

Routers and Security

Welcome to this training lesson on **Routers and Security**. In this lesson, we'll look at the ways you can ensure your router is set up securely.

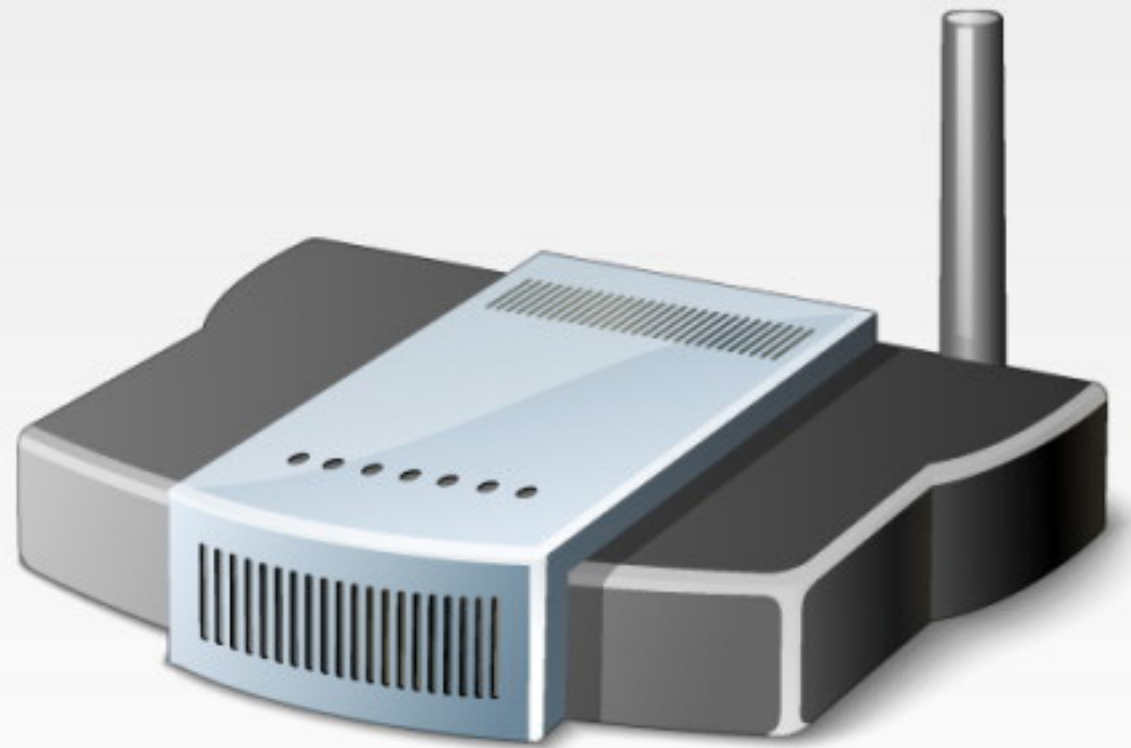
Estimated Completion Time: 8 minutes.

Routers and Security

What is a Router? In this lesson, the router we refer to is the home or small office router. It is the device that connects directly to the Internet - looking something like the image below - and allows you to connect a number of devices to the Internet.

Most home or small business routers today allow you to connect to it via an ethernet cable, or wirelessly.

Although not quite correct, a router may also be commonly known as a modem.



Routers and Security

Warning. On the following steps, we look at ways you can configure your home router.

This may be a little confusing for casual users. In fact, for most users, the steps we describe here will never be necessary, assuming your router was set up correctly in the first place.

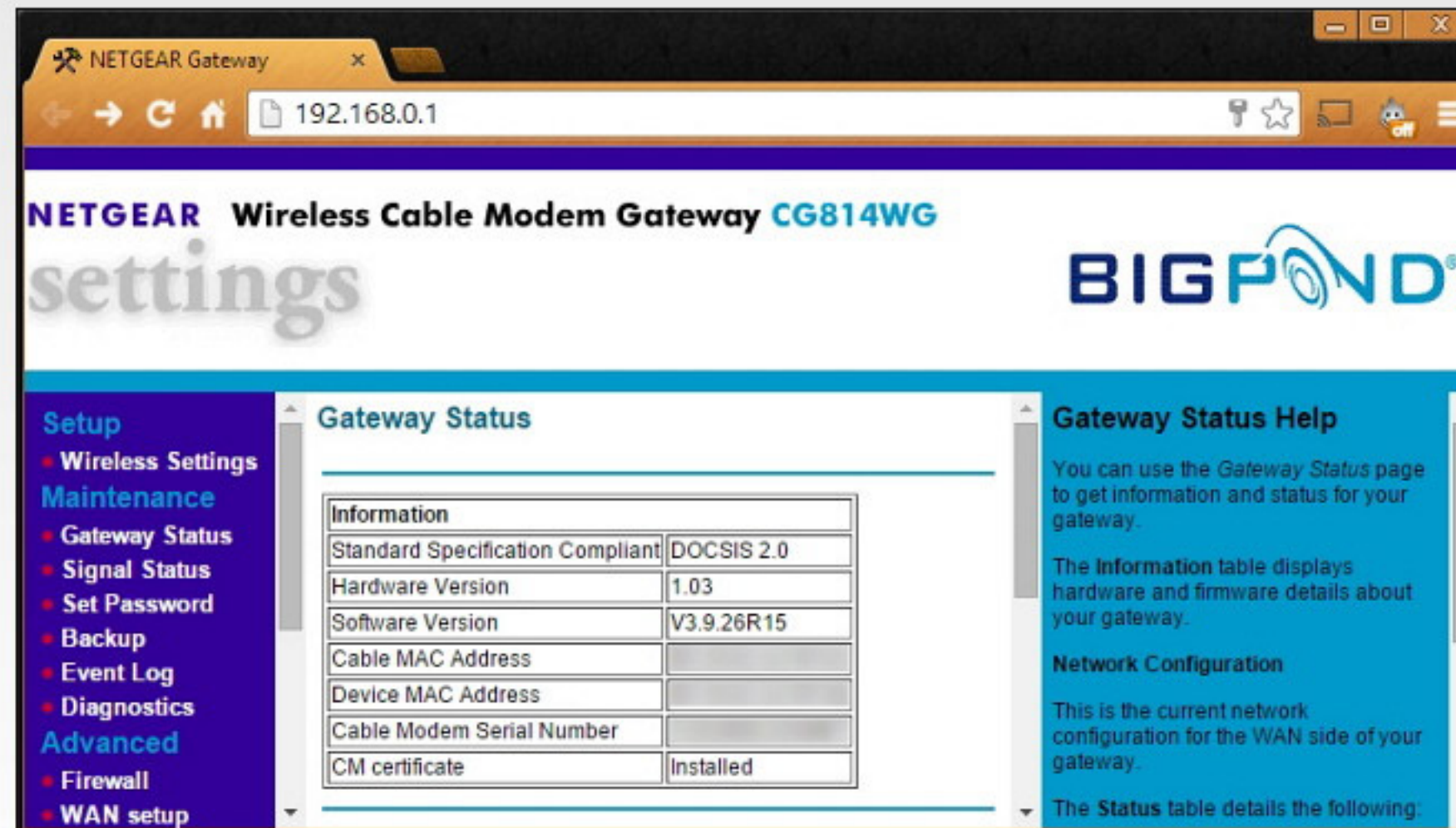
But read on anyway - so you can see what is possible.



