AirPcap User's Guide

May 2013

RiverbedTechnology
199 Fremont Street
San Francisco, CA 94105

Tel: +1 415 247 8800
Fax: +1 415 247 8801
www.riverbed.com

712-00090-02

Contents

The AirPcapProduct Family

AirPcap is the first open, affordable and easy-to-deploy 802.11 packet capture solution for Windows. All of the AirPcap offerings will capture full 802.11 data, management, and control frames that then can be viewed in Wireshark, providing in-depth protocol dissection and analysis capabilities. Below, we provide a feature matrix that gives a high-level overview of the feature sets of the various adapters in the AirPcap Product Family.

More detailed information regarding each AirPcap model can be found on the Riverbed website: http://bit.ly/airpcap/.

	AirPcap Classic	**AirPcap Tx**	**AirPcap Nx**
Captures full 802.11 frames	Yes	Yes	Yes
Fully integrated with Wireshark	Yes	Yes	Yes
Open API	Yes	Yes	Yes
Multi-channel monitoring (with 2 or more adapters)	Yes	Yes	Yes
Packet transmission	No	Yes	Yes
Form factors	USB dongle	USB dongle	USB dongle
Frequency bands	2.4 GHz (b/g)	2.4 Ghz (b/g)	2.4 and 5 Ghz (a/b/g/n)

Table 1. Feature comparison of the AirPcap product family

A Brief Introduction to 802.11

Terminology

The terms *Wireless LAN* or *WLAN* are used to indicate a wireless local area network, e.g. a network between two or more "stations" that uses radio frequencies instead of wires for the communication.

All components that can "connect" to a WLAN are referred to as *stations*. Stations fall into one of two categories: *access points* or *wireless clients*.

Access points transmit and receive information to/from stations using radio frequencies. As we shall see later, the particular choice of a radio frequency determines a wireless "channel." An access point usually acts as a "gateway" between a wired network and a wireless network.

Wireless clients can be mobile devices such as laptops, personal digital assistants (PDAs), IP phones or fixed devices such as desktops and workstations that are equipped with a wireless network interface card.

In some configurations, wireless devices can communicate directly with each other, without the intermediation of an access point. This kind of network configuration is called *peer-to-peer* or *ad-hoc*.

A *Basic Service Set (BSS)* is the basic building block of a WLAN. The "coverage" of one access point is called a BSS. The access point acts as the master to control the stations within that BSS. A BSS can be thought of as the wireless version of an IP subnet. Every BSS has an ID called the *BSSID*, which is the MAC address of the access point servicing the BSS, and a text identifier called the *SSID*.

802.11 Standards

802.11 is a standard that defines the physical layer and the data-link layer for communication among wireless devices. The original 802.11 specification was ratified in 1997, uses the 2.4 GHz frequency band, and allows transmission rates of 1 or 2 Mbps.

802.11a, ratified in 1999, is an extension of 802.11 that operates at 5 GHz. It supports 8 additional transmission rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

802.11b, ratified in 1999, is an extension of 802.11 that uses the same 2.4 GHz frequency band, and supports two additional transmission rates: 5.5 and 11 Mbps.

802.11g, ratified in 2003, is backward compatible with 802.11b, and supports the same additional transmission rates found in 802.11a: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

802.11i, ratified in 2004, defines an enhanced security mechanism based on AES.

802.11n, ratified in 2009, is backward compatible with 802.11a, b, and g, and operates at 2.4 GHz and optionally 5 GHz. It can potentially support data rates up to 600 Mbps.

Channels

802.11b and 802.11g divide the 2.4 GHz spectrum into 13 channels, beginning with channel 1 and ending with channel 13. The center frequency of channel 1 is 2,412MHz, channel 2 is 2,417MHz, etc. The center frequencies of adjacent channels are 5 MHz apart. The bandwidth of each channel is 20 MHz which means that channels may "overlap." The commonly-used non-overlapping channels are channels 1, 6, and 13. There is a 14th channel whose center frequency is 12MHz above channel 13. These frequency bands are referred to as *channels* and stations communicate using a particular channel.

