7SIGNAL®
THE WI-FI PERFORMANCE COMPANY

WHITEPAPER

MYSTERIES OF Wi-Fi ROAMING REVEALED

Understand Wi-Fi roaming problems so you can solve them

Table of Contents

The realities of client roaming on wireless LANs (WLANs) can create major headaches for the enterprise. In this paper, we explain how roaming works and how you can discover roaming problems on a wireless network. We begin with an explanation of roaming basics and then move on to explore client decision factors as roaming is nearly always a decision of the client. Next, we explore the great variation in client behaviors and how this impacts your design and troubleshooting decisions. We then show the features of 7signal's Wi-Fi Performance Management System that can assist in roaming problem detection and problem resolution.

Basics of Roaming

Roaming in WLANs is most often a reference to the process used when a client disassociates with one access point, or a basic service set (BSS) and reassociates with another access point (AP) in the same Extended Service Set (ESS). These APs in the ESS are interconnected with a distribution system – typically Ethernet connections. This section defines roaming in detail, connection metrics related to roaming, and coverage requirements needed for proper roaming operations. An additional form of roaming, sometimes called inter-ESS roaming, is not considered here as it is not the commonly desired roaming type in enterprise deployments.

Roaming Defined

The roaming process includes monitoring signal strength and other factors, scanning for other APs qualified as roaming targets, parsing the discovered APs, and then reassociation to the selected target AP. Each of these basic steps is defined below:

- Monitoring Signal Strength: The mobile device will monitor the signal strength of the current connection. If it gets below a specific threshold, it will begin seeking other APs that are potential roam candidates.

- **Scanning for Qualitied Roaming Targets:** The mobile device will either look at beacon frames on channels supported by the regulatory domain and the chipset in the device, or send probe requests on the channels, or both. This may occur only after the minimum Received Signal Strength Indicator (RSSI) threshold is reached or at all times depending on the proprietary algorithm utilized by the mobile device.
- **Parsing Discovered APs:** After scanning and retrieving a list of APs, the client must gather the retrieved information into a logical order of best targets and select the appropriate AP to which to roam. The decision to select a given AP may vary by client device. Some will simply choose the strongest signal in the current band and some may scan other bands as well. Sadly, such capabilities and decisions are not always well-documented (in fact, they typically are not).
- **Reassociation with the Target AP:** Finally, the mobile station should perform a roam to the target AP, which includes authentication and association (and may include additional tasks depending on the network security implemented).

Connection Metrics

You should be familiar with several metrics are important to the roaming process. These include:

- **Signal Strength:** Reported in dBm (decibels to milliwatt) or RSSI (Received Signal Strength Indicator) values, signal strength is a measure of power in the received wireless signal. Clients use this to qualify APs as roam targets and to determine when roaming should be initiated.
- **SNR:** The signal-to-noise ratio (SNR) is a measurement of the variance between the power of a received signal and the RF energy in the environment (the noise floor). The SNR is used in data rate selection and may be used by APs to reject probe requests based on low SNR values. SNR is typically represented as a decibel (dB) value. For example, if the noise floor is at -95 dBm and a signal is as -75 dBm, the SNR would be 20 dB.

- **Data Rate:** This is the rate at which bits are sent across the wireless medium. It should not be confused with throughput, which is typically measured at Layer 4 (TCP and UDP traffic). The data rate is often a factor in client roaming decisions, thus important to understand.
- **Retries:** When a wireless station does not receive an acknowledgement for a transmitted frame, it resends the frame. This action is called a retry. High retry rates may trigger a roaming scan. In addition, they may also trigger data rate shifts to lower data rates. Again, this depends on the algorithms developed by the manufacturers of APs as well as client devices.
- **CRC errors:** The frequent sibling to a retry is a CRC error. CRC errors occur at the receiver, while retries occur at the transmitter. High CRC errors may also result in a roaming scan initiation. The assumption is that the client device is receiving corrupt frames from the AP and another AP may be able to provide better communications to the client.

Preemptive vs. Roam-time Discovery

Many vendors reference roaming as either preemptive or roam-time[i]. With preemptive roaming, the client scans for potential target APs before the actual roam-time occurs. Alternatively, when a client performs roam-time discovery, the client scans for potential target APs only after it has determined that it must roam. The difference is in the gap between a scanning threshold and a roaming threshold.

The scanning threshold is typically triggered based on signal strength, missed beacons or both. When this threshold is breached, the client will scan for potential target APs; however, it will not actually roam to a target AP until another threshold is crossed – the roaming threshold. The roaming threshold may simply be that the target AP now has an equivalent signal strength to the current AP (the assumption of advancement in mobility) or it may be that the target AP has some measure of greater strength than the current AP (the use of hysteresis, discussed later in this paper).

