CACE TECHNOLOGIES

USB 2.0 Wireless Capture Adapter
User's Guide

Copyrights

AirPcap USB 2.0 Wireless Capture Adapter User's Guide

Document Version: 1.0
Document Revision: August 23, 2006

CACE Technologies, LLC
Davis, CA 95616
(530) 758-2790
(530) 758-2781 (fax)
support@cacetech.com
http://www.cacetech.com

CACE TECHNOLOGIES

Contents and Figures

Contents

Figures

CACE TECHNOLOGIES

A Brief Introduction to 802.11b/g WLANs

Terminology

The terms *Wireless LAN* or *WLAN* are used to indicate a wireless local area network, i.e. 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 *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.
802.11b, ratified in 1999, is an extension of 802.11. It uses the same 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 8 additional transmission rates: 6, 9, 12, 18, 24, 36, 48 and 54 Mbps.

Channels

802.11b and 802.11g divide the 2.4 GHz spectrum into 14 frequency bands whose center frequencies are 5 MHz apart. These frequency bands are referred to as *channels* and stations communicate using a particular channel.

The actual use of the channels, however, depends on the country: In the USA, the FCC allows channels 1 through 11, whereas most of Europe can use channels 1 through 13. In Japan, you have only one choice: channel 14.

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 points are 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, 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

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 additiona details, you can consult the following websites:

http://www.wi-fiplanet.com/tutorials/article.php/1447501

http://technet2.microsoft.com/WindowsServer/en/library/370b019f-711f-4d5a-8b1e-4289db0bcafd1033.mspx?mfr=true

Another good source is the book *802.11® Wireless Networks: The Definitive Guide* by Matthew Gast.

How the AirPcap Adapter Operates

The AirPcap adapter captures 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. The AirPcap adapter can be set to any valid 802.11b/g channel, from 1 to 14.

By using more than one AirPcap adapter and setting each of the adapters to a different channel, you can capture traffic from multiple channels simultaneously.

The AirPcap adapter is completely passive. This means that it captures the traffic on a channel without associating with an access point, or interacting with any other wireless device. Since it does not transmit, it is not detectable by any other wireless station.

The AirPcap adapter works 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.

The next sections will show how to configure the AirPcap adapter and software using the AirPcap control panel, and how to capture the traffic and change the configuration directly from Wireshark.

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. The 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

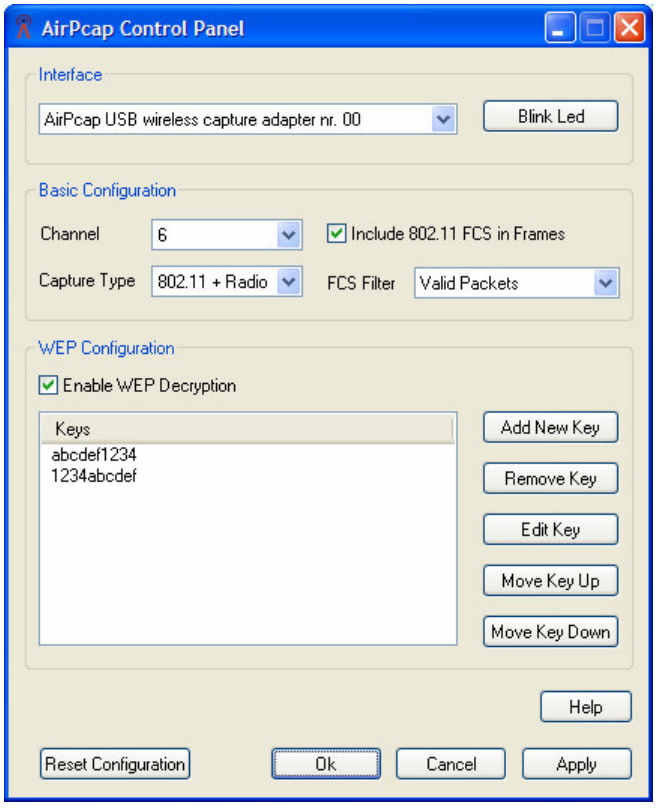

Figure 1: The AirPcap Control Panel

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

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.**

Basic Parameters

The basic parameters that can be configured are:

- Channel Number: ranges from 1 to 14.
- Capture Type: 802.11 frames only, or 802.11 frames plus radio information. Radio information includes additional information not contained in the 802.11 frame: transmit rate, signal power, signal quality, channel.
- 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 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.

