netAlly®

Wi-Fi Troubleshooting: Connection Problems

White Paper

Table of Contents

Remote Site Troubleshooting

INTRODUCTION

Are you ready for the dreaded "Wi-Fi-is-not-working" complaints?

As IT professionals we have all encountered them, the dreaded "Wi-Fi-is-not-working" complaints. You're peacefully getting some work done at the office and then out of nowhere someone comes in and starts complaining about not being able to connect to the wireless network or about the wireless network being slow, about getting disconnected from the wireless network all the time, about not being able to connect to the internet, and so on. These are very common complaints, and all of them concerning since figuring out the root cause of these common wireless network problems can be very time consuming and sometimes difficult. Or is that really the case? Could it be possible that solving these common wireless problems is not that difficult after all? Well, reality is it is not. With the right tools and a little knowledge, finding the root cause of the most common wireless network problems can be quick and simple.

It is important to know how to differentiate between Wi-Fi and back-haul problems

This first entry on our series of Wi-Fi troubleshooting whitepapers will focus on showing you how to quickly and effectively troubleshoot "Connection Problems", or to be more accurate, problems connecting to the Wi-Fi network, which are not to be confused with problems connecting to a specific website or IP address. Most users will not know the difference and will complain by saying something like "The wireless is not working. I can't connect to the Internet."

So, on this paper we will first start by showing how to differentiate between problems connecting to the Wi-Fi and problems accessing network resources. After that we will show you how to identify the most common causes for connection problems on the Wi-Fi network and we will provide recommendations on how to resolve those problems.

Let us get started!

Identify the Problem

Before you can start troubleshooting a Wi-Fi connection problem you need to make sure the problem is really Wi-Fi related. As mentioned in this paper's introduction, most users will not know the difference between a Wi-Fi related problem, a DHCP server problem, a DNS problem, etc. All the user knows is that they cannot connect to the network. So, the first step of the troubleshooting process is to duplicate the problem and find out if the problem is on the Wi-Fi network.

Duplicating a connection problem is a relatively easy process and can be done in multiple ways:

Users become frustrated any time they have problems connecting to the Wi-Fi network

1. You can ask the persons that complained about not being able to connect to the network to show you the problem they encountered or the error message they have received. This method may not provide a lot of details regarding the root cause of the problem, but it allows you to confirm if there really is a problem. Not only that, if the user's device is really having problems connecting to the Wi-Fi network, having the problem device at hand will allow you to identify configuration problems on the client device or user errors. After all, the most common reason for network connection problems is not the network, but user errors or simple Wi-Fi network configuration issues.

   a. Some of the most common user errors are:

      i. User trying to connect to the wrong network – This happens a lot in busy environments. The user could select the wrong SSID by mistake, or the user's device could try to automatically connect to a known hotspot that is too far away for a successful connection.

      ii. User entering the wrong security credentials – Typos happen, and they are the main reasons for this type of problem.

      iii. User trying to connect to a network using a device that is not authorized – Very common when certificates are required to gain access to the network, or on cases where only devices with a specific MAC address can connect to the network.

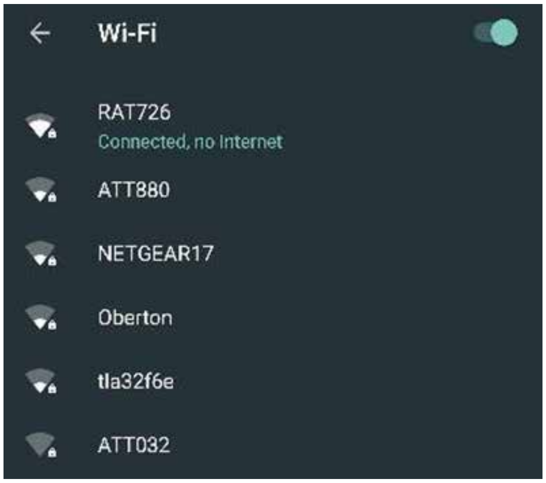
      iv. Using an outdated device – The user may have problems connecting to a specific SSID if the client device does not support the 5.0GHz band or the extended channels.