802.11a and 802.11n operate in the 5 GHz range which is divided into a large number of channels. The center frequency of channel 0 is 5,000 MHz, the

center frequency of channel 1 is 5,005 MHz. The formula for relating channels to center frequencies in the 5 GHz range is:

Center frequency (MHz) = 5,000 + 5*n, where n = 0, …, 199,
Center frequency (MHz) = 5,000 – 5*(256 – n), where n = 240, …, 255.

Note that channels 240 to 255 range from 4,920 MHz to 4,995 MHz. As with the 2.4 GHz band, each channel is 20 MHz wide. 802.11n allows for "wide" channels – that is, two adjacent 20 Mhz bands (note that the channel numbers of the two adjancent 20 MHz bands are not adjacent) can be used "side-by-side" in order to be backward-compatible with 802.11a, b, and g, or they can be combined into a single 40 MHz channel in "Greenfield" mode.

The actual use of the channels, however, depends on the country. For example,in the USA, the FCC allows channels 1 through 11 in the 2.4 GHz band, whereas most of Europe can use channels 1 through 13. No matter where you are, you can use AirPcap to listen on any supported channel. The regulations for the 5GHz band are much more complex.

Each BSS operates on a particular channel, i.e., the access point and all of the wireless clients within a BSS communicate over a common channel. The same channel may be used by more than one BSS. When this happens, and if the BSSs are within communication range of each other, the different BSSs compete for the bandwidth of the channel, and this can reduce the overall throughput of the interfering BSSs. On the other hand, selecting different channels for nearby access points will mitigate channel interference and accommodate good wireless coverage using multiple BSSs.

A BSS is formed by wireless clients "associating" themselves with a particular access point. Naturally, a wireless client will have to "discover" whether there is an access point within range and its corresponding channel. For this purpose, access points advertise themselves with "beacon" frames and wireless clients can (passively) listen for these frames. Another discovery approach is for the wireless client to send out "probe" requests to see if certain access pointsare within range. Following the discovery process, wireless clients will send requests to be *associated* with a particular BSS.

Types of Frames

The 802.11 link layer is much more complicated than the Ethernet one. The main reason is that wireless links have lower reliability compared to the reliability of wired links, and therefore the 802.11 link layer has features to reduce the effects of frame loss. For example, every data frame is acknowledged with an ACK frame. Moreover, the protocol needs to support access point discovery, association and disassociation, authentication, wired/wireless bridging, and many other features that are not necessarily needed in a wired link layer.

When capturing on a wireless channel, you will see three main kinds of frames:

- Data frames
- Control frames
  - Acknowledgement
  - Request to Send
  - Clear to Send
- Management frames
  - Beacons
  - Probe Requests / Probe Responses
  - Association Requests / Association Responses
  - Reassociation Requests / Reassociation Responses
  - Disassociations
  - Authentications / Deauthentications

Additionally, frame headers may contain Quality of Service (QoS) and High Throughput (+HTC) information.

The Control frames are used to improve the reliability characteristics of the link. The establishment of a BSS through the process of discovery and association is supported by the Management frames, including possible authentication steps in the process.

It is beyond the scope of this brief introduction to describe the details of these frames and their usage in the 802.11 protocol. If you are interested in additional details, you can consult the following websites:

http://standards.ieee.org/getieee802/802.11.html
www.wi-fiplanet.com/tutorials/article.php/1447501

Another good source is the book *802.11® Wireless Networks: The Definitive Guide (2nd Edition)* by Matthew Gast (ISBN-0596100523).

How AirPcap Adapters Operate

AirPcap adaptesr capture the traffic on a single channel at a time. The channel setting for the AirPcap adapter can be changed using the AirPcap Control Panel, or from the "*Advanced Wireless Settings*" dialog in Wireshark. If you are using AirPcap with Cascade Pilot, you can set the channel through the Channels option on the Home Tab ribbon. Depending on the capabilities of your AirPcap adapter, it can be set to any valid 802.11a/b/g/n channel for packet capture.

