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.

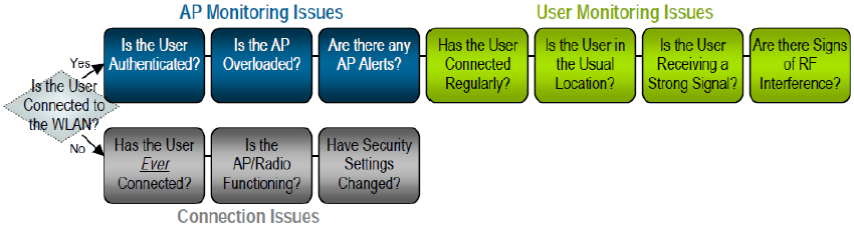
The AirWave Wireless Management Suite™ (AWMS) provides an end-to-end wireless operations management solution for the entire IT staff, from Network Engineering to the Help Desk. This quick reference guide is designed specifically to enable the Help Desk staff to:

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™ software, usually while the end user is still on the telephone. The basic trouble-shooting workflow process for the Help Desk is depicted in the following image:

Figure 1 *Basic troubleshooting workflow*



Troubleshooting Steps

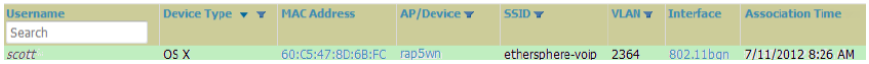
Basic troubleshooting can be summarized in four steps:

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 highlighted in green on AMP's Search Results page.

Figure 2 *Determine whether the user is connected*



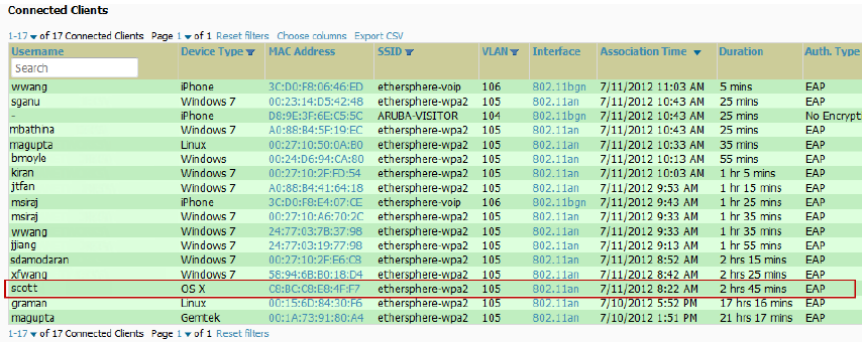
- If the user is currently connected, click on the "AP" link to open the AP Monitoring Page for that access point. Proceed to "Step Two: Check for AP-Related Issues" on page 2.
- If the user is not currently connected, check the search results to determine whether that user has ever successfully connected 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: Check the "Association Time" field in the search results to determine when the user most recently connected.
    - If the user has connected recently: Verify verbally that the user is in his or her usual location. Click the "AP" link to go to the AP Monitoring Page to verify that the AP is up and that other users are connected (See Step Two below). 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.

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 contact Network Engineering immediately and instruct the user to shut down his or her wireless connection.

Step Two: Check for AP-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. To do this, locate the user's name in the list of Connected Clients on the A**Ps/Devices > Monitor** page.

