Wi-Fi Troubleshooting: Slow Speeds

White Paper

Table of Contents

Introduction 3
Measure your Throughput 3
Identify the Root Cause 7
Capacity 8
Co-Channel Interference 9
Adjacent Channel Interference 10
Non-Wi-Fi Interference 12
Conclusion 13

Wi-Fi Troubleshooting: Slow Speeds

Wi-Fi is an essential part of work life; slow speeds are frustrating and costly.

INTRODUCTION

At one time or another we've all experienced problems with slow Wi-Fi speeds. Maybe you are at the office and noticed that during certain times of the day your Wi-Fi network connection is slower than normal (video conferences lag, the quality of voice calls diminishes), or maybe you are a business traveler and ended up having to stay in a hotel where the Wi-Fi network speed is so slow you can't even check your emails. Regretfully, we've all experienced Wi-Fi problems like this. After all, slow network speeds are one of the most common Wi-Fi problems, so common in fact that some people just assume that's how Wi-Fi works. Still, does it have to be that way? Could it be possible that solving problems with slow Wi-Fi network speeds is not that difficult after all? Well, the reality is it isn't that difficult. With the right tools and a little knowledge, finding the root cause for most slow Wi-Fi network speed problems can be quick and simple.

This second entry in our series of Wi-Fi troubleshooting whitepapers will focus on showing you how to quickly and effectively troubleshoot "Slow Speeds". We will start by showing how to verify if you really have problems with slow Wi-Fi network speeds, or if the problem is somewhere else (wired Ethernet network, Internet Service Provider, or other). After that, we will show you how to identify the most common reasons for slow Wi-Fi network speeds and provide recommendations on how to speed up your network.

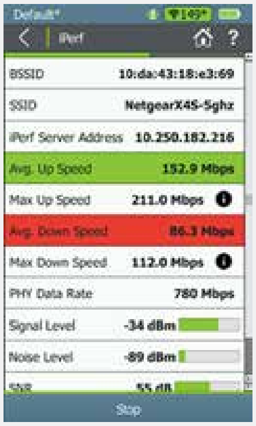
Let's get started!

MEASURE YOUR THROUGHPUT

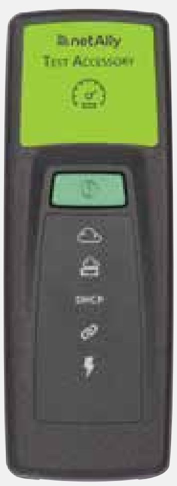
Before you can start troubleshooting problems with slow Wi-Fi network speeds, you need to verify if there really is a problem. You also need to verify if the problem is really on the Wi-Fi network. After all, many times the root cause of the problem is not Wi-Fi related. Sometimes slow Wi-Fi network speeds could be caused by problems on the Ethernet backhaul, client-device limitations, or even by problems with the service provided by your ISP.

The easiest way to verify if there really is a problem with slow speeds on the Wi-Fi network is to measure your network's actual upload and download speeds, or basically to measure the throughput. Throughput is defined as the actual amount of data that travels over a communication channel, or the maximum achievable data transfer speed. Throughput is usually measured in bits per second (bps) or megabits per second (Mbps).

Also, notice that throughput is not the same as bandwidth or data rates. Bandwidth is defined as being the maximum amount of data that can be delivered over a communication channel, not the actual amount of data, so it does not take into consideration data encoding, modulation, encryption, noise levels, interference, etc. Meanwhile, data rates are the speed at which data is transferred over a communications channel, which is not the same as the actual amount of data being transferred. Same as with the bandwidth, data rates don't take into consideration data encoding, modulation, encryption, noise levels, interference, etc. **Thus, the actual amount of data being transferred is always lower than the supported data rates.** Normally, the actual throughput is 60-70 percent of the supported Data Rates.



Example of iPerf performance test on a NetAlly AirCheck G2 and a NetAlly Test Accessory (iPerf based Test Point).



