The Triple Blendy:
Multi-Channel Capture for Mobile Clients

White Paper

March 2009
Version 1.00

Author:
Devin Akin, CWNE #1
Chief Technology Officer
CWNP, Inc.
Devin.Akin@cwnp.com

Contributors:
Chris O'Donnell, CWNE #64
Shawn Jackman, CWNE #54
Marcus Burton, CWSP
Chris Bloom
Jay Botelho

Table of Contents

Executive Summary

Clients roam. It's what they do. Today's wireless network is 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 "The Triple Blendy." 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.

Intent

We will introduce the hardware, software, and techniques that make it possible to capture frames on multiple channels simultaneously, while the analyzer merges all frames into a single capture display window and performs real-time expert analysis. Problems were encountered during the creation of this whitepaper. Some of those problems are still not solved, such as USB adapter drivers and L2 vs. L7 roaming parameters within Roaming plug-in.

Naming

Just because I know you're asking yourself, "Why 'The Triple Blendy?'" I've decided to briefly answer that question here. It comes from, "The Triple Lindy" from the Rodney Dangerfield movie called, "Back to School." The Triple Lindy was a dive thought to be impossible – until Thornton Melon (played by Dangerfield) pulls it off to win the swim meet. In case you missed the movie…

http://en.wikipedia.org/wiki/Back_to_School

http://www.youtube.com/watch?v=J8zLSGvV454

Multi-channel capture was also a bit of a pipe dream until only recently, when it was implemented by WildPackets in their OmniPeek product line. Since we'll be using the usual 2.4 GHz suspects of channels 1, 6, and 11 in this whitepaper, this will be a triple channel capture and aggregation – hence The Triple Blendy.

Hardware & Software

Not every vendor's protocol analyzer can perform multi-channel capture, aggregation, and analysis; therefore, an analyzer with these capabilities had to be chosen for this whitepaper. Use of this vendor's analyzer is in no way an endorsement of their products over those of competing vendors. This statement also applies to the Velcro, USB cable and hubs, laptop, and the Wi-Fi adapter. Each piece of hardware and software was chosen to perform a specific task. Functionality and aesthetics were the only two criteria. You have to admit that we chose some great USB hubs though.

Hardware and Software Configurations

The following is a list of hardware and software required to perform The Triple Blendy; deviate at your own risk. Other hardware configurations might work, but we have only tested this configuration.

The hardware and software for The Triple Blendy:

- (3) Linksys WUSB600N USB 2.0 802.11n Dual-Band Wi-Fi Adapters
  - o http://www.linksys.com/servlet/Satellite?c=L_Product_C2&childpagename=US%2FLayout&cid=1175243256159&pagename=Linksys%2FCommon%2FVisitorWrapper&lid=5615933028B33
- (1) USBGeek.com "USB X Hub" USB 2.0 Hub – Desktop-mounting
  - o http://www.usbgeek.com/prod_detail.php?prod_id=0943
- (1) Gadget4All.com "UHUB000200" USB 2.0 Hub – Laptop-mounting
  - o http://www.gadget4all.com/prod_detail.php?prod_id=00372&dept_id=003&cat_id=014
- (1) USBFever.com "E129-B092" USB 2.0 Cable, Dual Power Inlets
  - o http://www.usbfever.com/index_eproduct_view.php?products_id=236
- (1) Industrial Velcro Strips, 2-inch x 4-inch
  - o http://www.amazon.com/Velcro-brand-Industrial-Strength-Tape/dp/B0001DRZM2/ref=pd_sbs_op_5
- (1) WildPackets OmniPeek Enterprise, Wi-Fi Protocol Analyzer
  - o http://www.wildpackets.com/products/omnipeek/enterprise_overview
  - o WildPackets Ralink drivers for the Linksys WUSB600N wireless adapter
  - o Roaming Analysis Plug-in (available with a MyPeek login only)
  - o MultiChannel Aggregator Plug-in (available with a MyPeek login only)
- (1) Laptop PC with stacked USB 2.0 ports, at least 2 GB of RAM, a fast CPU, and Windows XP/sp3

CWNP does not sell this hardware or software, nor do we guarantee that you will be able to get The Triple Blendy working problem-free if you do exactly as we instruct in this whitepaper. There are far too many "unknowns" for us to guarantee anything, so please do not expect us to support you in any way. The best suggestion we can offer is to start a "Triple Blendy" forum thread on cwnp.com where end-users can collaborate.

FIGURE 1 - Linksys Dual-Band Wireless USB2 Adapter (WUSB600N)

The Linksys WUSB600N wireless client adapter is dual-band 802.11n capable, has a Ralink chipset, and is supported by the OmniPeek MultiChannel Aggregator Plug-in. 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 Enterprise and the MultiChannel Aggregator Plug-in.

FIGURE 2 - USB2 Hub Option 1 – Desktop Mount – Factory Picture

The USB2 "X Hub" is bus-powered, compliant with USB 2.0, and has 4 ports that are positioned in such a way that up to 4 Linksys WUSB600N wireless adapters can easily fit while oriented/polarized in the same way. We'll only be using three ports in this whitepaper. This hub is best suited for portable (as opposed to mobile) analysis, so if you are performing The Triple Blendy from your desk, this hub will do the trick nicely.

FIGURE 3 - USB2 Hub Option 1 – Desktop Mount – Real World Picture

The X Hub balances well on a flat surface with 1-4 Linksys WUSB600N adapters.