Routers and Security

Connecting to Your Router. Once your router is set up, normally by a technician, you'll be able to connect to your router easily from any computer or mobile device.

However, if you want to modify router settings, like to change or add security features or settings, you'll need to connect to your router in a slightly different way.



The screenshot shows the NETGEAR Gateway settings page for a Wireless Cable Modem Gateway CG814WG. The browser address bar shows the IP address 192.168.0.1. The page has a purple header with the NETGEAR logo and the product name. The main content area is divided into three sections: a left sidebar with navigation links, a central 'Gateway Status' section, and a right sidebar with 'Gateway Status Help'.

Gateway Status

Information	
Standard Specification Compliant	DOCSIS 2.0
Hardware Version	1.03
Software Version	V3.9.26R15
Cable MAC Address	
Device MAC Address	
Cable Modem Serial Number	
CM certificate	Installed

Gateway Status Help

You can use the Gateway Status page to get information and status for your gateway.

The Information table displays hardware and firmware details about your gateway.

Network Configuration

This is the current network configuration for the WAN side of your gateway.

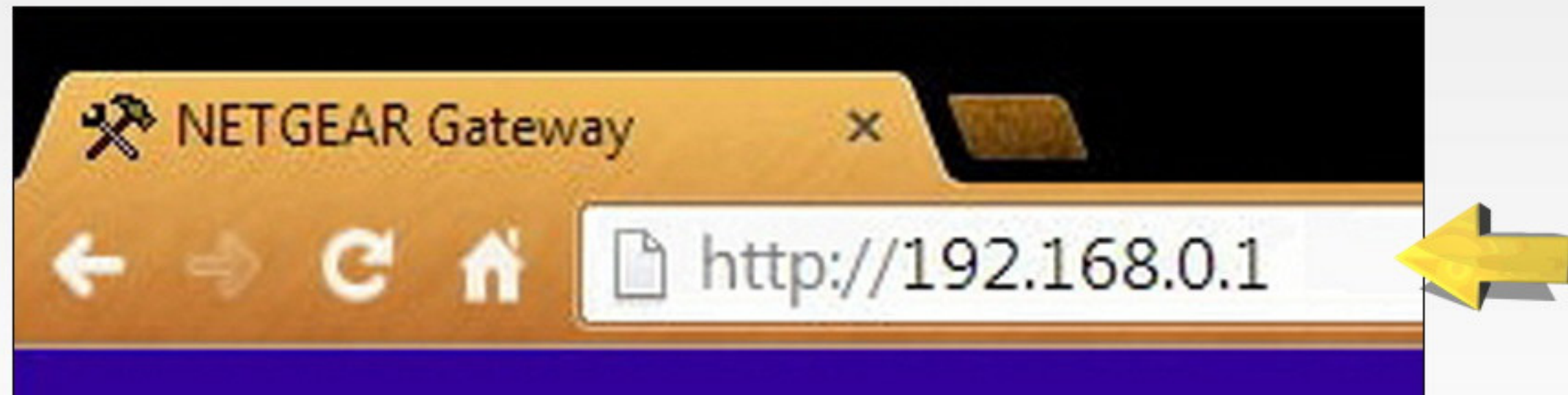
The Status table details the following:

Routers and Security

Connecting to Your Router (2). To connect directly to your router, you'll need a browser. You enter the address of the router into your browser, and once you've done this, you'll be able to adjust all router settings.