Clients that perform roam-time discovery will **not** look for another AP until they determine that they must roam. As such, these tend to become sticky clients and these algorithms should be avoided in client implementations. However, many still exist, therefore, they must be considered in WLAN design, management and monitoring. In addition to the stickiness problem, clients that perform only roam-time discovery are also likely to lose connection to the current AP before gaining access to another. This behavior results in poor WLAN quality and possibly dropped higher layer connections, including streaming voice or video communications.

For example, the default drivers for Linux often result in sticky clients as they place great emphasis on the missed beacons metric. With this metric used as the only measure or primary measure, clients wait far too long before connecting to another AP. Thankfully, most adapter drivers heavily modify the default driver and this algorithm is one key area of modification.

Coverage Requirements

If roaming is to work effectively, the WLAN must be designed with coverage overlap. If APs are spaced too far apart, the client will not have another AP to which it can roam before the connection is lost to the existing AP. For this reason, many vendors make recommendations such as placing indoor APs approximately 50 feet apart; however, such recommendations must be coupled with an understanding of AP output power and antenna gain. It’s possible to set the output power too low, even at 50 foot spacing, such that walls and other materials attenuate the signals and result in improper coverage. Therefore, good design, post-deployment validation surveys, and continuous WLAN monitoring are key to an effective implementation that allows for seamless client roaming.

Figure 1 illustrates the importance of coverage. The client can roam successfully from access point A to access point B, but would fail when roaming from AP B to AP C. Of course, the assumption is that some mobile path physically exists between APs B and C, but if it does, this coverage design will not accommodate roaming. Good site survey tools and monitoring solutions will reveal such gaps in coverage.

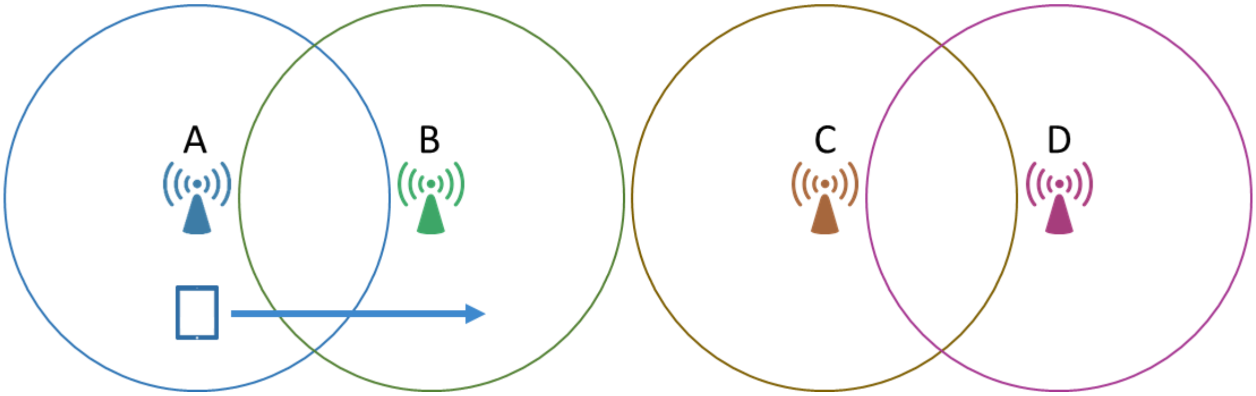


Figure 1: Roaming and Coverage

Roaming Times

The final issue addressed here is that of roaming times. It is important for upper layers of the OSI model that roam times be minimized as much as possible. If roaming is working properly, you should see roam times in the following ranges:

> *NOTE: Given that the primary topic of this whitepaper paper is roaming and not actual performance or capacity while connected to an AP, the focus here is on coverage. Capacity is an equally important factor in WLAN design and proper roaming assists in providing sufficient capacity as well.*

- 10-20 ms for open networks
- 20-35 ms for pre-shared key (PSK) networks

- Goal of <150 ms for 802.1X/EAP networks

The reason that 802.1X/EAP networks are referenced with a goal is because the roaming feature of the infrastructure will determine whether you can reach that goal or not. Such solutions are beyond the scope of this paper, but include Opportunistic Key Caching (OKC), preauthentication, PMK caching and 802.11r Fast BSS Transition (FT).

OKC, preauthentication, PMK caching and 802.11r FT are all roaming solutions that assist with secure roaming. In secure roaming, encryption key management becomes a factor. This is particularly true with 802.1X/EAP, as roaming would require a full EAP authentication process and 4-way handshake to generate encryption keys on every roam. This entire process can take seconds or at least hundreds of microseconds, and this is far too long for real-time applications. OKC and 802.11r FT are common solutions to this problem – both cache and/or share authentication information so that only a 4-way handshake is required at roam time. When using pre-shared keys, the problem is not significant as only the 4-way handshake is required on each roam.

Most modern infrastructure solutions support these technologies and they should be implemented to reduce roaming times. The 150 ms metric is based on the fact that real-time applications like Voice over IP (VoIP) require a one-way latency of 150 ms or less.

