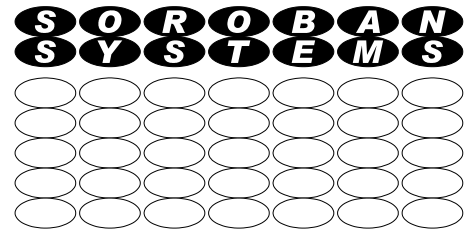# Soroban Support Guide

Internet Slow - Why?

Some steps to take before changing ISP

There are a number of factors that can make Internet access slow. It could be your Internet Service Provider but in ALL cases that the author has investigated it is local factors that cause this behaviour and not the Internet Service Provider.

This document attempts to explain some relatively simple diagnostic steps that can/should be taken first before considering changing Internet Service Providers.

Some diagnostic tools are mentioned and are either already installed on your PC or are free to download.

The author doesn't have access to Apple devices but if suggestions are received for equivalent products then these can be added to this comment.

Original Author:	**John Steele**
Revised by:	**John Steele**
Version:	**1.0**
Date:	**7 Oct 2025**

Copyright Notice

Revisions

Version	Date	Changed by	Summary of change
1.0	7 Oct 2025	John Steele	First released version

Table of Contents

Table of Figures

Index of Tables

1   OVERVIEW

1.1   Objective

If you are experiencing regular unacceptably poor performance of your Broadband Internet connection it is only natural to blame your Internet Service Provider (ISP). There are however factors, outside your ISP's control that can affect the performance of your Internet connection and you should investigate whether this is the actual cause of your issue BEFORE leaping to the conclusion that your ISP is to blame and switching providers.

This guide describes how very common local neighbourhood factors can severely impact your Internet performance and explains why changing Internet service providers probably will not help.

> **The author has had many years of experience in investigating such performance issues and has NEVER concluded that changing Internet Service Providers would help.**

It is important therefore to understand the real cause for poor performance and this document explains how this can occur, and how to identify the real cause of poor performance using simple free diagnostic tools, before taking the more disruptive step of changing ISP as this, quite probably, will make no difference.

This document identifies some simple, and proven, steps that you can take to identify the real cause of poor throughput and steps that you can take to improve the situation.

1.2   Possible causes of slow Internet

Your broadband speed is poor and possibly intermittent. Sometimes it is fast but sometimes it is very slow. There are several potential causes of slow internet speed or even breaks of service. While this MIGHT be caused by your Internet Service Provider, there are often other reasons, and changing providers will then NOT improve the situation.

Here are some typical symptoms that may cause you to investigate poor Internet performance:

1. The most easy to spot is excessive buffering on streaming video
2. A web page may not load correctly
3. A web page may be slow to load
4. Etc.

There can be a number of reasons why this is happening. This might be caused by:

External factors e.g.:

1. Overloading of the server you are accessing over the Internet
   a) There are just too many users trying t access it,
   b) There is little you can do in this case – just be patient
      i   Changing you ISP will NOT improve this situation
2. Overloading of the link between your location and the local Internet Service Provider connection to the wider Internet
   a) This may be caused by your Internet Service Provider having insufficient capacity on one of its links but is probably the **least likely** to be the cause of slow service but is most often suspected

3. Overloading of the intermediate network between your ISP node and the target host node.
   a) This is almost impossible and would affect all ISPs equally

Internal or local factors:

1. Too many devices on your home network so that your link to your ISP is overloaded
   a) **This is very unlikely to be the case**
2. Congestion on the WiFi network which is described in some detail later.
   a) **This is frequently the cause of poor performance and an explanation of how it can occur is described below**
   b) **This may be on your own network or interference from neighbouring networks**

<div style="border: 1px solid red; color: red;">

Local congestion on your Wi-Fi network where the available bandwidth is shared with your neighbours is probably the most common cause of performance issues and the reason is explained below.

</div>

1.3 How Wi-Fi Works and local congestion

When you are using Wi-Fi your data is being transmitted via radio waves which are not constrained to cables unlike a wired network. This means that your data is broadcast to any device within range of the transmitter which is typically a computer or other device such as a TV on your network. Although the signal strength is deliberately low this can reach several hundred metres from your property.

This is never a privacy issue as the data is encrypted using a network key that is private to you. Your data also contains a source and destination address so that only your devices process your data.