All of the AirPcap adapters can operate in a completely passive mode. This means that they can capture the traffic on a channel without associating with an access point, or interacting with any other wireless device. Unless you are transmitting with either AirPcap Tx or Nx, none of the adapters is detectable by any other wireless station.

The AirPcap adapters can work in, so called, *Monitor Mode*. In this mode, the AirPcap adapter will capture all of the frames that are transferred on a channel, not just frames that are addressed to it. This includes data frames, control frames and management frames.

When more than one BSS shares the same channel, the AirPcap adapter will capture the data, control and management frames from all of the BSSs that are sharing the channel and that are within range of the AirPcap adapter.

The AirPcap software can optionally be configured to decrypt WEP-encrypted frames. An arbitrary number of keys can be configured in the

driver at the same time, so that the driver can decrypt the traffic of more than one access point at the same time. WPA and WPA2 support is handled by applications such as Wireshark and Aircrack-ng. See the section *WEP Keys* on page 13 and The *Decryption Keys Management Dialog* on page 20 for more information.

Multiple Channel Capture

This section applies to all members of the AirPcap Product family. When listening on a single channel is not enough, multiple AirPcap adapters can be used at the same time to capture traffic simultaneously from different channels.

The AirPcap driver provides support for this operation through the *Multi-Channel Aggregator* technology, which exports capture streams from multiple AirPcap adapters as a single capture stream. The Multi-Channel Aggregator consists of a virtual interface that can be used from Wireshark, Pilot, or any other AirPcap-based application. Using this interface, the application will receive the traffic from all installed AirPcap adapters as if it were coming from a single device.

The Multi-Channel Aggregator can be configured like any real AirPcap device, and therefore can have its own decryption, FCS checking and packet filtering settings.

Configuring the Adapters: the AirPcap Control Panel

The AirPcap control panel (Figure 1) provides a convenient and intuitive way to configure the parameters of currently-connected AirPcap adapters. Changes made to an adapter using the AirPcap control panel will be reflected in all of the applications using that adapter.

To start the AirPcap control panel, click on:

START » PROGRAMS » AirPcap » AirPcap Control Panel

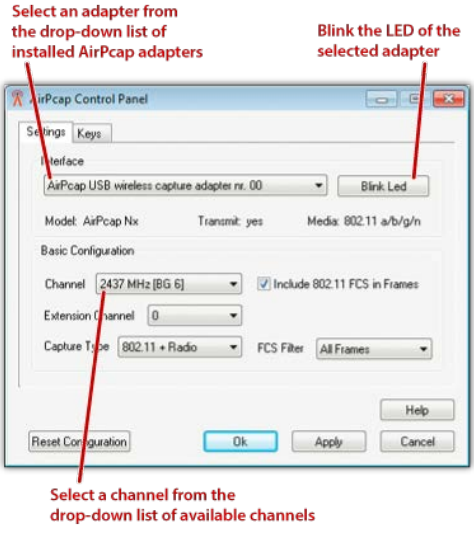

Figure 1. The AirPcap Control Panel—Settings Tab

The drop-down list in the Interface box at the top of the panel presents a list of currently-installed adapters. Selecting one of the adapters in the list allows you to view/edit its configuration.

Identifying AirPcap Adapters

The drop-down list identifies the AirPcap adapters using adapter numbers (e.g. 00, 01, …) and does not distinguish between AirPcap Classic, AirPcap Tx, and AirPcap Nx. Fortunately, the AirPcap adapters have an LED that can be caused to blink by first selecting the adapter from the drop-down list and clicking on the *Blink LED* button. This feature is useful in distinguishing

among the AirPcap adapters when multiple adapters are plugged into your system, and an easy way to associate the physical adapters with the adapter numbers assigned by thesystem.

