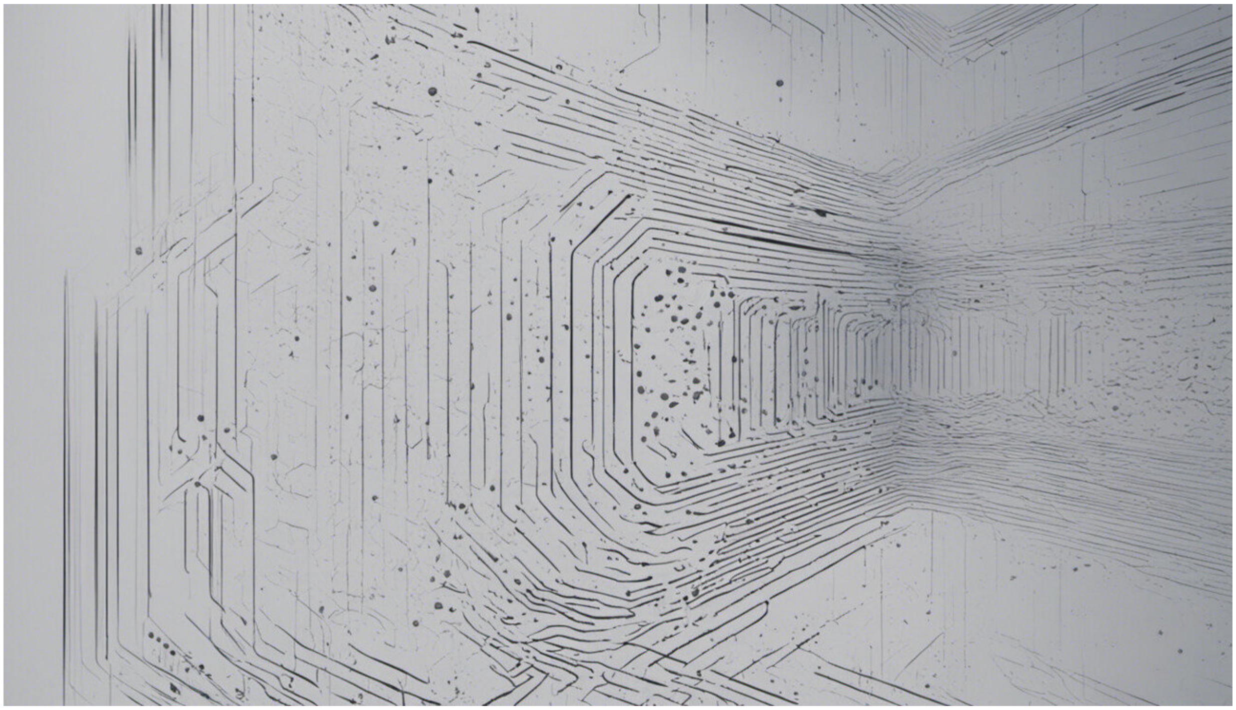
PHYS.ORG

How internet routers work, and why you should keep them secure

July 3 2017, by Nicholas Patterson



Credit: AI-generated image (disclaimer)

Most of us would be bereft without Wi-Fi but give a little thought to the technology that beams us the internet.

The device we pay so little attention to is called a router. Its main role is to connect networks and send and receive data from an internet provider.

But many routers aren't particularly secure.

The importance of understanding how routers work and how to protect them from malicious attacks was highlighted by WikiLeaks's recent revelations about the existence of an alleged CIA hacking tool, code named "CherryBlossom". This tool can apparently hack routers, allowing the perpetrator to monitor traffic and perform software exploits on victims.

The average person is unlikely to be targeted by this level of attack. But if you're going to have a router at home, it's important to understand exactly how it works.

How does a router work?

A router is like a post office for the internet: it acts as a dispatcher, choosing the fastest and most effective delivery paths.

Let's assume you have a smartphone at home that's connected to your router and through that, the internet. You're keen to find a song to listen to. Here's how it works:

Your smartphone takes your song request, and converts it into a radio signal using the specification (it's called a 802.11 Protocol) that controls how your Wi-Fi works
This information is sent to the router, including your smartphone's Internet Protocol address (essentially, its internet street address) and the track you requested
This is where the Domain Name Server (DNS) comes into play. The main purpose of this platform is to take a text based address (let's say, www.spotify.com) and convert it into a numeric Internet Protocol address

The router will then send off the request information to your internet provider, through their proxy and then on to Spotify.com
Along this journey from your home to your internet provider to Spotify.com, your request information will "hop" along different routers. Each router will look at where the the requested information has to reach and determine the fastest pathway
After going through a range of routers, an agreed connection between your home internet, your iPhone and Spotify will be established. As you can see in the image below, I have used a trace route service from Australian-based company Telstra to Spotify showing 16 routers along the journey
Then data will begin to travel between the two devices and you'll hear the requested song playing through your smartphone.

Explaining the back of your router

Even if you now understand how your router works, the machine itself is covered in mysterious ports and jargon. Here are some to look out for:

Ethernet ports: these exist to enable hard wired networking to the router itself in cases where a Wi-Fi connection is not possible.

SSID: this refers to "Service Set Identifier", and is an alphanumeric set of characters that act as your Wi-Fi network's identifier.

Telephone/internet port: this port allows your router to gain a hard wired (RJ-45) connection to the internet, usually through telephone lines.

WPS: this stands for "Wi-Fi Protected Setup". It allows users faster and easier access to Wi-Fi, because they will not have to enter in the passkey once pushed.

LAN: a "Local Area Network" refers to a grouping of computers and devices being networked together, typically with cables and routers in a singular space – often a university, small company or even just at home.

WAN: when we take a series of geographically distributed LANs and connect them together with routers, this is what we call a "Wide Area Network". This is useful for larger companies that want to connect all their office locations together.

WLAN: closely related to a LAN, "Wireless Local Area Networks" are LANs whereby users who are on mobile devices can connect through a Wi-Fi connection, allowing complete mobility and thus reducing the need for any cables.

Cyber safety with routers

It's important to protect your router and Wi-Fi network from being compromised.

You should:

- Change your router's administrator password and make it strong
- change the identifying SSID name so it doesn't give away any details about the model of your router or who owns it
- ensure encryption is turned on in the router settings: this will ensure the traffic travelling over your network is unreadable
- change the passkey you enter in when connecting to Wi-Fi
- ensure your router's firmware – the software that's hard coded into your router – is up to date.

Routers ensure your home and internet service provider can stay connected. Look after your router, and it will (hopefully) look after you.

This article was originally published on The Conversation. Read the original article. This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How internet routers work, and why you should keep them secure (2017, July 3) retrieved 24 April 2024 from https://phys.org/news/2017-07-internet-routers.html