When one device, e.g. your computer, wishes to communicate with another device e.g. your router it has to first check that no other devices are actually transmitting. If they are it has to wait until all traffic stops. If two devices are waiting to send data and they start simultaneously they recognise the clash, stop transmitting, and wait a short randomised time before trying again. One should win and succeed in transmitting its data.

This is a simple mechanism and the data transmission speeds are such that it works well when there are only a few devices communicating.

BUT the wireless signals are not constrained to your property. ALL devices within range have to obey the same rules. Only one can transmit at any one time over the same radio channel. **Your near neighbours wireless systems within a locality are competing with yoour data signals for the same bandwidth.**

<div style="border: 1px solid red; color: red;">

If you have several neighbours in range this can seriously degrade the data rates you can get between your computer and your router.

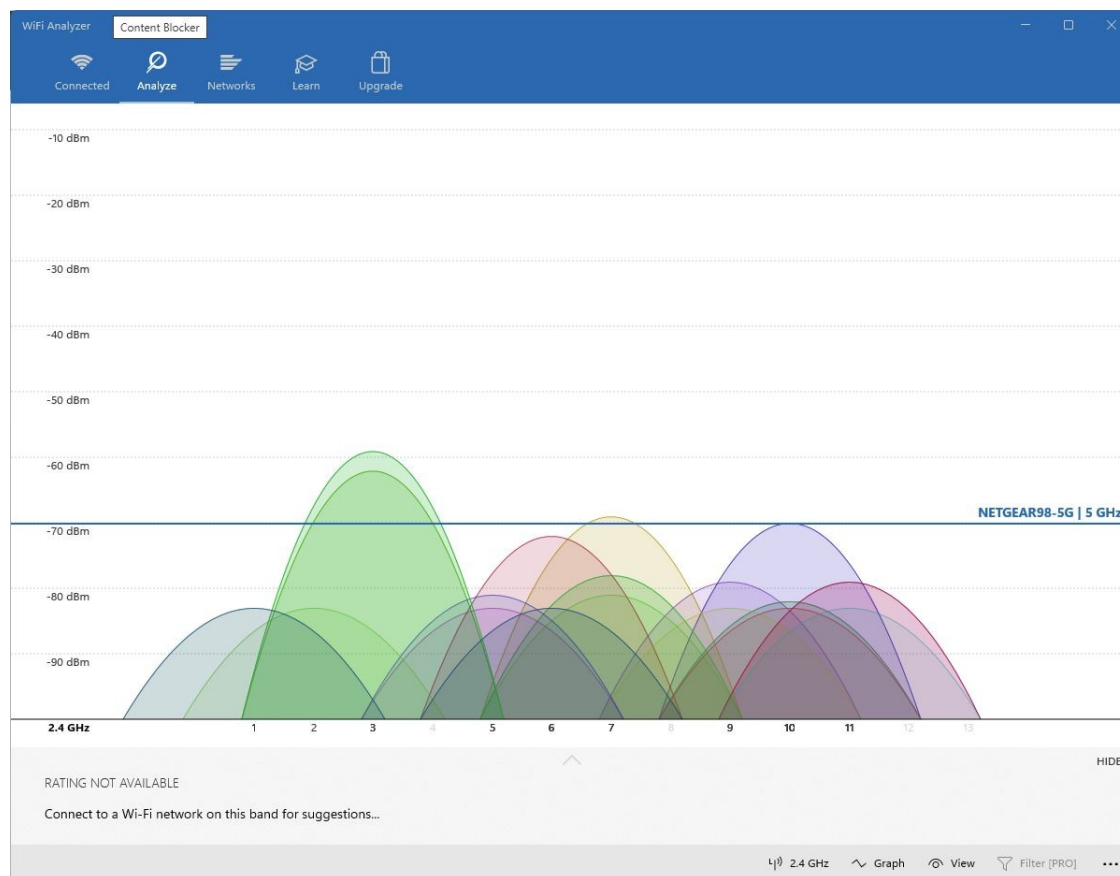**See Figure 1 Multiple Neighbors on 2.4 GHz band below for a real life example.**

</div>

Figure 1: Multiple Neighbors on 2.4 GHz band

Figure 1 shows a real world case from an urban environment and is typical of what frequently occurs. This image comes from a free Windows tool, WiFi Analyzer, and more details of how to install and use it can be found in 4.1.2 below. Alternative tools are available for Android phones (see section 4.1.2 below and probably for Apple computers and iPhones.