   b. Some of the most common Wi-Fi network configuration issues are:

      i. Missing SSID – If the SSID the user is trying to connect to is not showing up, this could mean the SSID has been configured to be hidden by mistake. It could also mean there is a real problem with the Wi-Fi network like insufficient coverage or access points that have stopped transmitting. This can be easily verified by using other devices to find the SSID you want to connect to, just remember that the second device needs to be physically located on the same area as the problem device.

ii. Invalid IP Address – Some but not all user devices are able to provide this type of detail, with those that do telling you the user device could connect and authenticate successfully to the Wi-Fi network, but had problems getting an IP address. This type of problem normally points towards DHCP server configuration problems as the root cause of the problem (for example, not enough IP addresses available or an unresponsive server). Still, it could also happen if the connection to the Wi-Fi network is unstable or if there is excessive packet loss.

iii. Invalid DNS Address – If the client device says it could connect to the Wi-Fi network successfully, but there is no internet connection, this normally means configuration problems on the DNS server. It could also mean problems with the internet service provider.



Wi-Fi

RAT726
Connected, no Internet

ATT880

NETGEAR17

Oberton

tla32f6e

ATT032

Common Wi-Fi connection error on Android devices

2. Another option that will allow you to verify if there are problems connecting to the Wi-Fi network is to try to connect to the network using another device. In this case, you could use a device such as that one being used by the person having the problem, which would allow you to verify if there are connection problems with the Wi-Fi network. Or you could run a full “Connection Test” using a dedicated Wi-Fi test tool that will allow you not only to verify connectivity, but will also provide details that will help you get

closer to the root cause of the problem. For example, some useful information that a dedicated test tool can provide is:

a. **Connection Status and Time** – This helps you verify if you can connect to an access point and how long it took. Problems at this stage will prove that there is indeed a connectivity problem on the Wi-Fi network, which are normally caused by coverage problems, interference, low SNR, etc.

b. **Authentication Status and Time** – This helps you verify if you could authenticate successfully and how long it took. Problems at this stage would mean the wrong passphrase is being used, and on the cases where WPA2-E is being used it could mean the wrong certificate is being used. A long authentication time normally means problems with the authentication server, but it could also be caused by an unstable Wi-Fi connection.

c. **Gateway Status and Response Time** – This will help you verify that the device can communicate with the gateway and it will help verify how fast it can communicate.

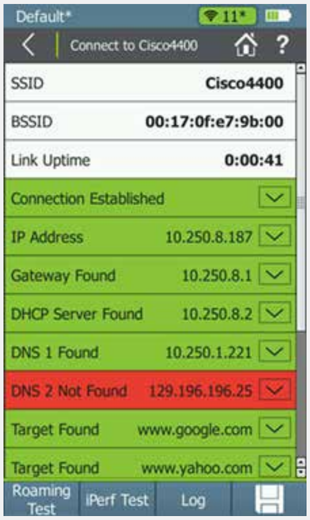
d. **DHCP Status and Response Time** – This will show you if the device was able to get an IP address and how quickly. Problems at this stage normally point towards issues with the DHCP server, or stability problems on the Wi-Fi network.

e. **DNS Status and Response Time** – This will show you if the device was able to communicate with the DNS server and how long it took. Problems at this point show that you can successfully connect to the Wi-Fi network, but will not be able to use a URL to access the Internet because of problems with the DNS server.

f. **Target Found** – Some test devices will allow you to verify connectivity to a specific target. It could be a URL or an IP address. This can be used to verify connectivity to commonly used local resources or the Internet.

g. **Connection PHY Data Rate** – This will allow you to verify the PHY Data Rate measured during the connection test. Low data rates could highlight problems with the Wi-Fi network, and they could also highlight outdated client devices or access point configuration problems.

h. **Retry Rate** – This normally provides the percentage of transmitted frames that are retry frames. A retry rate higher than 20% will indicate problems with the Wi-Fi network.



