

Factsheet 16 – Securely configuring your broadband modem/router

To connect to the Internet nowadays, you'll most likely use a broadband modem or similar device. This factsheet explains some of the terms you'll see when configuring your broadband modem router and how these affect the security of your device.

This factsheet assumes the device is already connected to your computer/s and you have Internet access through the device.

You may use a different term other than broadband modem. If you have cable broadband, you have a *cable modem*, but if you use ADSL you probably have a *modem router*. So, why are these terms so often used interchangeably?

What is a (broadband) modem?

A broadband modem is a device that acts as the connection point for your home network to the line from your communications provider. A cable modem is connected to the outside world by coaxial cable, and a DSL modem by your pre-existing telephone wire pair. A pure modem acts as a bridge from your ISP to your network and implements no security features.

What is a modem router?

A modem router, in addition to having the properties of a broadband modem, enables your home network to have a different addressing scheme from your communications provider. This provides the opportunity to implement security features such as Network Address Translation (NAT) and firewalling.

So, a broadband *modem* does little more than connect your home computer network to the Internet via your ISP. A broadband modem may incorporate a router, in which case it will often be referred to as a *modem router*.

In this document, the term *modem/router* will be used whenever a particular feature or description applies to both types of device.



Popular broadband modem/router brands include Belkin, Billion, D-Link, Linksys, Motorola, Netcomm and Netgear and these come in a variety of models. It is recommended you refer to the user guide for your particular device, which is usually available from the manufacturer's web site. A list of the most common manufacturers' web pages is at the end of this factsheet.



Images are courtesy of Billion, D-Link, Netcomm, Netgear and Linksys.

Many of the configuration options described in this factsheet are not enabled by default and care should be taken when setting up a broadband device to only enable what is required.

Often, a broadband modem/router will also function as a (Wi-Fi) wireless access point. For information about securely configuring your Wi-Fi network, see [Factsheet 17 – Wi-Fi Security](#).

Steps to secure your broadband modem/router

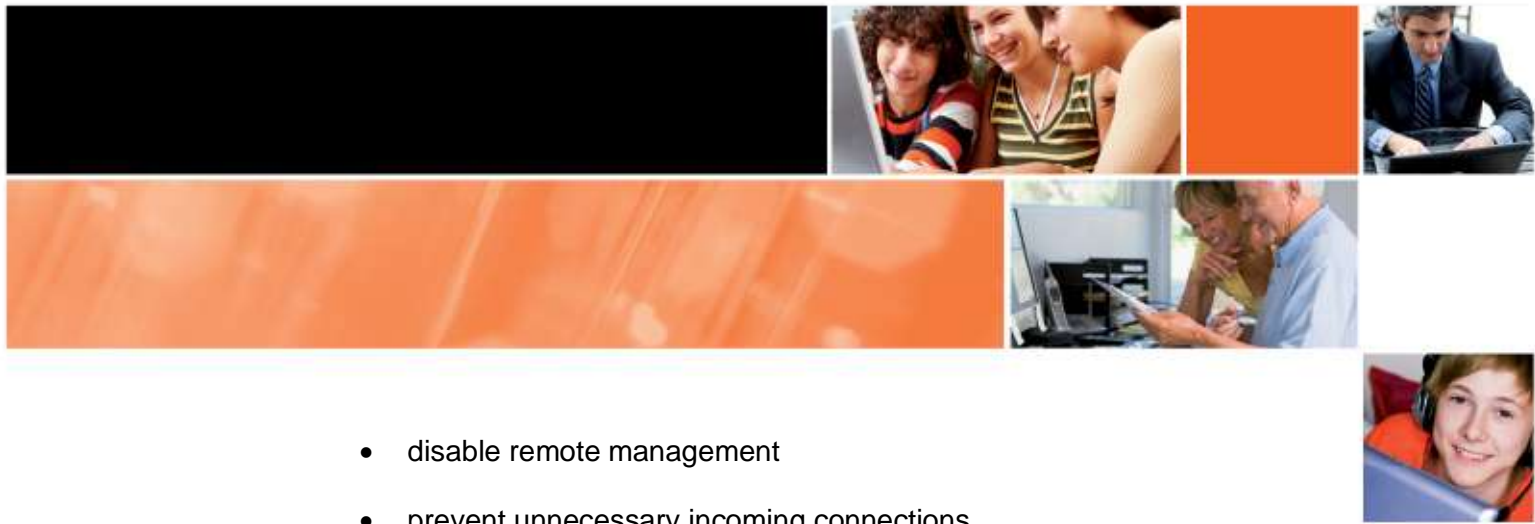
Broadband devices include a variety of security features. For example, you may find one or more of the following features listed in your broadband device guide/manual:

