savvius™ | TECH BRIEF

How to Perform Multi-Channel Analysis for WLAN Mobility

Clients roam. It's what they do. Today's wireless networks are primarily about mobility, and rarely about portability. If clients roam, then troubleshooting tools must follow. For a long time, analysts have captured frames (aka packets) traversing a single channel, but what happens when a client roams to another channel as it is designed to do? Poof! The client vanishes from the analyzer's view and troubleshooting stops right there. This has been a particularly perplexing problem for Voice over Wi-Fi (VoWiFi) analysts given that they are troubleshooting highly-mobile connectivity.

Enter Multi-Channel Analysis. No longer will analysts have to suffer the limitations imposed by single channel protocol analysis. This tech brief illustrates how to perform a triple-channel capture for the purpose of monitoring roaming clients. It is certainly possible to scale this technique beyond three adapters, but for simplicity's sake, we'll stick with three. For the sake of examples, we'll be using the usual 2.4 GHz suspects of channels 1, 6, and 11 even though the techniques are applicable for any channels in either the 2.4 or 5GHz bands.

Contents

Hardware and Software

Not every protocol analyzer can perform multi-channel capture, aggregation, and analysis. Savvius Omnipeek® is one of the few products on the market that does have this capability. But to accomplish multi-channel analysis several other products also come in handy. Throughout this tech brief you will find references to several products to make it easier for you to find exactly what can work. But we freely admit these may not be the only products that work. Use of any vendor's products is in no way an endorsement of their specific products over those of other vendors. Each piece of hardware and software was chosen to perform a specific task. Functionality and aesthetics were the only two criteria.

Hardware and Software Configurations

The following is a list of hardware and software required to perform multi-channel analysis as described in this tech brief; deviate at your own risk. Other hardware configurations might work, but we have only tested this configuration.

The hardware and software needed for multi-channel analysis:

- (3) Savvius WiFi Adapters for Omnipeek: https://www.savvius.com/products/network_visibility_performance_diagnostics/omnipeek_family/wlan_usb_capture_adapter
- (1) Savvius Omnipeek Enterprise Network Analyzer: https://www.savvius.com/products/network_visibility_performance_diagnostics/omnipeek_family/omnipeek_network_analysis
- Savvius Ralink drivers for the Savvius WiFi Adapters for Omnipeek (included with Omnipeek)
- (1) Laptop PC with stacked USB ports, at least 4 GB of RAM, a fast CPU, and Windows 10.

The Savvius WiFi Adapters for Omnipeek are USB-connected WLAN devices designed for wireless packet captures. Certified for use with Omnipeek and Capture Engine for Omnipeek, they are available in both 2-stream 802.11ac and 3-stream 802.11n versions. Having a USB 2.0 or 3.0 interface let you use multiple simultaneous adapters on the same laptop PC. Special Savvius drivers are required for this adapter to operate properly with Omnipeek and its associated features.

Savvius Omnipeek Enterprise is our flagship product, and is the leading 802.11 protocol analyzer in the market. As you can see, multi-channel analysis requires only a few components — Omnipeek and WiFi Adapters for Omnipeek. Everything else that's needed, including roaming analysis, is built into Omnipeek.

