

# Boost your Wi-fi network range

If you find your wireless network doesn't reach far enough, it's easy to extend its range

**W**ireless networking is unarguably the most convenient form of networking – until you move out of range. Thankfully, this is not an insurmountable problem, as it's simple to add a **repeater** to a wireless network.

A repeater is a small device that connects to the existing wireless network and extends the range by **re-transmitting** the signals. Despite the claims for increased range on the latest wireless equipment, repeaters are often still

necessary. Thick walls, and even microwaves and wireless phones, can reduce the range of the network.

This workshop will show you how to install a Belkin **wireless repeater** on a wireless network that already has an existing Belkin **wireless router**, though the instructions will be very similar for devices from other manufacturers. Wherever possible, however, you should choose a repeater of the **same brand** as your current router or **access point**.

## Step 1

During the setup of the repeater, you'll need to access some settings on the network router. Some routers come with software on a CD, but all can be controlled via a **special web page**. To access these pages enter the network address (**IP address**) of the router into the address bar of Internet Explorer. This is made up of four sets of numbers and will probably be 192.168.1.1 or 192.168.2.1. If neither of these addresses works, click on the Start button and select Run. Type **cmd** and then, in the window that appears, type **ipconfig** and press Enter. The address of the router is listed as **Default Gateway**, and you can connect to it by typing that address into your **web browser**.

```
D:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\Tim>ipconfig

Windows IP Configuration

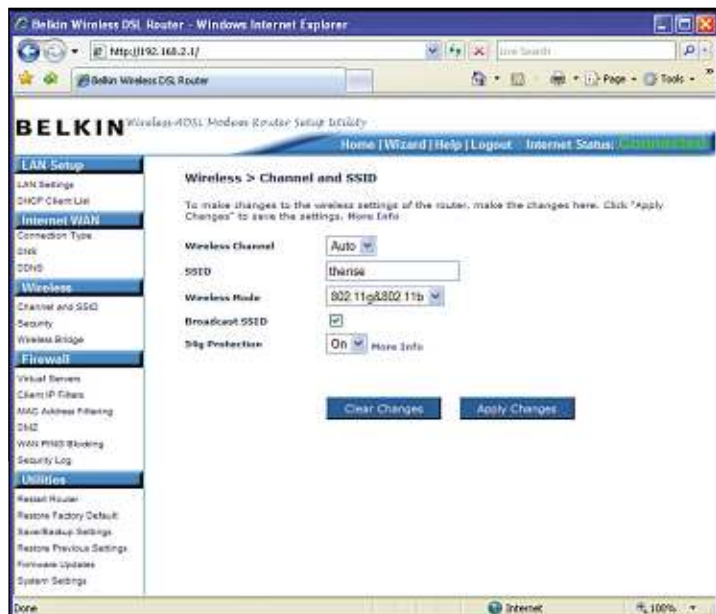
Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnect

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . : Belkin
    IP Address . . . . . : 192.168.2.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

D:\Documents and Settings\Tim>
```



## Step 2

In order to set up the wireless repeater correctly, it's a good idea to have some information about the wireless network written down so it's easy to refer to. Enter the **IP address of the router into the address bar** of Internet Explorer and press Enter. Click on the Login link at the top right and **enter the admin password**. Click on the **Channel and SSID** link in the left-hand column and note down the SSID, or network name. Next, **click on the Security link** below and **note down the type of encryption and the key**. It's best to note down both the key and the passphrase, in case the repeater requires one or the other. If you're using a different brand of wireless equipment the screens will look slightly different, but you'll still be looking for the same information.

## Step 3

If there is **no encryption on the wireless network**, the Belkin Wireless repeater is very simple to set up. **Place it near the existing router** and plug in the power supply. When the power and wireless lights are illuminated and the searching light flashing continuously, **locate the light grey button** on the back of the repeater labelled Autoconnect, **hold it down for at least 10 seconds** and then release it. The repeater will **connect to the wireless network with the strongest signal** – hence the importance of placing it as close as possible to your existing router. The repeater is ready when the red searching light goes out, and you can **relocate it** to extend the range of your wireless network.

