# What's Really Happening on Your Wireless Network…

# Multi-Channel Analysis for WLAN Mobility

WHITE PAPER

In this white paper, we introduce the hardware, software, and techniques that make it possible to capture frames on multiple channels simultaneously, while the network analyzer merges all frames into a single capture display window and performs real-time Expert analysis.

**Author:**
Jay Botelho
Director of Product Management
WildPackets, Inc.
jbotelho@wildpackets.com

**Contributors:**
Devin Akin, CWNE #1
Chris O'Donnell, CWNE #64
Shawn Jackman, CWNE #54
Marcus Burton, CWSP
Chris Bloom
Matthias Lichtenegger

WildPackets, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
925.937.3200
www.wildpackets.com

# Multi-Channel Analysis for WLAN Mobility

# Multi-Channel Analysis for WLAN Mobility

## Introduction

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 so long, 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! It vanishes from the analyzer's view and troubleshooting stops right there. This has been a particularly perplexing problem for 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 whitepaper 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 in this whitepaper.

Multi-channel capture was a bit of a pipe dream until only recently, when it was implemented by WildPackets in the OmniPeek product line. For the sake of examples, we'll be using the usual 2.4 GHz suspects of channels 1, 6, and 11 in this whitepaper, even though the techniques are applicable for any channels in either the 2.4 or 5GHz bands.

## Hardware and Software

Not every protocol analyzer can perform multi-channel capture, aggregation, and analysis. 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 white paper you will find references to several specific products to make it easier to 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 white paper; 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) OmniWiFi USB 2.0 802.11a/b/g/n Dual-Band WLAN Adapters: http://www.wildpackets.com/products/omniwifi_adapter
- (1) WildPackets OmniPeek Enterprise Network Analyzer: http://www.wildpackets.com/products/omnipeek/enterprise_overview
- WildPackets Ralink drivers for the OmniWiFi WLAN adapter
- (1) Laptop PC with stacked USB 2.0 ports, at least 2 GB of RAM, a fast CPU, and Windows 7

**Figure 1 OmniWiFi USB 2.0 802.11a/b/g/n Dual-Band WLAN Adapters**

# Multi-Channel Analysis for WLAN Mobility

The OmniWiFi WLAN adapter is dual-band 802.11n, 3-stream capable (up to 450Mbps data rate), has a Ralink chipset, and is supported by the multi-channel aggregation and roaming analysis features in OmniPeek. Having a USB 2.0 interface allows for use of multiple simultaneous adapters on the same laptop PC. Special WildPackets drivers are required for this adapter to operate properly with OmniPeek and its associated feature.

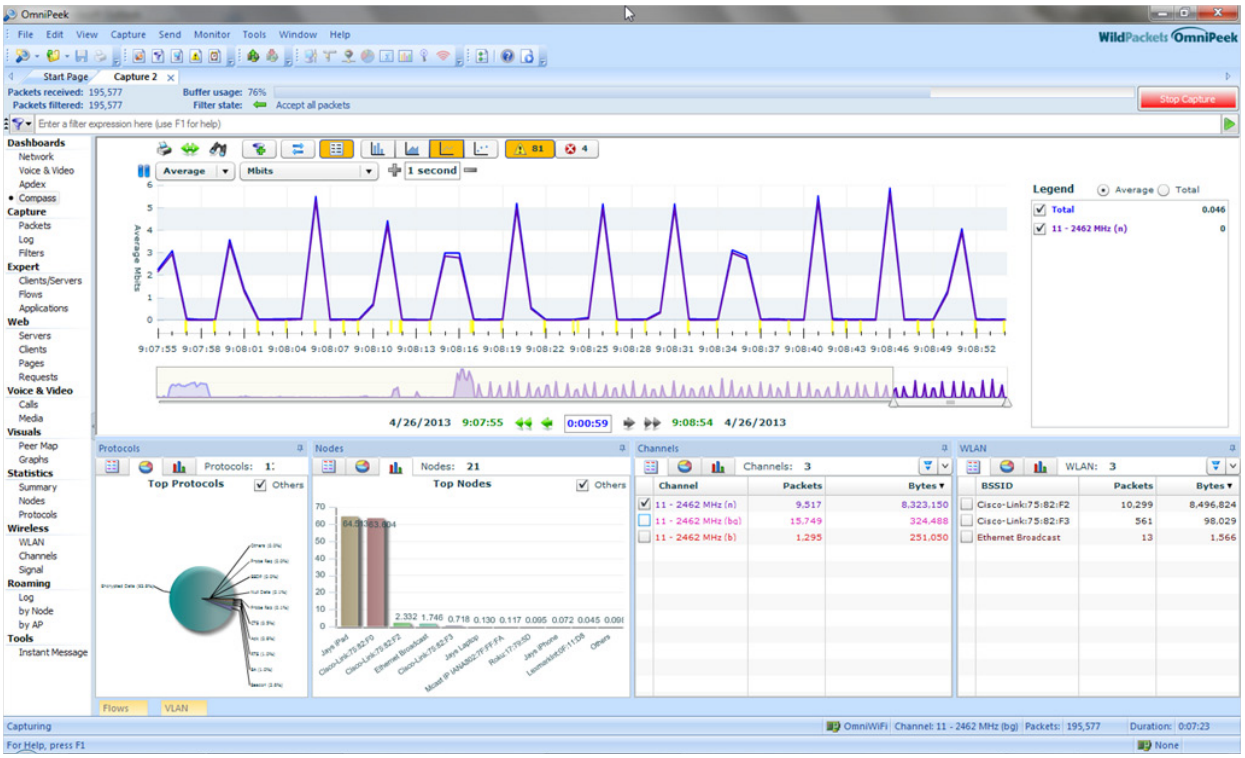


**Figure 2: WildPackets OmniPeek Compass dashboard showing wireless utilization, channels, and wireless networks**

OmniPeek Enterprise is WildPackets' 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 OmniWiFi. Everything else that's needed, including roaming analysis, is built into OmniPeek.