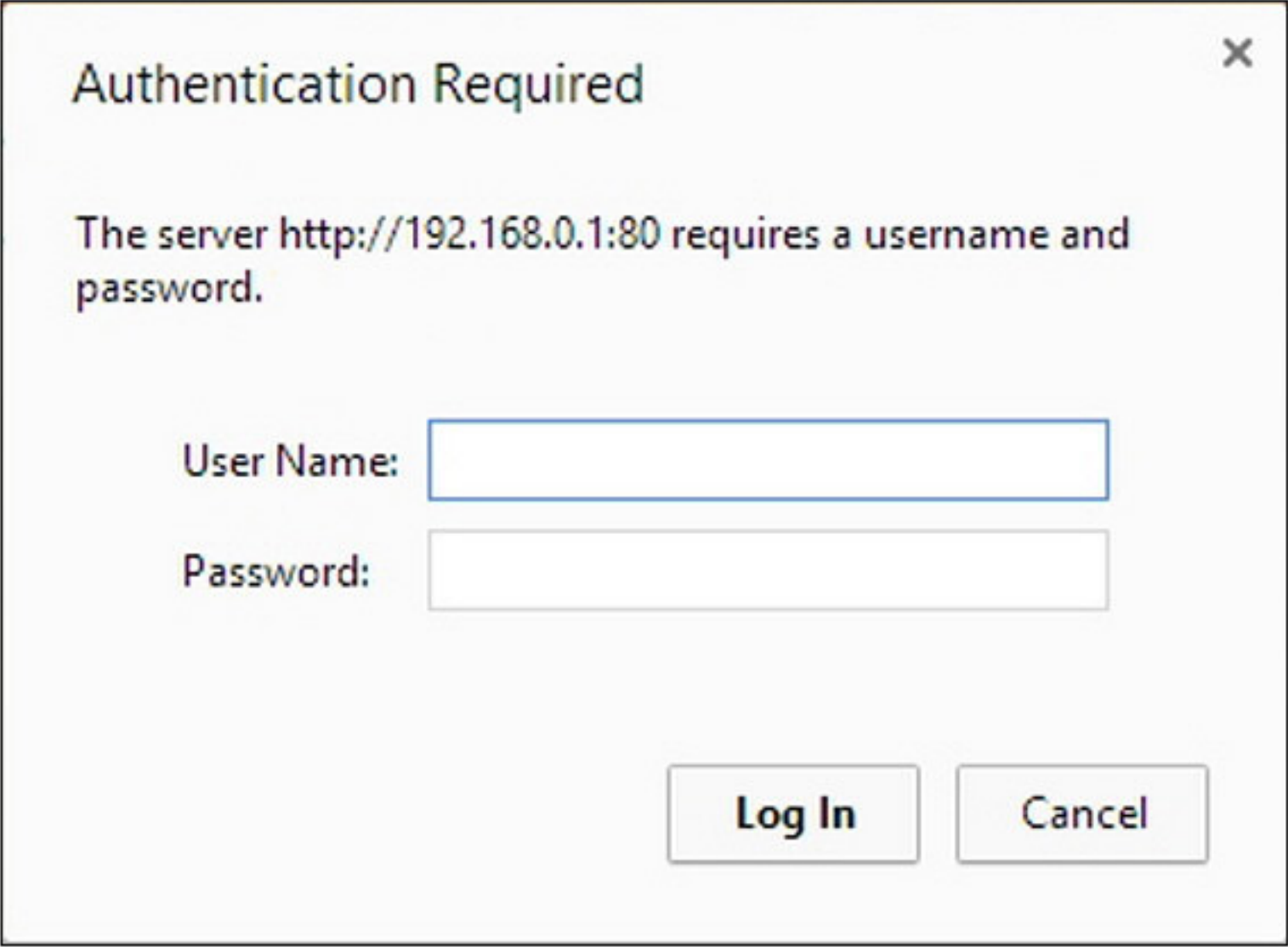
Two things you will need to know. 1 - the address of the router. You may need to consult your router documentation for this. The address to enter into your browser is *normally* **http://192.168.0.1**, or **http://192.168.1.1**..

Secondly, you'll need to know the router user name and password.



Routers and Security

Router Password. If you don't know the router user name or password, you'll need to contact the installer, consult your documentation, or try the default name and password for your router (often, this is listed on the bottom of your router).



A screenshot of a web browser's authentication dialog box. The title bar says "Authentication Required" with a close button (X) in the top right corner. The main text reads: "The server http://192.168.0.1:80 requires a username and password." Below this text are two input fields. The first is labeled "User Name:" and the second is labeled "Password:". At the bottom of the dialog are two buttons: "Log In" and "Cancel".

Authentication Required

The server http://192.168.0.1:80 requires a username and password.

User Name:

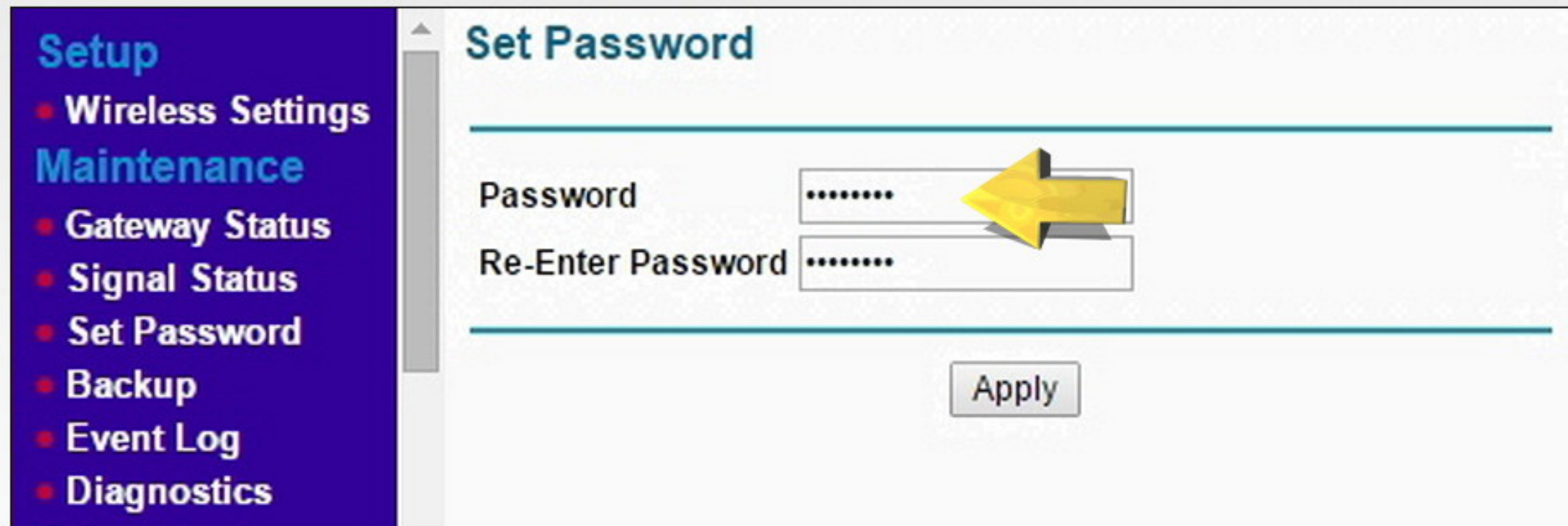
Password:

