WLAN Troubleshooting Using AirCheck™ Wi-Fi Tester

Our thanks to Fluke Networks for allowing us to reprint the following article.

AirCheck Troubleshooting Capabilities

AirCheck™ Wi-Fi Tester is a powerful troubleshooting tool that can help you identify and resolve many Wi-Fi related problems.

The following guide steps you through four of the most common scenarios:
1. Unable to Connect
2. Network is Slow
3. Detecting Security Risks in General
4. Finding Unauthorized Access Points

To understand how best to use AirCheck for troubleshooting, it is important to understand what specific functions AirCheck has that will assist you. These include:

- Viewing a complete list of available wireless networks in both 2.4 and 5 GHz bands and details about them.
- Obtaining a list of access points.
- Connecting to an access point (even secure ones), obtaining an IP address, and verifying IP-level communications.
- Measuring signal and interference levels in every channel.
- Measuring signal and interference levels for the channel used by a particular access point.
- Determining whether a channel is congested.
- Displaying whether interference in a channel permits or blocks WLAN operation.
- Identifying authorized and unauthorized access points against a pre-established list.
- Tracking down a rogue access point.

Fluke Networks provides a wide range of Wi-Fi troubleshooting tools for solving nearly any wireless problem. For more information, visit **flukenetworks.com/wireless.**

Scenario 1 – Unable to Connect

AP issues
1. Look to see if network is available.

- Select • **Home/Networks** to review list of visible SSIDs (Figure 1).

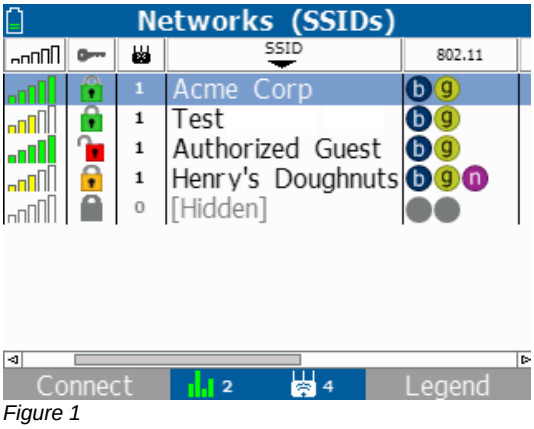

Figure 1

- Select individual networks for additional information.
- Make sure the desired AP is in the list.If not, restart the AP.If • it still does not show up, it may be

1547 N. Trooper Road • P. O. Box 1117 • Worcester, PA 19490-1117 USA
Corporate Phone: 610-825-4990 • Sales: 800-832-4866 or 610-941-2400
Fax: 800-854-8665 or 610-828-5623 • Web: www.techni-tool.com

misconfigured (e.g., wrong SSID), defective, or not powered.

- If the AP is not powered, you can use the optional PoE detector to determine if Power over Ethernet voltage from 802.3af and higher-power 802.3at devices is available on the twisted pair network cabling.
- Make sure that there is sufficient signal-to-noise ratio (SNR) for the AP.10 dB SNR is usually the practical minimum, 20 dB will provide solid connectivity, 30 dB and higher is excellent. You obtain higher throughputs with higher SNR.
- If the SNR is too low, the AP may be too far away or something may be blocking the signal.

2. Check access point configuration

- Select **Home/Networks/SSID/ Access Point** or **Home/Access Points**.
- **Access Point Details** allows you to verify that the access point is supporting the correct 802.11 mode (802.11a/b/g/n) and correct security (Open, WEB, WPA, WP2, etc.) Make sure that the client device matches these settings. Note that 802.11 will not support previous mode unless operating in a legacy-support mode. For example, Figure 2 shows an access point that supports both 802.11b & g.