- Stateful Packet Inspection (SPI) firewall
- Intrusion prevention features
- Denial of service protection
- Port scan protection

All these features are useful and will, in most cases, not cause any slowness or other problems on your home network. These features are customarily turned on by default, and should be left that way unless there is a specific reason to turn them off.

In summary, you should aim to take the following actions, which are explained in more detail further on:

- change the default administrator (admin) password for the device



- disable remote management
- prevent unnecessary incoming connections
- disable unneeded services

The first thing you will need to do is log in to your device.

1. Open the modem router configuration interface. This involves using a web browser to browse to a specific address. Each manufacturer has set its own address and you will need to refer to the instruction manual for your particular device. Examples of possible addresses for your modem router are:

`http://192.168.0.1`

`http://192.168.1.1`

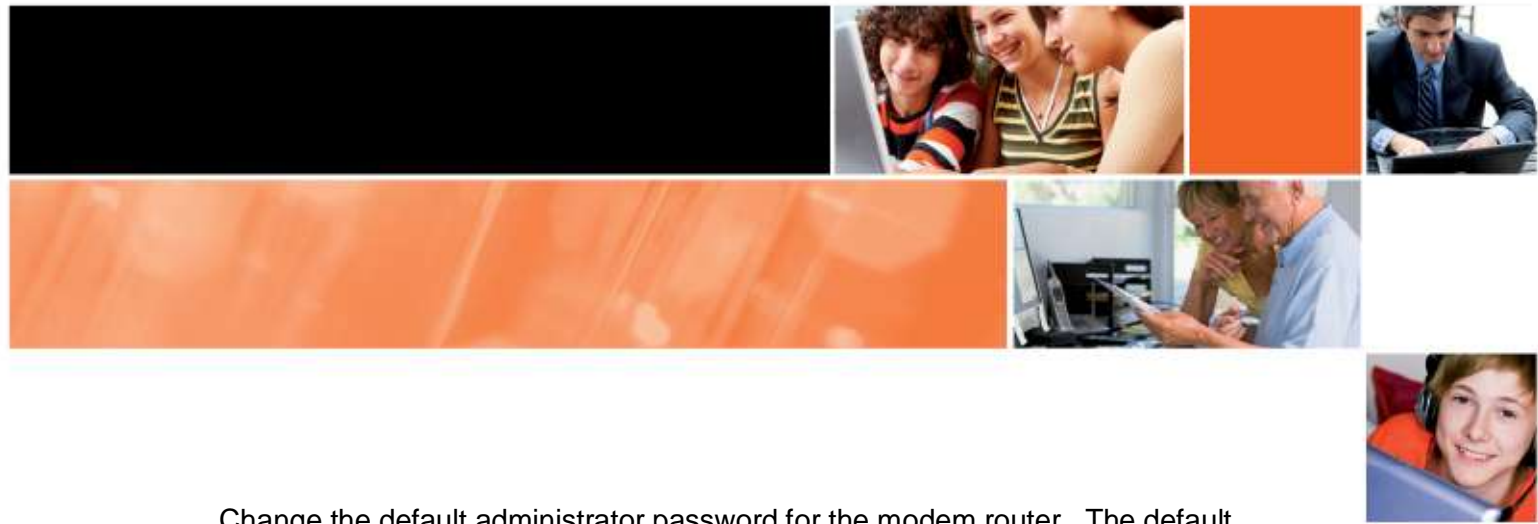
`http://192.168.1.100`

If your modem router was supplied by your ISP, you may need to contact the ISP for further details about how to log in.