Log In Cancel

Routers and Security

Changing the Router Password. Once you've connected to your router in this way (and your screen may look different to the one we've pictured), the first thing you should do is change the default password - if it is still being used.

Hackers know the default passwords for all routers - and if they do, they can connect to your router, and change any settings they like.

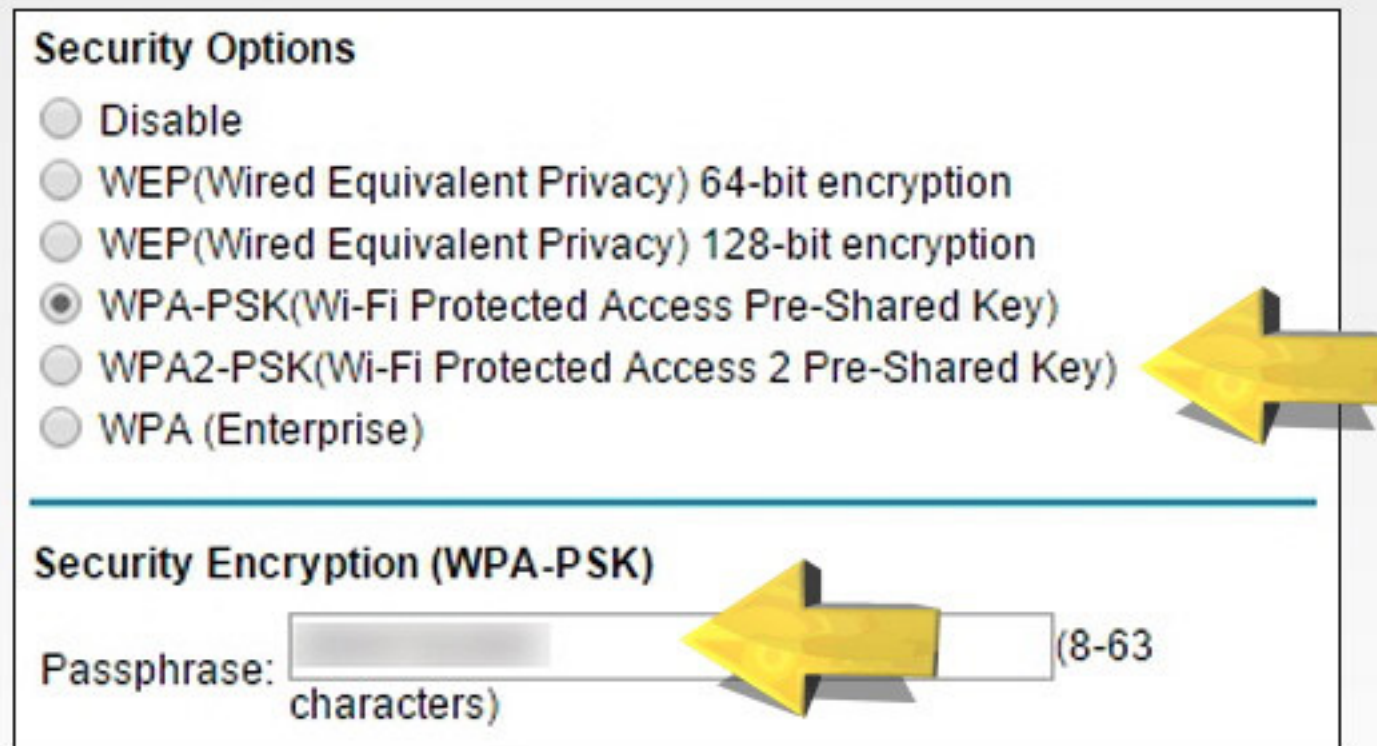


The screenshot shows a router's web interface. On the left is a dark blue sidebar with a menu. The top menu item is 'Setup' in light blue. Below it are 'Wireless Settings' and 'Maintenance' in white. Under 'Maintenance', there is a list of options: 'Gateway Status', 'Signal Status', 'Set Password' (highlighted with a red dot), 'Backup', 'Event Log', and 'Diagnostics'. The main content area has a title 'Set Password' in blue. It contains two input fields: 'Password' and 'Re-Enter Password', both with masked text (dots). A large yellow 3D arrow points from the 'Re-Enter Password' field to the 'Password' field. Below the fields is an 'Apply' button.

Routers and Security

Router Security. Most routers have security already enabled for standard Internet wireless access. This means no one can connect to the router unless they know the password.

