Troubleshooting WLAN Issues

AirWave Help Desk Guide

Wireless LAN Troubleshooting for the Help Desk

In a typical IT organization, it is the Help Desk's job to take incoming user support calls and determine whether the problem is an individual client/device issue or a broader network issue that might affect multiple users. The Help Desk itself is usually responsible for handling the individual user problems, while escalating broader network issues to the Network Engineering or Network Operations team.

With wireless networks, most user complaints boil down to one of two observable problems:

- The wireless network is slow.
- I cannot connect to the wireless network.

Of course, there are literally hundreds of different potential root causes for either of these two symptoms. Many, if not most, of these problems are related to the client device settings or authentication issues, which should be handled by the Help Desk. Yet, when the Help Desk does not have the tools and diagnostic capabilities to perform this 'triage,' most issues are instead escalated directly to Network Engineering. The result is not pretty: users are unhappy because their problems are not resolved quickly; the Help Desk staff becomes frustrated because they cannot do their jobs; and Network Engineers suffer because they are swamped with wireless related calls.

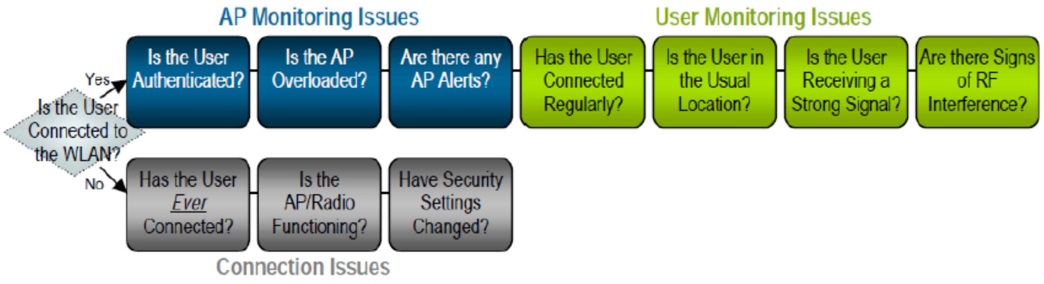
The AirWave Wireless Management Suite™ (AWMS) provides an end-to-end wireless operations management solution for the entire IT staff, from Network Engineering to the Help Desk. This quick reference guide is designed specifically to enable the Help Desk staff to:

Distinguish between common user/device problems and network issues:

- Diagnose and resolve client issues
- Gather useful information to enable faster problem resolution when issues must be escalated to network engineering.

Most of these steps can be performed in minutes with read-only access to the AirWave Management Platform™ (AMP) software, usually while the end user is still on the telephone. The basic troubleshooting workflow process for the Help Desk is depicted in the following image:

Figure 1: *Basic troubleshooting workflow*


AP Monitoring Issues
User Monitoring Issues
Is the User Connected to the WLAN?
Yes
No
Is the User Authenticated?
Is the AP Overloaded?
Are there any AP Alerts?
Has the User Connected Regularly?
Is the User in the Usual Location?
Is the User Receiving a Strong Signal?
Are there Signs of RF Interference?
Has the User *Ever* Connected?
Is the AP/Radio Functioning?
Have Security Settings Changed?
Connection Issues

Troubleshooting Steps

Basic troubleshooting can be summarized in four steps:

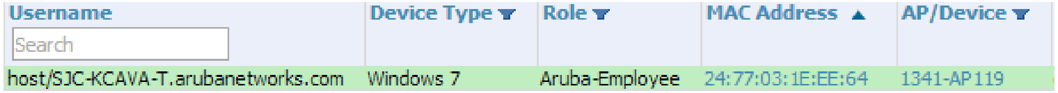
- "Step One: Determine Whether the User is Connected" on page 2
- "Step Two: Check for Network-Related Issues" on page 2
- "Step Three: Examining User Information" on page 4
- "Step Four: Using Location Information, RF Heatmaps, and Frames/Sec" on page 6

Step One: Determine Whether the User is Connected

The first step in the troubleshooting process is to determine whether the user is actually connected to the wireless network.