Note: Links to equivalent programs for Apple MAC computers and iPhones would be appreciated and would be incorporated in future updates to this document.

The congestion is obvious!

Every overlapping WiFi neighbouring channel is consuming bandwidth that is depriving YOU of bandwidth = download speed from your connection to your ISP.

Sometimes the mutual interference can be mitigated, to some extent, by choosing a different channel for your wireless network. On the 2.4 GHz band, which is the original Wi-Fi band and still tends be the default used, the Wi-Fi standards state there are 13 available channels (11 in the USA) but in practice it is not that simple. For technical reasons only channels 1, 6, an 11 are recommended in practice to ensure no cross channel interference but this is often ignored as in this case.

The author has frequently seen 10 networks sharing the 2.4 GHz band and in one extreme case over 30 sharing the same band. In these cases the data rates observed by a user on those networks was abysmal and very variable.

Recent updates to the Wi-Fi standards have added two new Wi-Fi ranges that can help. There has been a 5 GHz range of channels for some years now and, very recently, a 6 GHz range has been introduced but many devices are not yet able to use this range. The router

that support these speeds will also still support the older 2.4 GHz band and this may be needed for some non computer devices such as TVs, PVRs, CCTV, central heating controllers etc.

> **All that was needed in almost every case of poor performance was to simply change the Wi-Fi channel being used by a simple configuration change on the router.**
>
> **Choosing a 5 Ghz band, if available, is a better option if it can be accessed in every room. Many modern router provide a "mesh" option to extend the range.**
>
> **Changing the Internet Provider would NEVER have made ANY difference if the same WiFi channel/band were to be used.**
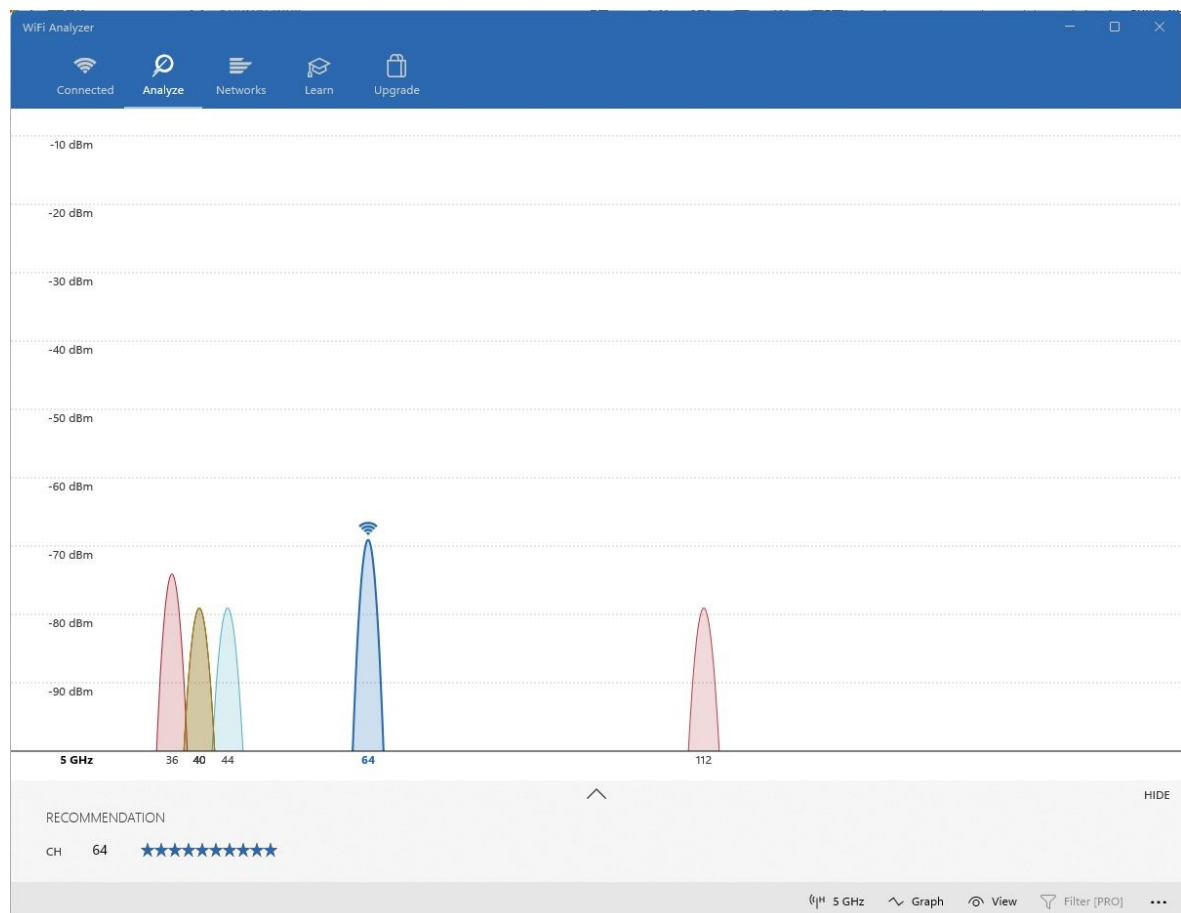
Figure 2: Multiple Neighbors on 5 GHz band