FIGURE 4 - USB2 Hub Option 2 – Laptop Mount – Factory Picture

The laptop-mounted USB hub shown has the perfect amount of spacing between the USB 2.0 ports, has a flat bottom that is well-suited for Velcro attachment to the back of a laptop screen, and is bus-powered. There is also a 4th USB port for further expansion.

FIGURE 5 - USB2 Hub Option 2 – Laptop Mount – Real World Picture

This picture shows the laptop-mounted USB hub with three WUSB600N adapters attached. Even with the three wireless adapters mounted, a small strip of Velcro holds the hub securely. It is best to mount the top edge of the USB hub to the top edge of the back of the laptop screen. This prevents the laptop screen from blocking RF signals. We have cut the Velcro that attaches directly to the USB hub to fit with no overlap. On the laptop, you can just have a nice square piece of Velcro.

FIGURE 6 - USB2 Cable – Dual Power Inlets – USB A Male (2) x USB B Mini (1)

Regardless of which USB hub you choose, you will need this cable. Neither USB hub can power three or more WUSB600N wireless adapters off a single USB port. This cable allows a secondary USB port to be used for power only while the primary port supplies both power and data connectivity. Both USB hubs use USB Type B Mini ports, so this cable has the correct attachment on the hub-end.

FIGURE 7 - USB2 Cable – Dual Power Inlets – Plugged Into Stacked USB Ports

In order to use the special USB cable, you will need two USB 2.0 ports very near each other on the laptop PC. It's usually best to have stacked USB 2.0 ports as shown above.

FIGURE 8 - Industrial Velcro Strips

You'll need this to attach the laptop-mounted USB hub to the back of the laptop screen. It's important to get the industrial-strength stuff so that a small strip will support the weight of the hub and three WUSB600N adapters.

FIGURE 9 - Wildpackets OmniPeek Enterprise with MultiChannel Aggregator Plug-in and Roaming Analysis Plug-in Software Enhancements

OmniPeek Enterprise is WildPackets' flagship product, and is a leading 802.11 protocol analyzer in the market. OmniPeek is the core product for The Triple Blendy, but not the entire picture. The Triple Blendy also requires both the MultiChannel Aggregator Plug-in and the Roaming Analysis Plug-in, and each of these pieces of software simply plug into OmniPeek. We'll explain how this works in the next section.

OmniPeek is a powerful, yet heavy piece of software. The laptop on which you run OmniPeek should have at least 2 GB 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 filtering and performance settings later in this whitepaper.

Installation & Configuration

In this section, we will illustrate installation and configuration of the WildPackets drivers for the Linksys WUSB600N wireless adapter, the MultiChannel Aggregator Plug-in, and the Roaming Analysis Plug-in software. Before installing either plug-in, you must successfully install and properly license OmniPeek Enterprise. This process is beyond the scope of this whitepaper, but more information can be found in the OmniPeek Enterprise product documentation.

Installation – Hubs and Drivers

The first step is to install the hub (using the dual power USB cable) that you've chosen to use for The Triple Blendy. Once installed, plug each of your three Linksys WUSB600N adapters into the USB hub. You will be asked for the drivers for these wireless adapters three times in a row.

> 📖 It's important to not install the drivers that are supplied by Linksys since we are dedicating these adapters to analysis only. Installing Linksys drivers first and then updating them with the OmniPeek driver causes the operating system to revert back to the Linksys driver upon reinsertion of the adapters.

The drivers consist of only two files: **rt2870.inf** and **rt2870.sys**. Load the WUSB600N drivers three times, and then verify proper installation by looking within the Windows XP Device Manager as shown in FIGURE 10.

FIGURE 10 - Driver Installation, Windows XP Device Manager
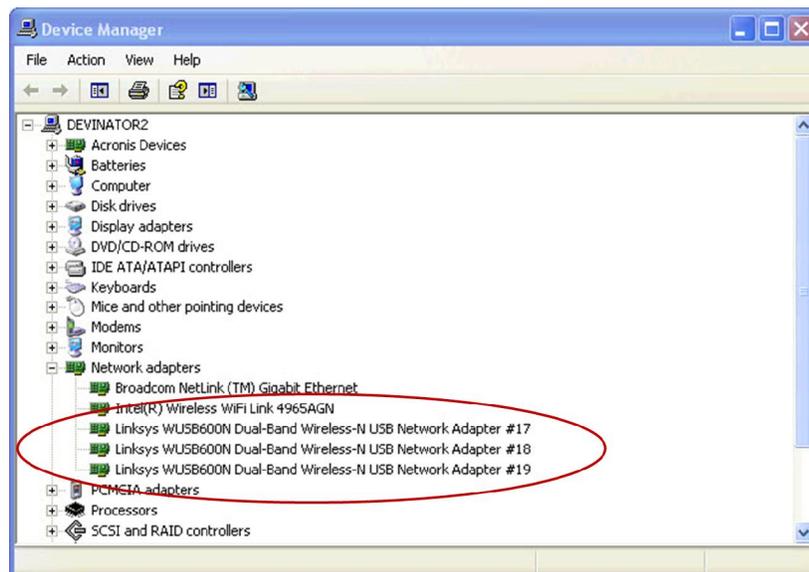
Bad driver installations or a lack of sufficient power to the USB hub will cause one or more of the WUSB600N adapters to have a yellow exclamation point or not to show up at all.

