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 almost all cases that the author has investigated it is local factors that cause this behaviour.

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 all 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: Draft 4
Date: 3 Oct 2025

Copyright Notice

Revisions

Version	Date	Changed by	Summary of change
Draft 4	3 Oct 2025	John Steele	Added private vs public routing explanation plus 1Pv4 and IP6v
Draft 3	3 Oct 2025	John Steele	Clarification of private IP address ranges
Draft	2 Oct2025	John Steele	Some typos corrected and minor text changes
Draft	29 Sep 2025	John Steele	First version -released for review and comment

Table of Contents

Table of Figures

Index of Tables

1 OVERVIEW

1.1 Objective

This document is intended to assist in identifying causes of poor Internet performance.

It is easy to blame your Internet Service Provider (ISP) for poor response times but there may be other causes and changing providers may not, **or even probably not**, be the answer!

This document identifies some steps that you can take to identify the real cause and steps that you can take to improves the situation.

1.2 Possible causes of slow Internet

Your find 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. This MAY be caused by your Internet Service provider, but often it is not, and changing providers will not necessarily improve the situation.

Here are some possible causes of poor Internet performance which can lead to a number of visible symptoms:

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 services e.g.:

1. Overloading of the server you are accessing over the Internet
   a) There are just too many users trying t access it, There is little you can do in this case – just be patient
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

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 tobe 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

Local congestion on your WiFi network is probably the most common cause of performance issues and is explained below.

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 like 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. It is also contains a source and destination address so that your devices only 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 for the same bandwidth.

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

This 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 tends be the default used, the standards state there are 13 available channels (11 in the USA) but life is not that simple. For technical reasons only channels 1, 6, an 11 are available in practice.

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

All that was needed in every case was to simply change the Wi-Fi channel being used by a simple configuration change n the router.

Changing the Internet Provider would NOT have made ANY difference if the same WiFi channel were to be used.

Recent changes 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 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 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 modern routers support 5 GHz where there are many more channels available and some even the new 6 GHz band that is beoming available. These new channels support significantly higher data rates that the older 24 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 this less likely to suffer 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 what limitations you know WHY you have a problem and fully consider what options you have. There are some free tools available that can analyse you 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.

There are some basic tests you can do on your local network to test that there is no obvious issues.

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”.

Binary numbers are inconvenient to for humans to follow so we group three “bits” together into an “octet” so the have 000 = 0, 001=1, 010=2, 011=3, 100=4, 101=5, 110=6 and 111=7. This notation is called Octal.

IP v4 address are 32 bits and they are usually written as 192.168.7.5 where each of the group of 8 bits, called octets is separated by commas. This is mush easier to read and document.

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. As 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.

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.

If one of your devices needs to communicate with another local device it simply uses the IP address 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 your internal private address with its own 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!

All devices on your local network have a unique private IP address on the local network. This obviously needs to be unique but in most cases local device have no need to communicate with each other. Typically when a device is switched on it will ask the router for an IP address and will not necessarily be given the same one. This again is a simplified description.

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 from any device is obviously reduced.

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.

This means that mutual interference between neighbours system is inevitable if they are configured to use the same 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. It can have problems with signals being absorbed or blocked by some building materials and is 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 WiFi bands have been added. 5 GHz has been available for several years. 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 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 this happening. 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.

4 TEST CONNECTIVITY

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 program name can vary between platforms however. The author is a Windows user. 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,

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	Swish/Cuckoo private addresses
3	4	3	3	172.20.0.132	
4	5	3	7	172.20.0.101	
5	5	4	4	172.20.0.60	
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. In this case, but not necessarily always, 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 Wifi, 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 provider or at least asking for an explanation.

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

4.1.2 Testing WiFI health

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 is a free program called WiFi-Analyzer. The website link is https://matthafner.com/wifi-analyzer. The website contains the download for Windows computers.

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 them here

I am not reproducing a full guide as to how to use the program here.

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 actually usable. The frequencies (channels) on wither side are actually used for data.