Client Decision Factors

Now that you understand roaming basics, it is important to explore the various methods used by clients when deciding to roam. Indeed, the factors vary greatly between client devices and this variance will be addressed in the next section. Here, the common decision factors are explained to illustrate the many options available to clients for roaming control. Figure 2 illustrates the common roaming decision factors.

Missed Beacons

A surprising metric used by some clients is missed beacons. Beacon frames are transmitted from APs, by default, every 102.4 ms. These beacons include information about the basic service set (BSS) offered by the AP. Clients use beacons for initial connection and power management functions once connected. For some clients, when a specific number of beacons have been missed (due to corruption or the simple fact that the client is too far away to receive them), the roaming process is triggered. Using this metric alone is quite problematic as it would mean that, without the presence of excessive interference, clients wait to roam until they are literally outside the boundary of the minimum data rate in the BSS. This is represented in Figure 2 with the Minimum Basic Rate Signal line showing an extreme roam point that would not be sufficient for real-time applications, or for many other applications for that matter. Thankfully, most clients that use the missed beacons metric (often called the missed beacon threshold or simply the beacon threshold) use it in conjunction with other metrics.

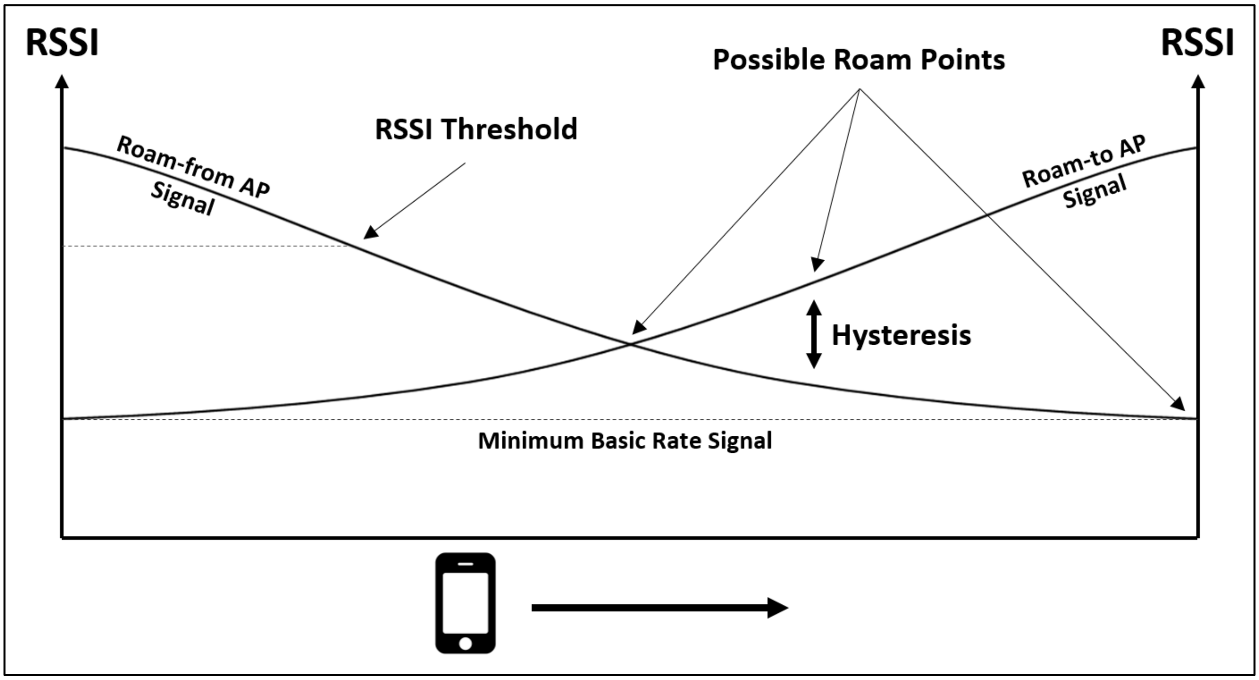


Figure 2: Roaming Decision Factors Illustrated

An additional use of missed beacons is the move away from a BSS because of localized interference near the client. For example, the client may be on Channel 1 in 2.4 GHz and have a signal strength of -62 dBm from the AP. However, if an interfering device is communicating on that same channel, such as a non-802.11 video transmitter, it may cause the client to miss several beacon frames from the AP. In such a scenario, while other clients further from the video transmitter may be operating effectively, this client may benefit from roaming to another AP.

Signal Strength

Signal strength, typically represented in dBm or RSSI, is used as a roaming threshold. When a client receives frames from the AP falling at or below the threshold, it will initiate a scan to locate alternate APs in the same extended service set (ESS). RSSI, in this case, is used colloquially and not as defined in the 802.11 standard. Many vendors use the term RSSI to be synonymous with dBm, although the two are technically different. RSSI is defined as a variable value in a range of 0-255 that is representative of the signal strength. However, some vendors choose the maximum value, some may choose 100 while others chose 255, which results in inconsistent values[ii]. For this reason, RSSI has come to be used more colloquially than technically in WLAN signal strength discussions.