FIGURE 1: SAVVIUS WIFI ADAPTERS FOR OMNIPEEK

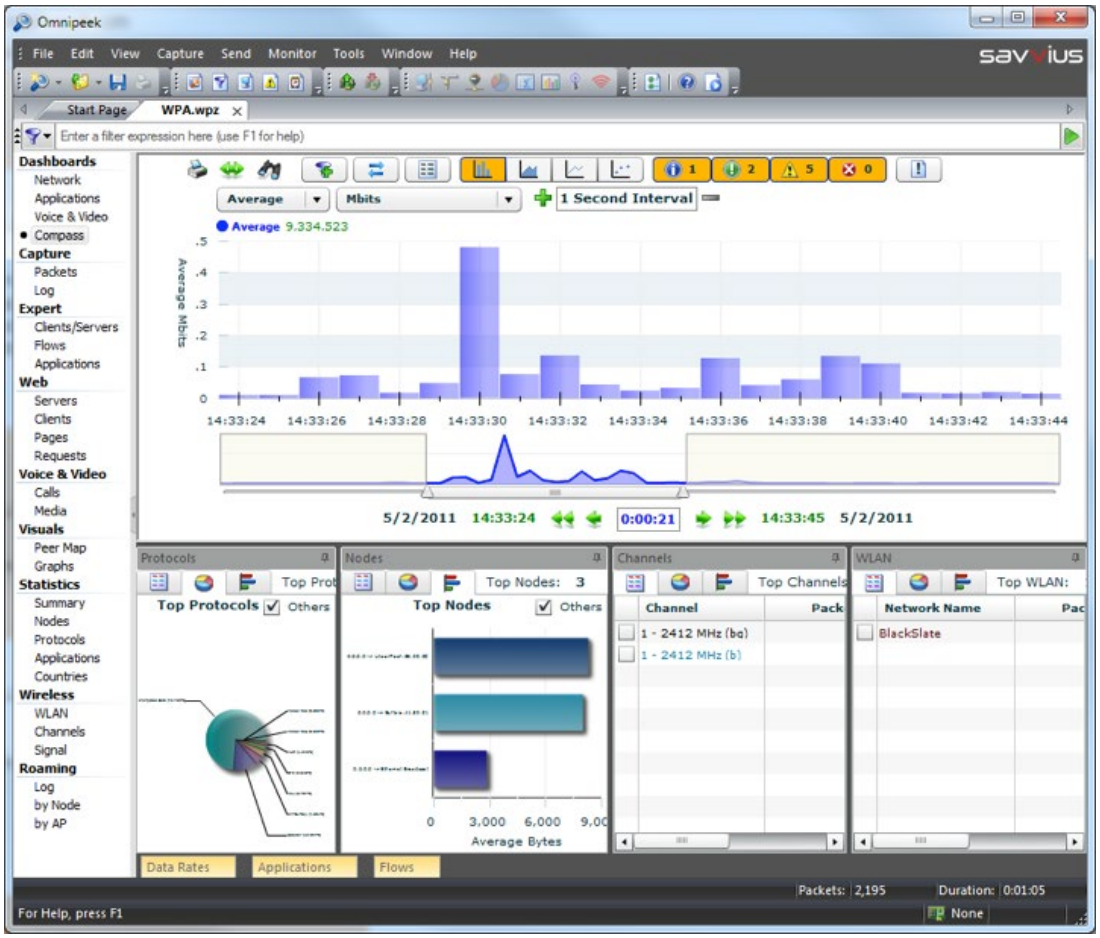

FIGURE 2: COMPASS DASHBOARD SHOWING UTILIZATION, CHANNELS, AND WIRELESS NETWORKS

Omnipeek is powerful software, and performs a great deal of analysis. The laptop on which you run Omnipeek should have at least 4GB of RAM so that at least 512 MB can be dedicated to the packet buffer, and the CPU should be pretty hefty. We will discuss settings for performance later in this tech brief.

Installation and Configuration of WiFi Adapter for Omnipeek Driver

In this section, we will describe the installation and configuration of the Savvius driver for the WiFi Adapter for Omnipeek. First, plug each of your three WiFi Adapters for Omnipeek into USB ports on your laptop, as illustrated in Figure 3. If you do not have three available USB ports, you can use a USB hub, but proceed with caution. WLAN adapters draw considerable power from the USB port, so an unpowered hub requires a single USB port on the laptop to drive all of the USB WLAN adapters connected to it. Performance varies with each USB hub. To avoid this issue, choose a powered USB hub. They're more expensive, but you'll save yourself lots of trouble. We don't have a specific recommendation here. Just about any powered hub should work, even battery powered hubs. If a powered hub isn't an option, look for a hub that plugs into two USB ports simultaneously. This should provide sufficient power for up to four WiFi Adapters for Omnipeek.

In our case, we have three available USB ports on the laptop, so we'll just connect each WiFi Adapter for Omnipeek to each port on the laptop (Figure 3). You will be asked for the drivers for these wireless adapters, or Windows will automatically install the default driver, three times in a row (once for each adapter — it's a Windows thing). It's OK to let this happen, but the driver that Windows installs is NOT the driver you will use with Omnipeek.

FIGURE 3: THREE WIFI ADAPTERS FOR OMNIPEEK CONNECTED TO USB PORTS ON A LAPTOP

WiFi Adapters for Omnipeek require a special driver to be used with Omnipeek. You need to update the driver from the one installed automatically by Windows when you connected the device, to this special driver.

Driver Location

WiFi Adapter for Omnipeek drivers are available in both a 32-bit and 64-bit version. For a typical Omnipeek installation, the drivers are available from the following locations:

- Windows (32-bit): C:\Program Files\Savvius\Omnipeek\Drivers\OmniWiFi\x86\
- Windows (64-bit): C:\Program Files\Savvius\Omnipeek\Drivers\OmniWiFi\x64\

NOTE: The most current WiFi Adapter for Omnipeek driver can be downloaded from here:
https://mypeek.wildpackets.com/driver_downloads.php.
You need to register for MyPeek before downloading the driver.

Driver Installation

To install the WiFi Adapter for Omnipeek driver:

1. Open the Device Manager Control Panel.
2. Right-click the appropriate WiFi Adapter for Omnipeek, and select 'Update Driver Software' (Figure 4).

