netAlly

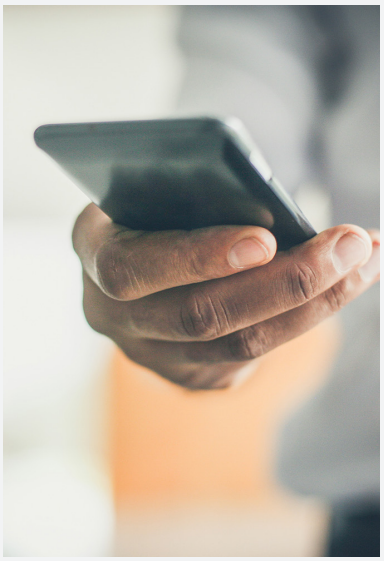
Wi-Fi Troubleshooting Roaming Problems

White Paper

Table of Contents

netAlly

Wi-Fi Troubleshooting Roaming Problems



Wi-Fi roaming is an essential part of wireless communications

INTRODUCTION

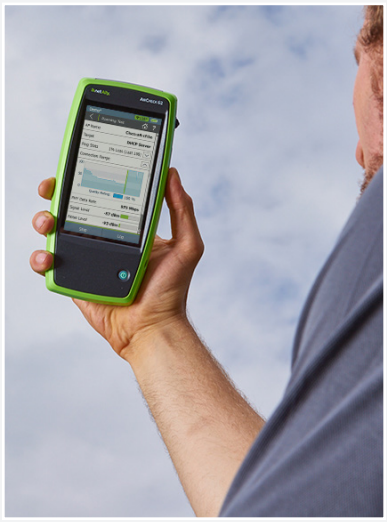
Have you ever noticed how while standing in one place the Wi-Fi network works great, but while walking around the building you get disconnected or the performance drops drastically? Well the reason for these issues you have encountered is problems with Wi-Fi roaming, which regretfully is one of the most common reasons for Wi-Fi connection and performance problems. After all, roaming behavior is hard to predict, and it is one of the most difficult parts of supporting a BYOD (bring your own device) environment. Not only do different devices roam differently, but sometimes a single Wi-Fi device will change its roaming behavior because of a different application is running, because there are too many AP's nearby causing congestion, or the AP's are misconfigured. The good news is that testing for roaming problems is very similar to testing for probing behavior since probing is the first step of roaming (probing is what a client device does when its looking a for Wi-Fi network to connect to), thus troubleshooting roaming problems is a lot easier than it may seem.

This Wi-Fi troubleshooting white paper will focus on showing you how to quickly and effectively troubleshoot "Roaming" problems. We will start by showing how to verify if you really have Wi-Fi roaming problems. After that we will show you how to identify the most common reasons for Wi-Fi roaming problems and we will provide recommendations on how to make your Wi-Fi network roaming problem free.

Let's get started!