As an example, many Apple® devices watch for frames with a signal strength below -70 dBm and begin scanning for alternate APs at this point[iii]. The roam does not actually occur unless a minimum hysteresis is met, but the scanning begins at this point. Signal strength is a major factor in all WLAN client decision algorithms.

Frame Retries

Frame retries provide a useful metric as it can cause a client device to roam to an alternate AP when a hidden node problem exists. Hidden nodes exist when two clients can both process the frames from the AP, but they cannot process each other's frames (among other hidden node scenarios). Such a scenario can cause frame corruption at the AP resulting in retries at the clients. If the roaming algorithm includes a frame retry threshold, the client may roam away.

NOTE: If missed beacons or frame retries are used to trigger roaming and a hysteresis is still required, the client may not roam away. Vendor algorithms should consider this factor when implementing roaming algorithms. A struggling client (one that cannot communicate effectively on its existing BSSID association) should be allowed to roam to another BSS even if the new BSS has a lower signal strength by some acceptable margin.

Hysteresis

Hysteresis is a reference to the difference in signal strength between a potential target AP and the currently associated AP. It is sometimes called the roam delta. A minimum hysteresis must be met before a client will roam to the new AP in clients that use this value. Apple clients often use this value. According to Apple, when operating in an enterprise WLAN, iOS devices use a hysteresis of 8 dB when actively transmitting and 12 dB when idle[iii]. Therefore, given a current association signal strength of -73 dBm, the device would only roam to another AP if the signal strength as -65 dBm for clients transmitting data or -61 dBm for clients currently idle. Figure 2 illustrates the hysteresis point in roaming algorithms.

It is important to remember that these values are used in the Apple algorithm referenced, but they are not the values used by all Apple devices and certainly not used for all non-Apple devices. This variation in client behaviors is addressed next.

Hysteresis is used to prevent AP jumping. AP jumping occurs when a client is on the perimeter of two AP cells and it roams back-and-forth between the two APs frequently. Having a 3 dB or greater hysteresis helps to prevent this behavior. However, at the same time, if the hysteresis is set too high, clients may not roam early enough. In nearly all cases a value of less than 15-20 dB should be used.

Variation in Client Behaviors

As stated previously, clients vary greatly in the algorithm used for roaming decisions. This is due, in part, to the fact that no real standard exists for this component of 802.11 communications. This section addresses these variations and includes some explanation of the issues that it may cause[iv].

Signal Strength vs. Connection Maintenance

One key area of device variance is in the primary methodology of the roaming algorithm selected by the vendor. Good algorithms are based on signal strength and poor algorithms lean more toward connection maintenance. The connection maintenance algorithms simply accept the current connection until it is no longer working (for example, looking at only missed beacons or a lost connection). Such algorithms result in sticky clients and are slowly being removed from the device pool as vendors are more aware of the importance of roaming. Many such devices were designed for the consumer space where it was assumed that one AP would be used; however, these devices made their way into the enterprise space and as a result, many vendors are moving away from such algorithms.

Signal-based algorithms use the signal strength as the trigger threshold to determine when roaming should occur. They monitor the signal strength of the current connection continuously and, if it falls below a threshold, they either initiate a roam or a scan for a potential future roam. The best algorithms scan early and roam later, resulting in better connections in most cases.

Band Roaming

Band roaming is a reference to roaming between bands, for example, between the 2.4 GHz and 5 GHz bands. If a client supports this, it will scan for APs in the alternate band to which it is already associated. Some clients do not support this and it can be a key factor in roaming issues. Because band roaming requires scanning many more channels (all channels supported by the client in both 2.4 GHz and 5 GHz), it is important to implement 802.11k on the infrastructure so that clients supporting it can take advantage of it.

With 802.11k enabled, supporting clients can request a neighbor report from the currently associated AP. This action is often taken just after initial association. The neighbor report includes the APs that can be seen by the associated AP and their signal strengths (as seen by the AP). The client can then send probe requests only on those channels to minimize scan times.

Initial access point selection for a client is usually based solely on signal level. If the 2.4 GHz signal level is stronger than the 5 GHz level, then the client may first try to associate to the 2.4 GHz radio. Even if 2.4 GHz and 5 GHz radios in the same access point are both set to the same power level, the 2.4 GHz signal level will appear clearly stronger to the client. The difference may be around 6-8 dBs. This is due to the 5 GHz band’s higher frequency, shorter wavelength and differences in signal propagation, as well as antenna operation. In order to have clients connect immediately to the 5 GHz band, the 2.4 GHz radio signal transmit power setting should also be set 6-8 dB below the 5 GHz radio transmit power level. This makes 5 GHz services appear most promising to the client during its initial scan. However, coverage aspects should not be overlooked when making this type of change.