SSID	Cisco4400
BSSID	00:17:0f:e7:9b:00
Link Uptime	0:00:41
Connection Established	
IP Address	10.250.8.187
Gateway Found	10.250.8.1
DHCP Server Found	10.250.8.2
DNS 1 Found	10.250.1.221
DNS 2 Not Found	129.196.196.25
Target Found	www.google.com
Target Found	www.yahoo.com

Connection test results on NetAlly's AirCheck ™ G2

Identify the Root Cause

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

- **Signal Coverage**
- **Signal to Noise Ratio (SNR)**
- **Legacy 802.11 Devices**
- **Security**
- **Capacity**
- **Wired Issues**

Signal Coverage

Poor signal coverage is still one of the most common reasons for Wi-Fi connection problems. After all, if Wi-Fi devices can't hear each other then they can't communicate. The problem is that there are lots of things that can affect how a Wi-Fi signal propagates throughout the environment, and thus can create coverage problems:

- **Loss (free space)** – The loss of signal strength caused by natural attenuation of the waves. As the signal goes farther the strength of the signal diminishes.

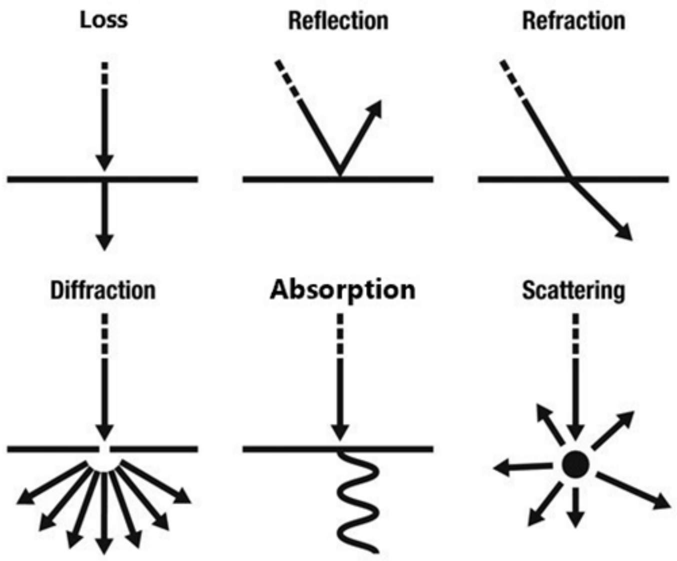
- **Reflection** – When a wave hits a smooth object that is larger than the wave itself, depending on the media, the wave may bounce in another direction. Reflection is a major source of poor performance for 802.11a/b/g networks since it causes an effect called multipath, which causes signal strength loss, and packet errors.

- **Refraction** – The bending of an RF signal as it passes through a medium with a different density, thus causing the direction of the wave to change. This most commonly occurs outdoors because of atmospheric conditions (water vapor, change in air temperature, change in air pressure). The signal may also refract through certain types of glass and other materials.

- **Diffraction** – The bending of an RF signal around an object. It is typically caused by some sort of partial blockage of the RF signal, such as a small hill or building.

- **Scattering –** Multiple reflections occur when the electromagnetics signal wavelength is larger than whatever medium the signal is reflecting from or passing through. This happens when you encounter uneven surfaces like chain link fences, wire mesh in stucco walls, rocky terrain, etc. which causes the main signal to dissipate as it is reflected in multiple directions and thus degrade signal strength.

- **Absorption –** If a signal does not bounce of an object, move around the object, or pass through an object, then 100% absorption has occurred. Most materials will absorb some amount of an RF signal to varying degrees causing signal strength loss. The worst offenders are brick walls, concrete walls, and water.



Examples of RF behavior

Also, different from what most people think, access point signal coverage is not the only thing you need to worry about. You also need to take into consideration client device signal coverage. After all, if the access point cannot hear responses from a client device then communication will fail.

- **Access Point Coverage –** The signal strength of an access point from a client device perspective. A strong signal is required to ensure that the client devices can hear the messages sent by the access points.

- **Client Device Coverage –** The signal strength of a client device from an access point perspective. A strong signal is required to ensure that the access point can hear the replies sent by the client devices.