As for how to easily measure your Wi-Fi network's throughput:

1) Use a dedicated test tool that will allow you to measure your throughput against test points (end-point devices used to generate traffic) on your network while using the following process:

   a. Connect a test point to a port on the Ethernet switch where the AP's are connected to.

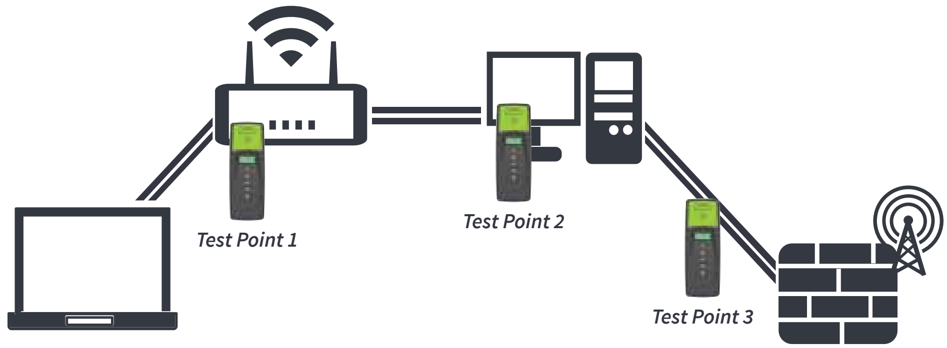
   b. Use your test tool to wirelessly connect to the same AP being used by the user's client device on which the slow speed problems were detected (an active connection to the Wi-Fi network is required to measure throughput).

   c. While actively connected to the AP run a throughput test against the test point you just installed.

      i. If a low throughput is measured, this tells you that you indeed have problems with slow Wi-Fi network speeds. So the next step is to identify the root cause of the problem by using the instructions provided on the sections further down in this whitepaper.

      ii. If no low throughput is measured, this tells you that the problem is not on the Wi-Fi network and that it is most likely on the wired side of the network, on the user's client device, or the service provided by your ISP.

If you suspect the problem is on the wired side of the network, you may want to install test points throughout the route being used to access the network resource the user is trying to use. This will allow you to run a throughput test against each test point and verify your speeds against different parts of the network until you find the problem area.



Example of Test Point deployment throughout the network

On the other hand, if you suspect the problem is the user's client device then you should verify if the device is able to support the amount of throughput being expected. This can be done by finding the following information:

1) SSID – Allows you to verify which network the Client device is connected to. Only available when the device is connected to a network, and used to verify that the Client device is connected to the right network.

2) AP Name – Allows you to verify to what AP the Client device is connecting to. Very useful when you want to make sure Client devices are connecting to the closest AP.

3) Connection Rate – Provides the connection data rate being used by the Client device. This helps you verify the maximum data rates supported by the Client device, and thus determine if the device has any data rate limitations that could prevent it from achieving a higher throughput.

4) 802.11 Type – Provides information on the types of 802.11 technologies supported by the Client device. This helps you verify if the client device can support the latest 802.11 technologies and thus higher data rates. Devices using an older version of the 802.11 technology may not be able to support the desired throughput.

5) Band – Provides information on the band being used by the client device. Allowing you to verify if the Client device can support both the 2.4 GHz and 5.0 GHz bands. Because of higher utilization on the 2.4GHz band, client devices limited to working on this band may not be able to achieve higher throughputs.

6) Channel – Provides information on the channel being used by the Client device. Some older client devices may not be able to support all the 5.0 GHz channels, which could limit them to use channels with high utilization, high noise levels, or interference that will lower their throughput.

Notice that not all the information mentioned above may be available on the client device. Still, most dedicated Wi-Fi network test tools will provide this information.

Example of Client information collected using NetAlly's EtherScope™ nXG

Last, if you suspect the problem may be caused by slow internet access, the best way to prove this is by using a web-based Speed Test that will allow you to measure the throughput of your internet service. If you identify that the problem is slow internet speeds, you should contact your ISP, so they can help troubleshoot the problem.