1. **Search by Username**: Ask the user for his/her username, and enter it into AMP’s Search box.
2. **Determine the user’s connection status**: Verify whether the user is currently connected to the WLAN. If the user is currently connected, the username and session information will be shaded in green on AMP’s Search Results page. If the user is not connected, the information will not be shaded, and the username will be italicized,.

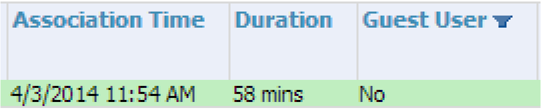
Figure 2: *Shading indicates that the user is connected; italics indicate the user is not connected*



Username	Device Type ▼	Role ▼	MAC Address ▲	AP/Device ▼
Search				
host/SJC-KCAVA-T.arubanetworks.com	Windows 7	Aruba-Employee	24:77:03:1E:EE:64	1341-AP119

- If the user is currently connected, click on the MAC Address link to open the diagnostic page for that client. Proceed to "Step Two: Check for Network-Related Issues" on page 2.
- If the user is not currently connected, check the search results to determine whether that user has ever successfully connected to the WLAN. (The most immediate previous connection - if any - will be listed in the search results but will not be highlighted in green.)
  - If the user has not connected before: The Help Desk may need to assist the user in configuring whatever security and other settings are required to connect to the WLAN.
  - If the user has connected before: Scroll to the right along the table to check the Association Time field, and determine when the user most recently connected, as shown in the following image.

Figure 3: *Check the last association time for the downed client.*



Association Time	Duration	Guest User ▼
4/3/2014 11:54 AM	58 mins	No

- If the user has connected recently: Verify verbally that the user is in his or her usual location. Proceed to "Step Two: Check for Network-Related Issues" on page 2. If you do not have a dense AP environment with overlapping coverage areas, a down AP can be the source of many end user trouble tickets.
- If the user has not connected recently: Determine whether the user has changed hardware recently or whether your organization has changed security policies, passwords, etc. since his or her last connection. Many organizations are migrating from WEP to WPA or WPA2. Intermittent or infrequent wireless network users may not be aware of changes to security policies that can affect their ability to connect to the network.

WARNING

If AMP does not show that the user is connected to your wireless network, but the user reports that he/she has network access, the user could be connected to a rogue access point or unauthorized ad hoc network. In this case, the Help Desk should instruct the user to contact Network Engineering if connected to the right SSID.

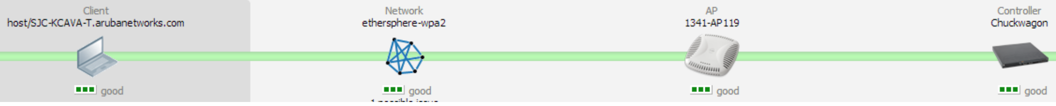
Step Two: Check for Network-Related Issues

1. **Verify that the user is connected to the AP**: After verifying that the user is connected to the wireless network, verify that the user is connected to the access point. Click on the user's MAC address. This takes you to the Diagnostic page for the client. If the user is connected, then this page includes the current connection table, as shown in the following table.