> 📖 It's important to label or color-code your WUSB600N adapters and USB hub
> so that you always put each adapter into the same USB hub port. Failing to
> do so will cause Windows to recognize the WUSB600N as a new adapter,
> which will mean loading the drivers for that adapter again.

Installation & Configuration – MultiChannel Aggregator Plug-in

Verify that OmniPeek is shut down before you start the installation of the MultiChannel
Aggregator Plug-in. The Aggregator Plug-in is packaged as an installer file, where you
can just double-click the **.exe** file, click next, next, next, and voila – you're done.

FIGURE 11 - MultiChannel Aggregator Plug-in Installation
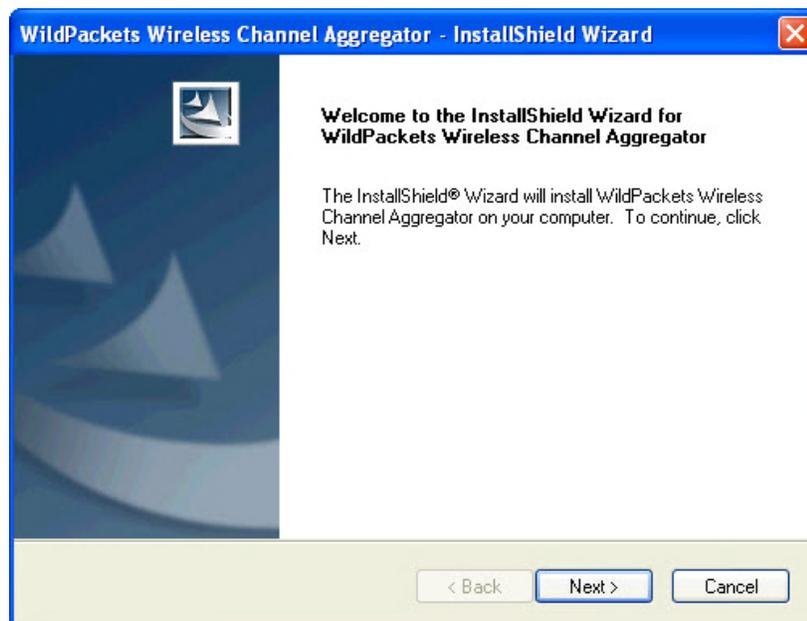
Once the MultiChannel Aggregator installation is complete, you can verify proper
installation by going to OmniPeek's Capture Options page where you should see the
MultiChannel Aggregator adapter. **Capture > Start Capture > Adapter**

FIGURE 12 - Capture Options – MultiChannel Aggregator
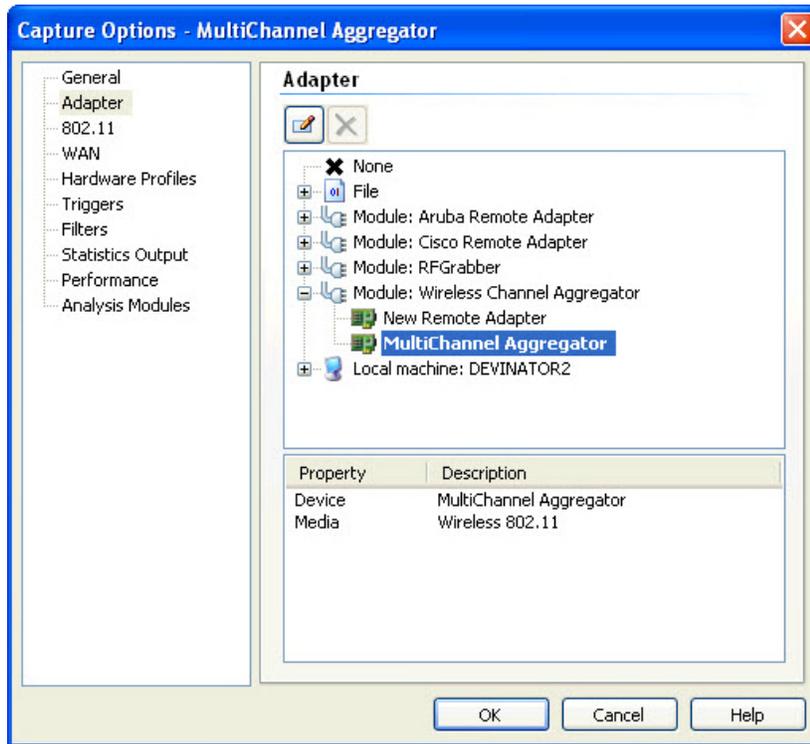
To configure the MultiChannel Aggregator, right-click on it and select **Properties**.