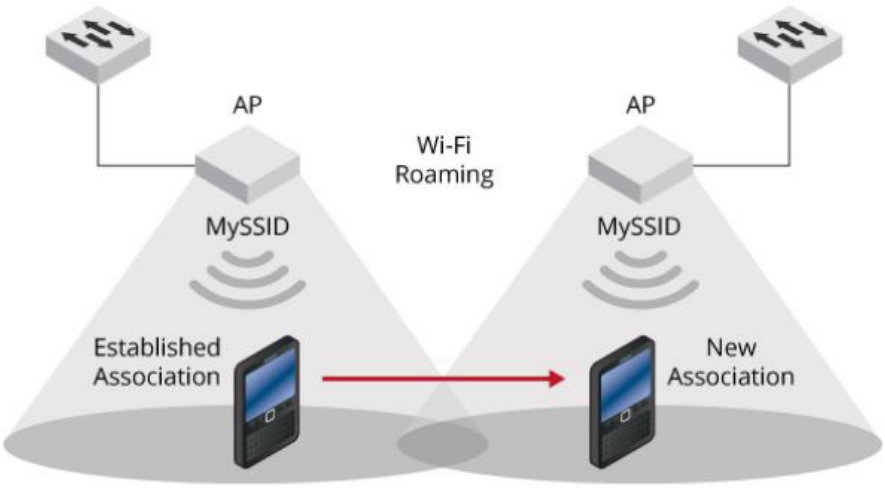
VERIFYING ROAMING PERFORMANCE

Before you start troubleshooting problems with Wi-Fi roaming you should understand how it works. Wi-Fi Roaming is a technology which enables a user's client device to change AP's while remaining connected to the network. The decision to roam from a connected AP to a new AP is generally the responsibility of the wireless client device. The roaming algorithms used by wireless client devices vary from vendor to vendor, but almost always involve the evaluation of the received signal strength indicator (RSSI). As a user moves away from the connected AP, the signal strength degrades. The client compares the RSSI to a pre-defined threshold and determines if a roam is required. Once the signal drops below this threshold, the wireless client performs an off-channel scan, scanning all available channels



NetAlly's AirCheck™ G2 can help you identify roaming problems

for a candidate AP, selects one with acceptable signal strength, and completes the roaming process by connecting or associating to the new AP. Note that some clients utilize additional parameters such as AP neighbor lists or capacity load on an AP to help optimize this roaming process.



Example of Wi-Fi roaming

So, now that we understand the basics on how Wi-Fi roaming works, you may be wondering how you prove if the Wi-Fi performance problems your users have been encountering are related to bad roaming. Well, the easiest way to do this is by measuring the performance and stability of your Wi-Fi connection during the roaming process.

To measure the quality of a Wi-Fi connection during roaming use the following steps:

1) Acquire a dedicated test tool that will allow you to constantly measure the quality of the Wi-Fi connection over time.
   a. Notice that there are many tools out there that can help with this. Still, you may want to use a tool that makes this process as easy as possible and that at the same time provides useful information like Quality Rating, PHY Data Rates, RSSI, Noise Levels, SNR, Retry Rates, Connection Statistics, and detailed Test Logs (all this information can be used to pinpoint the root cause of the roaming problem).
2) Identify the AP's for which you want to verify the roaming performance.
   a. Normally this AP's will be located on the same area on which users have been experiencing problems with the Wi-Fi connection dropping (or performance degrading) while they walk around.
3) Stand under one of the AP's, use your dedicated test tool to connect to the Wi-Fi network, and start measuring the quality of the connection.

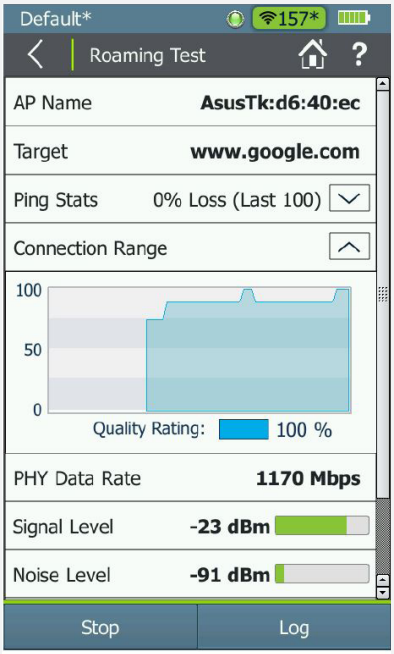
4) While actively connected to the Wi-Fi network walk towards the AP you want to roam to, and make sure that you are constantly measuring the quality of the Wi-Fi connection.

5) When your dedicated test tool decides to roam from one AP to the other you should see one of the following results:

a. Quality of the connection does not change much – If the quality of the Wi-Fi connection does not change much during the roaming process that tells you that the problem the users reported is not roaming related.

b. Quality of the connection becomes a lot lower – If the quality of the Wi-Fi connection becomes a lot lower than it used to be during the roaming process that tells you that the problem the users reported is indeed roaming related.

c. The connection is lost – If the Wi-Fi connection is lost during the roaming process that tells you that the problem the users reported is indeed roaming related.