Settings

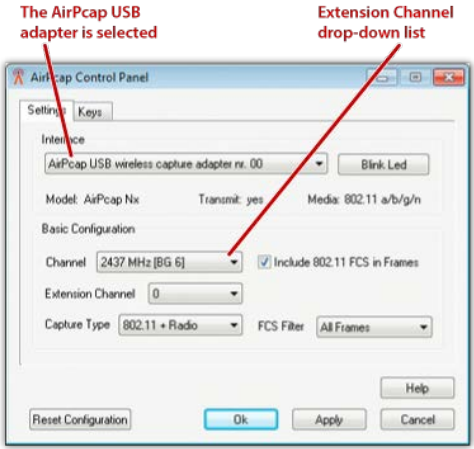

Figure 2. AirPcap Nx and Extension Channel Settings

The Basic Configuration box contains the following settings:

- Channel: The channels available in the Channel list box depend on the selected adapter. Since channel numbers 1, …, 14 in the 2.4GHz and 5GHz bands overlap and there are center frequencies (channels) that do not have channel numbers, each available channel is given by its center frequency.

  Where applicable, the BG or A channel numbers are also given. All of the channel center-frequencies supported by the selected adapter will be made available in the Channel list. The bandwidth of each channel is 20MHz.
- Extension Channel: For 802.11n adapters, one can use the Extension Channel list to create a "wide" channel. The choices are -1 (the preceding 20MHz frequency band), 0 (no extension channel), or +1 (the succeeding 20MHz frequency band). The channel of the additional frequency band is called the *extension channel*. The Extension Channel list box lets you choose a valid extension channel (above or below) for a given channel (See Figure 2). Not all channels have above and below extension channels. For example, BG channels 1, 2, 3, and 4 do not have a -1 (below) extension channel. The reason is that the center frequencies of the primary and extension channels need to be separated by 20MHz. So if 4 were the primary channel, channel 1 (which is the lowest BG center frequency) is only 15 MHz below channel 4.
- Capture Type: 802.11 frames only, 802.11 frames plus radio information (See http://www.radiotap.org), or 802.11 frames plus the Per-Packet Information (PPI) header (See http://www.cacetech.com/documents/PPI%20Header%20format%201.0.10.pdf for the current PPI specification). PPI and radio information includes additional information not contained in the 802.11 frame: transmit rate, signal power, signal quality, channel, and (for PPI) multiple antenna information.

- Include 802.11 FCS in Frames: if checked, the captured frames will include the 802.11 4-bytes Frame Check Sequence. This option can be disabled if an application has difficulty decoding the packets that have the Frame Check Sequence.
- FCS Filter: this drop-down list allows you to configure the kind of Frame Check Sequence filtering that the selected adapter will perform:
  - All Frames: the adapter will capture all the frames regardless of whether the FCS is valid or not.
  - Valid Frames: the adapter will only capture frames that have a valid FCS.
  - Invalid Frames: the adapter will only capture frames that have an invalid FCS.

Note:	AirPcap stores the configuration information on a per-adapter basis. This means that changing the configuration of an adapter does not affect the settings of any of the other adapters.

WEP Keys

The AirPcap driver can use a set of WEP keys to decrypt traffic that is WEP encrypted. If a frame is WEP encrypted, the driver will attempt to decrypt it using the user-supplied set of WEP keys. The driver will try all of the WEP keys for each frame until it finds one that decrypts the frame. If the decryption is successful, the unencrypted frame is passed to the user application; otherwise the original frame is passed along. By configuring the AirPcap driver with multiple WEP keys, it is possible to decrypt traffic coming from multiple access points that are using different WEP keys but transmitting on the same channel.

The list of keys can be edited by selecting the *Keys* tab in the AirPcap control panel (Figure 3).

To add or remove a key, use the "*Add New Key*" or "*Remove Key*" buttons, respectively. "*Edit Key*" allows you to change the value of an existing key. "*Move Key Up*" and "*Move Key Down*" can be used to change the order of

the keys. This may be an important performance consideration, since the driver uses the keys in the order they appear in this list.

The currently configured keys are shown in the "Keys" list.

It is possible to turn WEP decryption on and off at any time by using the "*Enable WEP Decryption*" check box.