OmniPeek is powerful software, and performs a great deal of analysis. The laptop on which you run OmniPeek should have at least 2GB of RAM so that at least 512 MB can be dedicated to the packet buffer, and the CPU should be pretty hefty. A laptop with 4GB of RAM is even better. We will discuss settings for performance later in this white paper.

## Installation and Configuration of OmniWiFi WLAN Adapter Driver

In this section, we will describe the installation and configuration of the WildPackets driver for the OmniWiFi WLAN adapter. First, plug each of your three OmniWiFi WLAN adapters into three available 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. Our experience is that two devices can typically be handled by an unpowered USB hub, but three devices often causes problems, including BSODs

in Windows and/or USB ports being made unavailable until the next reboot. Again, this is not a problem with adapters or the driver. It is simply an available power issue via USB. 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 OmniWiFi WLAN adapters.

In our case, we have three available USB ports, so we'll just connect directly to each (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 OmniWiFi Adapters connected to three unique USB ports on a laptop**

OmniWiFi requires 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, as follows.

To install the OmniWiFi driver:

1. Open the Device Manager Control Panel.
2. Right-click the appropriate OmniWiFi wireless adapter, and select 'Update Driver Software.'
3. Click 'Browse my computer for driver software.'
4. Click 'Let me pick from a list of device drivers on my computer.'