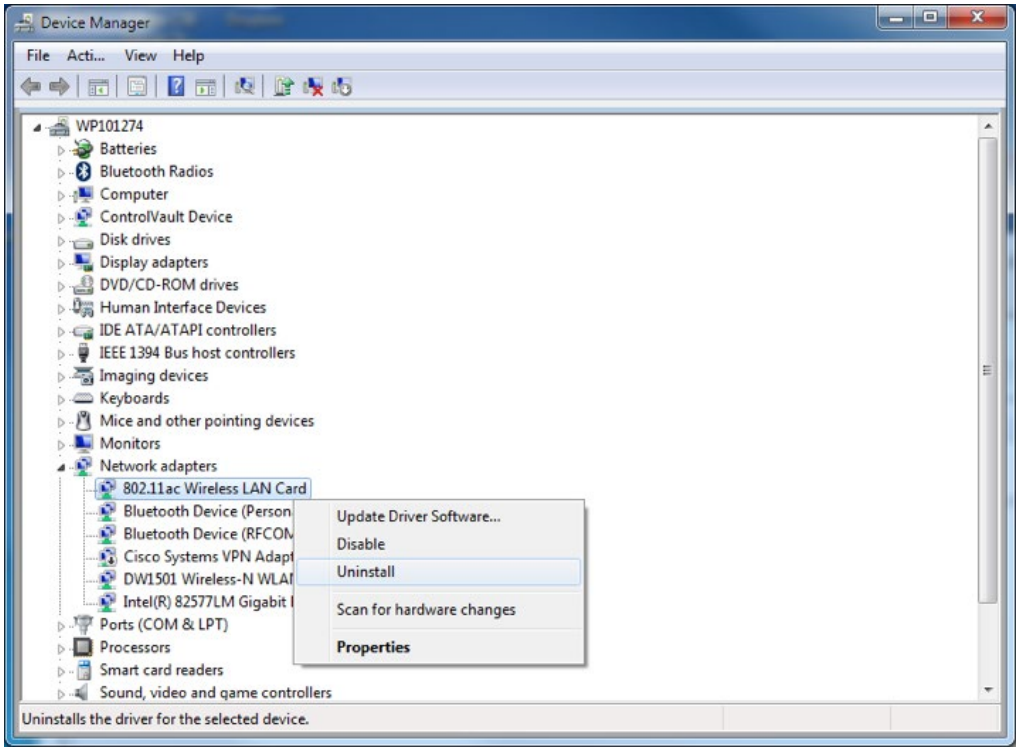

FIGURE 4: WINDOWS DEVICE MANAGER – CHOOSE THE ADAPTER WHOSE DRIVER YOU NEED TO UPDATE

3. Click 'Browse my computer for driver software.'
4. Click 'Let me pick from a list of device drivers on my computer.'
5. Click 'Have disk'.
6. Browse to the directory that contains the driver and select the rt2870.inf file.
7. Click Open and then OK.
8. Click Next and do not pick a manufacturer or network adapter. The wizard should automatically pick them for you.
9. Click Install if you receive a message 'Would you like to install this device software?'
10. Click 'Close' to complete the installation.
11. Select Yes to reboot if asked. We recommend that you reboot your computer anyway, even if the system does not ask if you want to.
12. You need to follow these steps for each adapter that you connected. It is also useful to give each adapter a unique name so you can distinguish between them in the future. You can do this by going to the Windows Control Panel -> Network and Sharing Center -> Change Adapter Settings (Control Panel\Network and Internet\Network Connections), choosing a device, right-clicking, and selecting "Rename" (Figure 5).

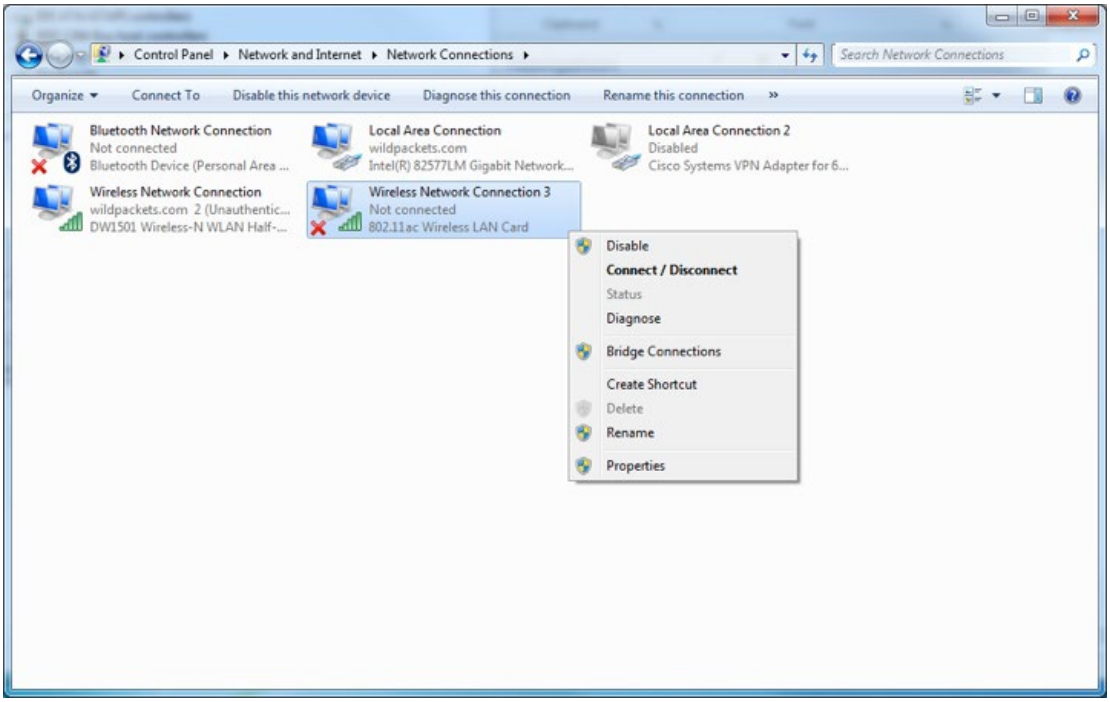

FIGURE 5: GIVE EACH WIFI ADAPTER FOR OMNIPEEK A UNIQUE NAME

13. To confirm that your drivers were successfully installed, start Omnipeek and select a WiFi Adapter for Omnipeek. You should see the following in the description window: “Omnipeek API: Yes” (Figure 6).

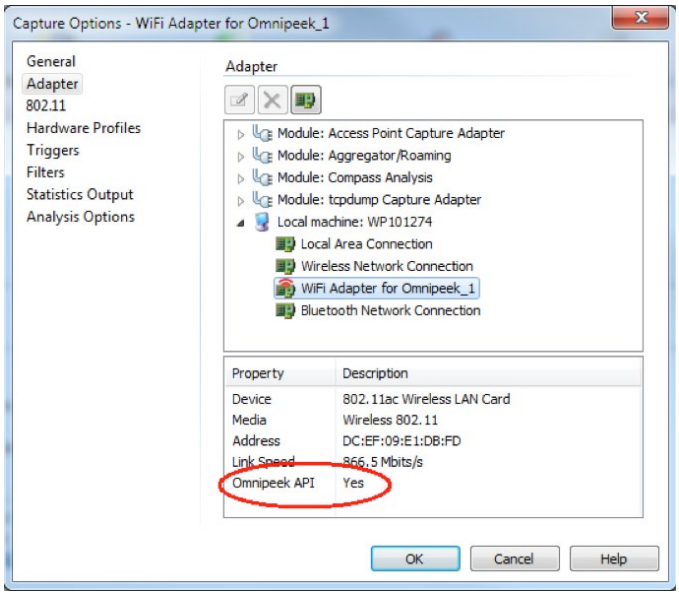

FIGURE 6: MAKE SURE THIS DIALOG SHOWS SAVVIUS API = YES

NOTE: The WLAN Analysis Modules within Omnipeek will only be loaded if “Omnipeek API = Yes”.