NOTE

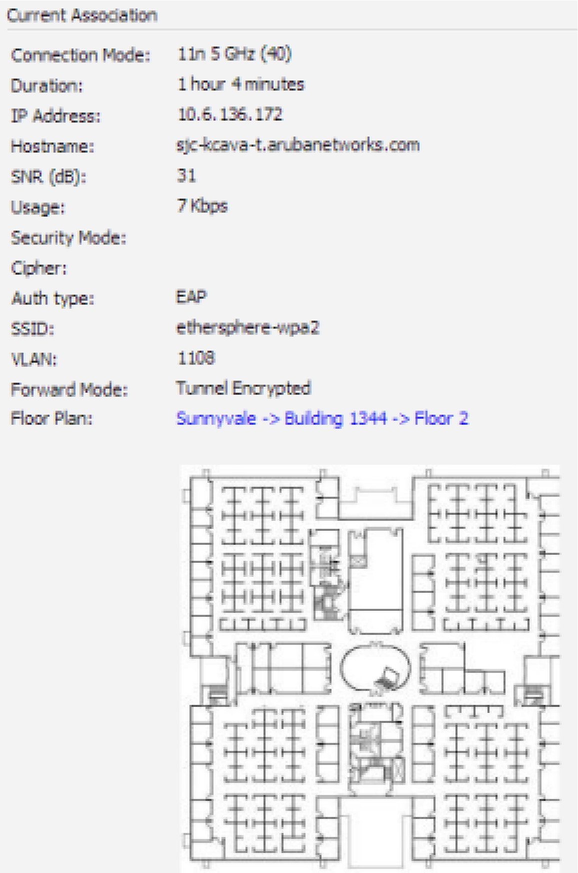
If the user is no longer connected, then selecting the MAC address link will take you to the Device Info page for the selected client rather than to the connection table.

Figure 4: *Network information*



2. **Verify that the user is authenticated**: Review the Current Association information in the left navigation pane on this page. Determine whether the user is currently authenticated by checking the Auth Type field and by verifying whether the user has been assigned an IP address. If your organization is using multiple VLANs and SSIDs, the Help Desk should also be able to verify that the user is connected to the appropriate VLAN (i.e., an employee is not connected to a Guest VLAN). If the user does not appear to be authenticated, you should determine whether the user has the appropriate credentials, etc. that are required to connect to your WLAN.

Figure 5: *Review the authentication information*

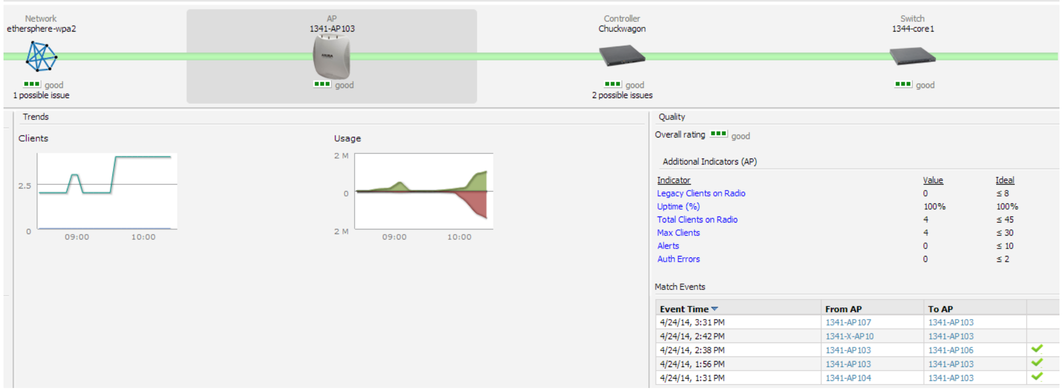


Current Association

Connection Mode:	11n 5 GHz (40)
Duration:	1 hour 4 minutes
IP Address:	10.6.136.172
Hostname:	sjc-kcava-t.arubanetworks.com
SNR (dB):	31
Usage:	7 Kbps
Security Mode:	
Cipher:	
Auth type:	EAP
SSID:	ethersphere-wpa2
VLAN:	1108
Forward Mode:	Tunnel Encrypted
Floor Plan:	Sunnyvale -> Building 1344 -> Floor 2

3. **Check AP Usage Levels**: Check the current usage levels on the AP or radio to which the user is connected to determine whether the AP is overcrowded, resulting in poor performance. Select the AP in the current connection table to review the AP's Client and Usage information.