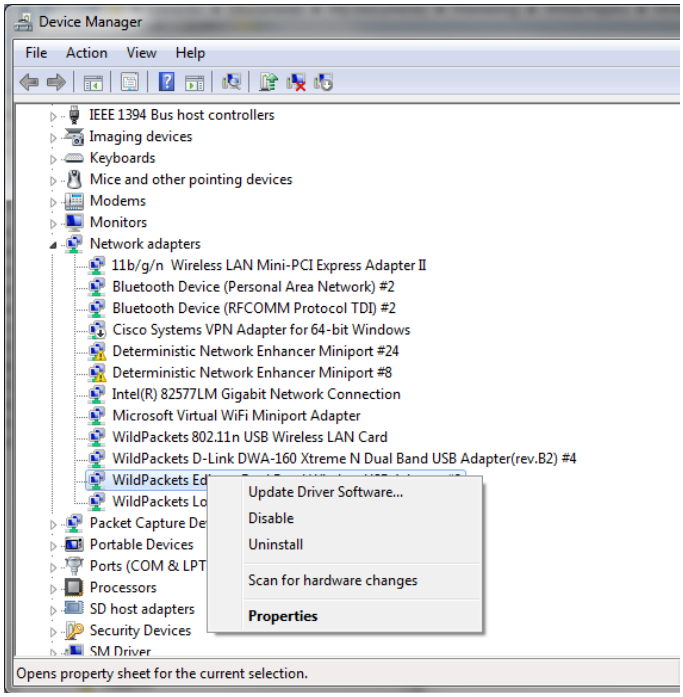


**Figure 4 Windows Device Manager – choose the adapter whose driver you need to update**

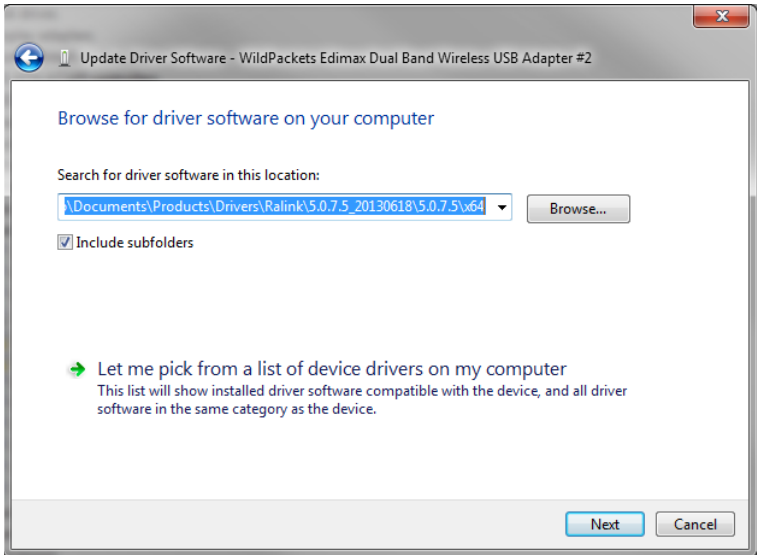


**Figure 5 Make sure to choose "Let me pick from a list of device drivers on my computer"**

5. Choose the type of your device and click Next

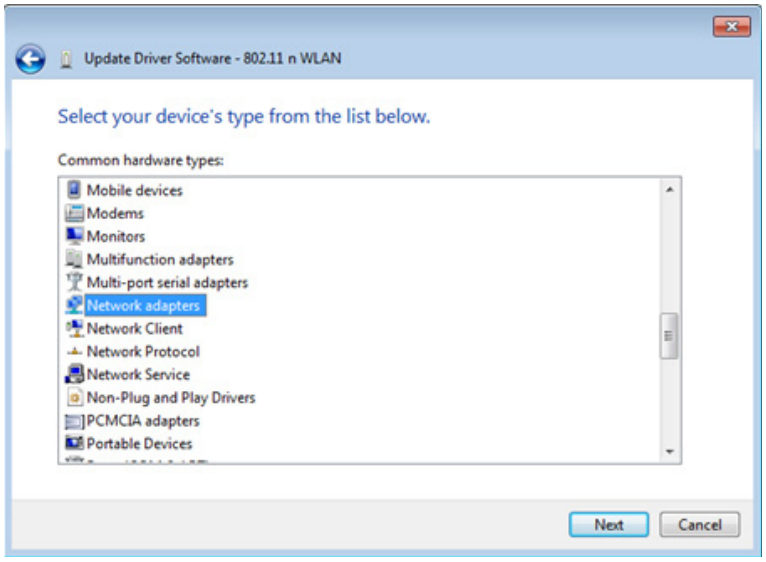


**Figure 6 Choose your adapter type**

6. Click 'Have disk'.

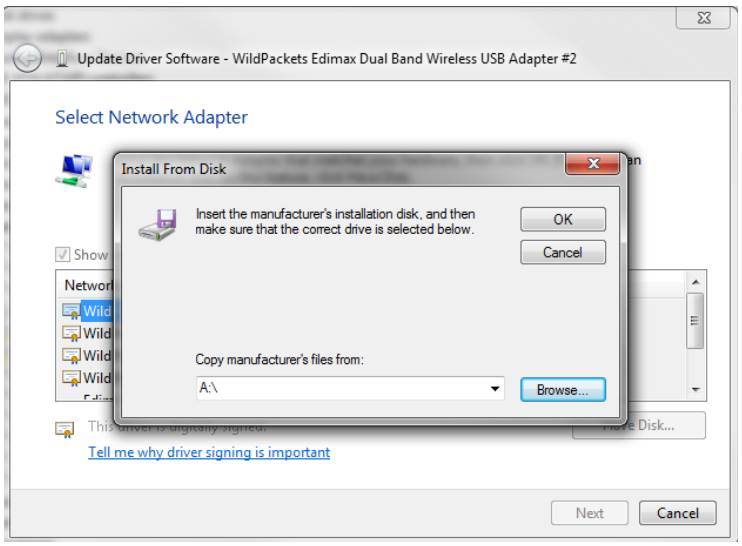


**Figure 7 OmniWiFi drivers can be found in C:\Program Files (x86)\WildPackets\OmniPeek\Drivers\OmniWiFi**

7. Browse to the directory that contains the driver and select the rt2870.inf file. This file is included with OmniPeek. For 32-bit Windows you can find the driver here: C:\Program Files (x86)\WildPackets\OmniPeek\Drivers\OmniWiFi\x86. For 64-bit Windows you can find it here: C:\Program Files (x86)\WildPackets\OmniPeek\Drivers\OmniWiFi\x86_64.

8. Click Open and then OK.

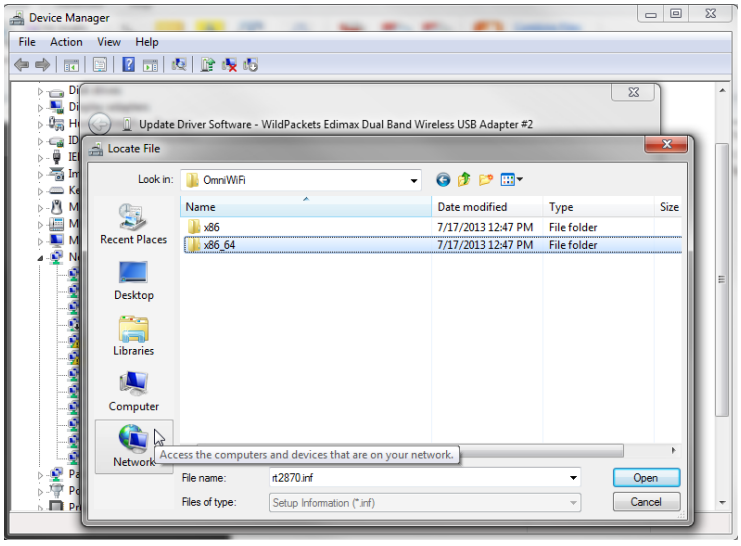


**Figure 8 Make sure to choose the right drivers (32 vs. 64-bit) for your OS**

9. Choose the appropriate manufacturer and network adapter and click Next.

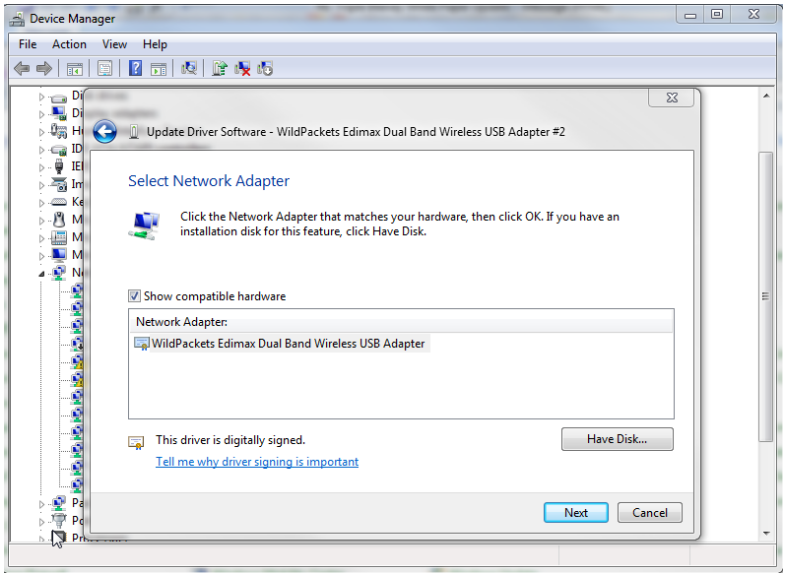


**Figure 9 Select your network adapter type**

10. Click Yes to continue the installation even if you receive a message saying 'Installing this driver is not recommended because Windows cannot verify that it is compatible with your hardware.'