Performing Multi-Channel Analysis

With Omnipeek and the WiFi Adapters for Omnipeek correctly installed, you're now ready to begin analyzing. Simply launch Omnipeek, and from the Start Page select New Capture. This brings up the Capture Options dialog box. This is where things are just a little bit different when you're doing multi-channel analysis. In the left-hand navigation bar choose Adapters, and then expand the option Module: Aggregator/Roaming. Double-click on New Adapter, and you'll see the dialog box in Figure 7.

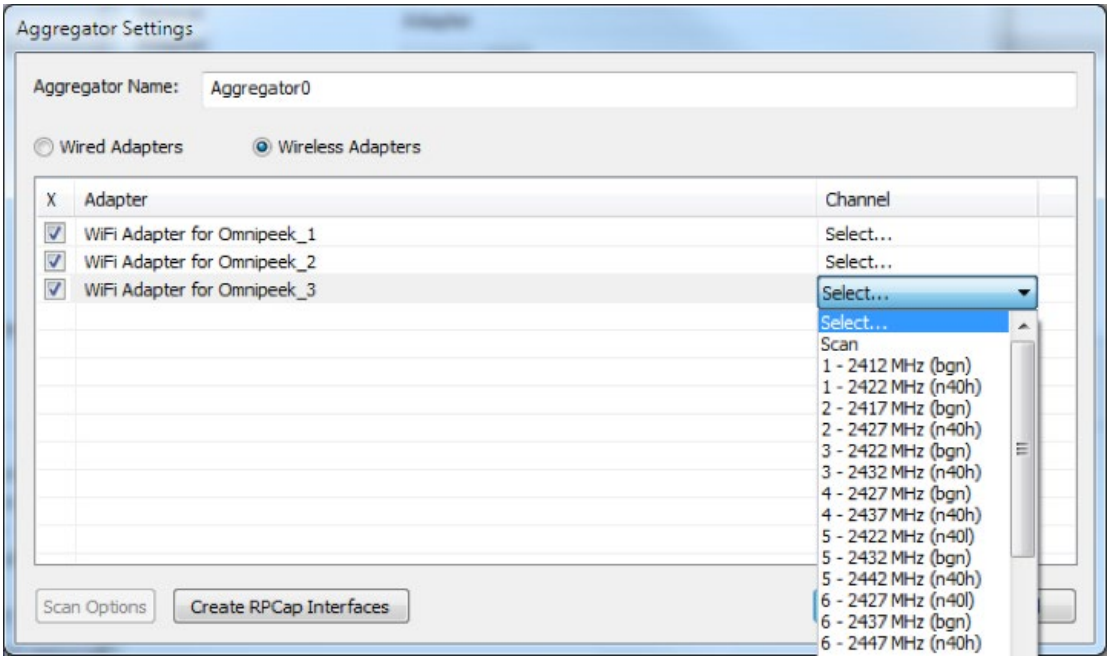

FIGURE 7: CONFIGURING OMNIPEEK FOR MULTI-CHANNEL ANALYSIS

The dialog box confirms that you have correctly installed the WiFi Adapter for Omnipeek drivers, otherwise the adapters will not appear in this dialog. Choose each WiFi Adapter for Omnipeek that you wish to use, and select the channel for each adapter from the drop-down channel selection box. In Figure 7 you can see that we are going to perform multi-channel analysis, capturing on channel 1 (11n – 40MHz), channel 6 (11n – 40MHz), and channel 11 (11n – 40MHz). Choosing an 11n 40MHz channel will allow Omnipeek to capture all packets on these three channels, including any b/g/n traffic using a 20MHz bandwidth (more on this later). Click OK, and then click OK again. Now click Start Aggregator to begin the analysis.

To verify that the Aggregator is working properly, begin a capture and verify that frames from each of the channels you configured in the Aggregator are captured. It's possible that one or more of these channels will have only small amounts of traffic, depending on your Wi-Fi environment. You can view traffic being captured on the channels you selected in several ways. For a graphical view, select the Compass dashboard from the left-hand navigation bar.

The Compass dashboard can include several different data views. If it is not already selected, choose the Channels statistics chart window by clicking the tab, and it will display on the dashboard. Figure 8 shows an example of the Channel statistics chart window.