Example of a roaming test on the AirCheck™ G2 Wi-Fi Tester

IDENTIFY THE ROOT CAUSE

After proving that the performance issues reported by the users are caused by Wi-Fi roaming problems it's time to identify the root cause of the problem. The most common reasons for Wi-Fi roaming problems are:

- Signal Coverage
- Unconnected Devices
- Congested Networks
- AP Misconfiguration

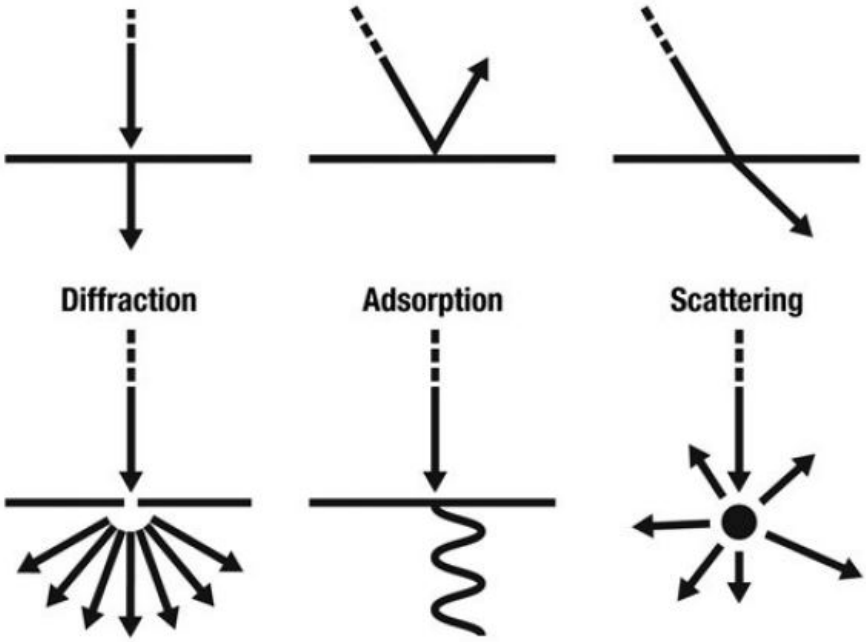
Signal Coverage

Bad signal coverage is one of the most common reasons for Wi-Fi roaming problems. If there are areas of your building with no Wi-Fi signal between AP's (no signal overlap), then client devices will get disconnected from the network while trying to roam from one AP to another. 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:

1) **Loss (free space)** – Is the loss of signal strength caused by natural broadening of the waves. As the signal goes farther the strength of the signal attenuates.

2) **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 multi-path. Which causes signal strength loss, and packet errors.

AirMapper™ Site Survey app on the EtherScope™ nXG being used to validate coverage



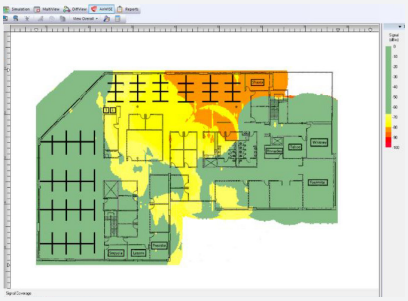
Example of a radio frequency (RF) behaviors

3) **Refraction** – Bending of an RF signal as it passes through a medium with a different density, thus causing the direction of the wave to change. 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 glasses and other materials.

4) **Diffraction** – The bending of an RF signal around an object. Typically caused by some sort of partial blockage of the RF signal, such as a small hill or building.

5) **Scattering** – Multiple reflections, occur when the electromagnetics signal wavelength is larger than whatever medium the signal is reflecting from or passing through. 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 will degrade signal strength.

6) **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. Still, the worst offenders are: brick walls, concrete walls, and water.



Example of a signal strength heatmap collected with the AirMagnet Survey PRO

Basically, having too little coverage will cause roaming problems. So, how do you identify coverage problems? Well, you have a few simple options:

1) **Troubleshoot a Problem Area** – Troubleshooting roaming issues caused by bad coverage in a known problem area is very simple. You only need a tool that will allow you to measure the signal strength of all the AP's on a specific area (many tools will provide this information). Measuring the AP's signal strength will allow you to confirm if there are any areas between AP's that have no coverage (no signal or a signal lower than -75 dBm).