Your router will have several forms of encryption available - generally WPA or WEP are most commonly used. It doesn't really matter what these terms mean - they just provide a secure, password protected connection. The bottom line here is that some form of encryption needs to be employed, and a password selected - otherwise *anyone* can connect to your router.



Security Options

- ☐ Disable
- ☐ WEP(Wired Equivalent Privacy) 64-bit encryption
- ☐ WEP(Wired Equivalent Privacy) 128-bit encryption
- ☒ WPA-PSK(Wi-Fi Protected Access Pre-Shared Key)
- ☐ WPA2-PSK(Wi-Fi Protected Access 2 Pre-Shared Key)
- ☐ WPA (Enterprise)

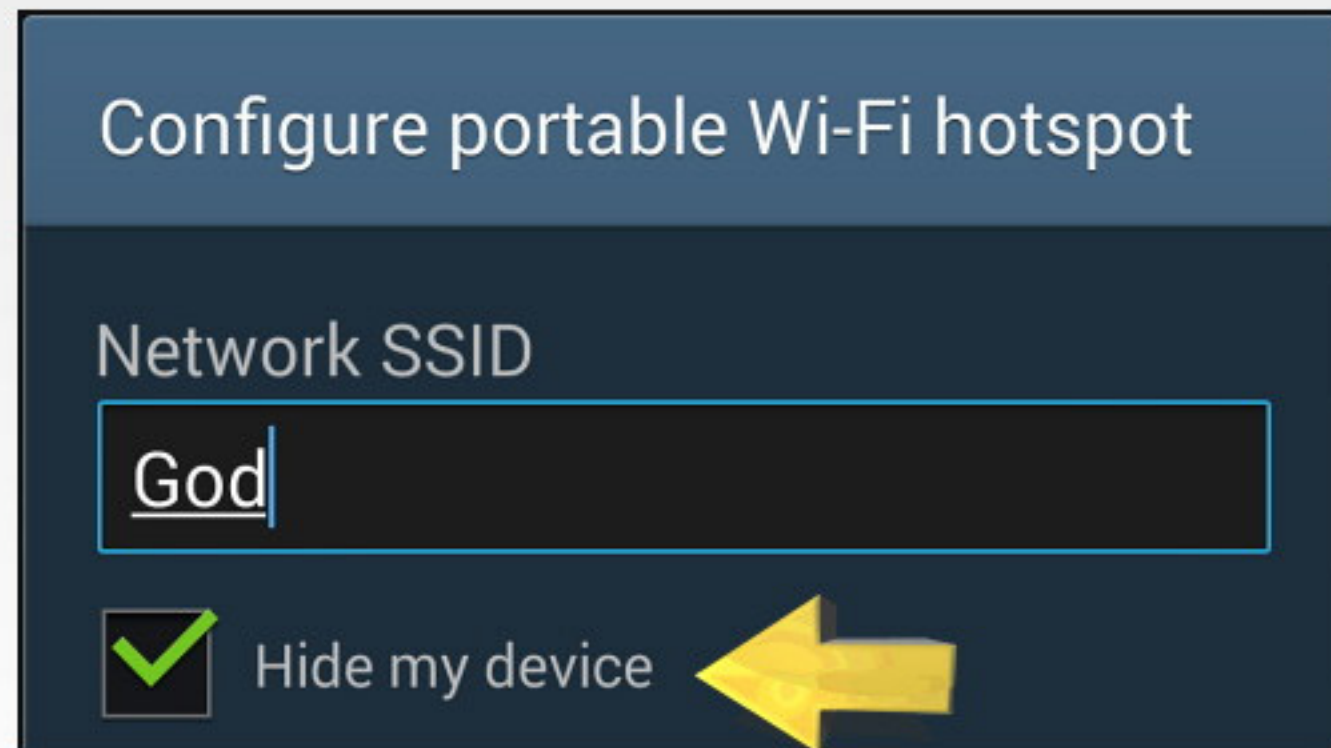
Security Encryption (WPA-PSK)

Passphrase: (8-63 characters)

Routers and Security

Broadcasting SSID. Every router has what is called an **SSID** - which is just the name of the router (which you'll be able to edit). By default, this is generally *broadcast*, which means that anyone in range will see the name of your router on their device.

Your router will have an option to either **Hide my device**, or **Allow Broadcast of Name**, or some similar option. If you do hide your SSID, it makes it harder for hackers to even know your device exists - but it will mean your local devices will have to initially manually connect to the router.