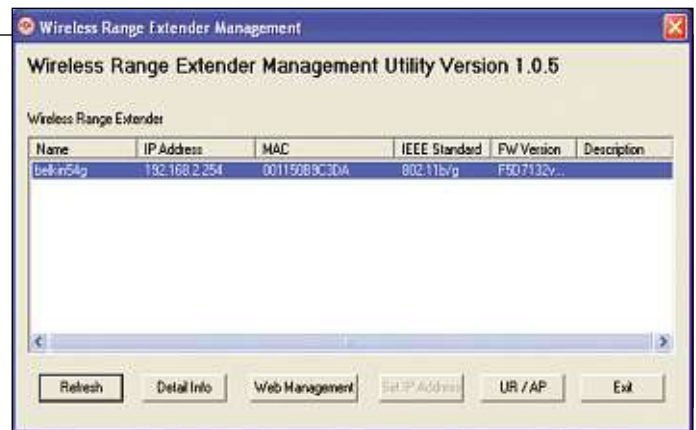


## Step 4

Even though it is easier to set up the repeater when there is no security encryption on the wireless network, it really is best to use security. Insert the **disc supplied with the repeater into your computer's CD-Rom drive**. When the set-up screen appears, click on **'Run the easy install'**. If this screen doesn't appear, double-click on the **icon** for the CD-Rom drive. Work through the installation and then close the set-up window.

## Step 5

**Disconnect the computer with the wireless utility from the wireless network and connect it to the wireless repeater using the network cable** supplied in the box. Plug in the wireless repeater, then click on the Windows Start button. Choose All Programs, Belkin Range Extender Utility and then **Belkin Range Extender Utility** again. Click on the **Refresh** button and the repeater should appear in the list with the IP address **192.168.2.254**, as shown here. Click once to select it and then click on **Web Management**. Your **web browser will connect to the repeater**. You should click on the **Login** link at the top right-hand corner of the screen, then click on **Submit**.



## Step 6

Click on the **security link** in the left-hand column and **change the settings so they match your original wireless settings**, including the password. Click on **Apply Changes**. Next, click on the **Basic link** to reach this screen and **change 'Parent AP SSID' to match the name of your existing wireless network**. Click on **Apply Changes** and the repeater will **reboot**. When it has rebooted, the status text towards the bottom of the screen should read **Connected** and you can unplug the repeater from the computer. There is now an **extra wireless network** called **belkin54g** with an **identical security password** to the existing network. The repeater can now be positioned near the edge of the range of the router to extend the wireless network and your laptop can connect to either access point, with the same password. Some routers support an option called **WDS (Wireless Distribution System)**, which means both access points can have the **same network name**, too.

# Wifi a risk?

Manchester plans free  
wifi for  
2 million

Wifi health stu  
gets no head

Wifi to  
boost  
broad-  
band  
in rural  
areas

# IS Wi-Fi safe?

WIFI  
FEAR  
UNPR

The safety of Wi-fi has been called into question, but experts have accused critics of presenting junk science as fact. We investigate

The Government has announced research into the potential long-term health effects of using Wi-fi. With 'experts' in the press and TV questioning whether or not we should be using the technology, while computer companies extol the freedom of wireless computing, it can be hard knowing what to believe.

Are wireless network users storing up health problems for the future and putting their children at risk? Are the concerns based on gut feeling, hard facts or junk science? Do you really need to worry about the built-in Wi-fi in your home, or is it all new-age mumbo-jumbo?

Over the past few months, Wi-fi has started to get some bad press, with at least one national newspaper writer urging readers to ditch it and a BBC Panorama report suggesting that it could be harming children in schools. And now the

Government's Health Protection Agency (HPA, [www.hpa.org.uk](http://www.hpa.org.uk)) has announced that it is carrying out more research into the use of Wi-fi. So is it time to unplug your wireless router? Frankly, probably not.

Behind the headlines and the hype, the scope of the HPA research is not quite as alarming as some have made it sound. Announcing the research, Professor Pat Troop of the HPA said: "There is no scientific evidence to date that Wi-fi adversely affects the health." And the new research isn't intended to discover whether or not Wi-fi can make people ill; instead, it's to measure the extent to which people are exposed to radio waves when a wireless network is in use. Using both laboratory tests and real-world environments, the HPA will study models – a sort of radio version of crash test dummies – to find out just how much of the signal reaches different parts of the body.