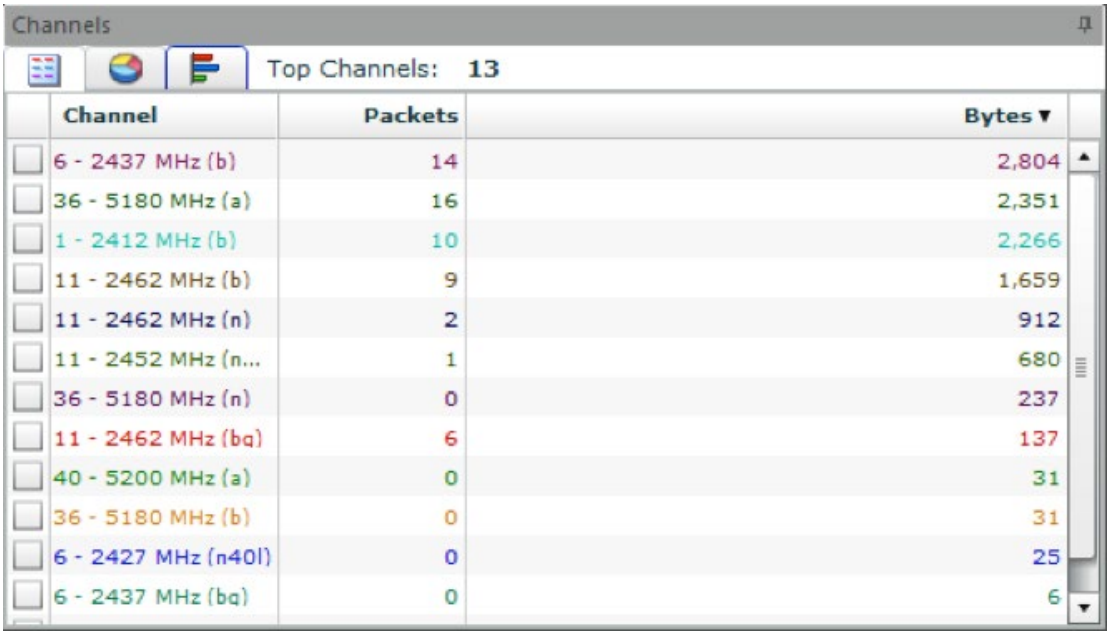

FIGURE 8: THE CHANNELS VIEW IN COMPASS—USE IT TO VERIFY THAT TRAFFIC IS BEING CAPTURED ON THE SELECTED CHANNELS

Another way to verify that you're capturing data from all the channels is in the Packets view. Be sure the Channel column is enabled. If not, then left-click anywhere within the column header to get the Packet List Options dialog and select Channel. You should see packets in this view that represent all of the channels that you selected.

Real-Time and Post-Capture Analysis Options

Based on your analysis requirements, and the performance of the computer running Omnipeek, it may be beneficial to configure Omnipeek's real-time analysis options (Figure 9). To be a bit more specific, Omnipeek is generally used for analysis in two ways: real-time or post-capture. While we have never heard of any shortage in computing power for 802.11 a/b/g analysis, three 802.11n adapters can capture so much data so quickly that it can become too much for standard notebooks to process everything in real time. 802.11ac makes things worse yet, but you can put your mind at rest: Omnipeek is already prepared to handle even the highest throughput rates. There are no hard-and-fast rules for how to configure the settings for online analysis: it is always a trade-off between the computing power of your measurement equipment and the data volume you need to analyze.

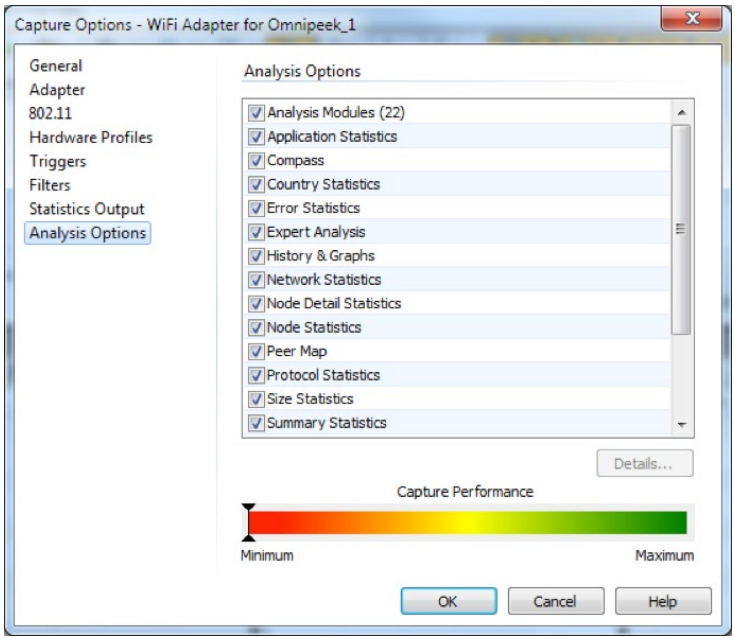

FIGURE 9: OMNIPEEK CAPTURE OPTIONS

Configuration depends on the various features you want to use in real time. You need to determine, based on your analysis needs and styles, what modules you want to have enabled and disabled. As you deselect options, the slider bar on the bottom will move to the right to indicate the impact of your choice. The options that affect analytical throughput the most are Expert Analysis and Voice and Video Analysis. If either of these options can be turned off, approximately half of your computing power is freed up for other tasks, such as write-to-disk without loss of any data (Figure 10).

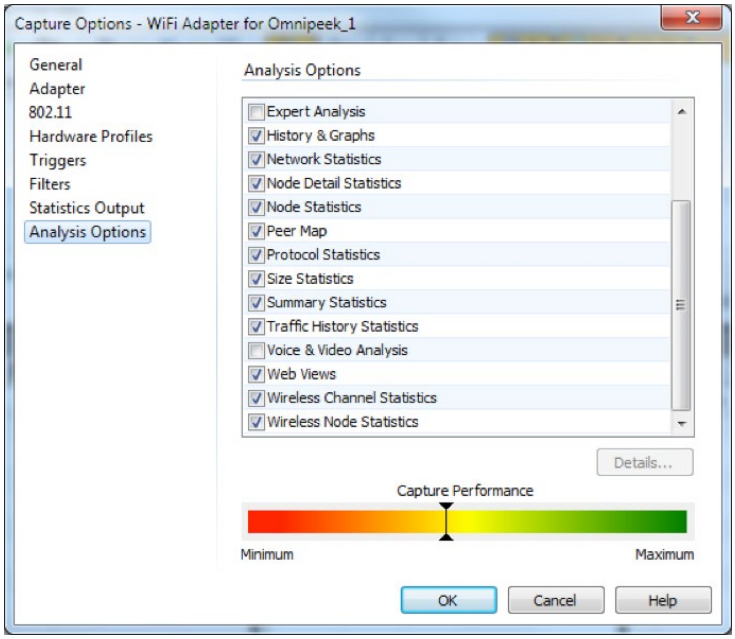

FIGURE 10: TURN OFF ALL UNNECESSARY ANALYSIS OPTIONS

If you are performing post-capture analysis, and want to capture and save the packets for future analysis (also referred to as capture-to-disk), then you can deselect all of the performance options during the capture. When you open the capture files later for analysis, you can re-enable the analysis options you choose. You will then have access to all of Omnipeek's analytical capability. For high-throughput networks (like 802.11n and 802.11ac) post-capture analysis might be the way to go. So you turn all Analysis Options off, write everything to your hard drive, and open the trace files afterwards, once you have captured the problem you want to analyze. But if you're just following a client around trying to figure out what's happening with roaming issues, then real-time analysis is more appropriate.