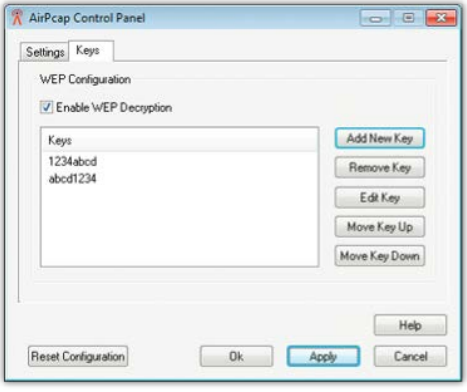

Figure 3. The AirPcap Control Panel—Keys Tab

The keys are applied to the packets in the same order they appear in the keys list. Therefore, putting frequently-used keys at the beginning of the list improves performance.

Note:	The keys are stored by the AirPcap Control Panel globally. This means that any keys specified in the list will be used by all AirPcap adapters.

Multi-Channel Aggregator

When more than one AirPcap adapter is plugged in, the AirPcap Control Panel will show one additional interface: the *Multi-Channel Aggregator*.

As explained in the *Multiple Channel Capture* section of this manual, the Multi-Channel Aggregator is a virtual capture interface that can be used from Wireshark, Pilot, or any other AirPcap-based application. Using this capture interface, the application will receive the traffic from all installed AirPcap adapters, as if it was coming from a single device.

Figure 4. Multi-Channel Aggregator

As Figure 4 shows, the Multi-Channel Aggregator has its own FCS, Capture Type and FCS Filter settings. These settings and not the ones of the physical

adapter will be used when capturing from the Aggregator.

Note that it's not possible to set the channel of the Multi-Channel Aggregator. Instead, the *channel* drop-down box will show the list of the aggregated channels. To change the channel of any individual adapter, select the Capture adapter from the *Interface* drop-down list, and set the desired value in the *channel* drop-down box.

AirPcap and Wireshark

The user interface of Wireshark is completely integrated with AirPcap. This increases your productivity and allows you to get the best from the network analyzer you are used to.

Identifying the AirPcap Adapters in Wireshark

Figure 5 shows the Wireshark Capture Interfaces dialog (*Capture » Interfaces*). The AirPcap Interfaces are easly identified by the icon next to them.

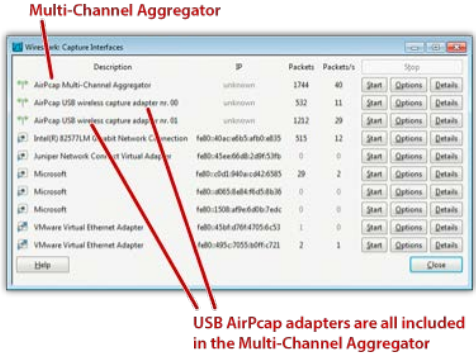

Figure 5. The Wireshark adapters list

When you insert more than one AirPcap adapter, you will see an additional capture interface, called *AirPcap Multi-Channel Aggregator*. This interface aggregates the traffic from all the available AirPcap adapters, and allows them to be used as a single multi-channel capture device.

The Wireless Toolbar

Figure 6 shows the Wireshark wireless toolbar. The wireless toolbar provides a fast and productive way to set up the most important wireless capture settings.

The wireless toolbar appears when at least one AirPcap adapter is plugged into one of the USB ports and can be used to change the parameters of the currently active wireless interfaces. If the currently active interface is not an AirPcap adapter, the wireless toolbar will be grayed.

When Wireshark starts, the active interface is the default one (*Edit » Preferences » Capture » Default Interface*). During Wireshark usage, the active interface is the last one used for packet capture.