Figure 3 *List of Connected Clients*



Connected Clients

1-17 of 17 Connected Clients Page 1 of 1 Reset filters Choose columns Export CSV

Username	Device Type	MAC Address	SSID	VLAN	Interface	Association Time	Duration	Auth. Type
wwang	iPhone	3C:D0:F8:06:46:ED	ethersphere-voip	106	802.11bgn	7/11/2012 11:03 AM	5 mins	EAP
sganu	Windows 7	00:23:14:D5:42:48	ethersphere-wpa2	105	802.11an	7/11/2012 10:43 AM	25 mins	EAP
-	iPhone	D8:9E:3F:6E:C5:5C	ARUBA-VISITOR	104	802.11bgn	7/11/2012 10:43 AM	25 mins	No Encrypt
mbathina	Windows 7	A0:88:B4:5F:19:EC	ethersphere-wpa2	105	802.11an	7/11/2012 10:43 AM	25 mins	EAP
magupta	Linux	00:27:10:50:0A:B0	ethersphere-wpa2	105	802.11an	7/11/2012 10:33 AM	35 mins	EAP
bmoyle	Windows	00:24:D6:94:CA:80	ethersphere-wpa2	105	802.11an	7/11/2012 10:13 AM	55 mins	EAP
kiran	Windows 7	00:27:10:2F:FD:54	ethersphere-wpa2	105	802.11an	7/11/2012 10:03 AM	1 hr 5 mins	EAP
jtfan	Windows 7	A0:88:B4:41:64:18	ethersphere-wpa2	105	802.11an	7/11/2012 9:53 AM	1 hr 15 mins	EAP
msraj	iPhone	3C:D0:F8:E4:07:CE	ethersphere-voip	106	802.11bgn	7/11/2012 9:43 AM	1 hr 25 mins	EAP
msraj	Windows 7	00:27:10:A6:70:2C	ethersphere-wpa2	105	802.11an	7/11/2012 9:33 AM	1 hr 35 mins	EAP
wwang	Windows 7	24:77:03:7B:37:98	ethersphere-wpa2	105	802.11an	7/11/2012 9:33 AM	1 hr 35 mins	EAP
jjiang	Windows 7	24:77:03:19:77:98	ethersphere-wpa2	105	802.11an	7/11/2012 9:13 AM	1 hr 55 mins	EAP
sdamodaran	Windows 7	00:27:10:2F:E6:C8	ethersphere-wpa2	105	802.11an	7/11/2012 8:52 AM	2 hrs 15 mins	EAP
xfwang	Windows 7	58:94:6B:B0:18:D4	ethersphere-wpa2	105	802.11an	7/11/2012 8:42 AM	2 hrs 25 mins	EAP
scott	OS X	C0:BC:C0:E8:4F:F7	ethersphere-wpa2	105	802.11an	7/11/2012 8:22 AM	2 hrs 45 mins	EAP
graman	Linux	00:15:6D:84:30:F6	ethersphere-wpa2	105	802.11an	7/10/2012 5:52 PM	17 hrs 16 mins	EAP
magupta	Gemtek	00:1A:73:91:80:A4	ethersphere-wpa2	105	802.11an	7/10/2012 1:51 PM	21 hrs 17 mins	EAP

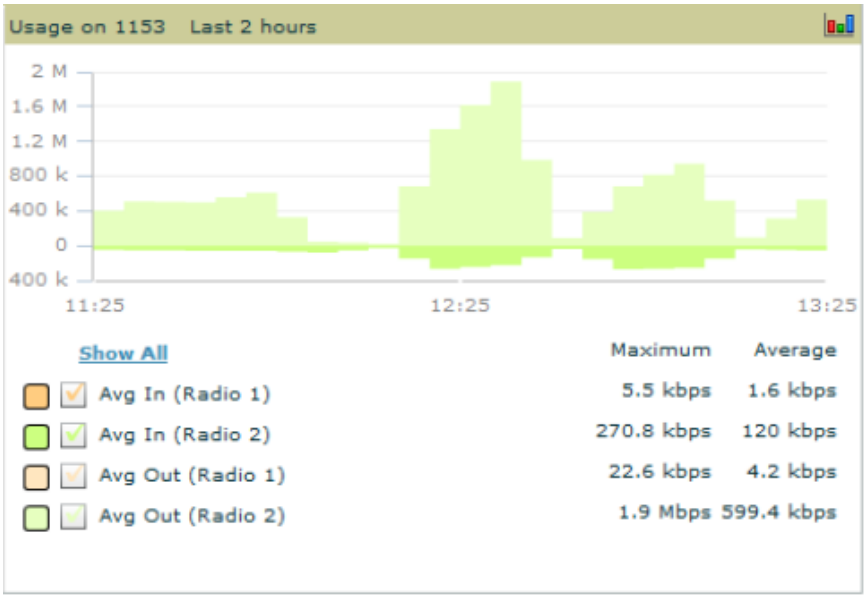
1-17 of 17 Connected Clients Page 1 of 1 Reset filters

2. **Verify that the user is authenticated**: Determine whether the user is currently authenticated by checking the "Auth Type" and "Auth Time" columns, and by verifying whether the user has been assigned a LAN 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.
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.
   - Use the "Client" graph to see how many total users are currently connected to that AP.

Figure 4 *Client graph*

   - If no other users are connected to that AP, then this can be a sign that something is wrong with the AP. Click the "Clients" graph to view historical information (by day/week/month/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. If usage is very high (especially on an 802.11bg radio), then this might affect the perceived speed of the wireless network because all users are 'sharing' the same bandwidth.