FIGURE 13 - MultiChannel Aggregator – Properties
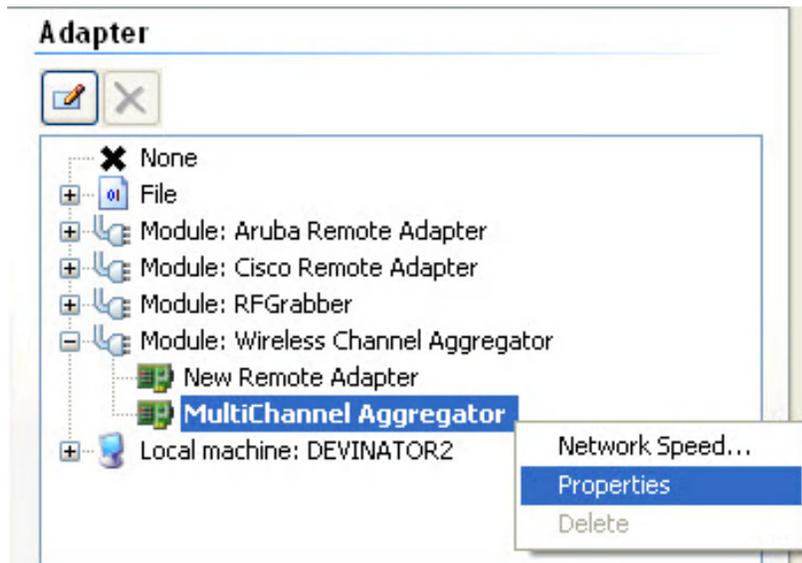
You should now be viewing the Wireless Aggregator Settings screen as shown in FIGURE 14.

FIGURE 14 - MultiChannel Aggregator – Adapter Selection & Settings
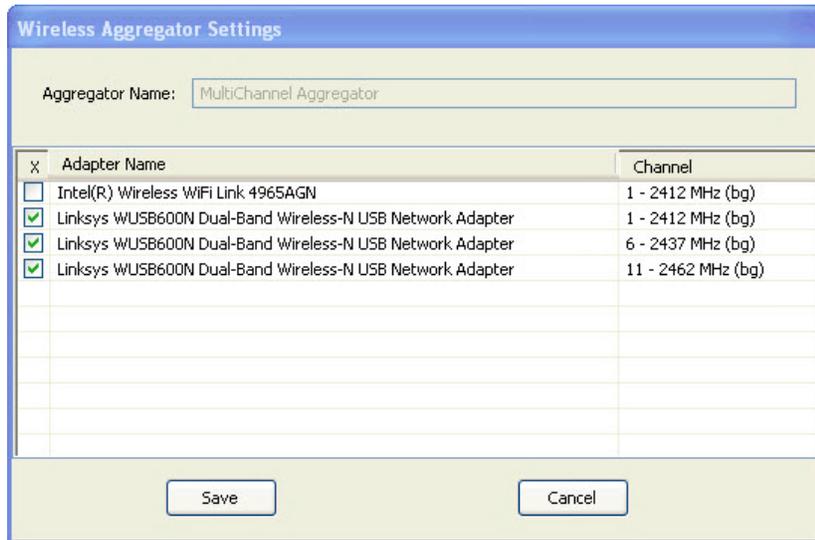
Note that in FIGURE 14, only the Linksys WUSB600N adapters are selected. Many laptops have integrated wireless adapters, and these will need to be *deselected* in the Aggregator. You can see that I have deselected my Intel 4965AGN adapter. Next, we need to configure each WUSB600N adapter just as we normally would for a single adapter.

    📖 Currently, Wildpackets is the only vendor supporting the Linksys WUSB600N wireless adapter for protocol capture and analysis.

FIGURE 15 - MultiChannel Aggregator – Channel Selection
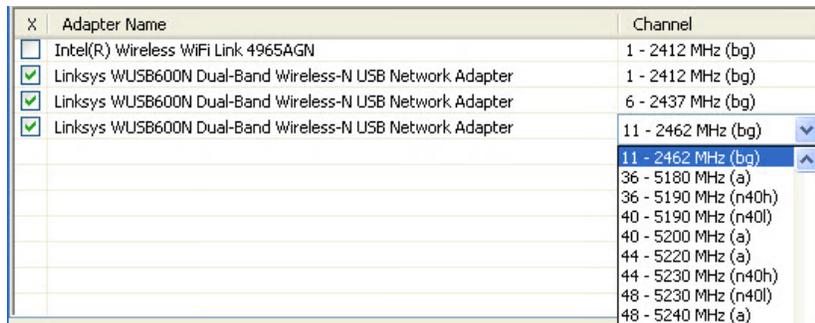
By clicking on the channel column in the row of each adapter, you will be able to select the channel for each adapter. Notice that both 20 MHz and 40 MHz channels are selectable, so be sure to select the appropriate channel widths for your intended capture. In this whitepaper, we will use legacy 20 MHz channels only. Select channels 1, 6, and 11 for the three Linksys adapters.

Performance Settings

Before performing a capture with the Aggregator, it's important to configure OmniPeek's performance settings. There are no hard-and-fast rules for how to configure the

performance settings, and configuration depends on the various features you are using. For example, if you aren't going to use the Peer Map, you could deselect that option as that will improve performance. To be a bit more specific, OmniPeek is generally used for analysis in one of two ways: real-time or post-capture.