Many organizations implement band steering, which is a technology that encourages clients to associate with 5 GHz APs whenever available. Band steering is implemented because many more channels are available in 5 GHz than in 2.4 GHz and the band can therefore support more clients in a given coverage area. The network must be carefully designed when using band steering so that 5 GHz APs are readily available in all coverage areas. If not, roaming may be delayed for unacceptable durations, resulting in dropped calls, lost connections and poor overall WLAN performance.

Thresholds Measured

Clients use varying measures to determine when to roam as well. The following metrics are often used in the decision process as detailed earlier in this paper.

- Missed beacons – some number of beacon frames not received during the scheduled delivery times.
- Disassociation – loss of connection.
- RSSI – the signal strength of the frames received in the current association.
- Retries – the number of frames requiring retries to be successfully transmitted.
- CRC Errors – the number of errant frames received from the current association.

Configuration Settings

Finally, clients offer some configuration settings related to roaming. These include aggressive roaming, roaming enablement and band preference. In most cases, only laptops and desktops expose these settings while other mobile devices (tablets, smartphones, etc.) do not.

- Aggressive Roaming: This setting will adjust the thresholds lower or higher. It does not reveal the actual thresholds used and, in many tests, seems to have no impact on the results. At best, this setting can be adjusted to discover if improved results can be achieved.

- Roaming Enablement: Some devices allow you to disable roaming completely. This setting may be useful for some stationary Wi-Fi clients, but is nearly always left in the enabled state for enterprise deployments.
- Band Preference: Some devices allow you to indicate a preference for either the 2.4 or 5 GHz bands. In most cases, this should be set to the 5 GHz band. Others allow you to disable one band or the other. However, in enterprise deployments, neither band should be disabled.

NOTE: Many adapters are sold as dual-band, but upon closer inspection you will discover that the 5GHz band does not work consistently out-of-the-box. In such cases, using an updated driver will often resolve the issue.

APs also offer configuration settings that can impact roaming. These include probe response thresholds, band steering and 802.11k support.

- Probe Response Thresholds: This threshold can be set so that an AP will only respond to a probe request if the received frame is above a specified signal strength or has a minimum SNR. The result is the prevention of probe responses to clients that should not associate.
- Band Steering: Enabling this feature may assist more clients in locating 5 GHz radios for association. However, it should be tested, as some implementations result in longer roam times.
- 802.11k Support: This should be enabled on any APs that support it so that any associated clients can use the provided neighbor reports to reduce roaming scan times.

Discovering Roaming Problems

7signal is currently developing a new Wi-Fi roaming test, which would move sensor connections between APs and measure roaming delays. We see this as an important new feature, which would allow enterprises to continuously benchmark Wi-Fi roaming performance and behavior offered by a network.

In addition to this coming enhancement, the following existing views will be helpful in analyzing potential roaming problems.

Beacon Availability

For roaming to happen, access points have to send beacons and respond to probe requests from clients. Sometimes access point radios may stop beaconing even if their central processor runs well. Access point software may not be aware of an issue with the radio. Beacon availability metrics help ensure that all access points are detectable by client devices.

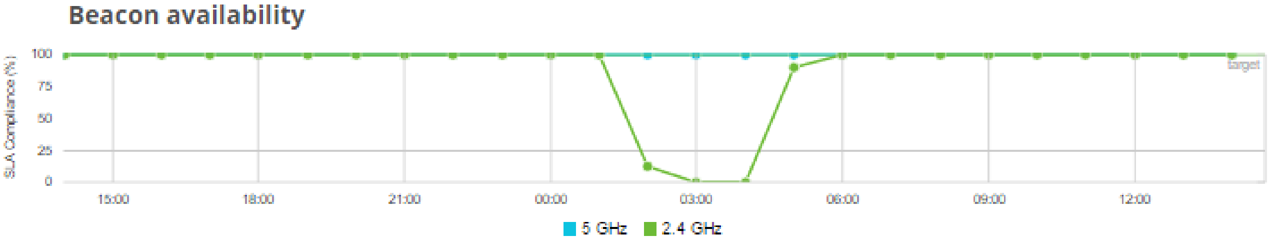


Figure 3: Access Point Beacon Availability KPI in 7signal EyeQ™

Data and Throughput Rates

Throughput rates cannot be greater than the data rate, but the throughput rate is often more important than the data rate. Why is this? If you have an acceptable data rate for your connection, but have excessive retries or a congested channel, the throughput will be minimal. Overloaded channels result in poor throughput for each user. If too many clients are sticking to an AP, instead of roaming away, the performance will be degraded. For this reason, 7signal reports have a greater focus on throughput than on data rates. Figure 4 shows some of the throughput views available to help you troubleshoot roaming and other performance issues.