Figure 5 *Usage graph*



NOTE

If usage appears unusually high, look at the **Usage** column in the **Connected Clients** table to determine whether one or a few users are responsible for most of the usage. If so, 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. **Check for Alerts**: Click on "AMP Alerts" on the bottom of the AP Monitoring Page to determine whether there are any relevant active alerts for that AP that might explain the problem. (For example, has the AP been "down" recently?)

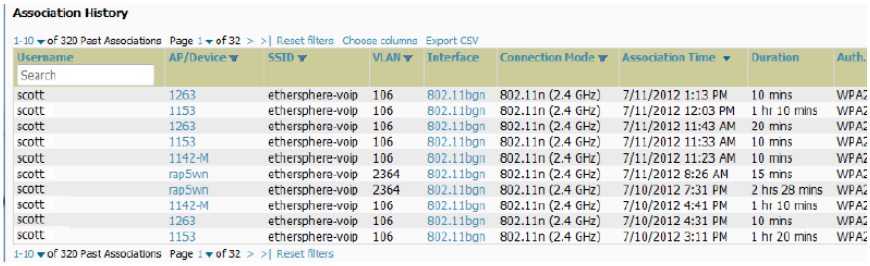
Figure 6 *AMP Alerts*

	Trigger Type	Trigger Summary	Triggering Agent	Time ▾	Severity
☐	User Bandwidth	>= 100 kbps for 30 seconds	00:18:DE:09:B9:09	2/12/2007 12:54 PM	Warning
☐	Device Up		hp-530-1	2/12/2007 12:32 PM	Normal
☐	Device Down		hp-530-1	2/12/2007 12:27 PM	Critical
☐	New Rogue AP Detected	>= 5 for rogue score	Unknown Lo-72:8F:26	2/12/2007 11:51 AM	Minor
☐	Device Up		roamabout-4102-3	2/12/2007 10:24 AM	Normal
☐	Device Down		roamabout-4102-3	2/12/2007 10:19 AM	Critical
☐	User Bandwidth	>= 100 kbps for 30 seconds	00:90:4B:F1:F0:D9	2/12/2007 9:09 AM	Warning
☐	New Rogue AP Detected	>= 5 for rogue score	Locally Ad-03:00:43	2/12/2007 3:00 AM	Minor
☐	New Rogue AP Detected	>= 5 for rogue score	Unknown Gr-02:02:01	2/11/2007 12:58 PM	Minor
☐	Configuration Mismatch		Tsunami_MP11	2/10/2007 8:16 PM	Major

Step Three: Examining User Statistics

1. **Navigate to the Client Details page**: Click the MAC Address link for the user on the Connected Clients list of the **APs/Devices > Monitoring** page. This takes you to the **Clients > Client Details** page for that specific user.
2. **Check the user's association and roaming history**: Scroll to the bottom of the page to view the user's Association History. Determine whether this user has been able to connect to the WLAN successfully multiple times in the past, and verify whether the user is currently connected to his or her usual access point.

Figure 7 *Association History*



Association History

1-10 of 320 Past Associations Page 1 of 32 > >| Reset filters Choose columns Export CSV

Username	AP/Device	SSID	VLAN	Interface	Connection Mode	Association Time	Duration	Auth.
Search								
scott	1263	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/11/2012 1:13 PM	10 mins	WPA2
scott	1153	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/11/2012 12:03 PM	1 hr 10 mins	WPA2
scott	1263	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/11/2012 11:43 AM	20 mins	WPA2
scott	1153	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/11/2012 11:33 AM	10 mins	WPA2
scott	1142-M	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/11/2012 11:23 AM	10 mins	WPA2
scott	rap5wn	ethersphere-voip	2364	802.11bgn	802.11n (2.4 GHz)	7/11/2012 8:26 AM	15 mins	WPA2
scott	rap5wn	ethersphere-voip	2364	802.11bgn	802.11n (2.4 GHz)	7/10/2012 7:31 PM	2 hrs 28 mins	WPA2
scott	1142-M	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/10/2012 4:41 PM	1 hr 10 mins	WPA2
scott	1263	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/10/2012 4:31 PM	10 mins	WPA2
scott	1153	ethersphere-voip	106	802.11bgn	802.11n (2.4 GHz)	7/10/2012 3:11 PM	1 hr 20 mins	WPA2