Figure 2 above shows the 5 GHz band at the same location as Figure 1.There is no sharing at all of each of the channels and hence no degradation in performance.

All modern routers support 5 GHz where there are many more channels available and some even support the new 6 GHz band that is besoming available. These new channels support significantly higher data rates that the older 2.4 GHz band. The other characteristic that can be both a limitation and a benefit is that their range is lower they are less likely to propagate as far outside your home and thus less likely to suffer degradation from neighbour traffic sharing.

They can also be built into a "mesh" network where nodes can be placed throughout the house but all participate in a single network.

2 DIAGNOSTIC STEPS YOU CAN TAKE

2.1 Overview

If you are experiencing issues with your home network you need to understand what is causing these issues. It may be you need a new Internet Service Provider but, if the problem is due to issues with your home network or Wi-Fi channel sharing with your neighbours as described above, you may be wasting your time and money when a slight adjustment to your current setup might be all that is needed.

What you SHOULD do is to understand WHY you have a problem and then consider what options you have.

There are some free tools available that can analyse your current network and help you, or any "expert" you invite to assist you, to come up with a cost effective solution.

> **Changing you provider is not necessarily the right solution. In fact the author has NEVER needed to recommend that step for performance issues.**
>
> **A simple configuration change was all that was needed.**

There are some basic tests you can do on your local network to test that there is no obvious issue that are described later – see section 4 below.

2.2 Some definitions and explanations

2.2.1 IP Address notation – IP version 4

The following explanation uses the conventional way of representing the Internet Protocol, usually abbreviated to IP, addresses. For those not familiar with the notation here is a brief explanation.

There are actually two possible standards for IP addresses. The older address standard was sufficient for many years but now so many devices are accessible the Internet a new, much larger, range of addresses are allowed.

The most widely used standard is still the original standard called IP version 4. Each IP address consists of a binary number (you count 0, 1, 10, 11, 100, 101, 110, 111 etc. which in decimal notion are 0, 1, 2, 3, 4, 5 ,6, 7. Each of these binary digits is conventionally called a "bit".

Internet or IP version 4 addresses are 32 bits long. For convenience they are usually grouped into four sets of 8 "bits" called Octets. Each of these is written as a decimal number which can range from binary "000" = decimal 0 to binary "111" = decimal 255.

An IP version 4 address theretofore could be something like 192.168.4.3 where each of the group of 8 bits, octets, are separated by dots. It is called "dotted decimal" This is much easier to read, and document, than binary!

2.2.2 Public versus Private IP addresses

The range of IP addresses was thought to be vast when computers started to talk to each other. However ss the use of personal computers arrived and the Internet stretched to people's homes the world was running out of space so a concept of Private Address space was born.

Three specific address ranges were identified a Private Address Space. The concept was that a device sat on the boundary between a local area network e.g. a company or a home, which had a SINGLE public IP address. Rather than each device connecting directly to the Internet the boundary would have a Router between the local network and the rest of the world. The router would take requests from the local network using the internal private address of the device and forward the packet using a public address. When the reply ws received from the remote server it would modify the data packet received and frward t h the local device.

This is called Network Address Translation and it is what your router is doing whenever it is asked to access a service over the Internet.

There are three Private address ranges defined for IP v4. These addressees should never be used on the public Internet. These are:

1. 192.168.0.0 to 192.168.255.255
    a) Most commonly used for small local networks
2. 172.16.0.0 to 172.31.255.255
    a) Used by Swish for its private wide are communication for example
3. 10.0.0.0 to 10.255.255.255
    a) Used by larger networks

2.2.3 IP version 6

This is a newer standard as the worlds is running out of Public IP addresses. This has a vastly greater address space and it would be possible for each device to directly connect to any server and for it to respond.