Figure 6: *Client graph*



Indicator	Value	Ideal
Legacy Clients on Radio	0	≤ 8
Uptime (%)	100%	100%
Total Clients on Radio	4	≤ 45
Max Clients	4	≤ 30
Alerts	0	≤ 10
Auth Errors	0	≤ 2

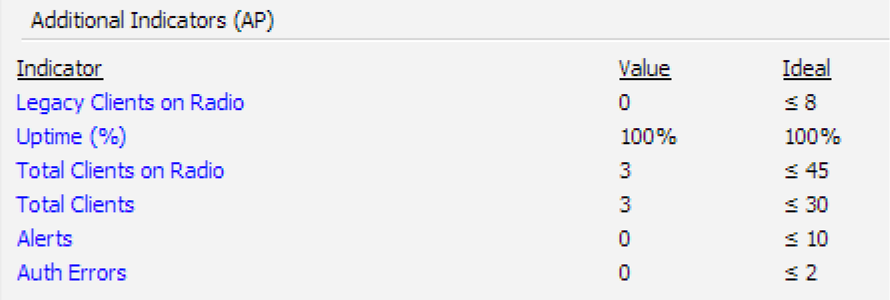
Event Time	From AP	To AP	
4/24/14, 3:31 PM	1341-AP107	1341-AP103	
4/24/14, 2:42 PM	1341-X-AP10	1341-AP103	
4/24/14, 2:38 PM	1341-AP103	1341-AP106	✓
4/24/14, 1:56 PM	1341-AP103	1341-AP103	✓
4/24/14, 1:31 PM	1341-AP104	1341-AP103	✓

- If no other users are connected to that AP, then this can be a sign that something is wrong with the AP. Click in the Clients graph to open the graph popup. Select a time range above the graph to view historical information (2 hours, 1 day, 5 days, 1 month, or 1 year) and determine whether it is unusual for no other users to be connected at this time of day. If no other users are connected at a time when usage is normally high, it is more likely that there is an AP or radio problem that should be escalated to Network Engineering.
- If many other users are connected to that AP, then check the Usage graph to determine whether these users are consuming most of that radio's capacity. Click in the Usage graph to open the graph popup. If usage is very high (especially on an 802.11bgn radio), then this might affect the perceived speed of the wireless network because all users are 'sharing' the same bandwidth.

  If usage appears unusually high, you can suggest that the user reporting the problem connect to the wired network temporarily while usage is high. You might also elect to contact those users with the highest bandwidth utilization levels to determine whether they can shift to the wired network temporarily to relieve over-utilization of the wireless network. If the AP appears to be overloaded on a consistent basis when you look at the historical usage graphs, you might want to alert Network Engineering that there may be a need to add capacity, change RF transmission power, shift more users from 802.11 b/g to 802.11a, etc.

4. **Review the Indicators**: In the right pane, review the Indicators for the AP to determine if any issues may result in slow network connectivity. Each indicator includes a link that you can select to view additional, detailed information.

Figure 7: *AP Indicators*



Additional Indicators (AP)

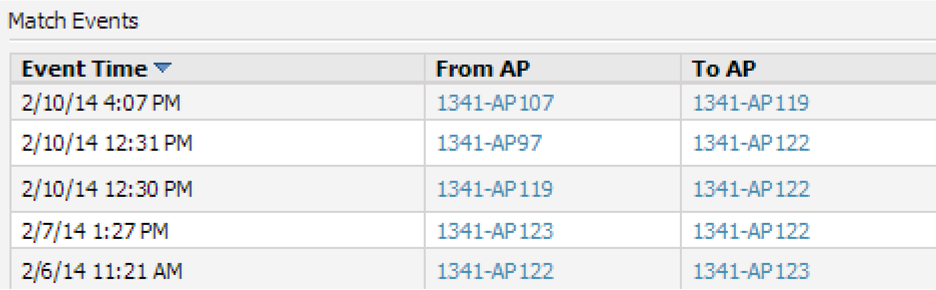
Indicator	Value	Ideal
Legacy Clients on Radio	0	≤ 8
Uptime (%)	100%	100%
Total Clients on Radio	3	≤ 45
Total Clients	3	≤ 30
Alerts	0	≤ 10
Auth Errors	0	≤ 2