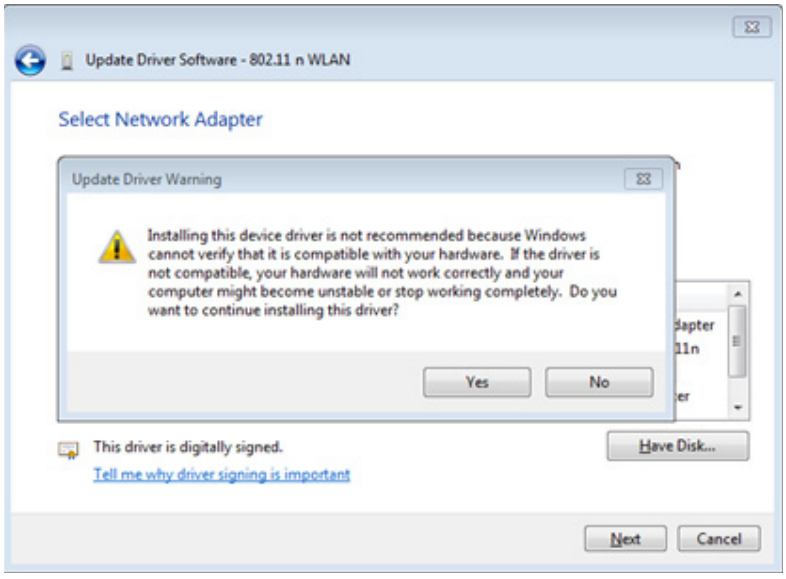


**Figure 10 Continue installing even if you see this message**

11. Click 'Continue Anyway' to continue the installation even if you receive a message saying 'The software you are installing for this hardware: '...' has not passed Windows Logo testing to verify its compatibility with Windows 7.'

12. Click ‘Close’ to complete the installation.
13. Select Yes to reboot if asked. If not asked, we recommend that you reboot the computer anyway.
14. Remember, you will 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”.

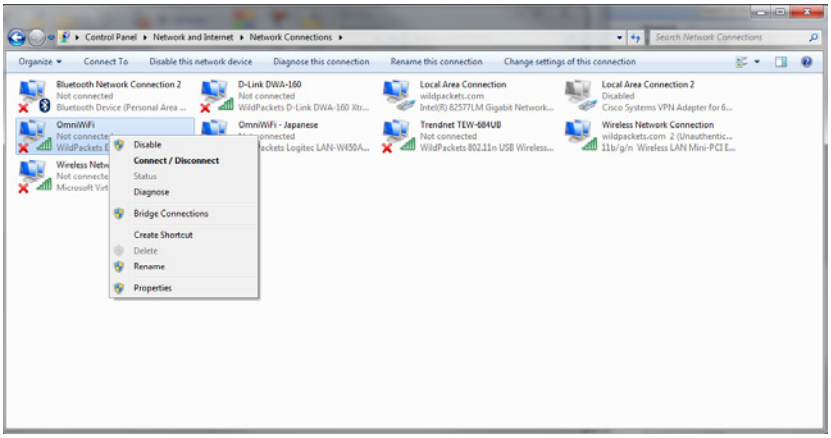


**Figure 11 Give each OmniWiFi adapter a distinguishing name**

To confirm that your drivers were successfully installed, start OmniPeek and select an OmniWiFi USB adapter. You should see the following in the description window: “WildPackets API: Yes”

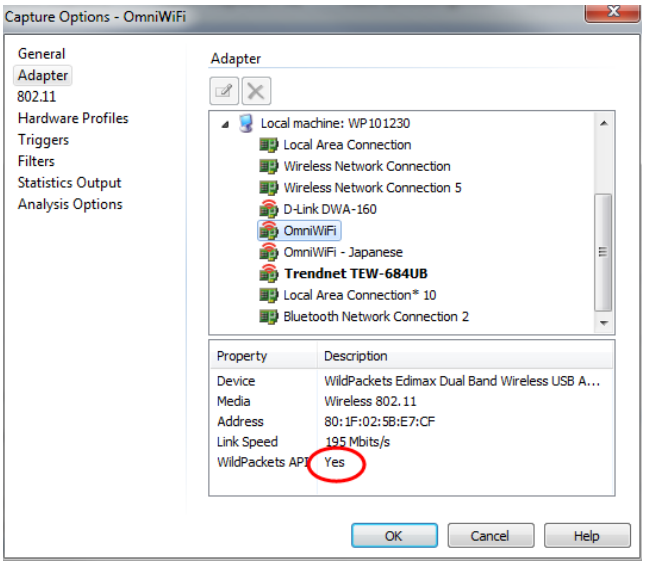


**Figure 12 Make sure this dialog shows WildPackets API = Yes**

Please note: the WLAN Analysis Modules within OmniPeek will only be loaded if “WildPackets API = Yes”.

It’s also important to label or color-code your OmniWiFi adapters and your USB ports so that you always put the same adapter into the same USB port. Failing to do so will cause Windows to recognize the OmniWiFi as a new adapter (again, it’s a Windows thing), which will mean loading the drivers for that adapter again.