> *Your router, by performing the address translation at the boundary between your network and the outside world can more easily provide a filter for protecting a malicious outside device attacking the internal network so it provides a very imported security barrier against an external attack so it s unlikely that Network Address Translation will stop happening when the public network moves to IPv6.*

2.2.4 Some more technical terms used in this document

There are some technical terms used in this description which are listed below

IP address	IP stands for Internet Protocol and is used throughout this document. There actually two standards for the address.
	The original (IP version 4) is usually written as four "octets" separated by dull stops. An octet is 8 binary digits and is normally written as a decimal number in the range of 0 to 255
	IP version 6 is rarely used in local networks but depending on your ISP may be used on the ISP connection to your router.
Local IP address	This is a number which is the address of a device on your local network. The most common that is represented as four numbers in the range of 0 to 255 separated by full stops e.g. 192.168.23.4.
	This is called an Internet Protocol address (IP for short) and each of the numbers can range from 0 to 255. These are called Octets. Most home networks use 192.168 as the first two numbers. Each device on your network typically has the same Third octet and

	the final on is unique for each device. Numbers 0 and 255 have special meanings. **The notation above is technically for an older standard called IP version 4 but is still generally still used for local networks**
External IP address	This is the Unique number used to identify your own location. Depending on the ISP this address can be IP V4 i.e. 4 Octets. **There is a newer standard called IP version 6 which has a different notation and a far greater range of IP addresses, 8 octets, and is sometimes used for external IP address This is beyond the scope of this document**

2.3   Your local network

Your local network consists of a Router, that provides the connection to the outside world, and a number of local devices which may include computers, tablets, phones, TVs etc.

Each device has a locally unique IP address which is used to communicate with the local router. The local network address space is purely local and has no relevance outside the local environment. This IP address is actually given to each device by the your router.

Your router has a single IP address that is a public address that makes your home network uniquely accessible from anywhere in the world so that responses can be sent back to you. It also has a fixed IP address on your local network and there is a local method for your router to issue a local IP address on your local network to all connected devices.

If one of your devices needs to communicate with another local device it simply uses the IP address of that device on the local network.

When one of your devices wants to communicate with an external site it sends the request to your local router that replaces its internal private address with its own worldwide unique public IP address. When the response is received it recognises that it is a reply and sends it to the local device that sent out the request.

Please note that this is a very much simplified description for the purpose of this document!

3 HOW DO DEVICES COMMUNICATE

3.1 Overview

In general a device on a local network will listen to the traffic on the network and, if it is quiet, will simply send its data to an IP address on its local network. If two devices try to send at the same time than the data is "scrambled" and they detect this happening and both back off for a random time and try again. If the network is quite then these collisions are rare and performance is not badly affected.

If the local network is very busy then traffic from any device is obviously delayed.

3.2 Wi-Fi considerations

On wired networks, which are still sometimes used, this is simple to understand. There can be no outside interference.

As described above a Wi-Fi network uses wireless signals to communicate between networked devices. In most cases this is device is your router although there are exceptions e.g. a printer or a shared storage device.

On a Wi-Fi network however there is an added complexity as the wireless signal can be transmitted outside your property and other people's Wi-Fi signals can be seen in yours. This now means that data transmitted between your neighbour's computers and their router can also collide with your own data traffic. On wireless networks there are multiple "channels" available but if your network is using the same channel as your neighbour there can be "collisions". In practice, on the initial Wi-Fi standards there were in theory 13 (in Europe, 11 in the USA) channels available but the data spreads deliberately over several channels so, in practice, only three can be actually used, 1,6,11, without interference with other traffic.

This means that mutual interference between neighbours system is inevitable if they are configured to use the same, or adjacent, channel and this can seriously degrade the throughput.

The standard older Wi-Fi band operates at 2.4 GHz. This can be usable over a range of several hundred metres. Signals on this band can have problems with the signals being absorbed or blocked by some building materials and is also absorbed by water so damp can be a problem. Microwave ovens also use 2.4 GHz to heat food but these ovens are well shielded and probably do not interfere much with Wi-Fi unless they are faulty.