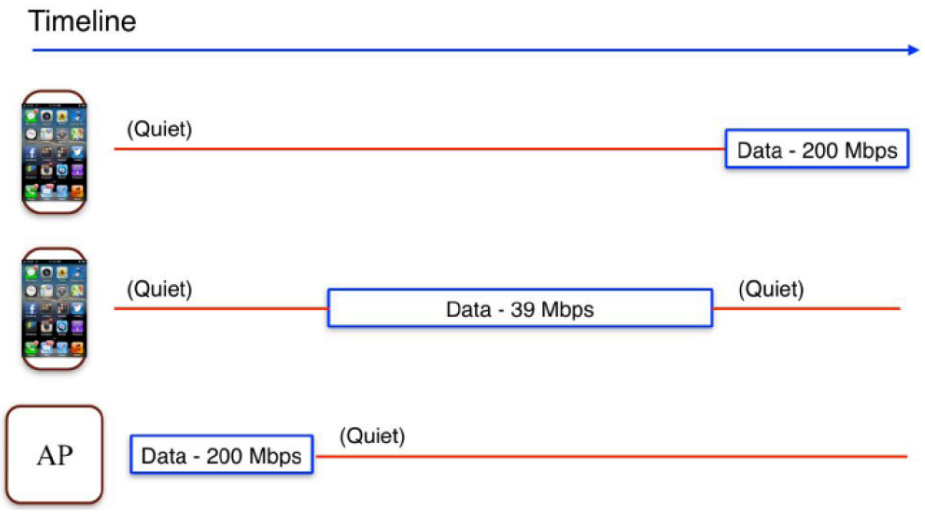
2) **Survey a Site** – Another option that is very popular is to survey an entire site instead of a single spot, and this is done by performing a site survey that will allow you to generate a graphical representation or heatmap of how your Wi-Fi network coverage looks like. There are multiple tools available 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. Notice 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 roaming problems in the future.

Low coverage problems are normally resolved by adding more AP's, using antennas with a higher gain, or increasing the transmit power of the AP's. Still, notice that increasing the power will also increase the Noise levels, thus it is normally recommended to go with better antennas or more AP's. If you decide to add more AP's, just be careful not to add too many AP's, else you'll end up having roaming problems caused by a congested network.

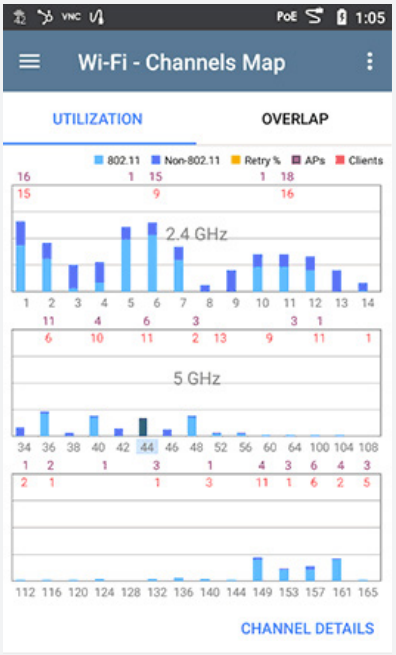
Unconnected Devices

It seems counter-intuitive that an unconnected Wi-Fi device could affect performance more than a connected device, but that's how Wi-Fi works. The problem is that Airtime, which can be defined as the time a Wi-Fi signal spends on the air, can be different for each Wi-Fi device. The reason is that Wi-Fi devices use a protocol called dynamic rate switching (DRS), which allows Wi-Fi devices to switch between different data rates as needed (data rates are the speed at which data is transferred over a communications channel). Normally DRS is a good thing for Wi-Fi because different devices may need different data rates. For example, when channel conditions worsen low data rate Wi-Fi traffic can remain successful even as high data rate traffic fails. Whether distance, walls, mobility, interference or something else

is causing unstable channel conditions, low data rates can allow a Wi-Fi connection to remain usable. Still, once different data rates are used, the Airtime used by each Wi-Fi device starts to change. Basically, since Wi-Fi uses half-duplex communications (only one device can transmit at a time) the entire Wi-Fi channel being used loses data capacity because the low data rate traffic takes up more Airtime while transmitting the same amount of data as devices using higher data rates.