2. Login to the modem router configuration interface. This means typing in the username and password. Each manufacturer has set its own default username and password. A common default username set by manufacturers is “admin” and a common default password is “admin” (without the quotation marks). Unless you already know it or have changed the username and password, you will need to refer to the instruction manual to find the username and password for your particular device.
3. It may be necessary to reset the modem router to the “factory defaults” or “manufacturer defaults” if a password was previously set and is now forgotten or lost. Again, refer to the instruction manual for your particular device if you do not know how to do this. Note that this action will also change any other configuration settings that may have been made that vary from the default settings.

Password Management

It is essential that once you have logged in to your modem router to change the default password. It is easy to find out the default passwords of broadband modem routers as many of the manuals are available on line.



Change the default administrator password for the modem router. The default password is the one set by the manufacturer at the time the device was purchased and installed. If your modem router is still using the default password, then change it.

If you obtained your wireless modem router through your Internet Service Provider (such as Telstra Bigpond or Optus), the ISPs may have changed the password for you, in which case refer to the information provided by the ISP when your Internet account was set up. If the password was given to you by the ISP it is still important to change the password to one that only you know. Refer to [Factsheet 15 – Understanding Password Security](#) before choosing your new password.

Write the new password down and hide it somewhere safe. It is not a password that you need to use very often and as such it easy to forget.

Remote Management

Many broadband devices include functionality that allows the device to be managed from a remote location away from the premises where the device is located, over the Internet. This feature is called “Remote Management”. Most devices do not have remote management enabled by default and if you don’t require it, leave it disabled.

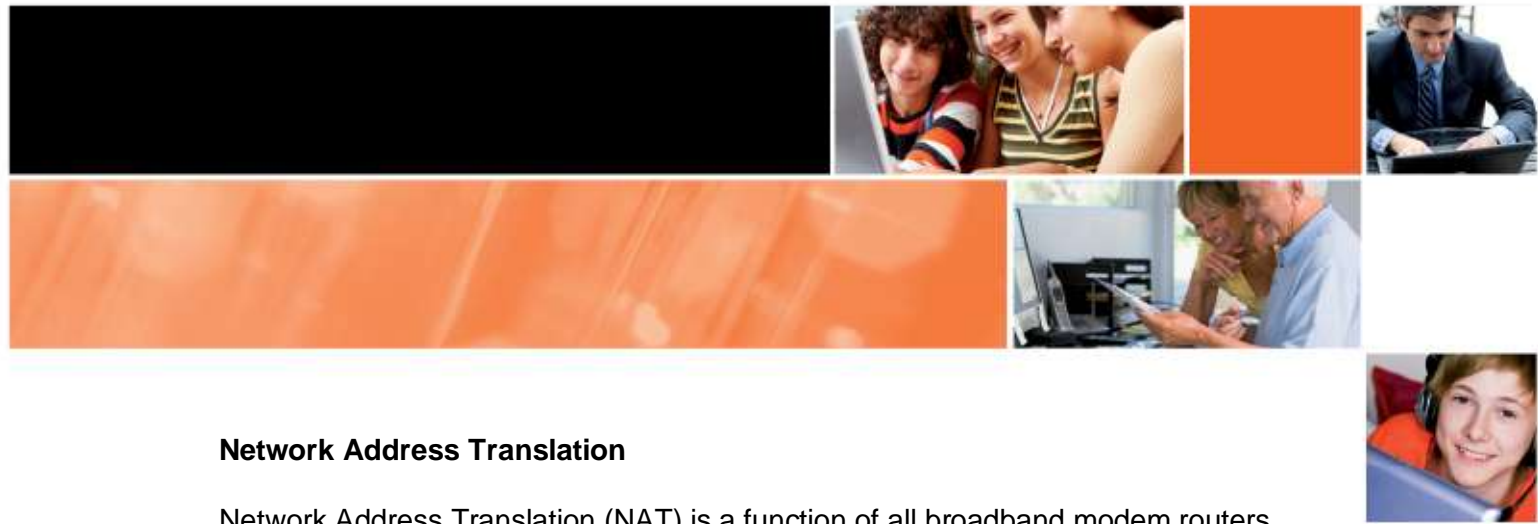
Carefully consider if this is required, before enabling remote management. Some devices allow you to limit which IP addresses can perform remote management – use this, if possible. If you need to enable remote management, turn it off as soon as it is no longer needed.