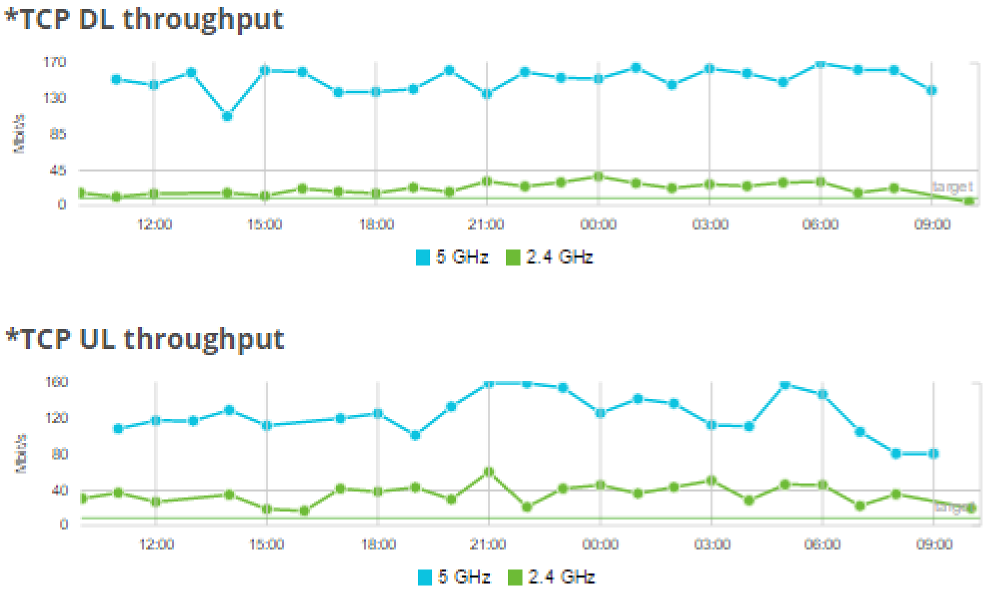
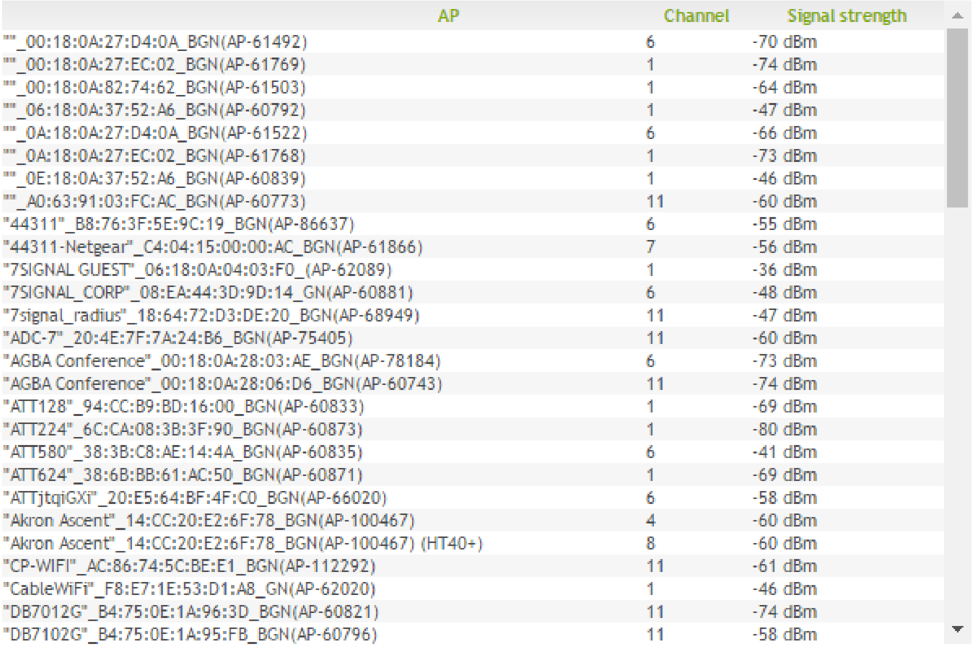


Figure 4: Throughput Measurements

Signal Strength

The Channel Values table shows all APs seen by the Sapphire Eye WLAN performance sensor and the metrics for those APs, as shown in Figure 4. This information can be used to ensure that sufficient APs at acceptable signal strengths are available for clients to select as roaming targets. If an area is discovered without sufficient coverage, the WLAN should be re-engineered to resolve the problem. The resolution may be as simple as changing output power settings on APs or it may require the installation of additional APs. While this issue may have initially been addressed during the WLAN design, due to the fact that many WLANs evolve over time, a view like this can be quite helpful.



