrint-compatible. If you don't want to spend the \$35 on a Raspberry Pi, your other option is to keep the printer connected to a Mac that's almost always left on, and to run some software such as Printopia. Printopia costs \$20, though there is demo available so you can see if it works in your setup.

You have a USB storage drive, and you want to share it to everyone without leaving your computer on all the time

Check your router first: if it has a USB port, it can likely share anything plugged in automatically. You can also purchase something called a "USB NAS adapter" for around \$100; these simply take a USB drive, and turn it into networked storage. They aren't fully-fledged NAS devices so you won't find drive redundancy or server features, but they will serve as a simple and reliable file store. The Pogoplug (currently \$20, down from \$100, which may indicate a new model is imminent) is one such device.

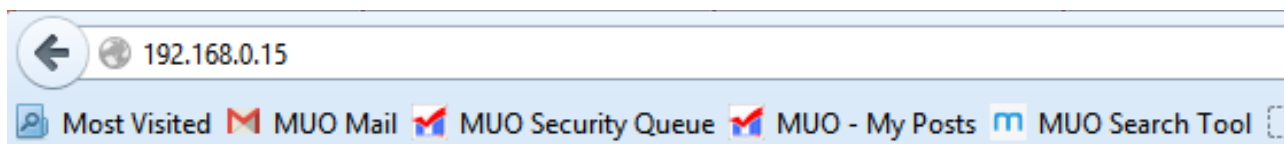


There's also the DIY route, with a Raspberry Pi.

You want to set up a web server to host a website

There are a number of steps to this: the first is to actually install a web server – typically, you’ll use an older computer and install a ready-made web server linux distribution, which automatically configures components such as Apache and a MySQL database.

You can also try a more generic “home server” distro such as Amahi, which includes a web server, file server, and other apps. Our most recent guide on setting up a webserver is for Raspberry Pi, which makes a good low-performance low-cost web server since it can be left on without consuming a lot of electricity.



It works!

This is the default web page for this RaspberryPi server.

The web server software is running but no content has been added, yet.

The second part is to use port forwarding to enable requests on port 80 to be forwarded to your server. Without setting this up, your web server will be inaccessible from the outside world because by default, the router firewall will block requests to that port. What is port forwarding and how can it help me?

Port Forwarding Rules

Name	Port Range	Protocol	IP Address	Enable	Delete
				<input type="checkbox"/>	<input type="checkbox"/>
HTTP	80	TCP	192.168.0.3	<input type="checkbox"/>	<input type="checkbox"/>
yawcam	8081..8888	TCP&UDP	192.168.0.9	<input type="checkbox"/>	<input type="checkbox"/>
plex	32400	TCP&UDP	192.168.0.5	<input type="checkbox"/>	<input type="checkbox"/>
torrent	55555	TCP&UDP	192.168.0.9	<input type="checkbox"/>	<input type="checkbox"/>
vpn	1194..1195	TCP&UDP	192.168.0.10	<input type="checkbox"/>	<input type="checkbox"/>
SSH	22	TCP&UDP	192.168.0.11	<input type="checkbox"/>	<input type="checkbox"/>

The final part is to give your web server a domain name. If you don’t want to pay for one, try using DynDNS to set up a free subdomain.

Endless Possibilities

Home networking opens up a whole new world of computing; the possibilities are exciting and endless. That's all for our introductory guide, but if you have some specific scenarios you're struggling with or need some general networking advice, please ask your question at [MakeUseOf Answers](#).

Read more stories like this at [MakeUseOf.com](#)