Note: *Web-based Speed Tests are a great way of verifying your Internet upload and download speeds, but they are not very useful when you try to verify the throughput of your network. The reason for this is that the test point being used by the Speed Test is not locally installed, thus the throughput test results will be affected by bandwidth limitations imposed by your ISP, and bandwidth limitations on the Speed Test servers.*

IDENTIFY THE ROOT CAUSE

After proving that the slow speeds reported by the users are caused by problems with the Wi-Fi network, it's time to identify the root cause of the problem. The most common reasons for Wi-Fi connection problems are:

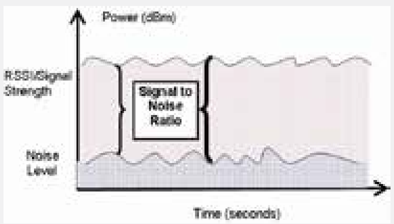
- Signal-to-Noise Ratio (SNR)
- Capacity
- Co-Channel Interference (CCI)
- Adjacent Channel Interference (ACI)
- Non-Wi-Fi Interference

SIGNAL-TO-NOISE RATIO

The quality and rate of a connection depends directly on the Signal-to-Noise Ratio (SNR) that a receiving device detects, which includes both AP's and clients. When an AP detects that the SNR of a client device connected to it diminishes, it automatically lowers the Data Rates being used to communicate with that client device, thus lowering the throughput.

This is the reason upload and download speeds are lower the farther the client device gets from the AP. As you move farther away from the AP, the signal strength will become weaker, which will cause the SNR to be lower.

Another factor that affects the SNR is the noise floor, which can be defined as the ambient or background level of radio energy on a specific channel. This background energy can include modulated or encoded bits from nearby 802.11 transmitting radios or unmodulated energy coming from non-802.11 devices such as microwave ovens, Bluetooth devices, cordless phones, and so on. The higher the noise levels are, the lower the SNR will be.



Example of Signal-to-Noise Ratio (SNR) graph.

Example of SNR graph on the Etherscope nXG.

The worst-case scenario is when you have a weak signal and high-noise levels, this fatal combination by definition results in a low SNR. This, in turn, will cause performance problems. Regardless, identifying SNR issues is very simple, you just need a tool that can measure both Signal Strength and Noise. Note that in the past most Wi-Fi adapters could measure noise levels, but there are few adapters in the market today that can, thus you should acquire a dedicated troubleshooting tool that will provide this information. There are many Wi-Fi troubleshooting or even surveying tools that can do this.

To resolve slow Wi-Fi speed problems caused by a low SNR:

1) Improve the coverage of your Wi-Fi network and make sure you have a signal strength that is at least 20 dBm higher than the noise floor (for voice over Wi-Fi deployments you want your signal strength to be 30 dBm higher).

2) Lower the noise floor on your environment by using channels with a low amount of Wi-Fi traffic, and by removing non-Wi-Fi devices (Bluetooth, cordless phones, wireless video cameras, microwave ovens, etc.) that increase the noise floor on the Wi-Fi channels you are using. In cases were the non-Wi-Fi device generating the noise can't be moved or disabled, you will need to reconfigure your AP's so they do not use channels with a high-noise floor.

CAPACITY

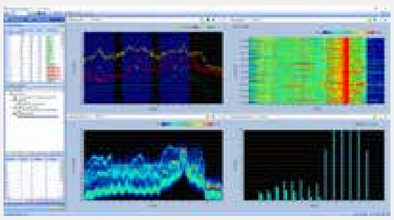
Capacity problems happen when you have too many client devices transmitting on the same area, or when there are one or more client devices generating an excessive amount of traffic, a bandwidth hog. Capacity problems could also happen when you have:

Example of Signal Level, Noise Level, and SNR measurements collected with NetAlly's AirCheck G2.

1) Under-provisioned AP networks – Not enough AP's to handle the amount of client devices available. It is recommended to have no more than 25 client devices connected on a single AP at the same time.