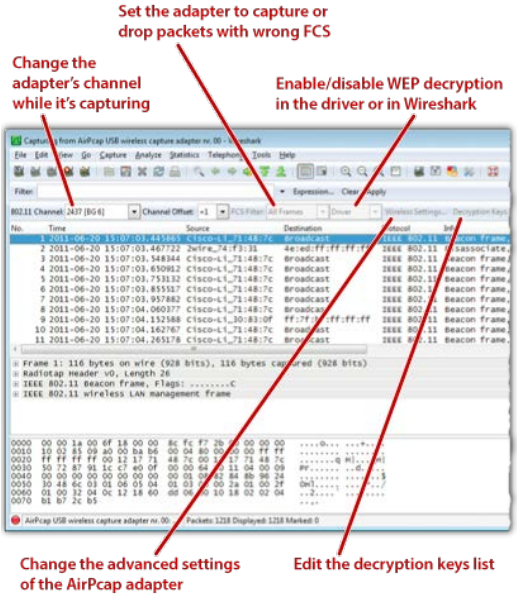

Figure 6. The Wireshark Wireless Toolbar

The Wireless toolbar has the following controls:

- 802.11 Channel: allows the user to change the channel on which the current AirPcap adapter captures. The channel can be changed at any time, even while Wireshark is capturing.
- Offset: for AirPcap Nx, allows the user to set an extension, or "wide" channel.

Tip:	When real-time packet updates are enabled (*Edit » Preferences » Capture » Update list of packets in real time*), switching from channel to channel allows you to see which channels have traffic and which ones are unused.

- FCS Filter: allows the user to select which packets the current AirPcap adapter should capture: all the packets, only packets with a valid FCS, or only packets with an invalid FCS. This feature can be used to get a quick check on the quality of the transmission on the channel and/or the quality of the adapter's reception.
- Decryption mode: can be one of the following:
  - None: no decryption is performed, neither at the driver level nor in Wireshark.
  - Wireshark: the driver doesn't perform any decryption of the captured packets, and they are decrypted by Wireshark while displaying them. This has the advantage of minimizing the CPU load during the capture process. Moreover, the driver doesn't manipulate the packets, so the captured data is a precise picture of the network traffic. However, capture filters (also known as BPF filters) on TCP/IP fields or packet payloads will not work. Since this kind of decryption is done by the analyzer, when you turn it on or off, you will see the changes immediately reflected in the Wireshark window.
  - Driver: the packets are decrypted by the driver before reaching Wireshark. This option has two advantages: capture filters on TCP/IP fields or packet payloads will work; when logging the network traffic to disk, it will be unencrypted. This will make it easier for third party applications to understand them. Since this kind of decoding is done during the capture, the changes you make will be effective starting with the next capture.

- Wireless Settings: this button opens the Wireless Settings dialog for the currently-selected AirPcap adapter. See the next section for details.
- Decryption Keys: this button opens the Decryption Keys Management dialog. See the "*Decryption Keys Management Dialog*" section below for details.

The Wireless Settings Dialog

The Wireless Settings Dialog (Figure 7) can be used to set the advanced parameters of an AirPcap adapter. The dialog can be accessed either from the Wireless Toolbar (*Wireless Settings*) or from the main menu (Capture » Options » Wireless Settings).

Figure 7. Wireless Settings Dialog in Wireshark

The parameters that can be configured are:

- Channel: the channels are specified in terms of their center frequencies and the range of channels varies from adapter to adapter.
- Channel Offset: set to -1, 0, or +1 for AirPcap Nx. This allows the use of "wide" channels.
- Capture Type: 802.11 frames only, or 802.11 frames plus Radio information (Radiotap header), or 802.11 frames plus the Per Packet Information (PPI) header. Radiotap and PPI include information such

as, transmit rate, signal power, signal quality, channel, and will be displayed by Wireshark in the radiotap header of every frame.

- Include 802.11 FCS in Frames: if checked the captured frames will include the 802.11 4-bytes Frame Check Sequence.
- FCS Filter: this drop-down list allows the configuration the kind of Frame Check Sequence filtering that the selected adapter will perform:
  - All Frames: the adapter will capture all the frames, regardless of whether the FCS is valid or invalid.
  - Valid Frames: the adapter will only capture frames that have a valid FCS.
  - Invalid Frames: the adapter will only capture frames that have an invalid FCS.