Step Three: Examining User Information

1. **Review the Matching Events**: In the left navigation pane, review the Match Events table for the client and check for frequent roams between access points. In this example, a user named abartz has moved to different APs several times within a few-hour period. If the user is mobile, this roaming pattern may simply reflect his physical movements. If the user has been stationary, however, this may indicate that the user is ping-ponging back and forth between two APs that are both within RF range, and this ping-ponging can explain certain performance problems. In this case, the Help

Desk may decide to assist the user in changing his client device settings by putting the settings back to the default. If this problem seems to be affecting multiple users over an extended period of time, Network Engineering may need to adjust load-balancing settings. Similarly, if the user became associated to an AP that is within RF range but farther away than his/her usual AP, the user may be receiving a poor signal as a result. You can then help the user disassociate from the current AP and re-associate to the closer AP with a stronger signal. The Help Desk might need to talk to the admin if client match setting need to be adjusted to be less aggressive.

Figure 8: *Match Events table*

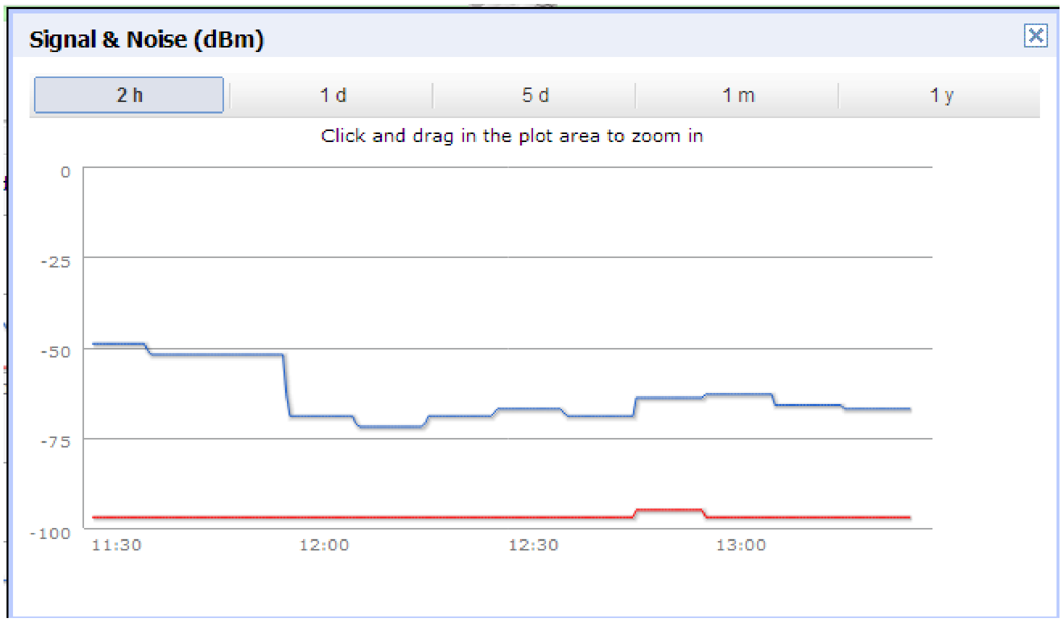


Match Events

Event Time ▼	From AP	To AP
2/10/14 4:07 PM	1341-AP107	1341-AP119
2/10/14 12:31 PM	1341-AP97	1341-AP122
2/10/14 12:30 PM	1341-AP119	1341-AP122
2/7/14 1:27 PM	1341-AP123	1341-AP122
2/6/14 11:21 AM	1341-AP122	1341-AP123