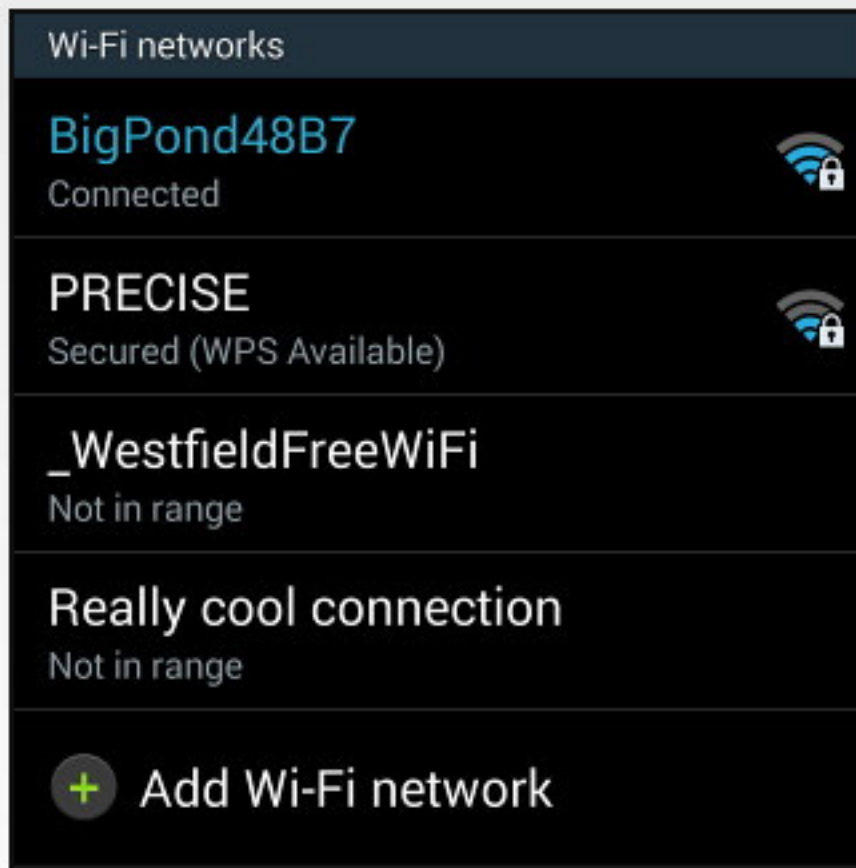


The screenshot shows a configuration window titled "Configure portable Wi-Fi hotspot". Inside, there is a section labeled "Network SSID" with a text input field containing the word "God". Below this, there is a checkbox with a green checkmark and the text "Hide my device". A large yellow arrow points to the "Hide my device" checkbox.

Routers and Security

Broadcasting SSID (2). When your router SSID is hidden, it will not appear in any list on any device.

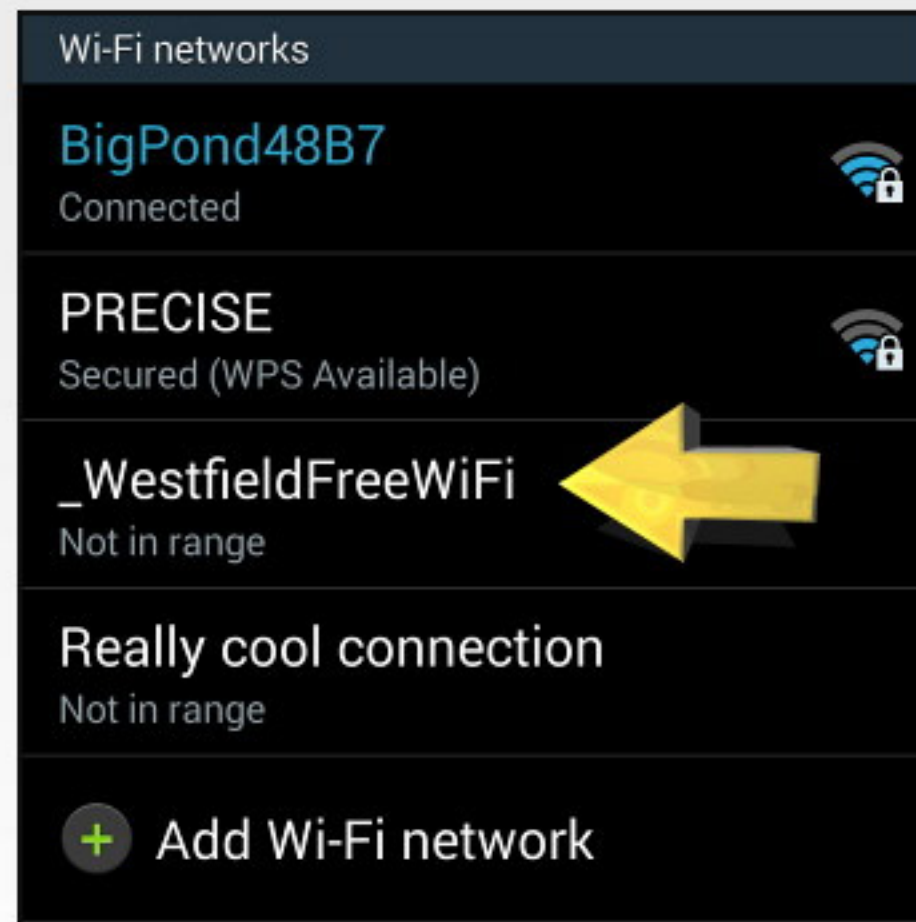
Below is the sort of list you see when connecting to a router - and it can contain anywhere from one to dozens of router names. Router names with a padlock icon next to them are password protected.



Routers and Security

Public WiFi. A good point to mention here - in the image below, a number of WiFi connection points are listed. Some of these are public - like **_WestfieldFreeWiFi**.

Connect to public available WiFi with extreme caution. Just because a WiFi connection point says **_WestfieldFreeWiFi**, it does not necessarily mean the Westfield Shopping Centre is providing it. It could be a hacker waiting for you to connect to *their* network.