The Decryption Keys Management Dialog

This dialog window (shown in Figure 8) can be used to organize the keys that will be used to decrypt the wireless packets. It is possible to decrypt packets encrypted with WEP, WPA and WPA2. However, notice that:

- In order to decrypt WPA and WPA2, you will need to capture the 4-way EAPOL handshake used to establish the pairwise transient key (PTK) used for a session.
- Wireshark can only decrypt "WPA personal" sessions which use pre-shared keys. Decryption of "WPA Enterprise" sessions is not supported.

As explained in "*The Wireless Toolbar*" section, there are three possible decryption modes: *None*, *Driver* and *Wireshark*. The keys specified in this dialog will be used either by the *Driver* or *Wireshark* depending upon the selected Decryption Mode. It should be noted that WPA and WPA2 are decrypted only in *Wireshark* mode.

Note that, no matter which setting is used, the keys are applied to the packets in the same order they appear in the keys list. Therefore, putting frequently used keys at the beginning of the list improves performance.

To add or remove a key, use the "*Add New Key*" or "*Remove Key*" buttons, respectively. "*Edit Key*" allows you to change the value of an existing key. "*Move Key Up*" and "*Move Key Down*" can be used to change the order of the keys. This may be an important performance consideration, since the driver uses the keys in the order they appear in this list.

Use the "*Select Decryption Mode*" drop-down box to switch among the different decryption modes.

Figure 8. Decryption Keys Management Dialog in Wireshark

WEP keys are an array of bytes of arbitrary length expressed in hexadecimal. WPA and WPA2 keys can be of two types:

- Passphrase (WPA-PWD): This is the Passprase and SSID combination most often used to configure WPA and WPA2. The passphrase is a string between 8 and 63 characters in length. The SSID can be omitted, in which case Wireshark will use the last-seen SSID on the network. Non-printable characters can be represented by a "%" character followed by a hexadecimal number for both the passphrase and SSID. The passphrase and SSID are used to derive Pre-Shared Key.
- Pre-Shared key (WPA-PSK): This allows the user to provide a binary TKIP

or CCMP key (used to derive the temporary key of each session) which is normally the kind of key returned by tools like Aircrack. The key is 256 bits long, and is expressed as a hex string (64 characters). A tool to convert a passphrase and SSID into a 256-bit PSK can be found on the Wireshark web site at www.wireshark.org/tools/wpa-psk.html.

The keys that you specify in this list are global. Every AirPcap adapter, including the Multi-Channel Aggregator, will use them.

Multi-Channel Aggregator

The Multi-Channel Aggregator has its own *FCS Filter*, *Capture Type* and option to Include *802.11 FCS in Frames*. These settings, and not the ones of the physical adapter, will be used when capturing from the Multi-Channel Aggregator.

However, it's not possible to set the channel of the Multi-Channel Aggregator. Instead, the channel drop-down box will show the list of the aggregated channels.

To change the channel of any individual adapter, select the *Capture » Options* menu item, select the desired interface, click on the *Wireless Settings* button and then set the channel value in the *channel* drop-down box.

Transmit Raw 802.11 Frames on Your Network

For advanced users, AirPcap Tx and AirPcap Nx have the ability to inject raw 802.11 frames into your wireless network which makes them an invaluable aid in assessing the security of your wireless network.

Using the AirPcap API, AirPcap Tx and Nx can inject any kind of frame, including control, management, and data frames. These frames can be transmitted at any allowable rate depending upon your adapter.

An application called *AirPcapReplay* is included in the AirPcap Software Distribution. Once AirPcap has been installed, the application can be accessed from the Start menu:

START » PROGRAMS » AirPcap » AirPcapReplay

The purpose of this application, as the name suggests, is to replay 802.11 network traffic that is contained in a trace file or simply a single packet. In addition to the replay feature, AirPcapReplay allows the user to edit individual packets using a built-in hex editor.