## Performing Multi-Channel Analysis

With OmniPeek and the OmniWiFi adapters 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 13.

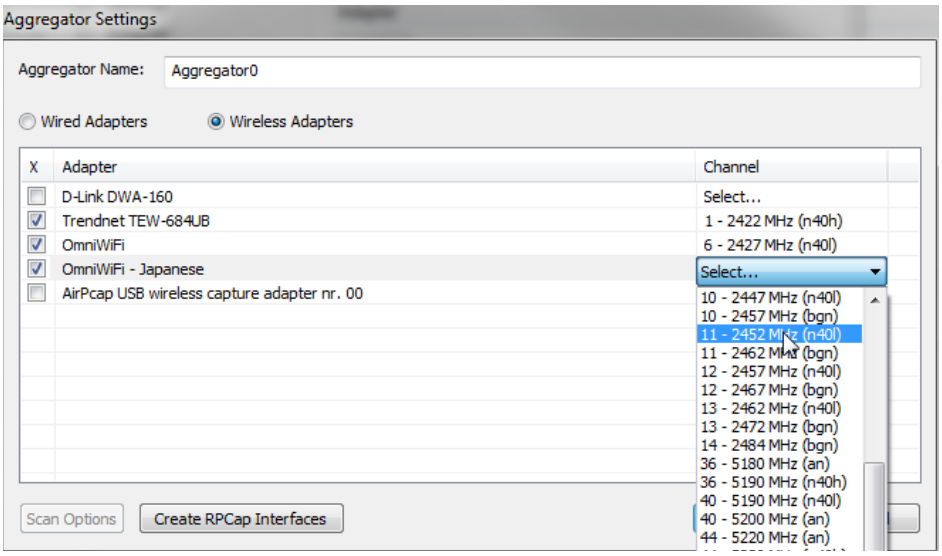


**Figure 13 Configuring OmniPeek for multi-channel analysis**

The dialog box shown in Figure 13 confirms that you have correctly installed the OmniWiFi driver, otherwise the adapters will not appear in this dialog. Choose each OmniWiFi adapter that you wish to use, and select the channel for each adapter from the drop-down channel selection box. In Figure 13 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 any and 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 on them depending on your Wi-Fi environment. You can view traffic being captured on the channels you selected in several ways. For a graphical view, go to the Compass dashboard (from the left-hand navigation bar).

The Compass dashboard can include several different data views. If not already selected, choose the Channels view by clicking the tab, and it will be included on the dashboard. An example of the Channels tab can be found in Figure 14.

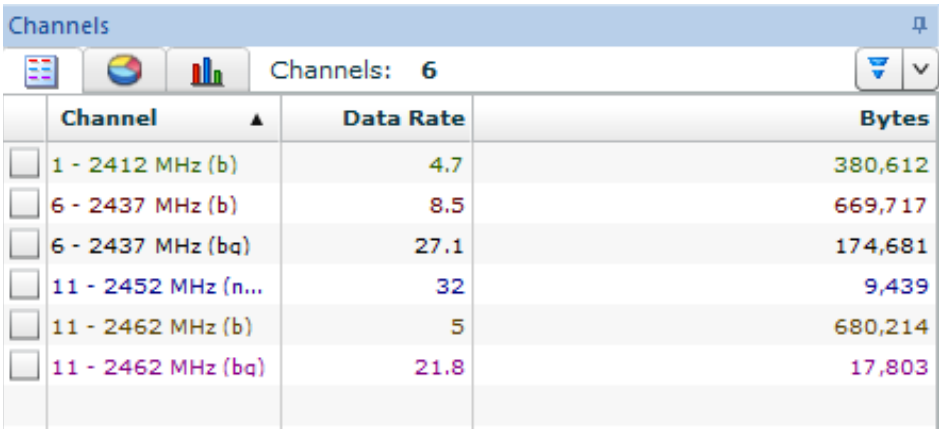


**Figure 14 The Channels view in Compass - you can use it to verify that traffic is being captured on the selected channels**

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. To be a bit more specific, OmniPeek is generally used for analysis in one of 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 will make 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

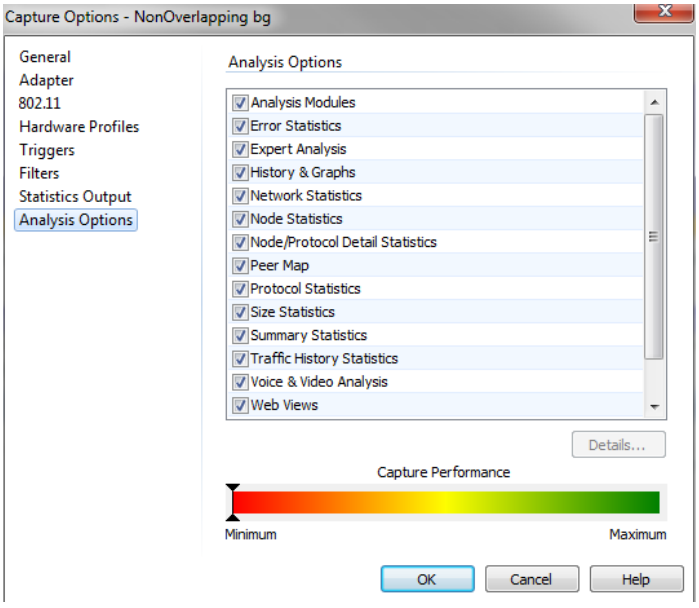


**Figure 15 OmniPeek capture options**

power of your measurement equipment and the data volume you need to analyze. 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 in a relative way to indicate the impact of your choice. The options that affect analytical throughput the most are the Expert Analysis and the Voice and Video Analysis options. If either of these options can be turned off, approximately half of your computing power is freed up for other tasks, e.g. write-to-disk without loss of any data.