The HPA expects that the research will provide a clear idea of how the signals from Wi-fi compare with those from mobile phones – for which there's presently no evidence of a health risk, despite extensive research both here and in Europe. And if the exposure from Wi-fi is less than that from mobile phones, then the HPA hopes the information will reassure people that wireless networks aren't causing problems for them and their children. It may be that lessons learned in the mobile phone research could be applied for wireless PC networks.

## Watts going on?

Much of the concern about radio waves – or electromagnetic radiation – is the amount of power they produce, which is measured in watts. The maximum power mobile phones can produce is up to two watts; the maximum permitted for a Wi-fi device in Europe is 20 times less at 0.1 watts – though a phone will turn down the power when it's in a good signal area. But it's



▲ Wi-fi has received some bad press in the past and, like mobile phones, its safety is in doubt



▲ Go to [www.powerwatch.org.uk](http://www.powerwatch.org.uk) for some independent advice on microwave and electromagnetic technology

also worth remembering where the signals are – you hold a mobile phone right next to your head, whereas Wi-fi equipment tends to be in the computer, a few feet away, or in the base station, even further away. And the laws of physics mean that if you move a radio device twice as far away, the signal you receive drops to a quarter of the strength – it's called the inverse square law.

It's very likely that the strength of the radio signals you're surrounded by from Wi-fi are much, much lower than those from your mobile phone. And even if there are several Wi-fi computers in the same room, they are unlikely to all be transmitting data at the same time. So a busy Wi-fi-equipped classroom is unlikely to expose children to significantly higher levels. But, as with all aspects of safety in schools, it's worth checking, and the HPA study will try to quantify exactly how much the level rises.

### Electrosensitivity

There are people who claim to be sensitive to wireless networks, mobile phones and other equipment. They call themselves electrosensitive and claim they suffer headaches and other symptoms, and can tell when a wireless network or mobile phone is operating, based on their symptoms. Some even claim to feel better when they're carrying a special crystal to re-align energies, or if they paint their walls with special paint to keep out radio waves.

So, who's right? Can some people detect 'electrosmog' and feel better when it's removed? There are certainly people who do feel better when they've turned off their wireless network but, so far, there hasn't been a proper scientific test that would prove whether electrosensitivity

is real. Many doctors suspect it might actually be more of a psychological phenomenon. That's not to say that radio waves don't have an effect on human cells, but so far no one has proved any illnesses are caused by mobile phones, let alone Wi-fi with its much lower power levels.

### No evidence

The HPA's study is going to take two years, so what should you do in the meantime? Well, it's impossible to say there's no risk, but all the available scientific evidence so far suggests you're quite safe to carry on using Wi-fi, along with your mobile phone.

More radio signals will be coming in through the windows of your child's classroom than from the Wi-fi on the computers they use. If you're the cautious kind and limit your child's use of mobile phones, you might consider not putting Wi-fi kit in their bedroom either, but you're probably more likely to be hurt tripping over network cables than by radio waves from a home wireless network. In the words of HPA's Professor Troop: "We have good scientific reasons to expect the results to be reassuring, and we will publish our findings."

### Jargon buster

- ▶ **Bluetooth** A technology that allows devices to communicate, like printers, with each other wirelessly over short distances.
- ▶ **Dect** A technology used by some cordless phones to maintain clear call quality within homes.
- ▶ **Router** A device used to connect more than one computer together and/or to the internet as an alternative to a modem.
- ▶ **Wi-fi** An umbrella term for various standards for wireless networking.

For more Jargon Buster definitions see page 97 or visit [www.computeractive.co.uk](http://www.computeractive.co.uk)

## Radio active?

Wi-fi and mobile phones don't transmit all the time, and this helps to decrease any theoretical effect of exposure. And they aren't the only sources of radio waves in your home, either. Microwave ovens, Bluetooth devices and Dect cordless phones all use radio, as do some video senders – and all can use the same radio frequencies as Wi-fi.

A Dect phone has a power of around 0.01 watts, while Bluetooth is even lower at just 1 milliwatt (0.001 watts), and a microwave oven is permitted by official safety guidelines to 'leak' around five milliwatts.



▲ Microwave ovens leak considerably more than Wi-fi

Finally, radiation might be a scary word out of context, but all radio waves – and even visible light from street lamps or the sun – are electromagnetic radiation in scientific terms.