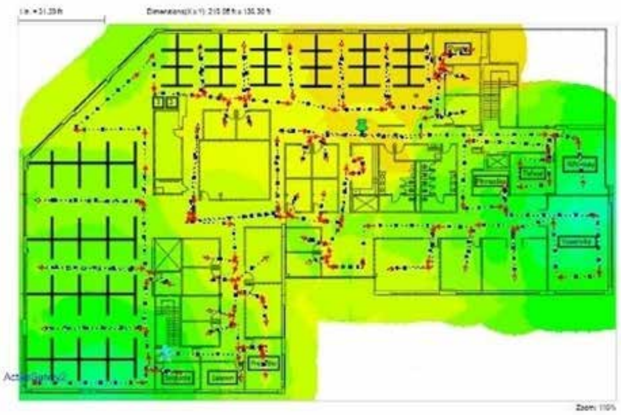
As for how to identify coverage problems, you have a few simple options:

1. Troubleshoot a Problem Area – Troubleshooting coverage problems in a known problem area is very simple. You only need a tool that will allow you to measure the signal strength of both access

points and clients. Verifying the access points signal strength in the problem area will allow you to confirm that all client devices should be able to see your network. Meanwhile, verifying the client device signal strength from the access points perspective will allow you to confirm that communication can be achieved. Notice that a common reason for client device coverage problems are access points on which the power levels have been increased to very high levels. If the coverage of an access point is too big, then client devices at the border of the coverage range and with weaker Wi-Fi transmit power may not be able to talk back to the access point, thus cause connection attempts to fail.

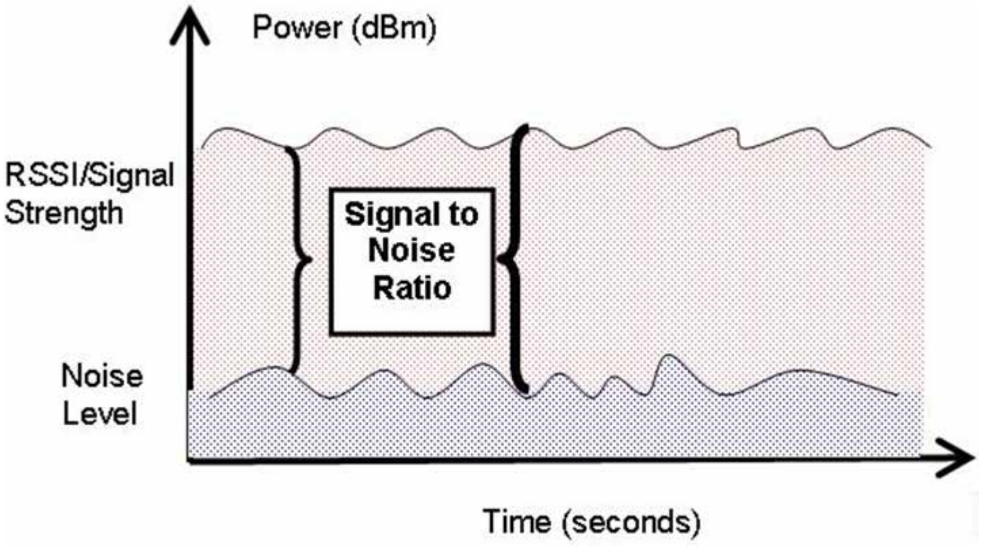
2. Survey a Site – Another option that is very popular is to survey an entire site instead of a single spot, which is done by performing a site survey that will allow you to generate a graphical representation or heatmap of how your Wi-Fi network is performing. There are multiple tools available that will allow you to perform a site survey. Some of them will provide basic visibility into coverage and Wi-Fi interference. Meanwhile, the most advanced of these tools will provide visibility into coverage, noise levels, SNR, Data Rates, Retry Rates, Wi-Fi interference, non-Wi-Fi interference, and a lot more. Note that it is highly recommended to perform a site survey after a new Wi-Fi network has been deployed and every few months after that. This will allow you to verify that your Wi-Fi network is working as designed and will allow you to identify any changes that could cause problems in the future.

Coverage problems are normally resolved by adding more access points, using antennas with a higher gain, or increasing the transmit power of the access points. Keep in mind that increasing the power will also increase the noise levels, thus it is normally recommended to go with better antennas or more access points.



