AirPcap Frequently Asked Questions

What is AirPcap?

AirPcap is a family of wireless capture devices and drivers representing the first open, affordable and easy-to-deploy 802.11 packet capture solutions for the Windows platform. More specifically, AirPcap is:

- A Windows-based, USB form-factor 802.11 wireless traffic capture device
- The only Windows-based wireless traffic capture device that fully integrates with Wireshark to present full management and data control frames
- The only wireless traffic capture device to fully integrate with Cascade Pilot
- Currently available in 3 versions: 2 for b/g channels and 1 for a/b/g/n channels
    - (CAS-APC) AirPcap Classic – 802.11b/g, receive only
    - (CAS-APC-Tx) AirPcap Tx – 802.11 b/g, send and receive
    - (CAS-APC-Nx) AirPcap Nx – 802.11 a/b/g/n, send and receive

Each AirPcap device, when used with Wireshark for example, delivers information about wireless protocols and radio signals, enabling the capture and analysis of low-level 802.11 wireless traffic including control frames, management frames, and power information in the Wireshark UI. Once AirPcap is installed, Wireshark displays a special toolbar that provides direct control of the AirPcap adapter during wireless data capture.

What are the differences between each of your AirPcap versions?

In addition to all of the packet capture features and functionality of the AirPcap Classic adapter, AirPcap Tx, and AirPcap Nx support packet injection. The ability to transmit raw 802.11 frames is an invaluable aid in assessing the security of your wireless network. Several security tools, including Cain & Abel and Aircrack-ng, can use the AirPcap Tx adapter transmit features, for example, for advanced penetration testing.

AirPcap Nx includes a USB-based 802.11 a/b/g/n adapter with two internal antennas and two external 2.4 GHz antennas with connectors. AirPcap Nx also provides on-board microsecond time-stamping precision, unlike the other two AirPcap versions. AirPcap Nx is the first solution to capture, decode, and visualize 802.11n protocol traffic from any Windows-based laptop or desktop PC.

How is AirPcap different from other WLAN packet capture tools?

There are many features that make AirPcap unique. For instance, AirPcap is an optimized device built with packet capture in mind from the firmware to the application. Instead of relying on a third-party vendor driver, we developed our own. This approach guarantees:

- No interference with your regular networking
- Support for any Windows OS from Windows 2000 to Windows 7
- Superior capture performance with minimal packet loss, especially when doing multi-channel capture on 802.11n networks

Our adapters are manufactured to our specifications and individually programmed, giving us a large measure of control over their feature set and the stability of those features. This also allows us to provide you with a product that offers great flexibility in terms of use. Use AirPcap adapters with Cascade Pilot for analysis, charting and reporting, use them with Wireshark for frame capture, packet analysis and protocol dissection, use them with Kismet for network discovery, with Aircrack-ng for WEP cracking, etc. Additional unique advantages offered by AirPcap include:

- Capture de-coupled from analysis. Just hand an AirPcap adapter to anyone with Wireshark installed and they can capture, filter, display, analyze, dissect, and save WLAN packets at will using the world's most popular, widely-deployed, and free network and protocol analysis tool. Or use AirPcap with Cascade Pilot and enjoy additional features likes channel scanning.
- Easy creation of a remote 24/7 capture probe by installing one or more AirPcap adapters and a copy of Wireshark on an old PC, letting it run continuously until something interesting happens.
- Listen to multiple channels simultaneously in Wireshark or Cascade Pilot or aggregate the packets from those channels in to a single data stream for analysis by using the multi-channel aggregator feature of the AirPcap driver.
- External antenna use. Any serious capture adapter needs to have this.
- AirPcap adapters are the only wireless adapters that can be used in conjunction with tools like Wireshark, tcpdump/windump and Kismet.
- Easily run under VMware on a Macintosh or Linux machine (or a VM session within Windows).
- Provide both signal and noise reporting.
- Deliver microsecond-precision hardware time-stamping. This is very important for roaming analysis.
- AirPcap Nx adapters are capable of packet analysis in the 4.9 GHz band, and in many non-standard 5GHz bands.
- The AirPcap Tx and Nx replay/injection feature is very useful for a variety of network and security testing exercises.

Which AirPcap versions provide support for multi-channel monitoring and aggregation?

All AirPcap adapters support multi-channel monitoring and aggregation.

I have a primary requirement to attach an external antenna for my WLAN analysis. Do you have any options?

AirPcap Nx (802.11a/b/g/n) ships with two 2.4 GHz antennas and pigtails. The Nx adapter also has two internal printed antennas that operate when external antennas are not present.

Do you provide support for 802.11ac?

Not today, but it is in our plans.