More recently two additional Wi-Fi bands have been added. 5 GHz has been available for several years. It has far more channels available and it does not propagate as far as 2.4 GHz so neighbour interference is significantly lower but it may not propagate as well through your property and older device do not support it. There is no reason why you cannot use both bands. 6 GHz is also a new option and the author has not yet had an opportunity to evaluate it.

There are free tools available to see what nearby networks exist, and how strong they are. It is recommended to use one of these if you have any suspicion that there is any chance of neighbour networks competing with yours for bandwidth. See section 4.1.2 below.

Changing Wi-Fi channels, or switching to a different band, has successfully cured ALL performance issues that the author has investigated over many years. If this simple

change to your router configuration solves these collisions there is no need to change Internet Service providers.

© John Steele, Soroban Systems

4   TESTING YOUR NETWORK

4.1   Introduction

There are simple tools that can be used to test the local and remote connectivity and can also be used to test performance to remote sites. The main tool is TraceRoute which gives detail information about how data passes from your computer to its destination.

4.1.1   TraceRoute

TraceRoute is available on most platforms. The actual program name can vary between platforms however. The author is a Windows user and the program name is "tracert" If anyone wants to provide the equivalent information for other platforms this can be added to future versions of this document.

This how to run the commend on a Windows 11 system.

Click the search on the toolbar and enter "command". Select command prompt, you do not need to be an administrator and it should open a command Prompt window. - something like this:

C:\Users\john>

Enter a command like the one below – the "soroban.co.uk can be replaced with any other known web site.

C:\Users\john>tracert soroban.co.uk

Report says: Tracing route to ******** [109.***.**.**] over a maximum of 30 hops:

Asterisks hide sensitive information, it will show the computer name and its IP address.

Detailed results are shown as a table - Table 1 Sample Trace Route results below.

No.	Times in ms			Address	
	1st	2nd	3rd		
1	1	2	2	SwishFibre**** [192.168.1.1]	
2	5	5	4	172.22.4.3	
3	4	3	3	172.20.0.132	
4	5	3	7	172.20.0.101	
5	5	4	4	172.20.0.60	Swish/Cuckoo private addresses
6	5	4	4	172.20.0.87	
7	4	5	4	172.20.0.86	
8	7	4	4	172.20.0.57	
9	6	5	5	linx.bb-c.the.lon.gb.oneandone.net [195.66.224.98]	
10	11	10	10	lo-0.rc-b.ce6.wtr.gb.net.ionos.com [212.227.117.201]	
11	10	9	9	212.227.121.15	

12				Request timed out.
13				Request timed out.
14	10	9	9	Server.******* [109.228.37.73] = my website

Table 1: Sample Trace Route results

> *In analysing these results it should be noted that some IP address ranges are "private". They are NOT unique worldwide and may be freely used within any network. In Table 1 there is an example of such usage where there are several "hops" from one Swish/Cuckoo owned node to another.*
>
> *The three private ranges are 10.x.x.x, 172.16.x.x to 172.31.x.x and 192.168.x.x where x= any value between 0 and 255. All other addresses should be worldwide unique. 192.168.x.x addresses are typically used in your local network but sometimes one of the other ranges are used.*

The time is measured for each "hop" three times and shows the total elapsed time to each node that the data passes through to its ultimate destination and for its response to be returned to the sender. In this case, but not necessarily for other Internet Providers, it passes through several nodes within the Swish network. Note that Swish is now owned by Cuckoo.

If any times are larger than a few milliseconds it points to congestion within the network.

> *If there is no large delay passing through the ISP network then no advantage will be gained by switching provider.*

> If there is a long delay to the first external node (line 2 in the table) and in particular if the three readings are wildly different this would suggest a problem on your LOCAL network, including issues with congestion on your Wi-Fi, as described elsewhere in this document.
>
> **Changing Internet providers in this case will give no direct benefit.**
>
> **If there is a long, and especially if it is variable, delay through your ISP nodes (identified in Table 1 above as Swish private addresses) then there might be a benefit in considering an alternative Internet Service Provider or at least asking for an explanation.**
>
> **If these times are low and consistent then there will be no benefit in changing Internet Provider.**

It is worth repeating this test at different times of the day. If the results vary and in particular the first few nodes show longer and variable times than then this will suggest a Wi-Fi issue.

4.1.2 Testing WiFI performance/congestion

In addition to the Trace Route test is is also worth running another free program to examine the Wi-Fi signals that are seen from your location.