Signal strength heatmap generated with NetAlly's AirMagnet® Survey Pro

Signal to Noise Ratio

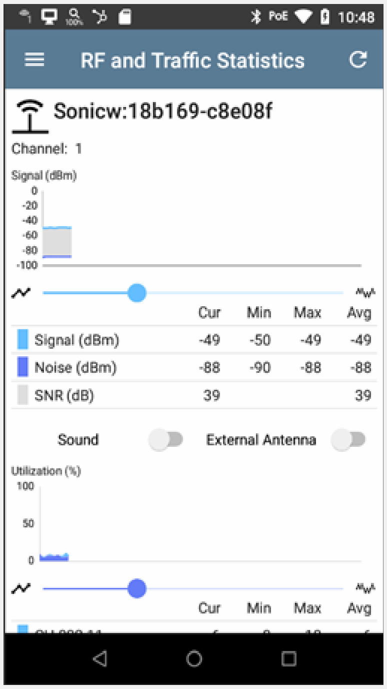


SNR represents the difference between Signal Strength and the environment's Noise Floor

The quality and rate of a connection depends directly on the signal-to-noise ratio (SNR) that a receiving device detects, which includes both access points and clients. As described in the previous section, attenuation or loss of signal strength happens easily. So, as the signal level goes down, the SNR goes down, and so does the transmission rate. For example, a device that is "too far" from an access point may be able to see the network to which it wants to connect, but if the SNR is too low the quality of the transmission will be so bad that it will not be able to connect successfully (a "weak but strong-enough" signal one moment may become a "too weak" signal the next moment).

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, then the lower the SNR.

The worst-case scenario is when you have a weak signal and high noise levels, this fatal combination will greatly lower your SNR, which in turn, will cause performance and connectivity problems. Regardless, identifying SNR problems 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 not many of those available in the market anymore, thus you may need to acquire a dedicated troubleshooting tool that will provide this information. There are many Wi-Fi troubleshooting or even surveying tools that can do this.



10:48

RF and Traffic Statistics

Sonicw:18b169-c8e08f

Channel: 1

	Cur	Min	Max	Avg
Signal (dBm)	-49	-50	-49	-49
Noise (dBm)	-88	-90	-88	-88
SNR (dB)	39			39

Sound

External Antenna

Signal Level, Noise Level, and SNR measurements collected with NetAlly's EtherScope® nXG

As for how to resolve connectivity 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 that increase the noise floor on the Wi-Fi channels you are using. On cases were the non-Wi-Fi device generating the noise cannot be moved or disabled you will need to reconfigure your access points, so they will not use channels with a high noise floor.

Legacy 802.11 Devices

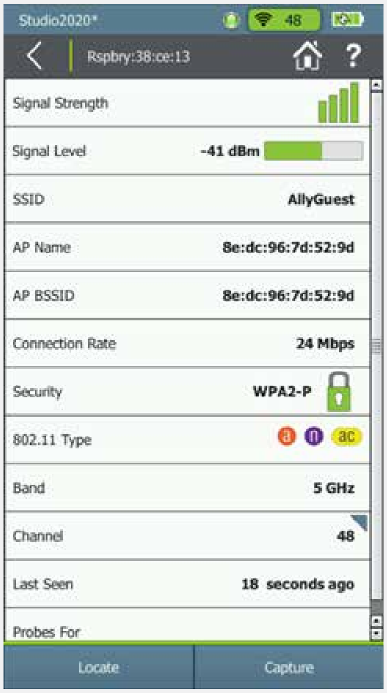
Older Wi-Fi devices are still around! But they do not support today's higher data rates, so when they connect to a Wi-Fi network, they will transmit only at lower data rates. Not only that, a user may be using a legacy device that does not support higher data rates without realizing it, which can be a problem since older legacy rates, particularly 802.11b, are sometimes blocked from operation at the access point to preserve precious airtime. A device which only supports these older rates will be unable to connect to the network.