2. **Check the user's signal quality**: A weak or poor quality RF signal may be the cause of unusually slow wireless network performance. Click in the Signal & Noise graph to view the graph popup. Review the Signal Quality graph to determine whether the AP is receiving a strong RF signal from the user's client device. If the signal quality appears weak, and the user is connected to his or her usual AP, change the day/time range to compare the user's current signal quality to historical levels from the past day, 5 days, month, and year. In Figure 9 below:
   - The blue line is the Signal Level. Client devices on a correctly designed network should be -65 dBm or stronger (-64 and -63).
   - The red line is the Noise Floor. It shows APs in a RF environment. A clean level is -90 dBm and lower (-91, -92, -93, -94, and -95).

Figure 9: *Signal Quality graphs for last 2 hours*

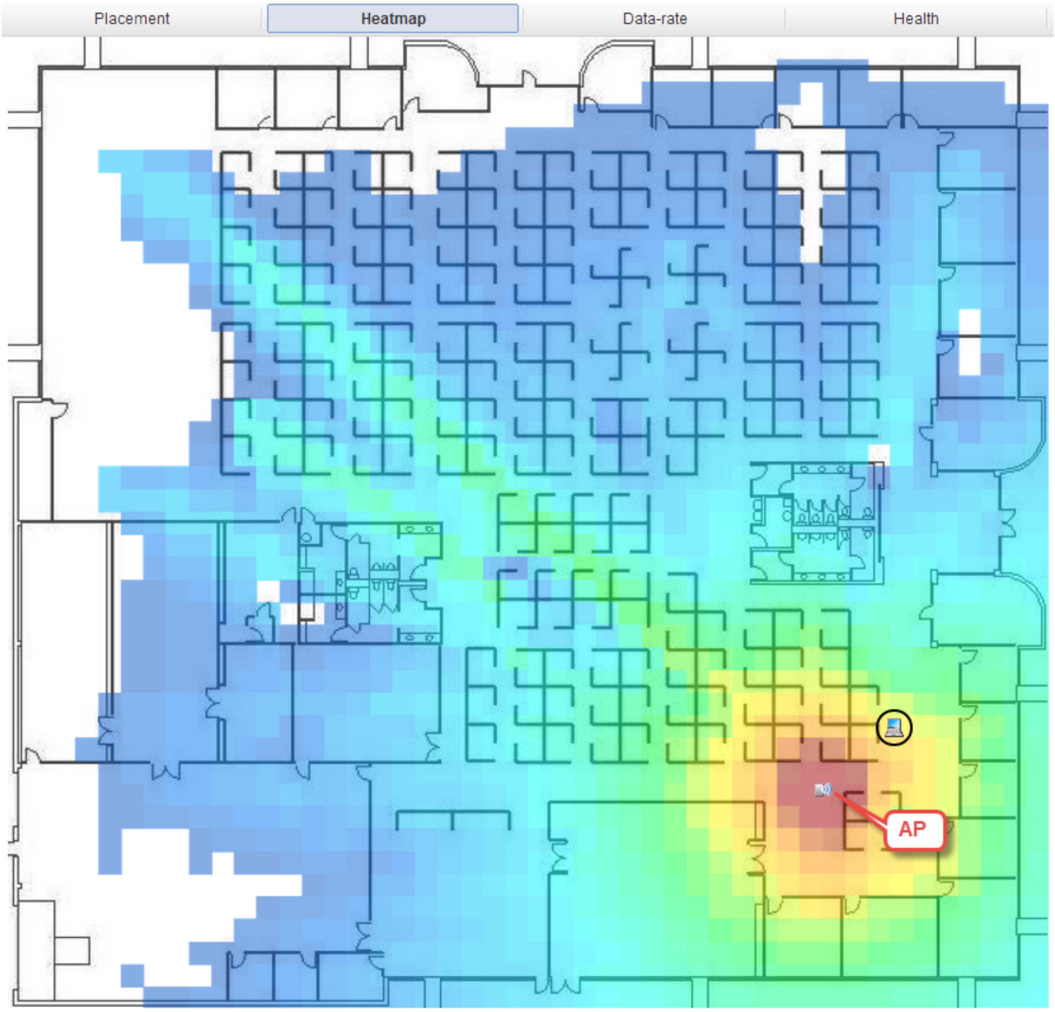


It is important to compare current RF signal quality levels to historical levels. If a user is complaining that the WLAN is unusually slow today, and the user's signal quality is low, there may be an RF problem affecting the user. However, if the user's signal quality is always low (for example, because his desk is 150' from the nearest wireless AP), then a low signal quality measure may not explain why the network performance today is worse than usual.

Step Four: Using Location Information, RF Heatmaps, and Frames/Sec

1. **Test Distance as a Cause of Poor Signal Quality**: If you suspect that poor RF signal quality might be the source of the user's problem, perform a simple test while the user is still on the phone to determine whether distance from a wireless AP is a major contributing factor.
   a. Go to the **Clients** > **Diagnostics** page for the Client. You can access this page after performing a search for a user, and then select the associated MAC address from the search results.
   b. In the **Current Association** section in the left pane, double-click the Floor Plan to open the pop-up, and click the Heatmap tab.
   c. Determine the physical location of the AP to which the user is connected.