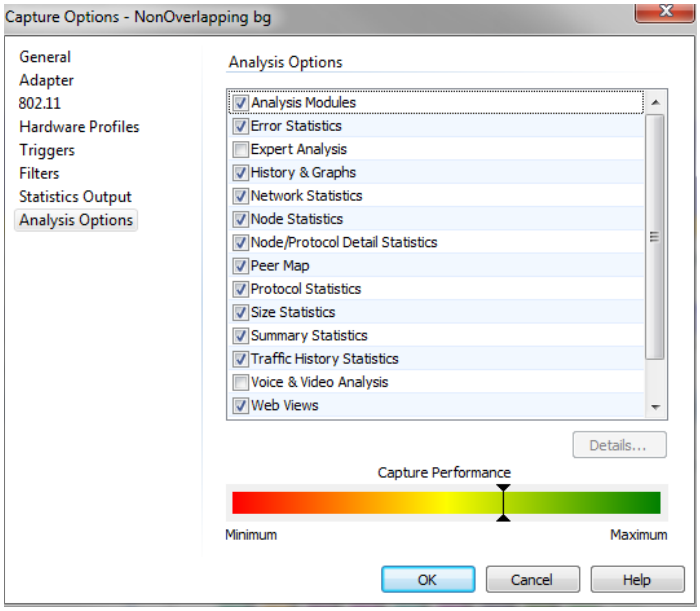


**Figure 16 Turn off all unnecessary analysis options**

If post-capture analysis is being performed, meaning that the user wants to capture and save the packets for future analysis (also referred to as capture-to-disk), then all of the performance options can be deselected during the capture. When the capture files are opened later for analysis, the analysis options of choice can then be re-enabled. The user 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, when 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 adapters can capture so much data so quickly that the screen instantly fills with clutter. Analysis is greatly simplified by selecting only the frame types you want to see. In Figure 17, the screenshot illustrates built-in wireless filtering options. Remember, custom filtering is also available. It is extremely easy to

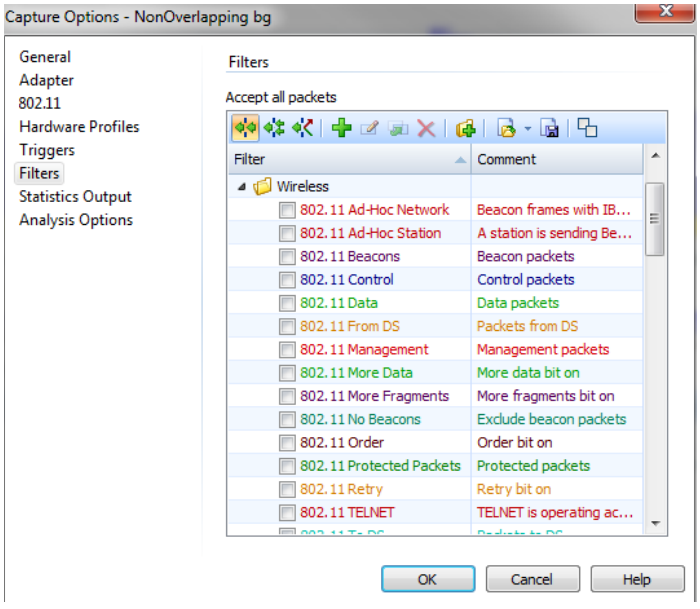


**Figure 17 Default wireless filters included with OmniPeek**

develop your own filters with the graphical filter builder.

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 the Accept Matching rule engine buttons 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. OmniPeek must be configured for the channels that are used by the APs in the surrounding areas. This may mean monitoring 3-6 simultaneous channels depending on the band and channel reuse pattern of the network infrastructure.

| Name | MAC | Roam Count | Avg Roam Time (sec) |
|---|---|---|---|
| Cisco:61:0A:A0 | 00:14:1B:61:0A:A0 | 40 | 31.154 |
| Cisco:61:0E:D0 | 00:14:1B:61:0E:D0 | 40 | 27.677 |

**Figure 18 An example of roaming analysis displayed by AP**

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.

## 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 now standardized in 802.11r, and the Wi-Fi Alliance is now certifying Voice-Enterprise based on 802.11r and 802.11k.

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 19). By simply double-clicking on one of the events, OmniPeek will isolate the packets related to just that roam in a new analysis buffer, allowing you to instantly drill in.