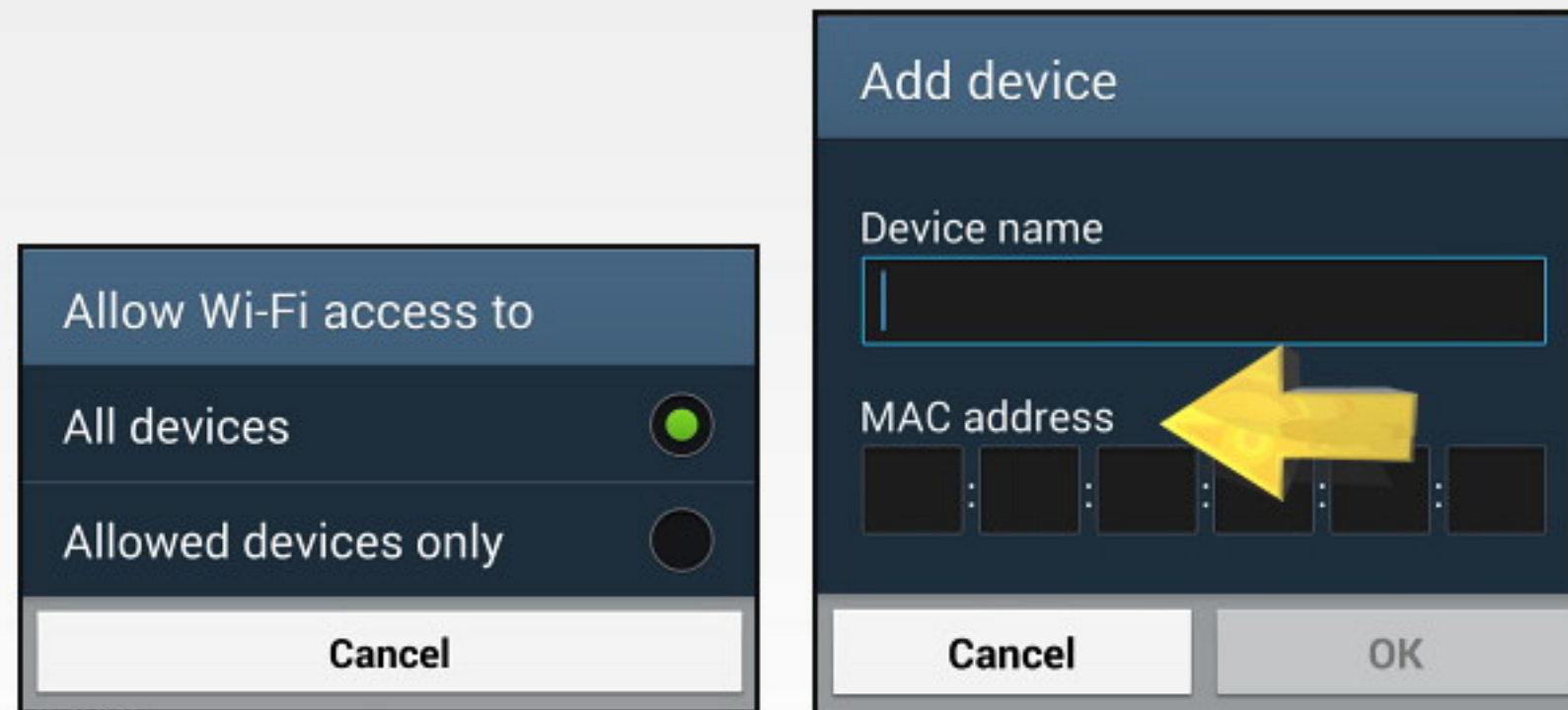


Routers and Security

MAC Addresses. For an even higher level of security, you can set your router so that it will only accept connections from specific devices. Each specified device is identified by what is known as its **MAC Address**.

This is a more complex operation, and should only be attempted with some good router documentation.

However, it can help protect your router and local devices by ensuring only specific devices can connect to the router for Internet access.