The AirPcap Software Distribution also includes several freeware and open-source tools that are compatible with AirPcap Tx and AirPcap Nx. Since these tools have not been developed by Riverbed, it is recommended that you visit their official websites for additional information.

- Aircrack-ng. This is a well-known suite of tools for auditing wireless networks: www.aircrack-ng.org
- Cain & Abel. This is a multi-function security tool for Windows that includes wireless access-point and host detection: www.oxid.it/cain.html
- Kismet. This is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card that supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic: http://kismetwireless.net/

It is important to point out that these tools are for advanced users. In addition, Riverbed is not in a position to provide support for tools not developed in-house.

Lastly, unlike passive reception, there are restrictions on the transmission frequencies/channels imposed by various countries. While there are no channel restrictions for monitoring 802.11 traffic, AirPcap Tx and Nx will allow transmission on only those channels that are permitted according to the ship-to country.

Where to Learn More

The best sources of information about the Wireshark network analyzer are:

- The documentation page on the Wireshark website, /www.wireshark.org/ docs/. From here you can download the User's Guide, the man pages, and the developer's manuals.
- The Wireshark wiki, wiki.wireshark.org/.
- The Wireshark mailing lists, www.wireshark.org/lists/.
- Wireshark University, www.wiresharktraining.com/. WSU features Laura Chappell, regarded by many as the best protocol analysis trainer in the world.

If you are a developer, the best sources of information are:

- The AirPcap developer's pack, downloadable from http://bit.ly/apcdevkit. . The AirPcap developer's pack contains all the components you need to create wireless-aware capture applications, including lib files, dlls, an online API documentation and a set of ready-to- compile example programs.
- The WinPcap developer resources page, www.winpcap.org/devel.htm, where you can download the WinPcap source code and developer's pack.
- The winpcap-users mailing list, http://www.winpcap.org/contact.htm.

Appendix A: 802.11 Frequencies

2.4 GHz Band

2312MHz to 2372 MHz in 5MHz steps.

The 802.11b/g center frequencies and corresponding channel numbers are: (2412MHz, Channel 1) to (2472MHz, Channel 13), where the frequencies are incremented by 5MHz and the channel numbers by 1. There is an additional frequency for channel 14, namely, 2484MHz which is 12MHz beyond channel 13.

5 GHz Band

The 5 GHz range is divided into a large number of channels. The center frequency of channel 0 is 5,000 MHz, the center frequency of channel 1 is 5,005 MHz. The formula for relating channels (n) to center frequencies in the 5 GHz range is:

Center frequency (MHz) = 5000 + 5*n, where n = 0, …, 199,

Center frequency (MHz) = 5000 – 5*(256 – n), where n = 240, …, 255.

Note that channels 240 to 255 range from 4920MHz to 4995MHz.

Channels Supported by the AirPcap Product Family

All of the 2.4GHz channels are supported by all of the adapters in the AirPcap ProductFamily.

AirPcap Nx

AirPcap Nx supports a wide range of center frequencies. The channel bandwidth around each center frequency is 20MHz. The center frequencies supported by the AirPcap Nx adapter are:

- 2412MHz to 2472MHz in 5 MHz increments. These correspond to BG channels 1 to 13
- 2484MHz corresponds to BG channel 14
- 4920MHz to 4980MHz in 20 MHz increments.
- 5040MHz to 5080MHz in 20MHz increments. These correspond to A channels 8 to 16 in increments of 4.
- 5170MHz to 5240MHz in 10 MHz increments. These correspond to A channels 34 to 48 in increments of 2.
- 5260MHz to 5320MHz in 20 MHz increments. These correspond to A channels 52 to 64 in increments of 4.
- 5500MHz to 5700MHz in 20 MHz increments. These correspond to A channels 100 to 140 in increments of 4.
- 5745MHz to 5825MHz in 20 MHz increments. These correspond to A channels 149 to 165 in increments of 4.

Riverbed Technology
199 Fremont Street
San Francisco, CA 94105

Tel: +1 415 247 8800
Fax: +1 415 247 8801
http://www.riverbed.com