FIGURE 16 - Performance Settings
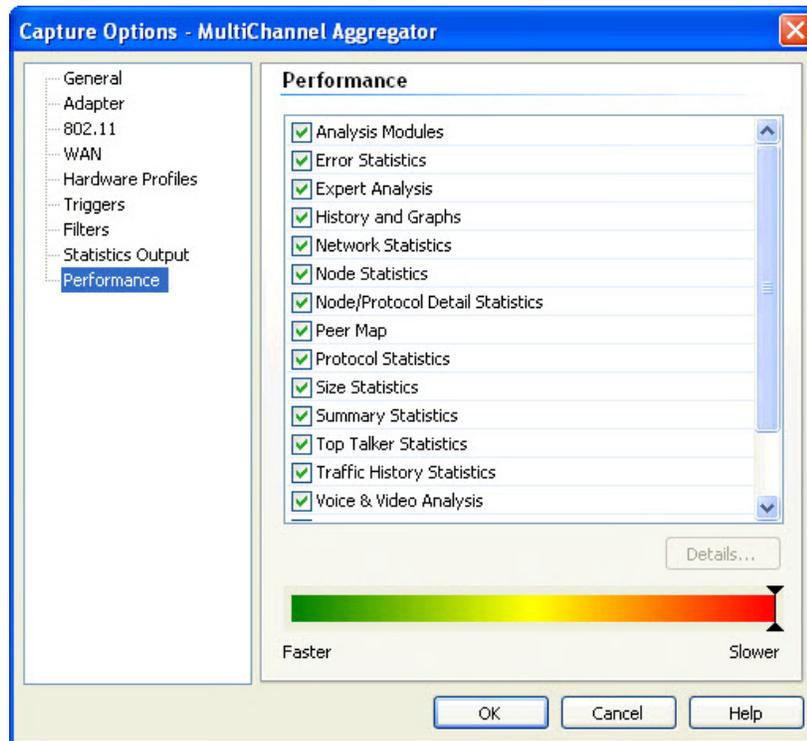
If real-time analysis is being performed, then you need to determine, based on your analysis needs and styles, what modules you want to have enabled and disabled. As you deselect options, the slider bar on the bottom will move to the left in a relative way to indicate the impact the particular choice made. The performance 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, analytical throughput will certainly increase. FIGURE 17 shows the Performance Settings with only the analysis modules enabled.

FIGURE 17 - Performance Settings – Analysis Modules Only
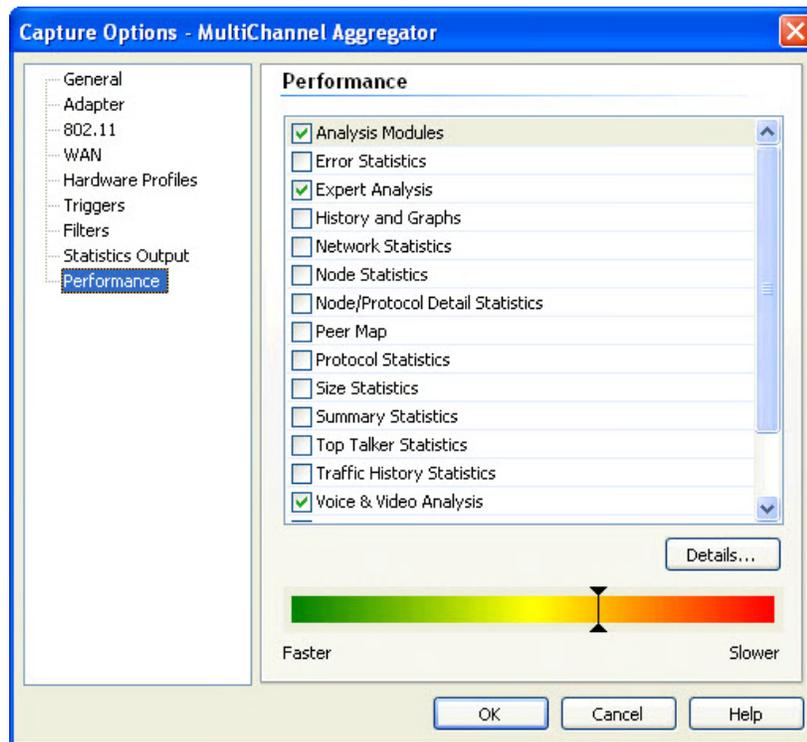
If post-capture analysis is being performed, meaning that the user wants to capture and save the packets for future analysis (also referred to as **capture-to-disk**), then all of the performance options can be deselected during the capture. When the capture files are opened later for analysis, the performance 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, post-capture analysis is the way to go, 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

Just as you would normally filter out frames that are not helpful with a single-channel capture, it is even more important to do so with a multi-channel capture, especially when using three 802.11n adapters at a time. 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 18, the screenshot illustrates default filtering options, but custom filtering is available.

FIGURE 18 - Default Protocol Filter Settings
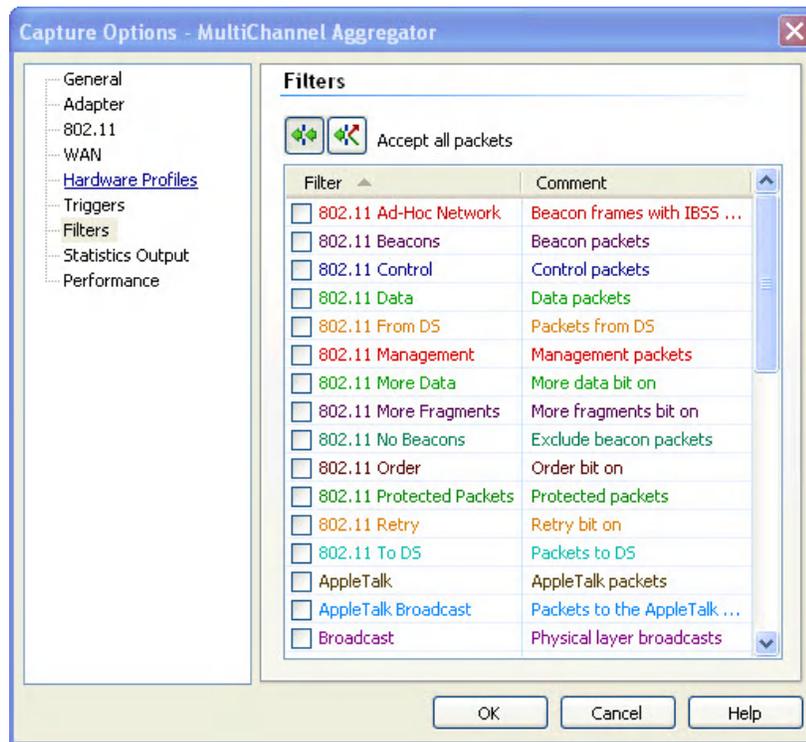
> 📖 If you are a field engineer, who is not the analyst, it might be more helpful to capture a wide variety of frames than to filter. Post-capture filtering and analysis can often be easier, and more frames give the analyst a better picture of the RF environment. If no filtering will be performed, then monitor capture performance to assure that frames are not being missed.