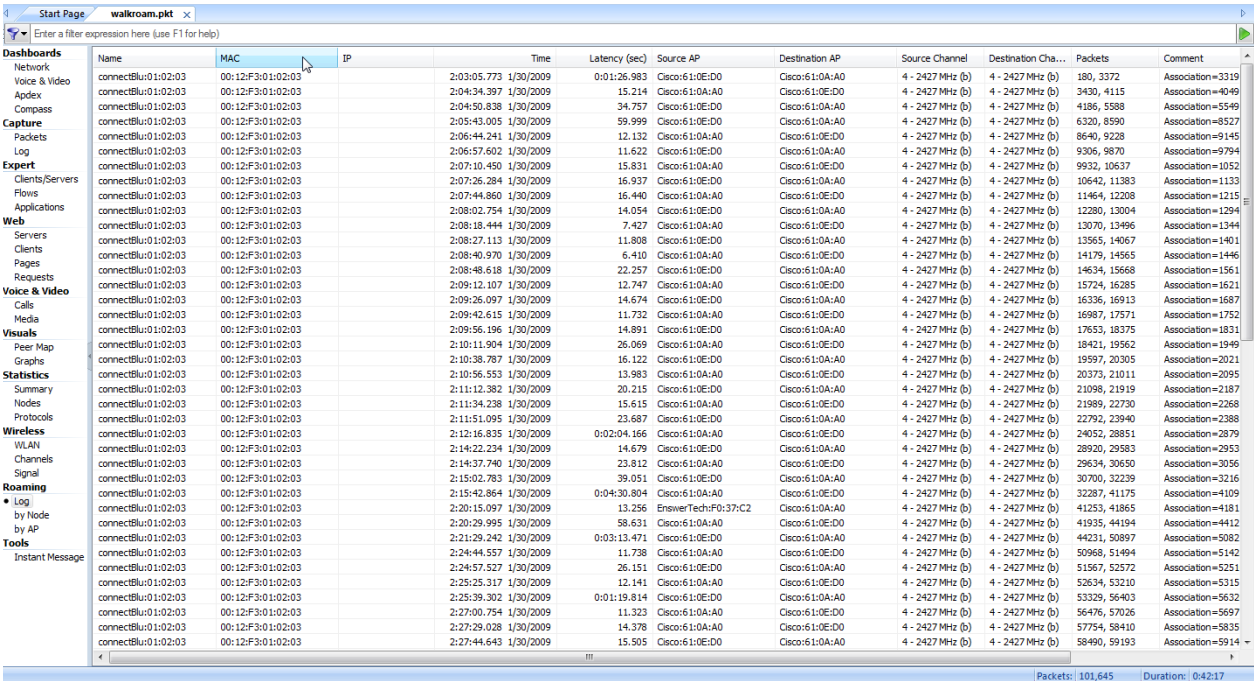


**Figure 19 Roaming Log from OmniPeek showing every roam that has occurred on the monitored channels**

Double-clicking on the 11th entry in Figure 19 illustrates this process. Isolate just the packets in this roaming event by choosing “Copy selected packets to a new window”.

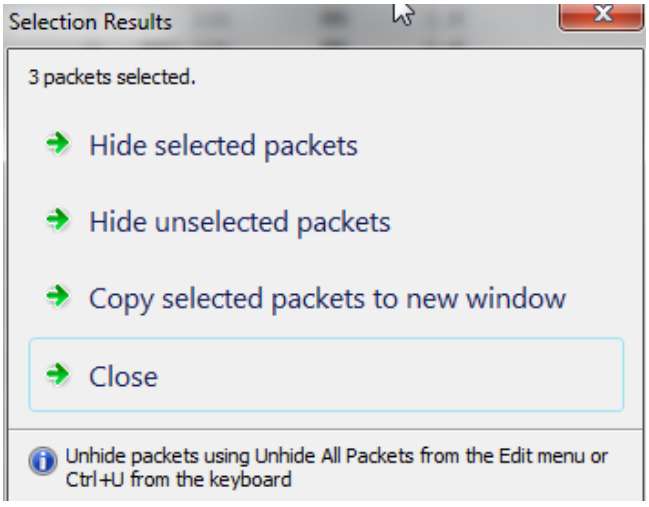


**Figure 20 Select Related packet options**

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

Choosing Date Rate as the display option in Compass, we can easily see the last data packet (encrypted data) sent