WEP Keys

The AirPcap driver is able to 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 the frame 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 cleartext 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.

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.

Note:	**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.**

Wireless Packet Capture in Wireshark

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

Identifying the Wireless Adapters

Figure 2 shows the Wireshark Capture Interfaces dialog (*Capture* >> *Interfaces*). The AirPcap Interfaces are easy to identify by looking at the icon near them.

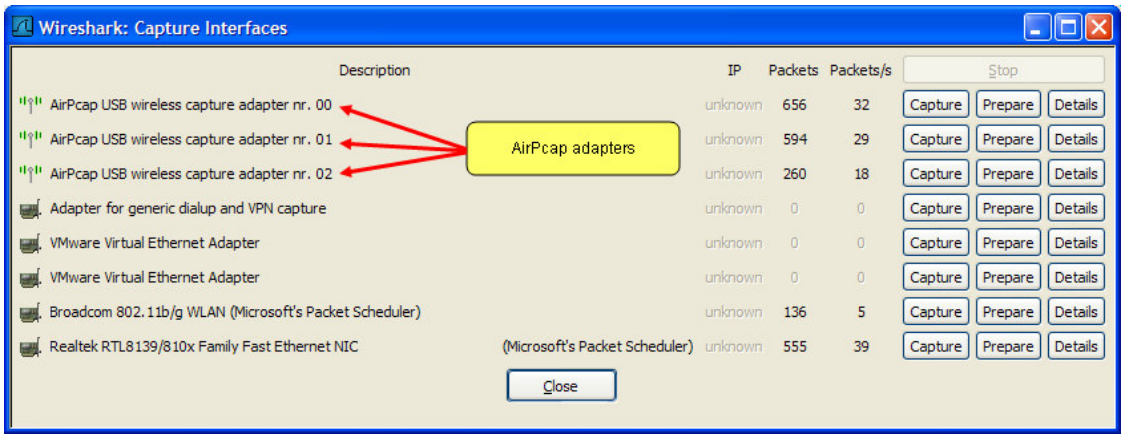

Figure 2: The Wireshark Adapters List

The Wireless Toolbar

Figure 3 shows the Wireshark wireless toolbar. The wireless toolbar provides a fast and productive way to setup 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.