FIGURE 19 illustrates creation of custom filters in OmniPeek. Notice that **Filters** is selected in the left pane. By clicking the ✚ (green plus) symbol, you can add a custom filter in the dialog provided.

FIGURE 19 - Custom Protocol Filter Creation
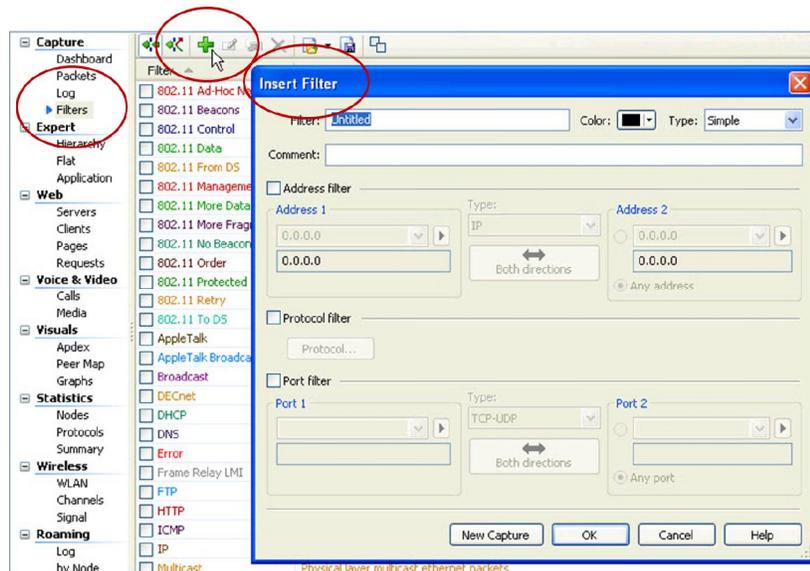
OmniPeek filters work by selecting either the **Reject Matching** or the **Accept Matching** rule engine buttons and then selecting the filters you want to use with the rule engine.

Now let's look at the packet buffer size configuration. In FIGURE 20, we have chosen 512 MB, but depending on what you're capturing, how long you're capturing, and how your filters are configured you may need more or less space for your packet buffer.

FIGURE 20 - Packet Buffer Size
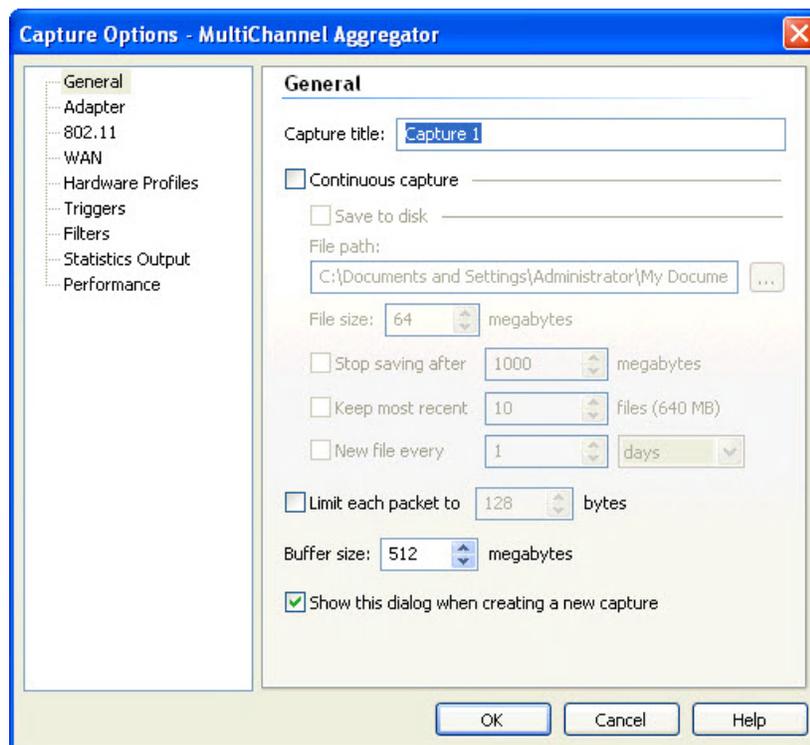
OmniPeek also provides the option to perform a continuous capture and save captures to disk in files of a discrete size and to perform packet slicing. Either might be advantageous depending on what you're capturing and for how long.