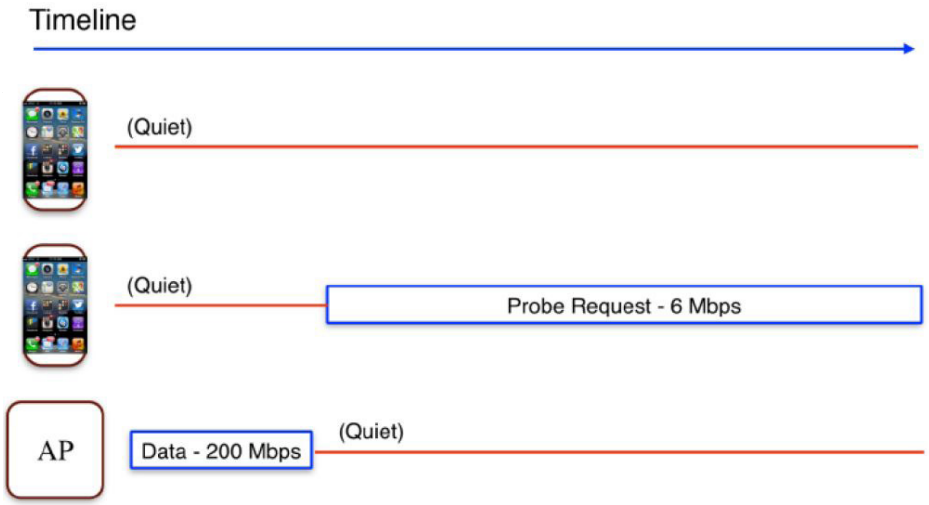
Example of Wi-Fi airtime usage. Devices using lower data rates take longer to transmit, which increases the time other Wi-Fi devices in the area must wait before they can transmit



Example of EtherScope™ nXG utilization channel map

So now that you know about Airtime and DRS you may be wondering what all that has to do with unconnected Wi-Fi devices. Well, this is where Wi-Fi probe requests come in. Wi-Fi probe requests are a type of Wi-Fi frame used by client devices to find AP's they can connect to. When Wi-Fi devices are unconnected, they send probe requests all the time because they are looking for a known Wi-Fi connection to use. Then when an AP that is part of one of the networks the client device is probing for receives the probe request it replies with information like SSID, type of 802.11 technologies supported, data rates supported, etc. and the Wi-Fi connection process starts. This technology was designed so your devices can connect to any know Wi-Fi networks (home, office, etc.) without requiring manual intervention. Meanwhile, when Wi-Fi devices are already connected to an AP, they only send probe request frames if they have initiated the roaming process. On this case the probe requests are used to find a new AP to connect to.

The problem with this methodology is that probe request frames always use low data rate transmissions, so the accumulated Airtime time taken up by probe requests sent by unconnected devices can often be greater than the accumulated Airtime time taken up by network data. Which means, when a client device sends a probe



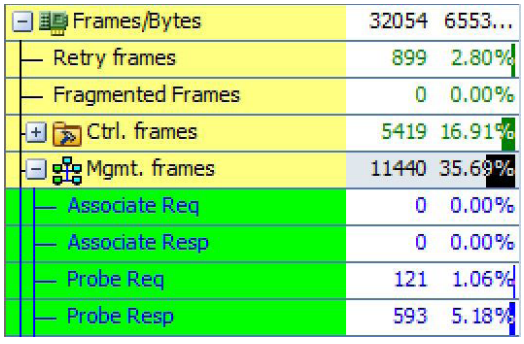
Example of probe requests taking a lot of Wi-Fi airtime, thus slowing down communications for other Wi-Fi devices

So, how do you find out if the number of probing requests generated by unconnected Wi-Fi devices is affecting the roaming performance of your network? The answer is simple, you just need a tool that allows you to track probe requests. There are a few tools out there that will provide this information, but it would be recommended to use a tool that simplifies this process by automatically counting the number of probe request on a channel and giving you that number. Also, when analyzing a Wi-Fi environment for Probe Request congestion, it is usually best to look for increasing numbers. If a device's Probe Request numbers perpetually increase, then that device is a contributor to the problem. If numerous devices show increasing numbers of Probe Requests, then a higher-level solution will be required.