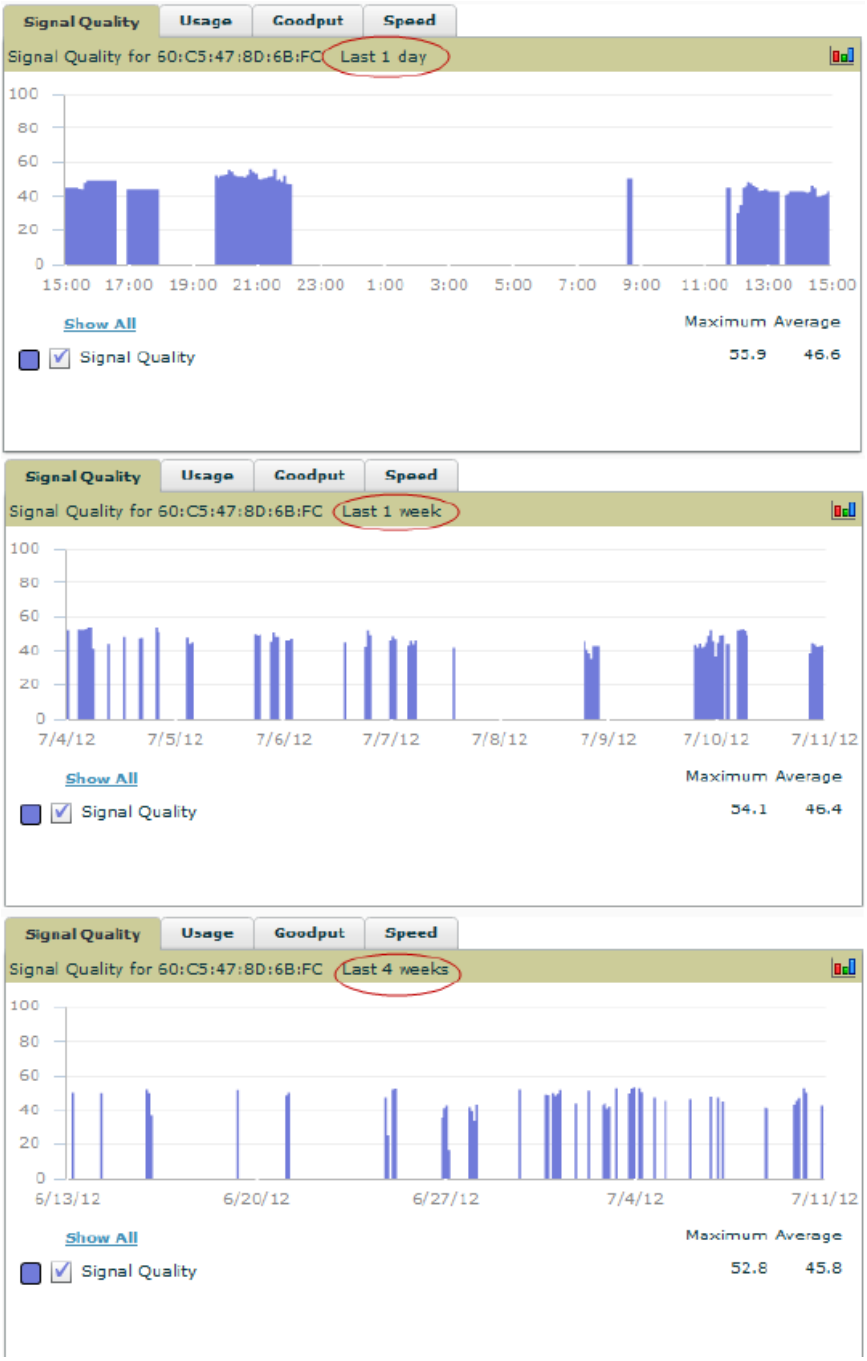
1-10 of 320 Past Associations Page 1 of 32 > >| Reset filters

If the user has little or no history of associations to the wireless LAN, the issue is much more likely to be a new client/device issue than if the user has a long history of successfully associating to the network through this AP with this particular device.

3. **Verify that the user is in the usual location**: Check the Association History section again to verify that the user is currently connected to his/her usual access point. 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 reassociate to the closer AP with a stronger signal.