Installation – Roaming Analysis Plug-in

Verify that OmniPeek is shut down before you start the installation of the Roaming Analysis Plug-in. The Roaming Plug-in is packaged as an installer file, where you can just double-click the **.exe** file, click next, next, next, and voila – you're done. Sound familiar?

FIGURE 21 - Roaming Analysis Plug-in Installation
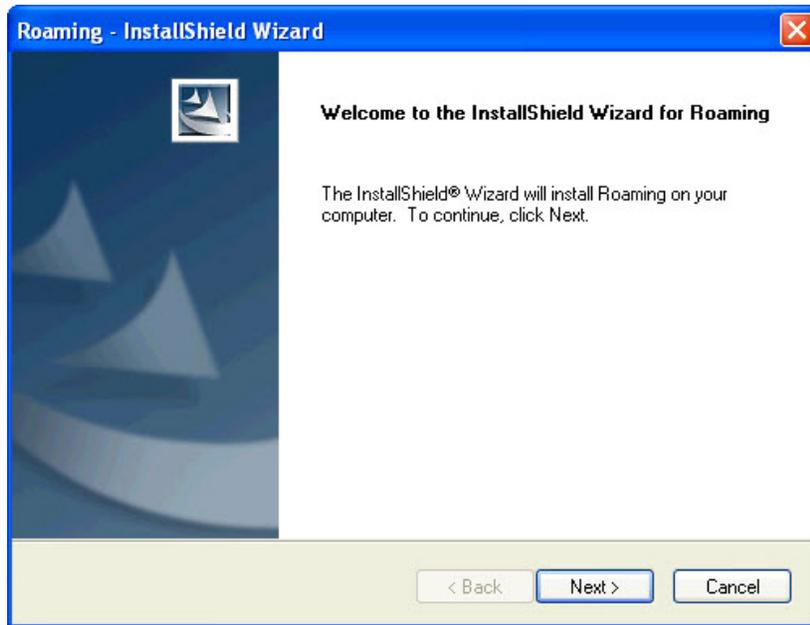
Once installed, prepare to start an OmniPeek capture using the Aggregator, and observe the bottom-left corner of the display. The Roaming Analysis Plug-in should be available.

FIGURE 22 - Roaming Analysis Plug-in Successfully Installed
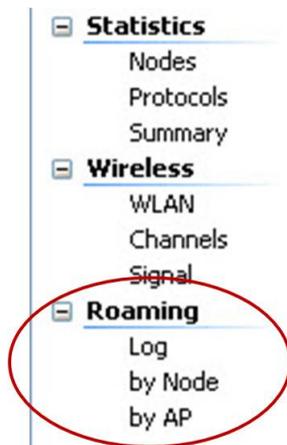
No configuration is required for the Roaming Analysis Plug-in to work properly.

Capturing with the Aggregator

To begin a capture, click on **OK** in the **Capture Options** dialog. If it isn't already selected, click on **Capture > Packets** in the left pane. Then along the top-right of the screen, you will have a button to use to start/stop capturing with the Aggregator as shown in FIGURE 23.

FIGURE 23 - Starting and Stopping Capture with Aggregator
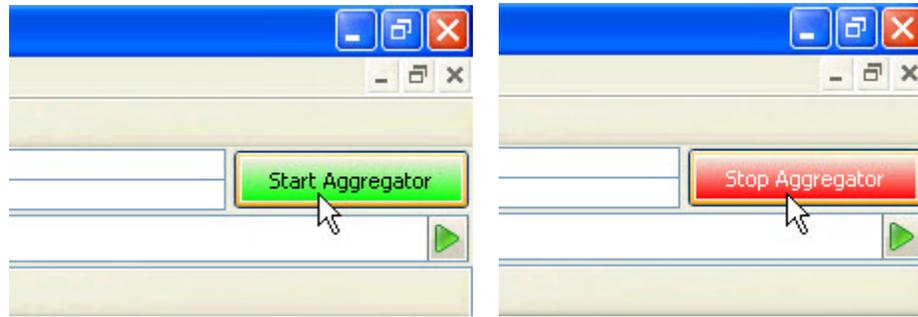
To verify that the Aggregator is working properly, begin a capture and verify that frames from each of the channels you configured in the Aggregator are captured. It's possible that one or more of these channels will have only small amounts of traffic on them depending on your Wi-Fi environment. In order to view which channels are being captured, verify that the **Channel** column header is enabled. If not, then left-click any column header to get the **Packet List Options** dialog and select **Channel** as shown in FIGURE 24.

FIGURE 24 - Column Header Selection: Channel
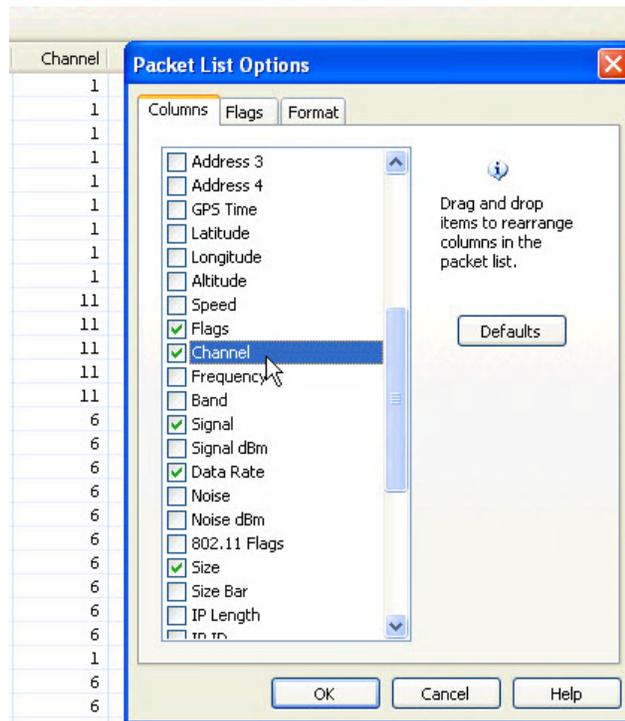
Aggregation and Roaming

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. Blendy 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.