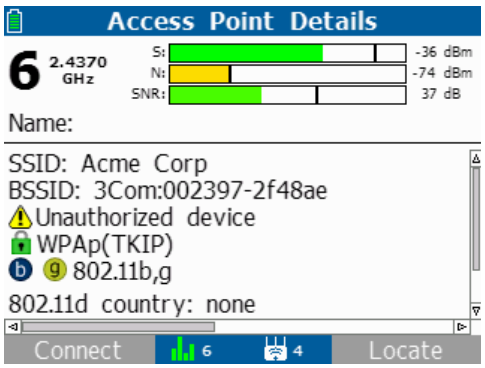

Figure 2

- If an SSID's name is not visible, the AP may have been configured to not broadcast it. AirCheck will display an AP that does not broadcast its SSID as [Hidden]. Clients can still connect to the AP, but they must be configured with the hidden SSID's name value.
- If an AP is using medium access control (MAC) address filtering, make sure that all client device MAC addresses are included. You usually configure the AP with a wireless management utility or web page that lets you manage your AP. In Windows, you can obtain the MAC of the client PC address by going to the Command Prompt and typing: **ipconfig /all.**

3. Exclude interference issues

- Select the **Home/Channels** screen to review interference in each channel (Figure 3).The blue portion of the bars shows the amount of 802.11 signals on the channel and the gray portion shows the amount of interference on the channel.

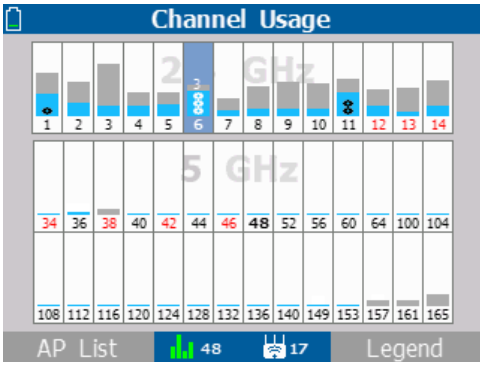

Figure 3

- Select the **desired channel** to monitor the channel over time (Figure 4).

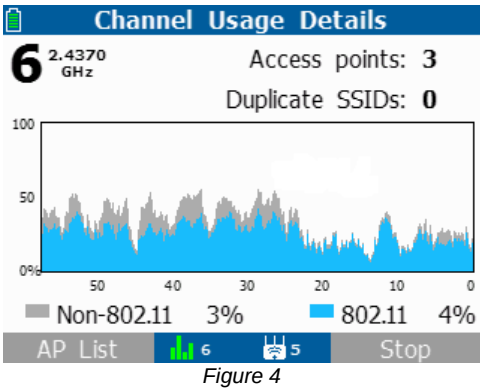

Figure 4

1547 N. Trooper Road • P. O. Box 1117 • Worcester, PA 19490-1117 USA
Corporate Phone: 610-825-4990 • Sales: 800-832-4866 or 610-941-2400
Fax: 800-854-8665 or 610-828-5623 • Web: www.techni-tool.com

- If you are seeing a high percentage of interference, you should attempt to locate and eliminate the cause of interference. Common sources of interference at 2.4 GHz include microwave ovens, Bluetooth® devices, and cordless phones.
- Excessive interference may suggest that you consider using a different channel, or even another band (e.g., 5 GHz band instead of 2.4 GHz band) to reduce the effect of interference on the channel.
- If interference is from other access points, consider reducing AP transmit power so coverage areas do not overlap.

4. Connect to the access point.

- Select **Home/Networks/cursor over the desired network/Connect (F1)** or **Home/Access Points/cursor over the desired AP/Connect (F1)**.
- In the first case above, you will be connecting to a specific network by SSID name. In the second case, you'll be connecting via the specified AP.
- The connect test will indicate: whether a connection to the AP is possible, including authentication, assignment of IP address and whether a PING control message can be sent and received. (Some of these items are configurable in AirCheck's profile.) After the connection test is complete, the **Start Tests (F1)** button provides additional test options.
- The **Log (F2)** provides details about the connection attempt that may assist further with troubleshooting.
- Failure to connect may be due to having incorrect security settings. For example a connection will fail if the access point is filtering MAC addresses and the AirCheck MAC address is not in the list of approved MAC addresses.