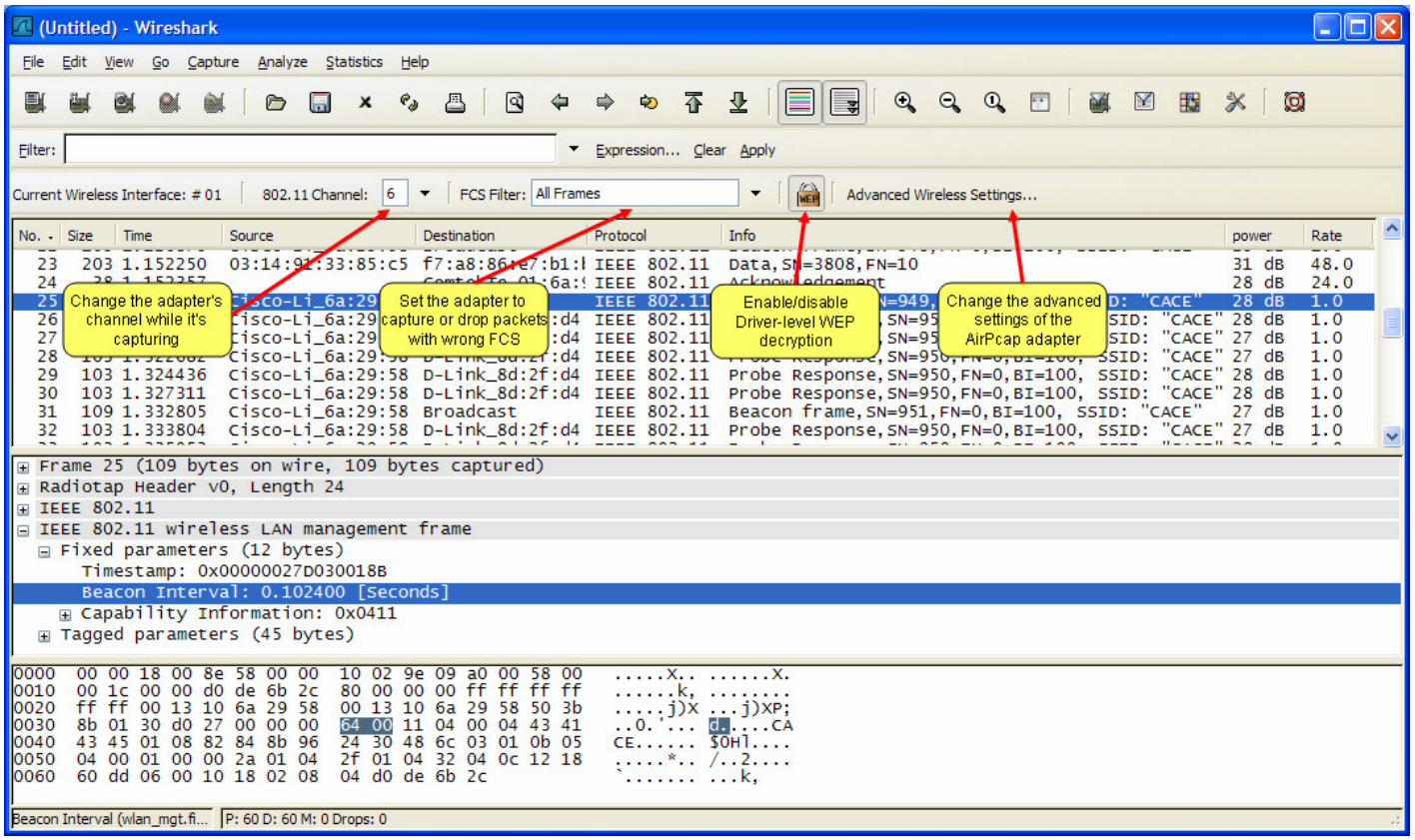

Figure 3: The Wireshark Wireless Toolbar

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.

Tip:	**When real-time packets listing is 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.

- WEP Decryption (lock) Button: this check button allows you to turn on and off the kernel-level WEP decryption on the currently-selected AirPcap adapter. You will need to configure one or more WEP keys for this button to have an effect.

- Advanced Wireless Settings: this button opens the Advanced Wireless Settings dialog for the currently-selected AirPcap adapter. See the next paragraph for details.

The Advanced Wireless Settings Dialog

The Advanced Wireless Settings Dialog (Figure 4) can be used to set the advanced parameters of an AirPcap adapter. The dialog can be accessed either from the Wireless Toolbar (*Advanced Wireless Settings*) or from the main menu (*Capture* >> *Options* >> *Wireless Settings*).

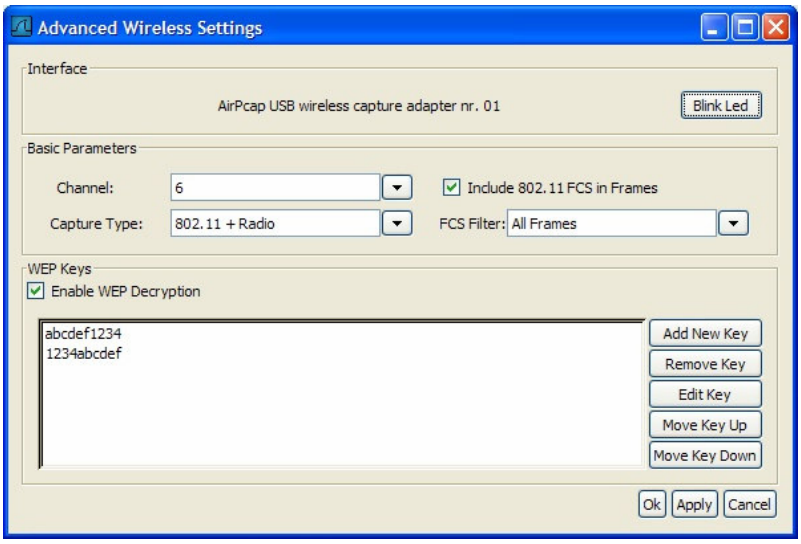

Figure 4: Advanced Wireless Settings in Wireshark

Basic Parameters

The basic parameters that can be configured are:

- Channel Number: ranges from 1 to 14.

- Capture Type: 802.11 frames only, or 802.11 frames plus radio information. Radio information includes: 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 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 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.

WEP Keys

The AirPcap driver is able to 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 the frame 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 cleartext 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.

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.