In a case where more than three WUSB600N adapters are used, it is recommended that you use two USB2 hubs, each with the same cable and wireless adapters. Additionally, each USB2 hub should be connected to a different set of stacked USB2 ports on the laptop. Running up to 6 simultaneous WUSB600N adapters and two USB2 hubs will cause significant battery drain on your laptop.

20 MHz vs. 40 MHz Channels

Some client devices, such as VoWiFi phones and barcode scanners, are currently only 20 MHz channel capable, meaning that they are 802.11a, b, or g devices. This isn't the case with new 802.11n client devices, such as laptops. In order to troubleshoot an 802.11n laptop as it roams, it may be necessary to troubleshoot 40 MHz channels.

The 802.11n amendment defines a 40 MHz channel as the combination of a primary 20 MHz channel and a secondary 20 MHz channel – let's call the set **{Pri, Sec}**. While the 40 MHz channel of {36, 40} covers the same frequency range as {40, 36}, the functionality of the analyzer is different. When wireless clients are configured to transmit data in a 40 MHz channel, they are in 20/40 MHz BSS mode. This means that some transmissions are sent at 40 MHz and others at 20 MHz. 20 MHz transmissions are always sent in the primary channel. Therefore, if your AP is an 802.11a compliant unit transmitting beacons on channel 40, you should use the 40 MHz channel {40, 36} in order to capture them.

Let's look at selecting 40 MHz 802.11n channels in OmniPeek. It's important to understand 40 MHz channel nomenclature in the analyzer. OmniPeek defines a 40 MHz 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 20 MHz channel and channel 40 is the secondary 20 MHz channel. See FIGURE 25 that illustrates selection of 40 MHz channels in OmniPeek.

FIGURE 25 - Selecting 40 MHz Channels: Nomenclature
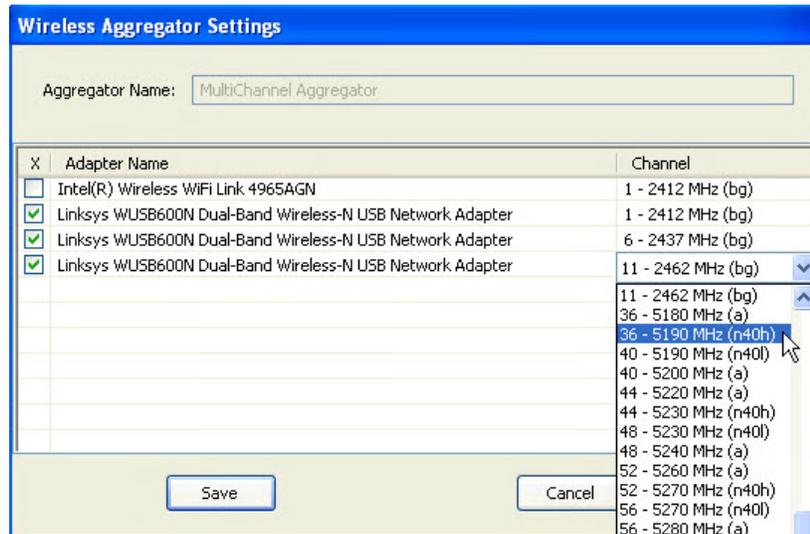
The reason for this section of the whitepaper is to assure that you, the analyst, understand that you can't cover 6 UNII band channels using three adapters. The adapters would not capture data on the secondary 20 MHz channels, but rather only primary 20 MHz and 40 MHz transmissions. Obviously, using multiple adapters can allow unique capturing combinations, but since channels are paired (e.g. 36/40, 44/48, 52/56, 60/64), it makes contiguous configurations such as **{36 – n40h, 40 – n40h, 44 – n40h, 48 – n40h}** impossible. For quick reference, FIGURE 26 illustrates 40 MHz channel pairings across the UNII bands for North America.

FIGURE 26 - 40 MHz Channel Pairings

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 working on the Voice-Enterprise certification based on 802.11r and 802.11k.

📖 For more information on Fast BSS Transition, see the whitepaper entitled, "Robust Security Network (RSN) Fast BSS Transition (FT)" in the **Learning Resources > Whitepapers** section of CWNP.com.

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. The Roaming Analysis plug-in will help with analyzing both L2 and L7 BSS transitions, enabling an entirely new level of troubleshooting capabilities.

Summary

This whitepaper is a basic "how to" that gets the analyst started doing triple channel capturing and analysis. It's not meant to be in-depth training on analysis or troubleshooting. For more information on these Wildpackets plug-ins, refer to mypeek.wildpackets.com. For more information on vendor-neutral training and certification, refer to cwnp.com.