Client issues

The following is a list of steps that can be used to resolve client issues:

- AirCheck: Select **Tools/List Probing Clients** to see if the client is transmitting probe request frames and to see basic settings such as channel and SSIDs the client is using in probes. Select the client of interest to obtain Probing Client Details. Note that many clients may not probe if they are connected to an AP.
- Access Point: Look at the AP status screen (usually accessible via a browser on a computer on the network or a management utility) to see if the AP has assigned the client device an IP address.
- PC: Restart client system and try again.
- PC: Verify that WLAN is active. (Windows typically provides a system tray icon for the WLAN utility.) Click on WLAN system icon or equivalent in other systems, to see WLAN status. Confirm that client is connected to correct network.(With multiple local networks, user may have connected to the wrong SSID.)
- PC: Confirm that client has correct networking settings, including file/printer sharing settings. PC: Confirm that client device has correct security settings.
- PC: In Windows, you can perform a "Repair Connection" to reinitialize the networking software. This sometimes will clear up issues.
- PC: Ensure that client-side firewall is not blocking communications.

Other networking issues

If clients and access points are functioning correctly, but network connectivity is still not available, some other networking element may be responsible, such as a firewall. You can use AirCheck to ping devices on the local wireless network or on the Internet to verify that they can be reached. (See Figure 5.) AirCheck will automatically provide the addresses of the gateway and DHCP server for testing – other address, including URLs, can be loaded through AirCheck Manager and will appear on the test screen.

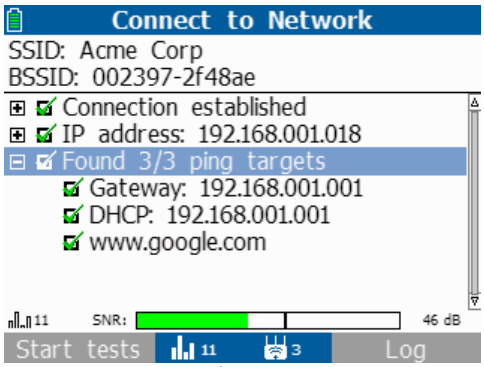

Figure 5

Scenario 2 – Network is Slow
There are multiple possible causes for slow networks including weak signal, interference, overloading/congestion, and mixed-network operation.

Weak signal

- Select **Home/Networks/SSID/ Access Point** or **Home/Access Points.**
- Check signal levels of access points. Review graphical display of signal strength or select **Access Point** for numerical signal strength and signal-to-noise (SNR) information.10 dB SNR is usually practical minimum, 20 dB will provide solid connectivity, 30 dB and higher is excellent. You obtain higher throughputs with higher SNR.
- If SNR is too low, consider: moving station closer; moving access point; increasing access point power level; removing obstructions; installing another access point; using a channel with less interference; moving to 2.4 GHz band if using 5 GHz band; replacing with 802.11n which has longer range; using a repeater.

Interference

- Select **Home/Channels** screen to review interference in each channel.
- Select **Home/Networks/SSID/ Channel (F2)** to monitor activity used by the access point in question. This will display how much of the channel utilization over time is signal versus noise.
- Attempt to locate and eliminate the cause of interference. Common sources at 2.4 GHz include microwave ovens, Bluetooth devices, and cordless phones.
- If interference is from other access points, consider reducing AP transmit power so coverage areas do not overlap.

Congested network

- Select **Home/Channels** to review channel activity.
- A dot indicates an access point. Multiple access points on the same channel is not desirable, but acceptable (and sometimes unavoidable) if overall usage on that channel is relatively low (e.g., less than 50%).
- Highlight **Channel/Select** for graphical view.
- If a channel is congested but other channels are available, reconfigure access point to use a less-congested channel.

Mixed network
A network configured with a mix of 802.11b and 802.11g access points operates slower than a network with 802.11g only access points. Similarly, 802.11n runs more slowly if it has to provide backwards compatibility for 802.11b and g.

- Select **Home/Networks/SSID/ Access Point** or **Home/Access Points**.
- Review modes in use in each channel. Figure 2 shows an example of an AP supporting both 802.11g and b.
- If you determine that there is no need to support the older technologies, you can reconfigure the AP to no longer support them.

Scenario 3: Detecting Security Risks in General

Encryption

- Select **Home/Networks**.
- Review security icons next to networks (see figure 1).The green open lock icon indicates an

unsecured network, while a yellow lock icon indicates WEP or Cisco LEAP security which is less secure than other protocols. The green locked icon indicates more secure protocols such as WPA or WPA2.