2) Client-loading imbalances – This occurs when client devices are connecting to the same AP instead of balancing the load between all the AP's in the area. This can all lead to excessive client transmissions on a single channel, and thus overload the channel. Also, it is important to understand that it is not simply the number of connected clients on a channel that increases the load on that channel, but how much traffic they generate. A few clients transferring large files or streaming 4K video can overload a channel too.

So, how do you determine if a channel is overloaded? This is done by measuring the utilization of a channel, or basically measuring how much space on a channel is being used (normally shown as a percentage value). Many dedicated Wi-Fi troubleshooting tools and even apps will provide this information. Still, most of them will only provide visibility on Wi-Fi utilization, which may not be enough information to determine how busy the Wi-Fi channels you are using really are. Thus, the best way to measure utilization accurately is by using a dedicated Wi-Fi troubleshooting tool that will provide visibility on both Wi-Fi and Non-Wi-Fi utilization.



Example of the Channel Duty Cycle chart on NetAlly's Spectrum XT comparing Wi-Fi vs Non-Wi-Fi Utilization.

As for how to resolve capacity problems, here are a few tips:

1) Use the AP Controller to limit the amount of bandwidth each client device can use. This will help prevent client devices from generating an excessive amount of traffic that could affect the performance of the network (by not leaving enough bandwidth for other devices).

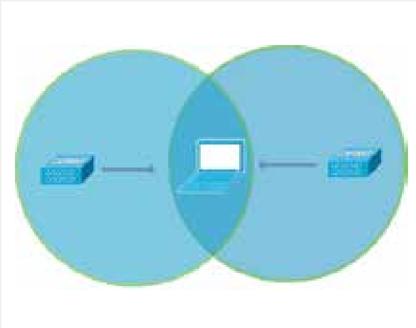
2) Move as many devices as you can to the 5.0 GHz band, which has more channels available. This can be done by enabling the Band Steering option on your AP controller. Basically, when you enable this option the controller will move client devices to the 5.0 GHz band and leave the 2.4 GHz band to legacy devices.

3) When planning your Wi-Fi network make sure that you will install enough AP's to support the maximum number of users you expect, and remember that even though many AP's will support more than 100 concurrent client connections it is recommended to limit the amount of concurrent connections to 25 or 30 clients per AP. The number of concurrent clients will depend on the amount of bandwidth you have available and the amount of bandwidth you plan to provide to each user.

4) Make sure to enable the "Load Balancing" option on your AP Controller. This will allow the controller to balance the client device load between AP's. That way you won't end up with most clients connecting to the same AP.

CO-CHANNEL INTERFERENCE

One of the most common reasons for slow Wi-Fi network speeds is Co-Channel Interference (CCI), which is what happens when you have too many AP's with overlapping signals working on the same channel. This condition results in every client device and AP in that area having to time-share the same channel airtime, which is a problem since Wi-Fi is by nature a half-duplex type of communication (only one device can talk at a time). So, if a client is sending data to the AP, the AP cannot also send data to that client or any other client at the same time. **Note that CCI starts being a problem when you have more than 8 AP's with overlapping signals working on the same channel,** and on which each AP has a signal strength higher than -75 dBm.



Example of Co-Channel Interference.

Example of the Co-Channel Interference heatmap generated using NetAlly's AirMagnet Survey Pro.

Determining if the level of CCI is high enough to cause Wi-Fi network slow speeds is simple, you just need a tool that will highlight how many AP's are working on the same channel as the AP on which the client device that identified the slow speeds problem was connected to. Many tools will provide this information, but some of them go beyond providing basic information by automatically alerting you on high levels of CCI. Another option is to perform a site survey of your Wi-Fi network, which can provide a graphical representation (heatmap) of the CCI levels on your network, thus allow you to visually identify areas of the building on which you have high levels of CCI.

As for how to resolve CCI problems, here are a few tips:

1) Make sure that AP's on your network with overlapping signals are working on different channels. This is easier to do when you are using the 5.0 GHz band since you have 25 non-overlapping channels available, but it could be more difficult to do while using the 2.4 GHz band since you only have 3 non-overlapping channels available.