Filter Settings

Another approach to handle high bandwidth captures is to filter out uninteresting traffic. Again, three 802.11n or 802.11ac adapters can capture so much data so quickly that the screen instantly fills with clutter. Simplify analysis by selecting only the frame types you want to see. Figure 11 displays the built-in wireless filtering options. Remember, custom filtering is also available. It is extremely easy to develop your own filters with the graphical filter builder.

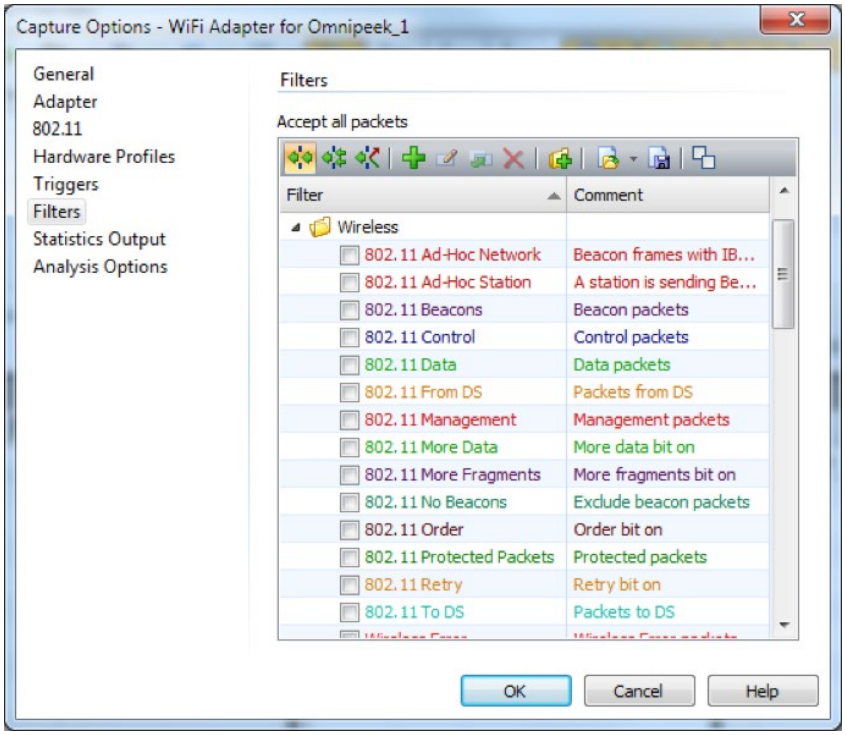

FIGURE 11. DEFAULT WIRELESS FILTERS INCLUDED WITH OMNIPEEK

If you are a field engineer, who is not the analyst, it might be more helpful to capture a wide variety of frames than to filter. Post-capture filtering and analysis can often be easier, and more frames give the analyst a better picture of the RF environment. If no filtering will be performed, then monitor capture performance to assure that frames are not being missed.

Omnipeek filters work by selecting either the Reject Matching or Accept Matching rule engine button and then selecting the filters you want to use with the rule engine.

Aggregation and Roaming

You already know that clients roam, but have you thought about the fact that in order to monitor clients, you must follow them? That's right — you need to be near the client in order to monitor its conversations with multiple APs operating on various channels. Configure Omnipeek for the channels that APs in the surrounding areas are using. This may mean monitoring 3-6 simultaneous channels depending on the band and channel reuse pattern of the network infrastructure.

Roaming analysis is another built-in feature in Omnipeek, but it is only available, and visible, when channel aggregation is in use. Roaming analysis is performed automatically. You can view the results of any roaming analysis by clicking any one of the roaming analysis views, Log, by Node, or by AP, from the left-hand navigation bar (Figure 12).