Detect adhoc networks
Adhoc networks may violate security policy.

- Select **Home/Networks.**
- Look for adhoc networks as shown by 

Scenario 4: Finding Unauthorized Access Points

Enter authorized access points

- Use AirCheck Manager to create a profile for your network that includes a list of authorized APs.

Monitor environment

- Select **Home/Networks**.
- Make sure there are not unexpected SSIDs.
- Alternatively, select **Home/Access Points**.
- Quick check: review list for access points that have no names or generic names (e.g. Linksys). Unnamed or generically-named APs are more likely to be unauthorized consumer-grade equipment.
- Select each AP to verify that it is an authorized device. By scrolling the screen to the left, you can see if devices are on the **Access Control List (ACL)** (Figure 6).

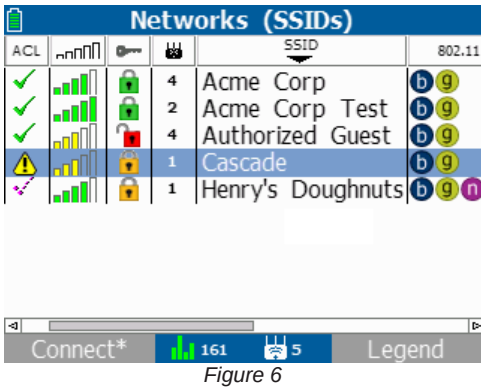

Figure 6

- If an access point is legitimate, but not defined in AirCheck's profile you can manually authorize the access point, from **Home/Access Points** press **ACL (F2)**.Be sure to save this change in your profile for future use.
- You can also flag an AP if you want to note it for later examination (Figure 7).

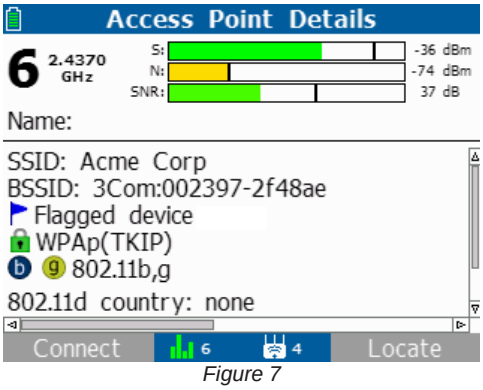

Figure 7

Compare environment against previously saved environment

- AirCheck Manager allows you to easily compare different saved sessions files against each other to quickly see changes in the WLAN.

Find rogue access points

- Once you have identified a suspicious access point, select **Home/Access Points/cursor over the desired access point/Locate (F2)**, to view its signal strength (lower negative number is stronger signal) and/or listen to sound pitch to locate the access point. The pitch of the sound will be higher the closer you are to the access point, and deeper the farther you are from the access point.
- Using the optional AirCheck External Directional Antenna may show you the direction of a signal source more precisely than the standard omnidirectional antennas in AirCheck.
- There are specific techniques for tracking down an access point using both unidirectional and omnidirectional antennas described in the Fluke Networks white paper

"Locating rogue 802.11n and legacy wireless access points".

Other Troubleshooting Hints

This lists some other common issues that affect WLAN operation.

1. Stations and access points should have the most recent version of firmware.
2. If you lose passwords stored in an access point, you may need to restore the AP to its factory default settings, though this will require additional configuration steps.

If the steps above don't solve the problems, it's likely a more complex or subtle issue that will require more sophisticated tools. AirCheck can help with this through its ability to save the troubleshooting session information. This can provide valuable details to others who might need to help solve the problem. As many wireless problems can be intermittent in nature, it also allows you to capture the problem for later analysis. By comparing results from the sessions before and after taking action, you can also validate that the actions you took really solved the problem. Finally, the saved session information provides a useful baseline if problems should occur in the future.

1547 N. Trooper Road • P. O. Box 1117 • Worcester, PA 19490-1117 USA
Corporate Phone: 610-825-4990 • Sales: 800-832-4866 or 610-941-2400
Fax: 800-854-8665 or 610-828-5623 • Web: www.techni-tool.com