Incoming connections

Allowing connections into your network past your broadband modem router significantly increases the risk of computers on your local network being compromised. This section explains how to limit incoming connections and only enable them when necessary.

Firewall

Most modem routers incorporate a firewall that has sensible default filtering. Unless you have explicitly configured extra rules in your device, you should confirm that no extra rules have been set, as these may allow malicious network traffic into you network.



Network Address Translation

Network Address Translation (NAT) is a function of all broadband modem routers. NAT is the function of translating from the private IP addresses used by computers in your home or office to a public IP address given to you by your ISP. Public IP addresses can be reached by computers on the Internet, whereas private IP addresses can only be reached by computers within the local area network.

Private IP address ranges are:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Most broadband devices use the 192.168.0.0 – 192.168.255.255 range.

If your computer is using a private IP address behind a broadband device that performs NAT, your exposure to Internet based attacks, particularly self-propagating malware, is greatly reduced. If you have a cable modem (or other non-routing modem), the option to use NAT is usually not available.

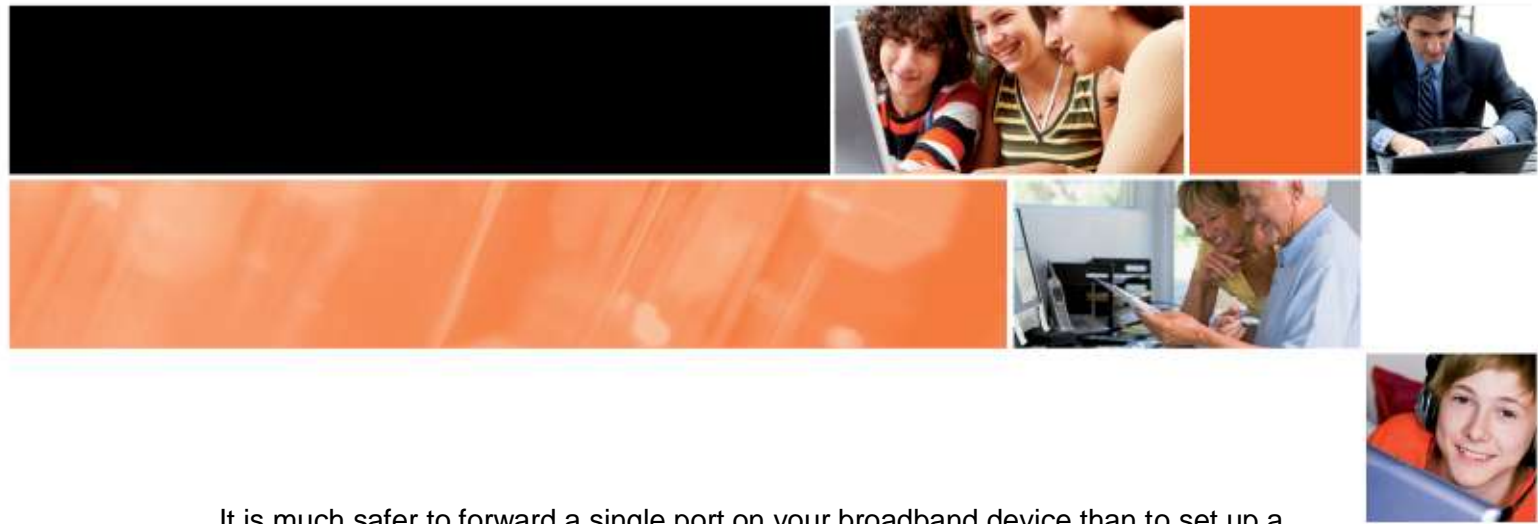
Responding to pings

A “ping” is a network test sent by one system to another to determine if that system and the network that connects them is working properly. Some broadband devices give you the option to respond to pings or not. It is recommended that you set your modem router to not respond to pings, as it is not essential in order to have a functioning Internet connection. By responding to pings you indicate there is a system at that IP address and this may be cause for further attacks to be directed at your computers.

Port Forwarding

In order for computers to keep track of connections, when they have more than one, they use ports. Ports are numbers that go with an IP address to make up the endpoints in a connection of two systems.

Port forwarding (also known as port mapping) occurs when the modem router transfers all traffic for a single port on your broadband modem router device to a port on a computer inside your home network. Many games require port forwarding in order to play multiple player versions via the Internet.



It is much safer to forward a single port on your broadband device than to set up a “DMZ Server” (see below). The reason is that you are only allowing traffic to a single port on the destination computer, rather than traffic to all ports to that computer. If you don’t need port forwarding (or are unsure) then leave this feature disabled.

DMZ Server