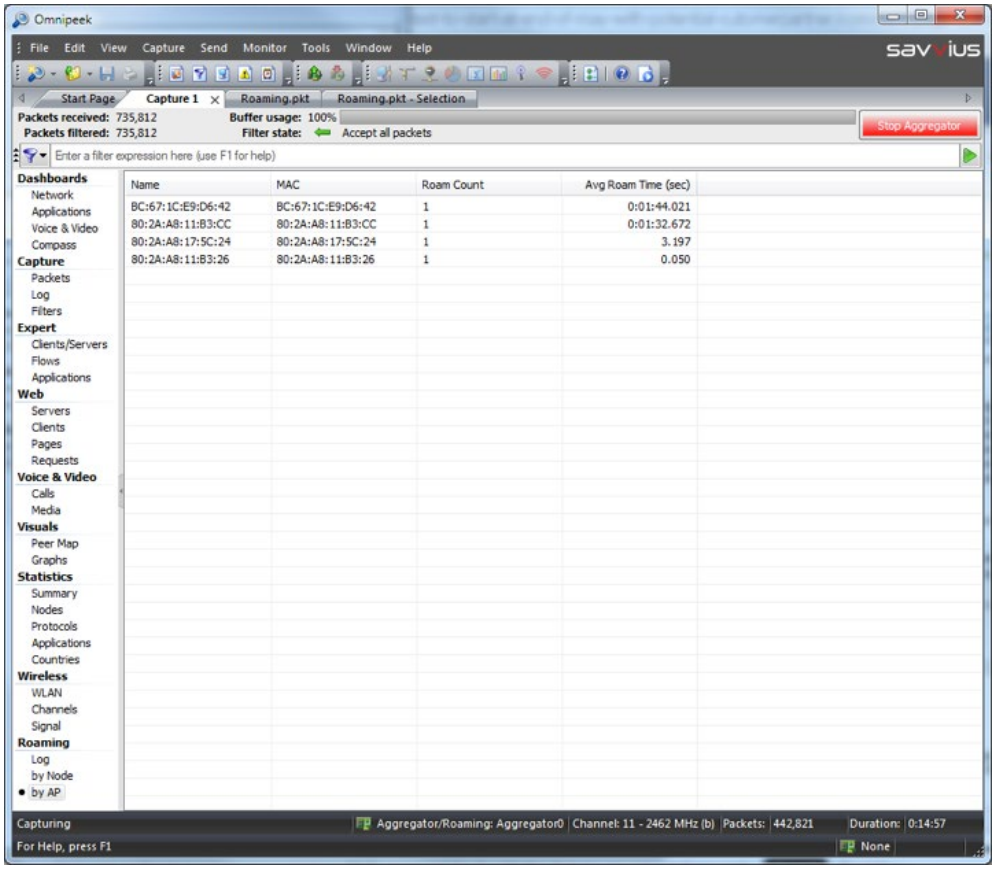

FIGURE 12. AN EXAMPLE OF ROAMING ANALYSIS DISPLAYED BY AP

L2 vs. L7 Roaming

BSS transition time (a.k.a. roam time) is important for all clients, but especially for latency-sensitive clients like VoWiFi phones and badges. Layer-2 (L2) roaming is the act of moving the client's association from one AP to another. Fast BSS Transition (the official name for roaming) is standardized in 802.11r.

Layer-7 (L7) roaming is an entirely different (and more important) analysis problem. Regardless of how fast the L2 BSS transition happens, if packets don't arrive at the upper layers in a timely manner, applications will experience problems. Roaming Analysis in Omnipeek helps with analyzing both L2 and L7 BSS transitions, enabling an entirely new level of troubleshooting capabilities.

For example, let's say we want to analyze a specific roaming event listed in the Roaming Log (see Figure 13). Double-click on one of the events, and Omnipeek will isolate the packets related to just that roam in a new analysis buffer, allowing you to instantly drill in.

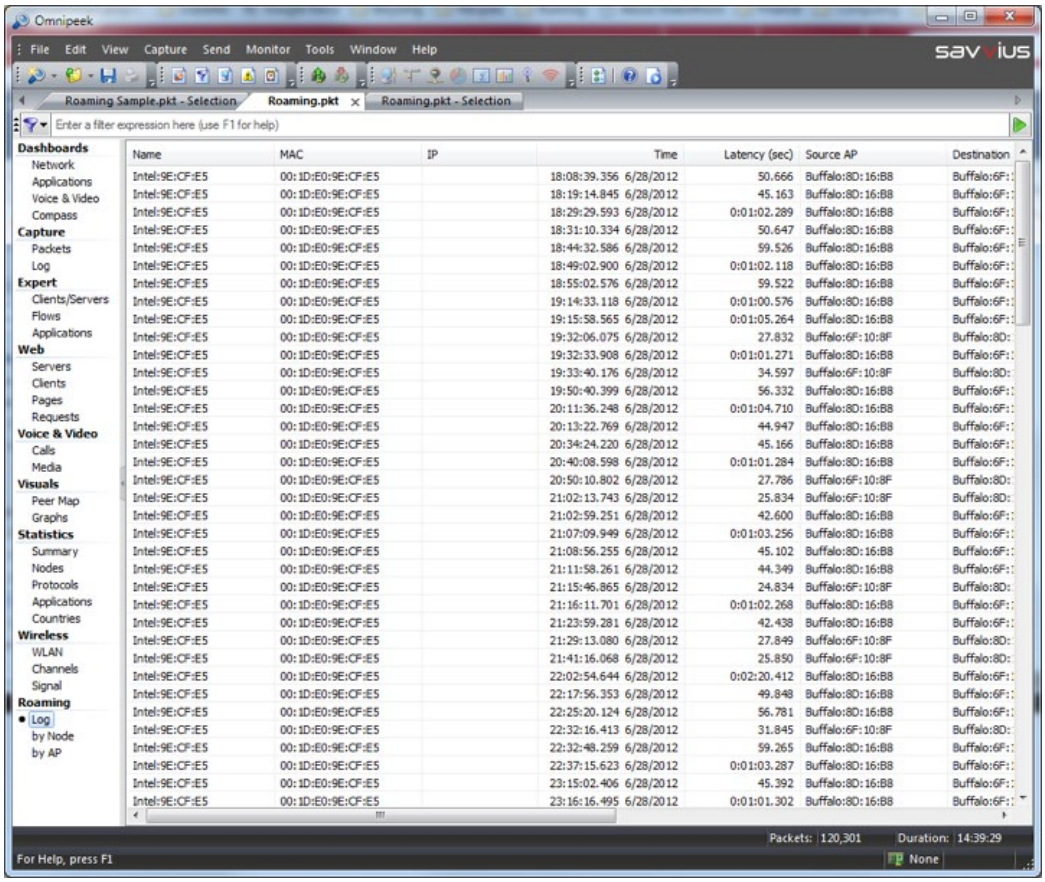

FIGURE 13. ROAMING LOG FROM OMNIPEEK SHOWING EVERY ROAM THAT HAS OCCURRED ON THE MONITORED CHANNELS

Double-clicking on the 5th entry in Figure 12 illustrates this process. Isolate just the packets in this roaming event by choosing "Copy selected packets to a new window" (Figure 14).