Another problem is older devices that do not support the 5.0 GHz band. Many corporate networks have been migrated to support the 5.0 GHz band only since there are more channels available and less interference, therefore on cases like this legacy 802.11 devices will not be able to connect to the corporate Wi-Fi network anymore. Not only that, some older client devices may support the 5.0 GHz band, but not all the channels on that band. For example, many older devices do not support the DFS channels (frequencies shared with Radar transmissions), and because of that, won't be able to connect to the network.

Regarding how to easily identify these limitations, the easiest way is to use a tool that can identify the capabilities of a client device. Some of the information you want the tool you select to provide on client devices is:

- **SSID** – Allows you to verify which network the client device is connected to but is only available when the device is connected to a network, and used to verify that the client device is connected to the right network.

- **Access Point Name** – Allows to verify to what access point the client device is connecting to and is very useful when you want to make sure client devices are connecting to the closest access point.



Signal Strength	
Signal Level	-41 dBm
SSID	AllyGuest
AP Name	8e:dc:96:7d:52:9d
AP BSSID	8e:dc:96:7d:52:9d
Connection Rate	24 Mbps
Security	WPA2-P
802.11 Type	a n ac
Band	5 GHz
Channel	48
Last Seen	18 seconds ago
Probes For	

Client device information collected using NetAlly's AirCheck G2

- **Connection Rate** – Provides the connection data rate being used by the client device. 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 connecting to the Wi-Fi network.
- **Security** – Provides information on the type of security being used by the client device and allows you to verify the client device security configuration.
- **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 the higher data rates.
- **Band** – Provides information on the band being used by the client device, which allows you to verify if the client device can support both the 2.4 GHz and 5.0 GHz bands.
- **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

The only solutions to this type of problem are to have the user upgrade their device to one that supports the latest 802.11 technology, or to change the configuration on your access points so they will support older technologies. Upgrading the client device would be the preferred option, however, as adding support for older 802.11 technologies could adversely affect the performance of newer client devices.

Security

Security is a good thing but managing security on access points and clients is not easy. Any passphrase mismatch, certificate missing, or mistake can leave client devices unable to connect.

Both the access points and the client devices must have the proper security credentials to successfully form a connection, as errors in the configuration of these credentials on either end can prevent authorized users from being authenticated.

Besides that, some networks are secured by allowing only certain MAC addresses to connect and authenticate, so if a device’s MAC address is not on the authorized list, the client device will not successfully connect.

As for identifying connection problems caused by security configuration problems, here are a few tips:

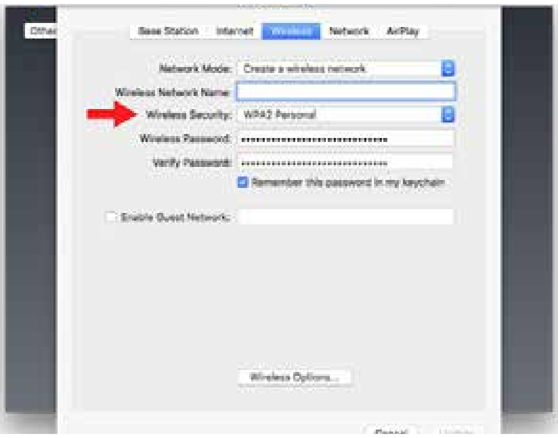
1. If you are using WPA-P or WPA2-P on your network, the first thing is to verify that the correct passphrase is being used.

2. If you are using WPA-E or WPA2-E on your network, you should start by verifying that the correct credentials are being used and that the client device has the required certificates installed.

3. If you are restricting access to the network to authorized devices only, using their MAC address, then you should also verify that the MAC address for the client device is on the approved list.
   - **a.** Using a tool that can spoof a client MAC address can definitively identify issues with the authentication service.

4. If you are using WPA-E or WPA2-E and more than one device is having the same issue, then in that case, you may want to make sure that the authentication server is still accessible.

After identifying the security configuration problem, you just need to fix the configuration on the client device, wireless network, or authentication server to resolve the issue.