AP	Channel	Signal strength
""_00:18:0A:27:D4:0A_BGN(AP-61492)	6	-70 dBm
""_00:18:0A:27:EC:02_BGN(AP-61769)	1	-74 dBm
""_00:18:0A:82:74:62_BGN(AP-61503)	1	-64 dBm
""_06:18:0A:37:52:A6_BGN(AP-60792)	1	-47 dBm
""_0A:18:0A:27:D4:0A_BGN(AP-61522)	6	-66 dBm
""_0A:18:0A:27:EC:02_BGN(AP-61768)	1	-73 dBm
""_0E:18:0A:37:52:A6_BGN(AP-60839)	1	-46 dBm
""_A0:63:91:03:FC:AC_BGN(AP-60773)	11	-60 dBm
"44311"_B8:76:3F:5E:9C:19_BGN(AP-86637)	6	-55 dBm
"44311-Netgear"_C4:04:15:00:00:AC_BGN(AP-61866)	7	-56 dBm
"7SIGNAL GUEST"_06:18:0A:04:03:F0_(AP-62089)	1	-36 dBm
"7SIGNAL_CORP"_08:EA:44:3D:9D:14_GN(AP-60881)	6	-48 dBm
"7signal_radius"_18:64:72:D3:DE:20_BGN(AP-68949)	11	-47 dBm
"ADC-7"_20:4E:7F:7A:24:B6_BGN(AP-75405)	11	-60 dBm
"AGBA Conference"_00:18:0A:28:03:AE_BGN(AP-78184)	6	-73 dBm
"AGBA Conference"_00:18:0A:28:06:D6_BGN(AP-60743)	11	-74 dBm
"ATT128"_94:CC:B9:BD:16:00_BGN(AP-60833)	1	-69 dBm
"ATT224"_6C:CA:08:3B:3F:90_BGN(AP-60873)	1	-80 dBm
"ATT580"_38:3B:C8:AE:14:4A_BGN(AP-60835)	6	-41 dBm
"ATT624"_38:6B:BB:61:AC:50_BGN(AP-60871)	1	-69 dBm
"ATTjtqiGXi"_20:E5:64:BF:4F:C0_BGN(AP-66020)	6	-58 dBm
"Akron Ascent"_14:CC:20:E2:6F:78_BGN(AP-100467)	4	-60 dBm
"Akron Ascent"_14:CC:20:E2:6F:78_BGN(AP-100467) (HT40+)	8	-60 dBm
"CP-WIFI"_AC:86:74:5C:BE:E1_BGN(AP-112292)	11	-61 dBm
"CableWiFi"_F8:E7:1E:53:D1:A8_GN(AP-62020)	1	-46 dBm
"DB7012G"_B4:75:0E:1A:96:3D_BGN(AP-60821)	11	-74 dBm
"DB7102G"_B4:75:0E:1A:95:FB_BGN(AP-60796)	11	-58 dBm

Figure 5: Channel Values Table in 7signal Analyzer

Retries/CRCs

When client devices have to retransmit frames, throughput is reduced. Clients with high retransmission rates should be roaming away, if they have a target to which they can roam. The 7signal EyeQ™ dashboard shows the retries from the AP to the client and from the client to the AP. If you see high retry rates on a consistent basis (above 10-20%), consider a redesign of the power plan or location of Aps. Also ensure that target APs are available to which the clients may roam. Figure 6 shows the retransmission view in EyeQ™.

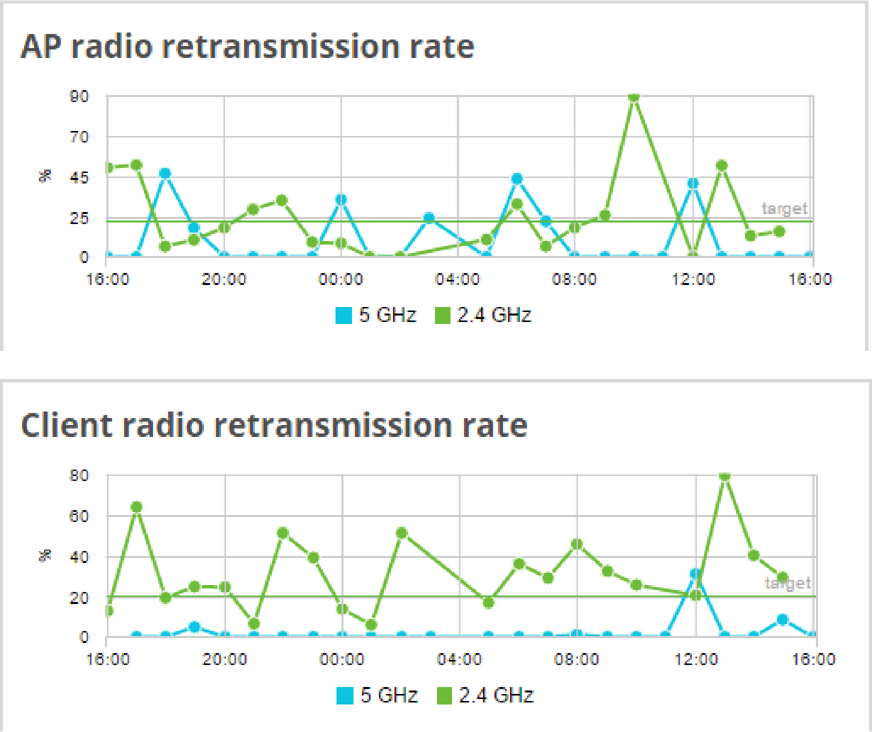


Figure 6: Retries in the 7signal EyeQ Dashboard

Association Time

The Radio Association Time section of the dashboard shows the time it takes for an association to an AP to complete. This can be an important metric for roaming as association is part of every roaming process. Figure 7 shows this view.