> **Historically this has almost always been the cause of poor and erratic broadband performance**

The best tool I have found for this purpose for Windows systems is a free program called WiFi-Analyzer. The website link is https://matthafner.com/wifi-analyzer. Screen shots from this program have ben shown in Figure 1 and Figure 2 above.

There is a similar program for Android devices that can be found here https://play.google.com/store/apps/details?id=com.vrem.wifianalyzer

If anyone can recommend equivalent programs for Apple devices I will be pleased to add links to them here

I am not reproducing a full guide as to how to use the program here. It is well documented on the web site.

The program wifi-analyzer can show:

1. What WiFi channels are available on your computer on each available Wi-Fi band and the strength of each signal
    a) Your own channel should be shown and will hopefully be the strongest although I have seen cases where it was actually smaller
2. The signal strength is shown in decibels and will identified as dBm . Note that:
    a) The signals should ALWAYS be show as a NEGATIVE number. -50dBm is stronger than -60dBm
    b) Any signal should NEVER be stronger than -50 dBm otherwise it is contravening it approval by the standards bodies.
    c) Usable signals should never be smaller than -80dm and for reliable operation -70dBm would be preferred as the lower limit
    d) You can select 2.4 GHz or 5 GHz and, if available, 6 GHz if your devices support it.
    e) You can switch between a graphical plot against time which is useful to survey signal strength throughout a property or a simple channel view

The important thing to check is that all other neighbour's networks are on different channels otherwise they will interfere with your own network throughput. This is by far the most likely cause of poor throughput from the author's own experience.

The 2.4 GHz band has 13 numbered channels but only channels 1, 6 and 11 are recommended but this advice is often ignored by default router configuration. The frequencies (channels) on wither side are actually used for data.

5   POSSIBLE REMEDIAL OPTIONS

If you have run the tests and suspect that Wi-Fi congestion is the cause of your poor performance you can try the following steps to improve your situation. How you do this will depend on the make and model of your router so detailed instructions are unfortunately not possible. You will need to log in to the administrator options on your router. Google will help in most cases to give details.

Changing to a different ISP will NOT solve your problem!

Some possible causes of weird results throughout your property are listed below. A walk test with a laptop or using a mobile phone can help here. Some rooms may have good Wi-Fi signals and others much weaker of even no signal. Here are some of the causes you might find – it is not an exhaustive list!

1. Construction of the property:
   a) Some internal walls in older properties may contain materials that absorb radio waves.
      i   A common filler of breeze blocks in 1920s and 1930s (and perhaps others) contain a high carbon content that absorbs radio signals – waste from coal fired power stations. The author has experienced this in several properties using the 2.4 GHz band.
      ii No similar surveys have been done since 5 Ghz became available
   b) Some walls may be dry-lined with foil backed plasterboard which blocks the Wi-Fi signals
   c) If Wi-Fi signals need to cross a space where walls can become damp then the 2.4 Ghz band is liable to be attenuated. It is the same band that microwave ovens use and water absorbs these signals converting them to heat.

Here is a summary of your options if the above issues are not happening:

1. Change your router to use a different channel on the same band if there is one that is not so busy
   a) You should not need to change your device configuration on any device to do that!
   b) New networks can however appear in you neighbourhood which may need you to change channels again
2. If your router is using 2.4 GHz change it to use 5 GHz or add 5 GHz as an option
   a) You may not need to change your device configuration to do this but if you need to use BOTH 2.4 GHz and 5Gz (or even 6 GHz) so that legacy devices can continue to work you may need to select the appropriate band on the device.
   b) Caution: 5 GHz may not travel as far through larger, and particularly multi-storey properties compared with 2.4 Ghz. If this is the case a more elaborate solution may be required.
      i   Technically a Mesh solution could be used which requires an appropriate router and additional nodes. This creates a number of very local Wi--Fi networks which then communicate via Wi-Fi to the router.
      ii Advice may be needed from a network specialist to select suitable equipment.
3. In some cases the network could be expanded by using Ethernet over the mains wiring which the author has used very successfully on several occasions.

a) This can create a new Wi-Fi network on a different floor passing the data via the property mains wiring.
b) Success does depend on exactly how the mains is wired in the property however but can be a very effective solution.
    i   Ideally it would be better to borrow a pair of devices to verify that your mains wiring is suitable.