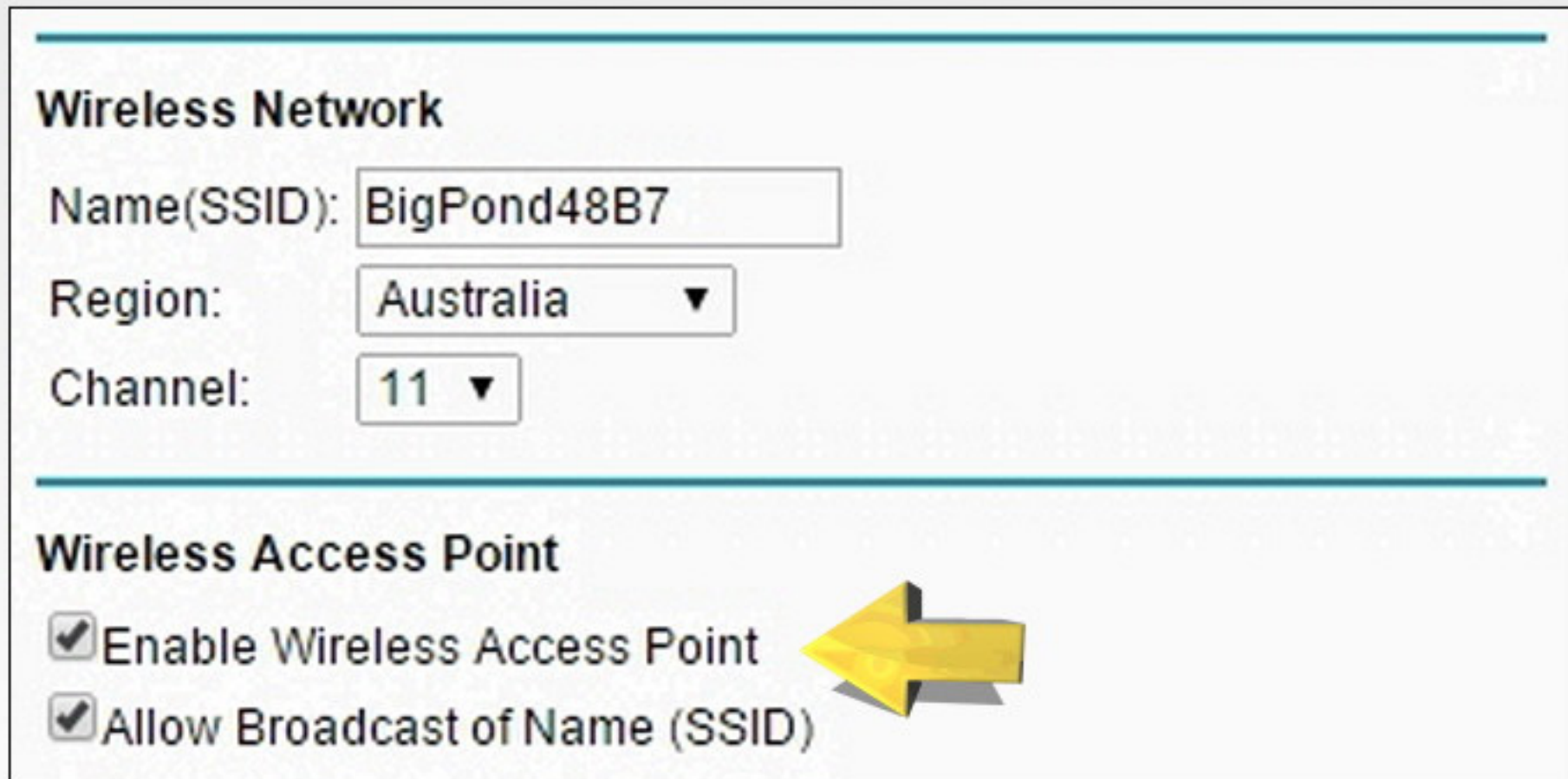


The image displays two screenshots from a router's web interface. The left screenshot shows the 'Allow Wi-Fi access to' settings, with 'All devices' selected (indicated by a green dot) and 'Allowed devices only' unselected (indicated by a grey dot). A 'Cancel' button is at the bottom. The right screenshot shows the 'Add device' dialog box. It has a 'Device name' text input field and a 'MAC address' field represented by six boxes separated by colons. A large yellow arrow points to the MAC address field. 'Cancel' and 'OK' buttons are at the bottom of the dialog.

Routers and Security

Turn Off Wireless. There may be circumstances where you only want to connect to a router with cables, rather than wirelessly.

If this is the case, you can turn off the wireless capability of your router. This protects you in that only devices that are connected to your router with a cable will get access. (This involves connecting to your router as we described earlier in this lesson).



Wireless Network

Name(SSID):

Region:

Channel:

Wireless Access Point

☒ Enable Wireless Access Point

☒ Allow Broadcast of Name (SSID)

Routers and Security

Phone Routers. Today, many phones or tablets have a router built right in. This allows you to share your phone's Internet connection with other people and devices around you.

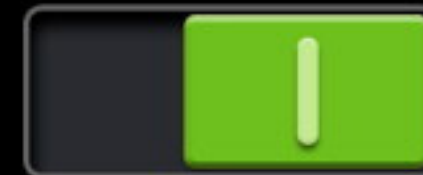
Most of the same rules apply - ensure security is enabled, for example, so that a password is required to connect. You'll have most of the same options, like whether to broadcast the SSID, or whether to allow connections to all or only specific devices.



Tethering and portable hotspot

Portable Wi-Fi hotspot

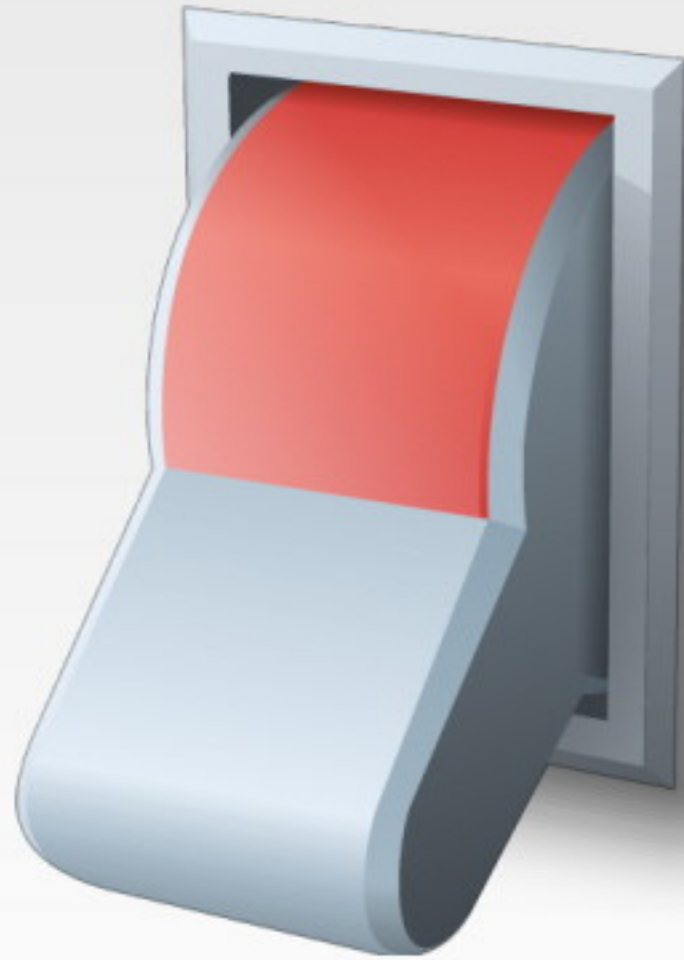
Portable Wi-Fi hotspot God active



Routers and Security

Turn it Off. If you are not going to use your router for some time, say, if you are off on vacation, it is a good idea to turn the router off.

Apart from saving electricity, it also prevents any hackers from trying to hack your router while you are away.



Routers and Security

You've now completed this training lesson on **Routers and Security**. In this lesson, we looked at the ways you can ensure your router is set up securely.