Network Mode: Create a wireless network

Wireless Network Name:

Wireless Security: WPA2 Personal

Wireless Password: ••••••••••••••••••••••••••••••

Verify Password: ••••••••••••••••••••••••••••••

☑ Remember this password in my keychain

□ Enable Guest Network:

Security setting on a MAC OS device

Capacity

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

1. Excessive co-channel interference – Too many devices working on the same channel. For example, it is not recommended to have more than four access points covering the same area while working on the same channel.

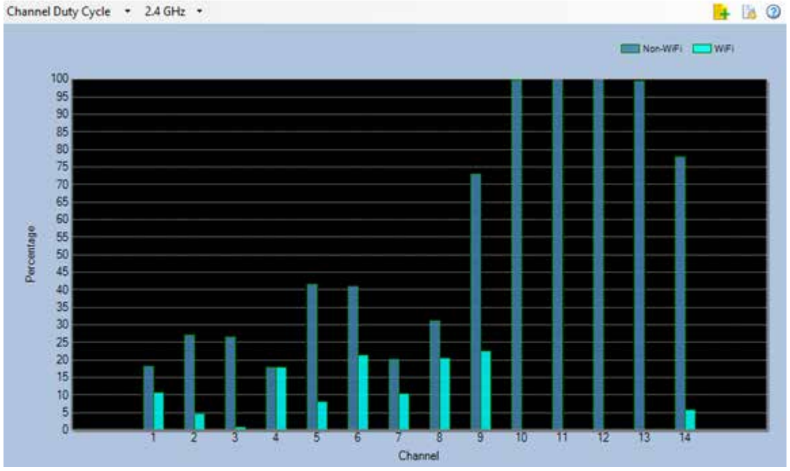
2. Under provisioned networks – Not enough access points to handle the amount of client devices in use. It is recommended to have no more than 25 client devices connected on a single access point at the same time.

3. Client loading imbalances – Most client devices are connecting to the same access point instead of balancing the load between all the access points in the area.

4. Non-Wi-Fi Interference – Devices that do not use the Wi-Fi network but generate an RF signal on the same frequencies will increase the channel utilization, thus lowering channel capacity.

These 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 increase the load on that channel, but how much traffic they generate. A few clients transferring large files or streaming HD 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 what percentage of a channel is being used. Many dedicated Wi-Fi troubleshooting tools and even mobile device apps will provide this information, but most of them will only provide visibility of Wi-Fi utilization, which may not be enough information to determine how busy the Wi-Fi channels you are using. Therefore, the best way to measure utilization accurately is by using a dedicated Wi-Fi troubleshooting tool that will provide visibility of both Wi-Fi and non-Wi-Fi utilization.



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 access point 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.

2. Minimize channel interference by having the access point controller adjust channels automatically. If this option is not available on your controller, then you need to manually adjust access point channel assignments in such a way that no two access points with overlapping signals are using the same channel.

3. 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 access point 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.

4. When planning your Wi-Fi network, make sure that you will install enough access points to support the maximum number of users you expect, and remember that even though many access points will support more than 100 concurrent client connections, it is recommended to limit the amount of concurrent connections to 25 or 30 clients per access point. 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.

5. Make sure to enable the “Load Balancing” option on your access point controller. This will allow the controller to balance the client device load between access points. That way you will not end up with most clients connecting to the same access point.

6. Use a spectrum analyzer to detect, identify and find any sources of non-Wi-Fi interference. You also want to use the spectrum analyzer to identify the channels being affected by the interference. After that, if possible, remove or disable the interfering device, and if not possible, make sure that your access points use a channel that is not being affected by the interfering device.

Wired Issues

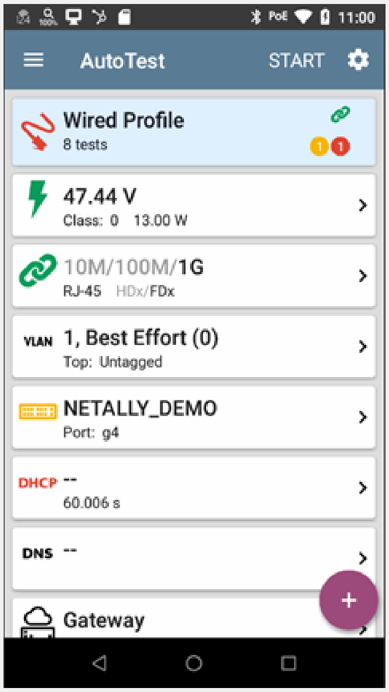
Every wireless access point has a backhaul connection to the network and this is nearly always Ethernet. The access point Ethernet connection to the network is a vital link in the overall connectivity chain. Even when a client device connects to the WLAN, they still need basic wired services like DHCP and DNS to access most resources. Some of the most common wired issues that will cause Wi-Fi connection problems are:

1. **DHCP and DNS Services access -** As mentioned in previous sections of this document, problems with DHCP or DNS services will cause the user to think they cannot connect to the Wi-Fi network. If the DHCP server is not accessible, the user’s client device will not be able to get an IP address. If the DNS server is not available, the user’s client device will not be able to access a website through its URL.

2. **WAN Connectivity -** Connection to the Wi-Fi network can appear to be broken to the user if the WAN connection to the Internet does not work. This could be caused by simple routing problems like such as an Ethernet cable plugged into a LAN port instead of a WAN port, the WAN interface requiring a static IP address, or Point-to-Point

Protocol over Ethernet (PPPoE) credentials needing to be entered on your internet service provider's modem.

3. Access Point Power - Most modern access points run off Power over Ethernet (PoE). So, if the power available at the switch drops, or the wrong PoE option is configured, performance of the access point may suffer dramatically. This could cause Wi-Fi connection problems and could cause the end users to think the Wi-Fi is not working.



Wired Profile
8 tests

47.44 V
Class: 0 13.00 W

10M/100M/1G
RJ-45 HDx/FDx

VLAN 1, Best Effort (0)
Top: Untagged

NETALLY_DEMO
Port: g4

DHCP --
60.006 s

DNS --

Gateway

Ethernet Test on NetAlly's LinkRunner® 10G

So how do you determine if the problem is on the wired side of the network? The easiest way is to use a dedicated Wi-Fi troubleshooting tool to run a connection test. As mentioned previously in this document, a connection test will allow you to identify which part of the connection process is failing. For example, failures during the connection or authentication steps would point toward a Wi-Fi connection problem (as previously described). Meanwhile, failures during the DHCP or DNS steps will point towards problems with the services on the wired side of the network. Add to that a step that will allow you to verify connectivity to an external website and you will be able to confirm if you have Internet/WAN connectivity problems. Last, we also recommend having available a tool that will help you verify both PoE and connectivity on the wired side of the network. Tools like this will allow you to measure the amount of power going to the access point and to run a connection test from the wired side of the network to quickly highlight problems with DHCP or DNS services.

As for how to resolve Wi-Fi connectivity problems caused by wired issues, here are a few tips:

1. Verify the configuration and availability of your DHCP or DNS server.

2. Verify the configuration of your Ethernet switch and of the VLAN's being used. This includes the PoE configuration, and you need to make sure it matches the access point's power requirements.

3. Verify the wiring, make sure there are no breaks on the cable, and make sure all connectors have been installed correctly.

4. Make sure the overall length of your horizontal cabling is not longer than 328 feet as this is the limit for PoE. If the runs are longer than the 100M specification, the power received by the access points will be lower than expected.

5. Make sure your switch PoE budget is not over-subcribed. Each switch has output power limitations, so if you try to power too many devices at the same time or multiple power-hungry devices are connected on a single switch, your switch may not be able to generate the required power output for your access points (even if it is configured correctly).

Conclusion

In conclusion, Wi-Fi connectivity problems do not have to be difficult to troubleshoot or resolve. With the right tools and a little knowledge, you should be able to resolve Wi-Fi connectivity problems quickly and easily. NetAlly strives to provide the best Wi-Fi troubleshooting tools on the market, ranging from survey tools that help you gain visibility on how your Wi-Fi network is performing, to software or handheld troubleshooting tools that allow you to run connection tests, identify sources of non-Wi-Fi interference, test the wired side of the network, and more!

For more information on the NetAlly troubleshooting tools please visit us at: https://www.netally.com/.