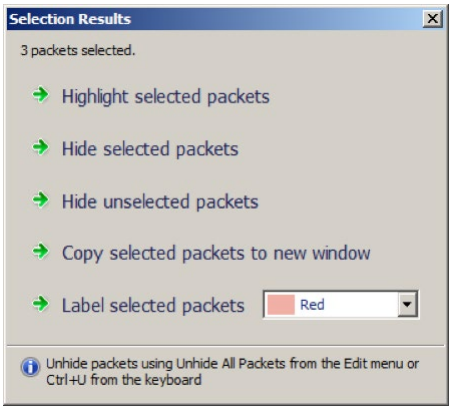

FIGURE 14. SELECT RELATED PACKET OPTIONS

Once the packets are isolated, it is easy to see in the Compass dashboard exactly what's happening.

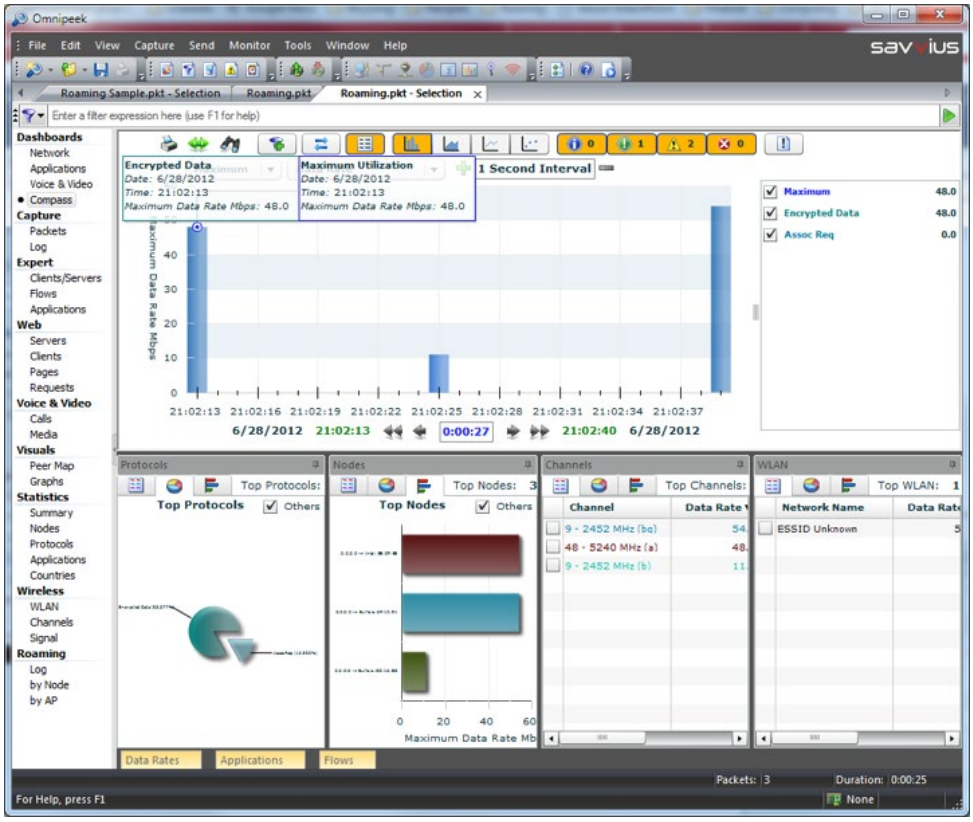

FIGURE 15. COMPASS VIEW OF ONE SPECIFIC ROAMING EVENT

Choosing Date Rate as the display option in Compass, we can easily see the last data packet (encrypted data) sent before the roam, the association request and first data packet after the roam, and the data rates for these packets (Figure 15). To gain more insight into the timing between the association request and the data packet, we can zoom in on just those packets using Compass, by selecting a time range of less than 10 seconds and zooming in from a "1 second interval" to a "50 Millisecond Interval." Doing this shows us the following.

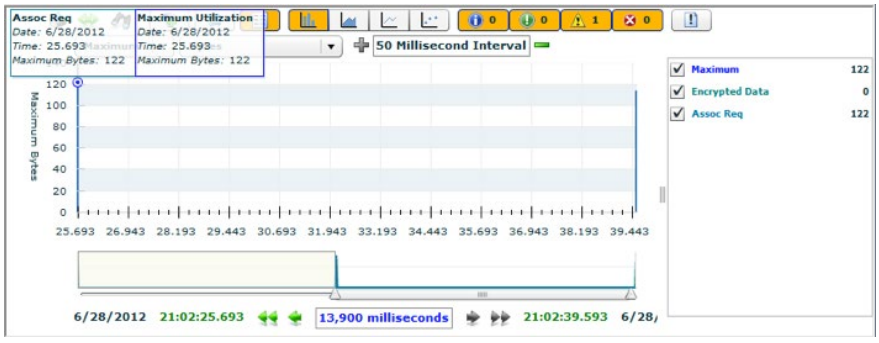

FIGURE 16. ZOOMING IN ON A ROAMING EVENT USING THE COMPASS DASHBOARD

On the left we see the association request at 25.693 and towards the right the encrypted data packet at 39.543, clearly showing a latency of 13,850 milliseconds between association and data being transmitted (Figure 16).

Summary

This tech brief is a basic “how to” that gets the analyst started doing multi-channel WLAN analysis. It’s not meant to be in-depth training on analysis or troubleshooting. For more information on the capabilities of Omnipeek, refer to https://www.savvius.com/products/network_visibility_performance_diagnostics/omnipeek_family. For more information on vendor-neutral training and certification, refer to cwnp.com.