2) Allow your controller to assign channels to each AP automatically, this is the easiest way to prevent and resolve problems with CCI. In this case, the AP controller will constantly scan the air for CCI and other types of interference and will automatically change the AP channel assignments as required. But, be sure to validate the correct operation of automatic channel assignment by using an independent, third-party tool.

3) While designing a new Wi-Fi network, the easiest way to prevent CCI problems is to use a Wi-Fi planning tool that will automatically calculate the placement of each AP and automatically assign channels to each AP while preventing CCI.

ADJACENT CHANNEL INTERFERENCE

Another common reason for slow Wi-Fi network speeds is Adjacent Channel Interference (ACI), which happens when the frequency bandwidth of nearby channels overlap, resulting in transmissions on one channel interfering with transmissions on a nearby channel. Notice that ACI mostly happens on the 2.4 GHz band since many channels on this band share the same frequencies, thus overlap and interfere with each other. There are only three non-overlapping channels on the 2.4 GHz band (channels 1, 6, and 11), so it is best to only use these channels when you want to prevent ACI. Another thing to remember is that AP's working on in-between channels can cause ACI for AP's on the preferred non-overlapping channels. ACI starts being a problem when you have more than 8 AP's with overlapping signals working on overlapping channels, and on which each AP has a signal strength higher than -75 dBm.

Example of Adjacent Channel Interference.

Determining if the level of ACI is high enough to cause problems with slow speeds on the Wi-Fi network is simple, you just need a tool that will highlight how many AP's are working on channels that overlap with the channels being used by the AP you are troubleshooting (the AP on which the slow speeds were reported). Many tools will provide this information, but some of them will go beyond providing basic information by automatically alerting you on high levels of ACI. Another option is to perform a site survey of your Wi-Fi network, which can provide a graphical representation (heatmap) of the ACI levels on your network, thus allow you to visually identify areas of the building on which you have high levels of ACI.

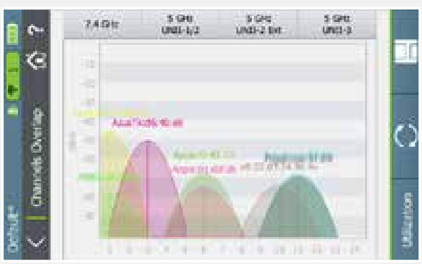
As for how to resolve ACI problems, here are a few tips:

1) Make sure that AP's on your network with overlapping signals on the 2.4 GHz band are using non-overlapping channels like 1, 6, or 11. Notice that on very busy environments designed to support a high number of users this might be difficult since you only have three non-overlapping channels available on the 2.4 GHz band.

2) Enable the Band Steering option on your AP controller, which will allow the controller to automatically identify devices that support both the 2.4 GHz and 5.0 GHz bands and will steer those devices to the 5.0 GHz option. This will free up space on the 2.4 GHz band and will help lower the effects of ACI.

3) Allow your controller to assign channels to each AP automatically, which is the easiest way to prevent and resolve problems with ACI. In this case, the AP controller will constantly scan the air for ACI and other types of interference and will automatically change the AP channel assignments as required.

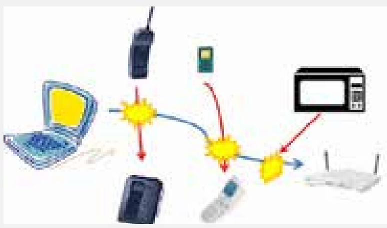
4) While designing a new Wi-Fi network, the easiest way to prevent ACI problems is to use a Wi-Fi planning tool that will automatically calculate the placement of each AP and that will automatically assign channels to each AP while preventing ACI.



Example of the Adjacent Channel Interference being highlighted by NETALLY's AirCheck G2.