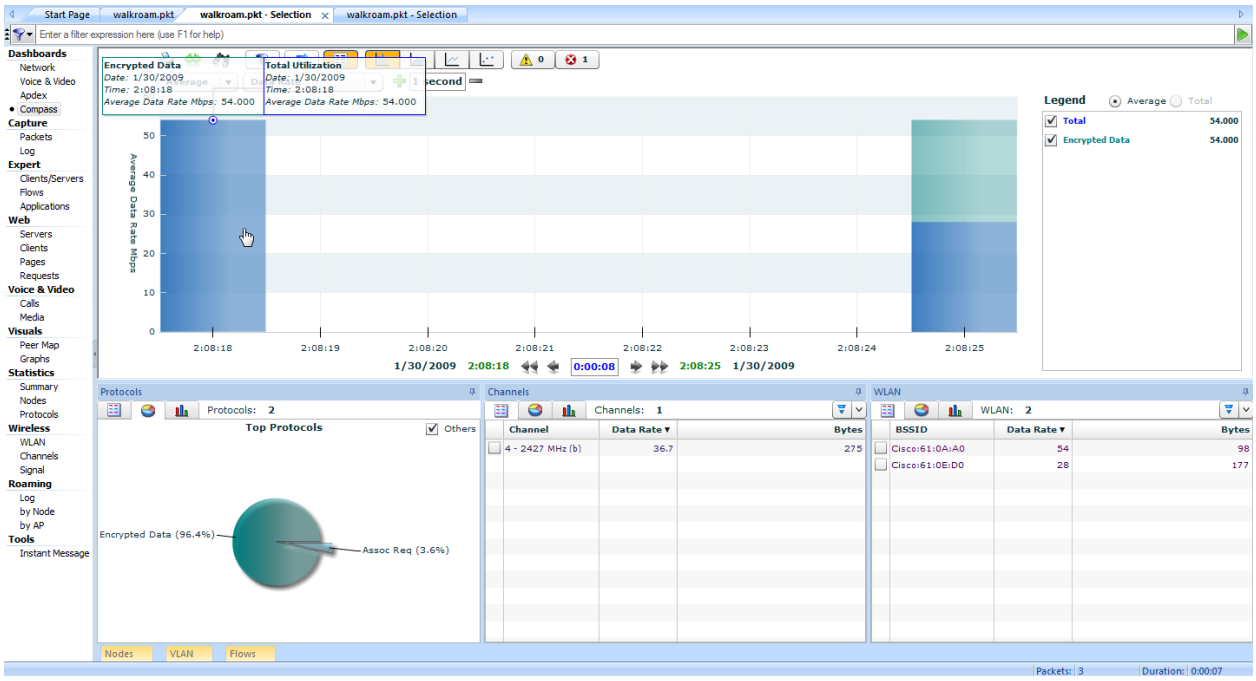


**Figure 21 Compass view of one specific roaming event**

before the roam, as well as the association request and first data packet after the roam, as well as the data rates for these packets (Figure 21). 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 switching from “seconds” view to “milliseconds” view. Doing this shows us the following.

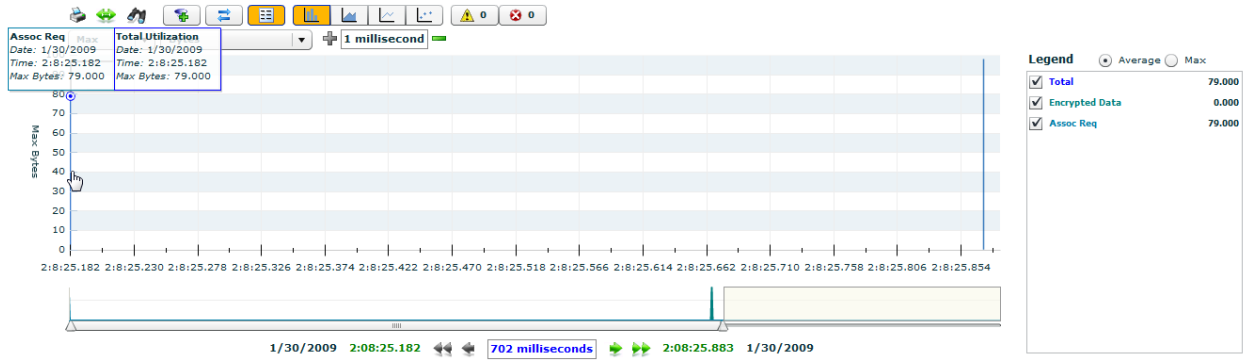


**Figure 22 Zooming in on a roaming event using the Compass dashboard**

On the left we see the association request at 02:08:25.182 and towards the right the encrypted data packet at 02:08:25.871, clearly showing a latency of 689 milliseconds between association and data being transmitted.

## 20MHz vs. 40MHz Channels

The 802.11n specification defines a 40MHz channel as the combination of a primary 20MHz channel and a secondary 20MHz channel. A 40MHz channel allows for a higher data rate than a 20MHz channel, but this feature is only available for 802.1n devices (and now 802.11ac devices). The primary 20MHz channel is used for all primary communications, including all management packets, providing backward compatibility for all devices, including a/b/g devices, or those 11n devices that are not compatible with the 40MHz mode (not all 11n devices allow the 40MHz mode). When an AP and a station are both compatible with the 40MHz mode, communications between just those devices will switch to 40MHz mode. The center frequency for communication is shifted from that assigned to the primary 20MHz channel to a frequency either higher or lower than that associated with the primary channel. For example, let's say the primary channel is 36, and we want to use the 40MHz bandwidth. Since there are no channels below 36, the only option is to bond channel 36 with one above it, channel 40, as illustrated in Figure 23. The center frequency for the 40MHz communication is shifted to be between the center frequencies of channel 36 and channel 40, and the WLAN radio shifts from 20 to 40MHz operation to send the specific packets.

Let's look at selecting 40MHz 802.11n channels in OmniPeek. It's important to understand 40MHz channel nomenclature in the analyzer. OmniPeek defines a 40MHz channel selection as {Pri - n40x}, where x is the secondary channel, which is either low or high. For example, {36 – n40h} means channel 36 is the primary 20MHz channel and channel 40 is the secondary 20MHz channel. See Figure 5 which illustrates the selection of 40MHz channels in OmniPeek. When a 40MHz 11n channel is selected in OmniPeek, for example 36-n40h, all communications on the primary channel (channel 36) are captured, as well as all communications using the bonded 40MHz channel, making this the correct selection when you have a mixed a/b/g and 11n environment.

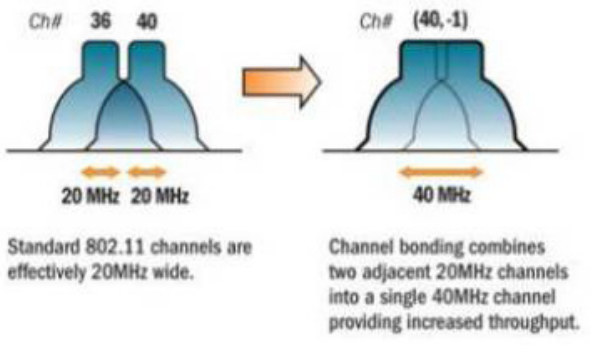


**Figure 23 Channel bonding using Channel 36 as the primary channel and channel 40 as the bonded channel (http://wifijedi.com/2009/01/25/how-stuff-works-channel-bonding)**

# Summary

This whitepaper 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 www.wildpackets.com/omnipeek, and for more information on the extensibility of OmniPeek, you can visit mypeek.wildpackets.com. For more information on vendor-neutral training and certification, refer to cwnp.com.