Often broadband devices will allow configuration of a “DMZ Server”. In computing, a DMZ system refers to computers which are accessible from the Internet. Setting a DMZ server in your broadband device will mean that anyone on the internet will be able to connect to any service on that computer. As a general rule, ordinary home users should have no need to enable this feature and it is recommended that it be disabled. If connections to a single port are required, then it is better that port forwarding is used (see above).

Small to medium businesses that operate a web site and mail servers, however, would use the “DMZ Server” feature.

Disable unneeded services


Generally, if your modem/router provides a feature or service that you do not need to enable, don’t enable it.

UPnP

Universal Plug and Play is a method to simplify the set up and configuration of network devices. It can also be used to perform things like automatically forwarding ports (see “Port Forwarding”, above). However, there are some security problems with UPnP and unless you have devices or software that need it, it is recommended that you turn it off.

Content filtering

Many broadband devices have a content filtering feature. This allows certain URLs (web addresses) to be blocked. This is useful if you wish to limit which web sites people using your Internet connection can browse to. However, it does not provide any more security protection beyond this. Typically, this feature is used by parents to block access to particular offensive web sites by their children. Rather than using this setting/feature, a more useful way to filter Internet access is to buy content



filtering software from a reputable computer store. This software comes with updates and other methods to ensure that a range of 'undesirable' content can be blocked in a more reliable manner.

Software (firmware) upgrades

Similar to other computers, many broadband devices have an operating system, called "firmware" or a "software image". It is important that you keep up to date with upgrades to broadband device firmware because, like any software, older versions may contain software vulnerabilities.

You can obtain firmware and the instructions on how to install it from the device manufacturer's web site, commonly in the "support" section. It is useful to keep a copy of your two most recent firmware images – in the event of problems with new firmware, you may need to re-install your old firmware.

Modem/router manufacturers

For more detailed instructions to securely set up your broadband modem/router device, look for the user manual/guide for your particular model in the support area of the manufacturer's web site:

Belkin	http://www.belkin.com.au
Billion	http://www.billion.com
D-Link	http://www.dlink.com.au
Linksys	http://www.linksys.com
Motorola	http://www.motorola.com
Netcomm	http://www.netcomm.com.au
Netgear	http://www.netgear.com.au

Report prepared June 2009