Problems with unconnected devices affecting the roaming process are normally solved by having those devices connect to a guest network. As mentioned earlier, a connected device doesn't use as many probe requests frames, thus encouraging users to connect to a guest Wi-Fi network is the best way to mitigate the problem.

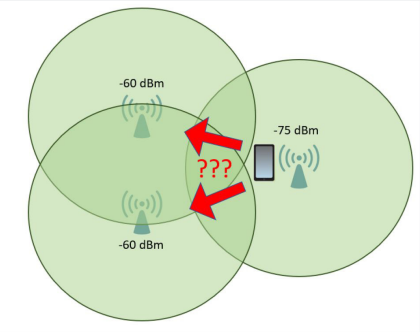
Congested Networks

Adding new APs to help improve coverage or performance on wi-fi networks seems to be the first step for most IT professionals; however,



Example of probe request count on a Channel provided on the AirMagnet WiFi Analyzer

adding new AP's could mess up the whole RF design, and result in network admins creating more problems than they are solving. As a new AP is added you increase the amount of signal overlap (signal of multiple AP's covering the same area), so you may end up having areas of your building on which you have a strong Wi-Fi signal coming from multiple AP's. As mentioned on the "Verifying Roaming Performance" section of this white paper client devices that are ready to roam will look for AP's with a strong signal to roam to, so what happens is that if a client device finds multiple AP's with a strong signal covering the same area it will have problems trying to decide which AP it should connect to (they all have a good signal). This will delay the roaming process, thus affecting the performance of the applications being used.



Example of a congested network, no more than two AP's covering the same area

Another thing that could happen when you have too many AP's covering the same area is excessive roaming. This happens when a client device keeps finding an AP with a stronger signal and thus keeps roaming constantly between AP's, thus preventing the client device from connecting to the network successfully.

Basically, having a congested network will cause you to have an excessive amount of coverage, which leads to roaming problems. So, how do you identify problems with congested networks? Well, you have a few simple options:

1) **Troubleshoot a Problem Area** – Troubleshooting roaming issues caused by a congested network in a known problem area is very simple. You only need a tool that will allow you to measure the signal strength of all the AP's on a specific area (many tools will provide this information). Measuring the AP's signal strength will allow you to confirm if there are any areas between AP's on which you may have a strong signal coming from more than two AP's (signal stronger than -65 dBm).

2) **Survey a Site** – Another option that is very popular is to survey an entire site instead of a single spot, and this is done by performing a site survey that will allow you to generate a graphical representation or heatmap of how your Wi-Fi network coverage looks like. 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 excessive coverage, noise levels, SNR, Data Rates, Retry Rates, Wi-Fi interference, non-Wi-Fi interference, and a lot more. Notice that it is highly recommended to perform a site survey after a new Wi-Fi network has been deployed (or new AP's have been added) 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 roaming problems in the future.

Roaming problems caused by a congested network have a simple solution: turn off some AP radios. Turn them into intrusion sensors, spectrum analyzers, capture radios or whatever else might be useful. Just make sure that enough of them get turned off so that no more than one AP has a significant signal in any given area.

Example of list of AP's and the signal strength provided on the AirCheck™ G2

AP Misconfiguration

AP controllers are great for configuration and management of many APs in a common network, but they are not perfect, and misconfiguration errors do occur. For example, if all APs on a network are not configured with the same basic settings, roaming will fail. Here are some of the settings you need to make sure are the same for each AP:

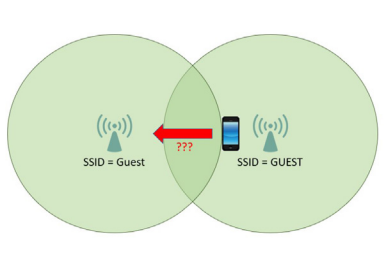
1) **SSID** – For a client device to roam successfully from one AP to another, all AP's need to be transmitting the same SSID. Notice that spelling of the SSID on all AP's needs to be the same. Typos or even differences between upper case and lower case will cause the roaming process to fail since the client device will think the AP's are part of different networks.