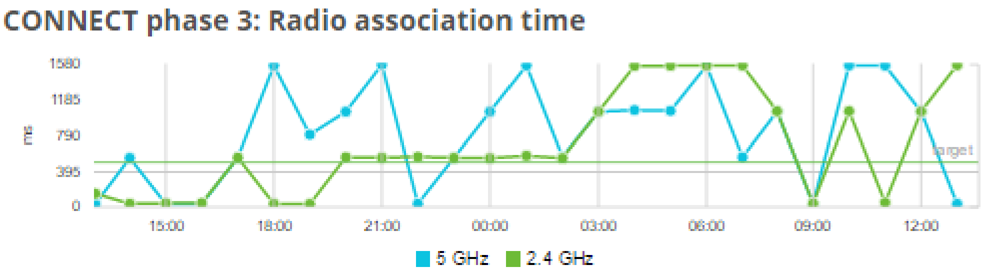


Figure 7: Radio Association Times

Number of Clients

An additional important metric is the number of clients associated with each AP. 7signal can provide this information in their EyeQ™ dashboard as well. If too many clients are associated to an AP, configuration changes may be required to encourage some clients to roam to an alternate AP. Figure 8 shows this view in the dashboard.

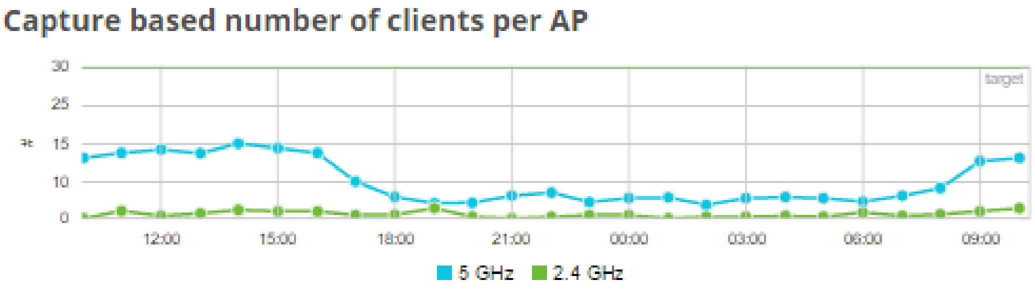


Figure 8: Number of Clients Per AP

Conclusion

In conclusion, the resolution of roaming issues comes down to three primary factors: WLAN design and configuration, client selection and client configuration. A monitoring solution, such as 7signal EyeQ, allows you to locate problem areas and resolve roaming issues that may or may not have been reported.

About 7signal

7signal develops cloud-based Wi-Fi performance management software that enables enterprises and service providers to manage the Wi-Fi user experience on their networks, against Wi-Fi performance Service Level Agreements. 7signal sensors and mobile apps collect Wi-Fi performance data across the enterprise and the 7signal analytics engine presents the data as Key Performance Indicators in a browser dashboard, giving network administrators immediate visibility of Wi-Fi health and performance, enterprise-wide. The system enables businesses to significantly improve Wi-Fi baseline performance without adding access points, reduce troubleshooting 80-90%, and lower the total cost of ownership of maintaining reliable, high performance WLANs.

[i] Wireless LAN Fundamentals: Mobility – http://www.ciscopress.com/articles/article.asp?p=102282&seqNum=2

[ii] CWNA Certified Wireless Network Administrator Official Deluxe Study Guide: Exam CWNA-106 by David D. Coleman and David A. Westcott

[iii] Wireless Roaming Reference for Enterprise Customers – https://support.apple.com/en-us/HT203068

[iv] Additional roaming solutions for internetworking with non-802.11 networks or 802.11 networks other than the currently associated WLAN are available based on 802.11u and Hotspot 2.0. They are beyond the scope of this paper. In addition to the roaming factors presented in this paper, authentication is a key factor in roaming time estimation. When key caching or pre-authentication of some form is not used, roaming times are excessive and will cause problems for real-time communications. Finally, solutions from vendors like Cisco provide for assistance in roaming through the enhancement of the 802.11 standard (Cisco Compatible Extensions (CCX)) on certified devices. However, Cisco states that, “Even though a wireless client may be CCX compatible, it may still rely on 802.11k or its own proprietary roaming algorithm instead of the CCX triggers.” Additionally, a Cisco infrastructure is required for this to work, when it does. Ultimately, today, the best solution to roaming problems is a well-designed WLAN and a powerful monitoring and management solution.