   You should also check for frequent “roams” between access points. In the example above, user ‘scott’ has moved from one AP (“1153”) to another (“1263”) several times within a two-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” may explain certain performance problems. In this case, the Help Desk may decide to assist the user in changing his client device settings. (In some case, the client device may need to be configured to minimize roaming.) If this problem seems to be affecting multiple users over an extended period of time, Network Engineering may need to adjust load-balancing settings.
4. **Check the user’s signal quality**: A weak or poor quality RF signal may be the cause of unusually slow wireless network performance. Check the Signal Quality graph on the **Client Details** page to determine whether the AP is receiving a strong RF signal from the user’s client device. If the signal quality appears and the user is connected to his or her usual AP, click the Signal Quality graph to compare the user’s current signal quality to historical levels from the past day, week, month and year.

Figure 8 *Signal Quality graphs for last day, week, and month*



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.

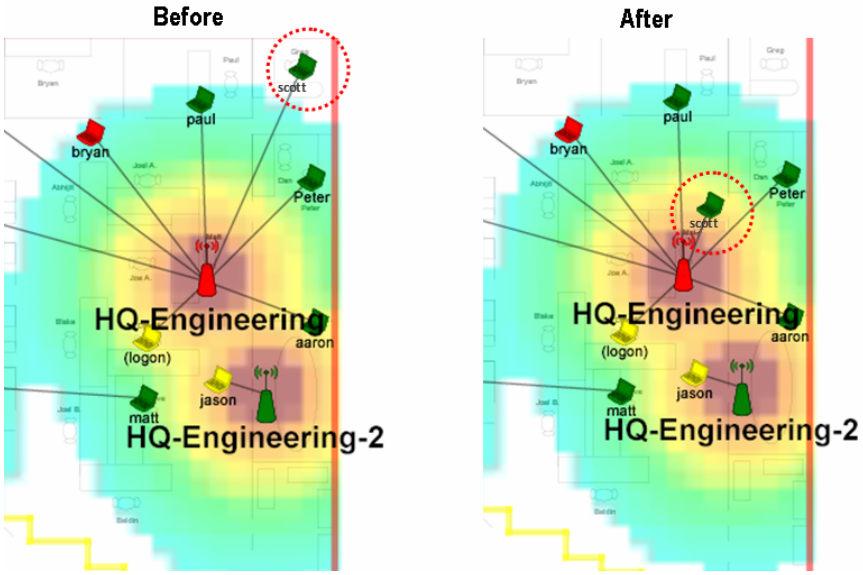
Step Four: Using Location Information, RF Heatmaps, and the ".11 Counters"

1. **Test Distance as a Cause of Poor Signal Quality**: If you suspect that poor RF signal quality may be the source of the user's problem, you can 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. Click anywhere within the floor plan on the **Client Details** page to open an enlarged physical RF map.

b. Determine the physical location of the AP to which the user is connected.

c. Ask the user to move closer to the AP and report whether performance improves. In the following image, the user is attempting to move closer to an AP named “HQ-Engineering.”

Figure 9 *User location information*

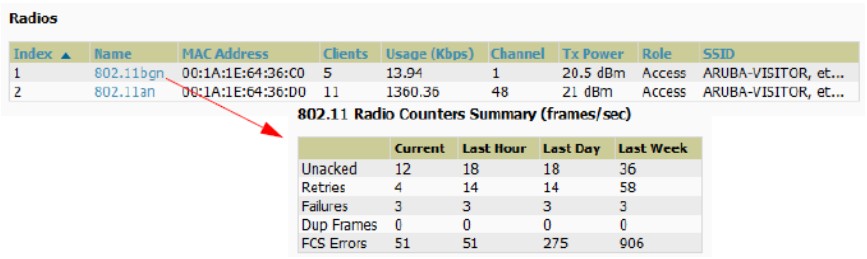


- If performance improves noticeably when the user is closer to the AP, then poor RF signal strength is a likely cause of the problem. You should check the “Heatmap” view in VisualRF to see if any neighboring access points might provide a stronger, clearer signal to the user. In the example above, the 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.

  (1) Click the AP name link at the top of the Client Details page to open the AP Monitoring view for the selected AP.

  (2) Click the radio to which the user is connected (i.e., 802.11bg vs. 802.11a radio in a dual-radio AP). This will bring you to the Radio Statistics Page.

Figure 10 *Select the radio*



(3) In the **802.11 Radio Counters Summary** table, 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.

(4) Check the table for the number of Retries. If the retry rate is high, it indicates that the AP has had to attempt to resend packets frequently – another sign of interference. If retry rates are high, this is important information to convey when escalating to Network Engineering.