2) **Type of Security** – Make sure that the type of security being used by each SSID is configured the same way on each AP. For example, if you have an SSID called GUEST that is using WPA2-P for security, the same setting needs to be applied to all AP's on your network. If different types of security settings are used for the same SSID the roaming process will fail. Basically, even if the client device tries to connect to a new AP, since the security type being used is different it won't be able to re-authenticate.
   a. Notice that many AP controllers this days have proprietary technologies that allow them to skip the re-authentication process while roaming. This is done to accelerate the roaming process (fast roaming).

3) **Security Credentials** – Besides making sure that each SSID is using the same type of security on each AP you also need to make sure the same security credentials are being used. For example, if you have an SSID called GUEST that is using WPA2-P security and on which the passphrase is ACKG2, then all AP's should use the same security credentials. If for some reason the security credential between AP's don't match then re-authentication will fail, thus causing the roaming process to fail.

4) **Hidden SSID** – Some client devices may have problems roaming while you are using a hidden SSID. This could happen if all AP's are using a hidden SSID, but is worst when some AP's are configured to use a hidden SSID while other AP's are transmitting the SSID. This client devices seem to take longer finding hidden networks or just don't like hidden networks, thus will cause the roaming process to fail.

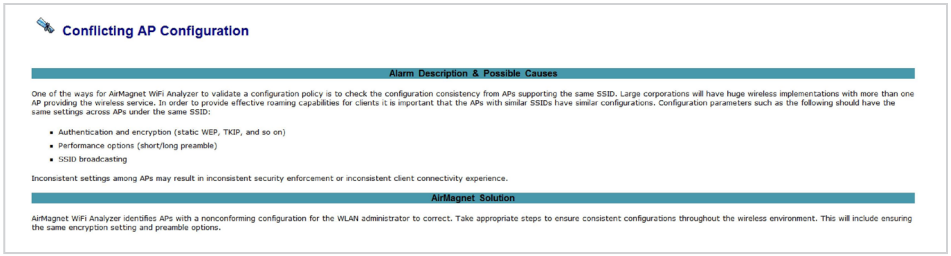
a. Note that this does not apply to every client device. Many client devices will roam without a problem even if hidden SSID's are used.



Example of conflicting AP configuration, different SSID's cause roaming to fail

Additionally, if the transmit power configured on the AP's is too high, then a client device will remain connected to an AP when it should be roaming to another AP (sticky client syndrome). A best practice in Wi-Fi is to have a secondary AP coverage overlapping with a primary AP coverage (on a different channel) and with sufficient signal levels (e.g., above -67 dBm). If a second AP of sufficient signal level is not present in a coverage area, a client device may not roam.

As for how to identify AP configuration problems, the easiest way is to use a tool that will allow you to confirm that all AP's on your network are configured the same way. At a minimum this tool should provide visibility on the SSID, security type, and transmission setting (hidden SSID or not) being used by each AP on your Wi-Fi network. Better yet, the tool you decide to use should detect AP configuration problems automatically.



Example of conflicting AP configuration problem automatically detected using AirMagnet WiFi Analyzer

AP configuration problems are easily resolved by using your AP controller to provide the same settings to each AP. If multiple controllers are being used to manage different AP's, then making sure that each AP controller is using the same configuration should help resolve any Wi-Fi roaming problems that were detected.

CONCLUSION

In conclusion, Wi-Fi roaming 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 Wi-Fi roaming problems quickly and easily. Which is why NetAlly strives to provide the best Wi-Fi troubleshooting tools on the market. Anything from Survey tools that help you identify coverage problems, to software or handheld troubleshooting tools that allow you to identify excessive probing, detect network congestion, find configuration problems, and lots more!