Tools for Troubleshooting Poor Wireless Performance

When wireless issues spring up they can be hard to diagnose, this guide will show some ways in which the Cisco Meraki Dashboard is capable of speeding up that process and giving some valuable information about the wireless environment itself.

General Information for Troubleshooting

Before the wireless issue can be addressed the following information should be gathered in order to attain a clear picture of what end user(s) experience. This information will be essential in tracking down the root cause.

- Size and scope of clients experiencing the symptom
- Device type (iOS, Windows), hardware (Macbook air, Lenovo X220), and drivers.
- Specific AP(s) or SSID linked to symptom
- Environmental factors such as inclement weather, tree growth or a newly built wall.
- Taking into account the limitations of the APs in terms of throughput will reduce any knee-jerk reaction to a perceived throughput issue.

With this information the issue should be more clear and it is time to take a more focused look at what the Cisco Meraki Dashboard can offer in terms of troubleshooting information.

Gathering Information from Dashboard

Dashboard offers a wide variety of ways to gather information about the wireless network. Through the Live Tools and event log network administrators can track a specific device, it's movements and 802.11 state.

- All Cisco Meraki products have a connectivity graph which can span hours, days, and weeks which allow for quick spotting of outages or any change in device status:
• All Enterprise and above Organizations have an event log which can be useful in gathering some information. Some events that should be looked into are as follows:
  ◦ Associations.
  ◦ Disassociations and Deauthentications.
  ◦ Timestamps for building a timeline of certain events.
  ◦ RSSI values, which can be interpreted as signal strength.
  ◦ The AP and SSID the events occurred on.

• Signal strength may be obtained from the event log by looking at the RSSI value. If associated to the wireless network, a wireless client can utilize the local status page by browsing to my.meraki.com and selecting Client survey tools.

• APs can be gateways or repeaters which can easily be determined by looking in the top right corner of the image that is displayed on the Monitor > Access Points page. A solid/hollow green circle denotes a gateway unit, a faded green circle is indicative that the unit is currently running as a repeater. This can be very useful when troubleshooting wireless throughput.

• The Live tools section can be useful when attempting to determine wireless issues. The Channel Utilization live tool is particularly useful for troubleshooting connectivity issues. For example, if the utilization is 75%+ it would be worthwhile to survey the other channels and determine if the utilization could be better on one of the other non overlapping channels.

• There is a historical graph for channel utilization that can be viewed in the same way as the connectivity graph. The channel utilization graph can help identify a temporary spikes or consistent saturation of a channel over time.
For issues where the channel utilization is showing a very large amount of interference with the bulk of it being 802.11 traffic it is important to check the Configure > Radio settings page. The Radio settings page can display the number of Cisco Meraki and Non-Cisco Meraki APs that are on the same channels as the APs in the network as well as the max interfering signal strength. If the utilization graph is showing extended durations of high channel utilization and the Configure->Radio settings page shows several APs on the same channel with a high signal strength, chances are the channel should be switched.

Air Marshal gathers a wealth of information even if an AP isn't a dedicated Air Marshal. Packet floods as well as spoofed SSIDs can be detected by Air Marshal.