NON-WI-FI INTERFERENCE

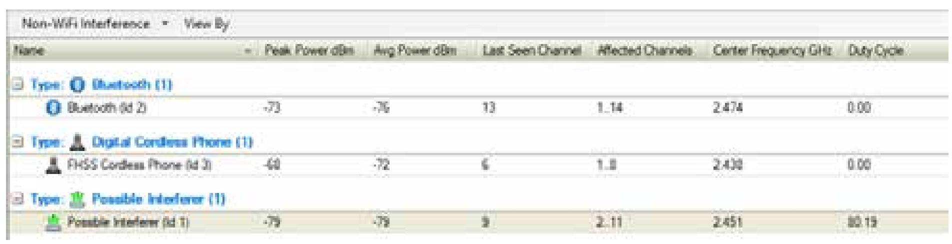
There are many other radio transmissions besides 802.11 that can occur in the same frequency bands used by Wi-Fi. Some examples of technologies that generate radio transmissions on the same frequencies as Wi-Fi are Bluetooth, cordless phones, microwave ovens, radars, ZigBee, and wireless security cameras. While Wi-Fi devices have a high tolerance for transmissions other than 802.11 transmissions, these non-Wi-Fi transmissions do not obey the same rules of airtime sharing (they don't take into consideration that Wi-Fi is by nature a half-duplex type of communication) and thus can present a significant source of interference, which can slow down the Wi-Fi network.



Example of non-Wi-Fi Interfering devices affecting performance on a Wi-Fi network.

The easiest way to determine if you have problems with non-Wi-Fi interfering devices slowing down your Wi-Fi network is to use a spectrum analyzer. Different from a Wi-Fi adapter, which is designed to send and receive data, spectrum analyzers are designed to measure power levels throughout the frequencies being scanned, thus can see not only Wi-Fi traffic, but traffic generated by non-Wi-Fi devices working on the same frequencies. There are multiple spectrum analyzers on the market that can provide good visibility into the Wi-Fi frequencies. Still, it is recommended that you acquire a spectrum analyzer that automatically identifies sources of interference for you. This will simplify troubleshooting and will allow you to find the root cause of slow Wi-Fi network speeds quicker.

As for how to resolve non-Wi-Fi interference problems, here are a few tips:



Non-WiFi Interference ▾ View By

Name	Peak Power dBm	Avg Power dBm	Last Seen Channel	Affected Channels	Center Frequency GHz	Duty Cycle
Type: Bluetooth (1)						
Bluetooth (Id 2)	-73	-76	13	1..14	2.474	0.00
Type: Digital Cordless Phone (1)						
FHSS Cordless Phone (Id 3)	-68	-72	6	1..8	2.430	0.00
Type: Possible Interferer (1)						
Possible Interferer (Id 1)	-79	-79	9	2..11	2.451	80.19

Example of Non-Wi-Fi Interfering devices automatically found and identified using NetAlly's Spectrum XT

1) Remove or disable the non-Wi-Fi devices generating the interfering signal. If this is not possible, try moving the device as far away as possible from the Wi-Fi network AP's. The amount of interference being caused by a non-Wi-Fi device will diminish as its signal strength grows weaker.

2) If removing, disabling, or moving the non-Wi-Fi device is not possible (the device may be essential for day-to-day operations), then the best course of action would be to use your AP controller to change the channels being used on your Wi-Fi network. You will want to use Wi-Fi channels that are not being affected by the non-Wi-Fi interfering device.

3) Allow your controller to assign channels to each AP automatically, which is the easiest way to prevent and resolve problems with non-Wi-Fi interference. In this case, the AP controller will constantly scan the air for sources of non-Wi-Fi interference and will automatically change the AP channel assignments as required. Note that on cases where the interfering device is affecting multiple channels the AP controller may not be able to find a suitable channel to use, so one of the two previous recommended solutions would be required.

CONCLUSION

In conclusion, slow Wi-Fi network problems don't have to be difficult to troubleshoot or resolve. With the right tools and a little knowledge, you should be able to resolve slow Wi-Fi network problems quickly and easily, which is why NetAlly strives to provide the best Wi-Fi troubleshooting tools on the market ranging from survey tools that help you identify ACI or CCI, to software or handheld troubleshooting tools that allow you to run performance tests, identify sources of non-Wi-Fi interference, measure SNR, and much more!