   d. Ask the user to move closer to the AP and report whether performance improves.

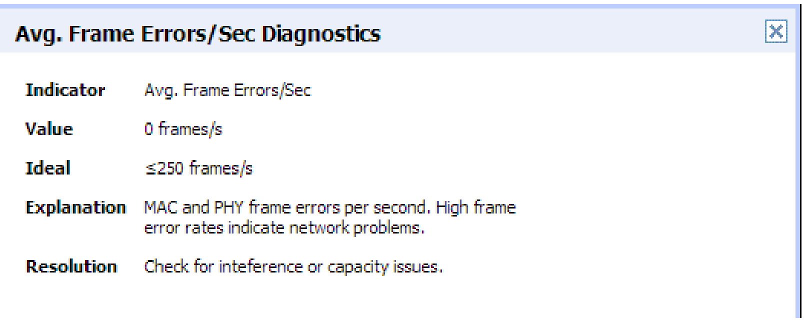
Figure 10: *User location information*



- If performance improves noticeably when the user is closer to the AP, then poor RF signal strength is a likely cause of the problem. The Heatmap view in VisualRF can show you if any neighboring access points might provide a stronger, clearer signal to the user. In the example above, the areas with the strongest signal are depicted in red, while areas with the weakest (or no) signal are in light blue (or white).
- If performance does not improve when the user is closer to the AP, then RF interference might still affect performance even when the user is receiving a strong signal from a nearby AP. You can quickly check whether RF interference is likely to be a cause of the problem. This will be valuable information to include when escalating to Network Engineering.

2. **Review the Number of Frame Errors per Second**: A high error rate for Frames per Second can indicate that wireless traffic is not flowing smoothly.
   a. In the **Client > Diagnostics** page, click the Network icon to navigate to the network information.
   b. In the **Quality** section for the network, select **Indicators within the ideal range**: > **Avg. Frame Errors/Sec**. .
   c. Check the number of FCS (Frame Check Sequence) Errors. If the error rate has been unusually high, it means that many wireless packets are being garbled. This is a clear indication of interference and a low signal quality. If error rates are high, this is important information to convey when escalating to Network Engineering. Keep in mind that it is important to compare current error levels to historical levels to see if current levels truly appear anomalous.

Figure 11: *Review the frames/sec information*



Avg. Frame Errors/Sec Diagnostics

Indicator	Avg. Frame Errors/Sec
Value	0 frames/s
Ideal	≤250 frames/s
Explanation	MAC and PHY frame errors per second. High frame error rates indicate network problems.
Resolution	Check for inteference or capacity issues.