Does AirPcap offer on-board time-stamping in microseconds?

AirPcap Nx provides support for hardware time-stamping with microsecond precision.

Is there a way to see the keys derived from the various EAPOL handshakes as long as the pass phrases and full exchange are present?

WPA temporal keys (PTK and GTK) are not displayed by Wireshark. Pairwise keys are derived but not displayed, and group keys are not, as yet, derived.

I'm using a laptop with a built-in adapter. Do you have a version of AirPcap that will support built-in adapters?

No, we don't, and for a very good reason. AirPcap Classic, Tx and Nx are USB-based, leaving you free to use your built-in adapter for normal network operations while simultaneously using AirPcap for analysis. This is much more convenient and flexible than trying to use a single adapter for everything.

When I plug my AirPcap Nx adapter into my Vista system and launch WireShark or the AirPcap Control Panel, the application freezes until I remove the adapter. Why is this happening?

There is a known bug in the USB stack of Vista SP2 that causes the AirPcap Nx adapter to lock-up. While Microsoft is aware of the situation, they have not yet provided a solution for Vista. We can supply a registry patch to fix the problem if you can first provide a registry dump of your Vista machine.

The below commands will generate a file called 'dump.reg' in the root directory of the C: drive:

1. Open a command prompt: Start > search box > cmd
2. Type: regedit /e c:dump.reg HKEY_LOCAL_MACHINESYSTEMCurrentControlSetEnumPCI
3. Click [Yes] to the prompt (if any) from User Account Control window.

Please email this partial registry dump file to support@riverbed.com. Once we have this file we will create and return a custom patch file for your computer.

Do you have a version of AirPcap that runs on Linux, OS X, FreeBSD, VMS, or OS/2?

AirPcap currently runs on the following platforms:

- Windows 2000
- Windows XP (service pack 2, 32 or 64 bit)
- Windows 2003 (32 or 64 bit)
- Windows Vista (32 or 64 bit)
- Windows 7 (32 or 64 bit)

There are no plans to port AirPcap to other platforms at this time.

I see that you provide packet-transmission in AirPcap Tx and Nx. Does the packet transmission include custom-crafted packets, or does this mean that you only play back .cap streams?

For the moment, our solutions allow you to create custom packets that can then be sent over the air. We don't have replay capabilities. The packets are sent one at a time, but the API gives you the flexibility to send pretty much any way you like.

Can AirPcap sniff multiple channels at one time and debug WPA/WPA2 data?

Yes, you can sniff multiple channels if you have multiple adapters attached to your Windows-based laptop or desktop. AirPcap can capture traffic from multiple channels at the same time and aggregate the data into a single capture. WPA and WPA2 can be decrypted and analyzed using Wireshark or Cascade Pilot.

I am using Wireshark to do Ethernet packet analysis and would like to do wireless packet capture as well. Do I just need to buy AirPcap and install it for Wireshark to be enabled to deliver wireless data automatically?

That's right. After installing our driver and plugging our adapter in the USB port, Wireshark, will start capturing wireless traffic.

Is the signal strength of the AirPcap Tx adapter adjustable?

No. The Tx frequency and strength are very strictly regulated by the FCC. The signal strength is set to the maximum allowed by the ship-to country.

Can AirPcap Tx and Nx be set in totally passive mode?

Yes. AirPcap Tx and Nx are totally passive unless you use a program that explicitly injects packets.

Does AirPcap run under BartPE?

We've never tested it under BartPE, but our understanding is that BartPE is just a stripped down version of Windows that runs from a CD. In that case, we can't see any reason why AirPcap shouldn't work with it. You probably want to include the AirPcap driver when you build the BartPE image to avoid installing it every time.

Why do AirPcap NX adapters have two antennas? I understand that 802.11n offers MIMO capabilities. Is this related to that? Can you explain how the RF reception of these two antennas are aggregated or filtered on baseband?

The use of two antennas is due to both MIMO and two other RF techniques used by 802.11n to offer higher rates and better reception. Different techniques to merge the signals are used, depending on the specific modulation used (HT-OFDM with 20 or 40MHz channels, or DL-OFDM). In some cases, the packet is transmitted on both antennas, and each antenna transmits a part of the packet using a slightly different modulation. In other cases, the packet is "duplicated" on the two antennas and on reception the RF combines the two "copies" of the packet (a sort of redundancy). In the case of receiving packets with an 802.11b/g modulation (OFDM) the two antennas are used for "antenna diversity", i.e., they use the fact that separate antennas receive a slightly different RF signal. In this case, the RF section combines the two signals for better reception.

A complete explanation of all these techniques can be found in the IEEE 802.11n specification.

I'm interested in AirPcap but the PCs in my test lab do not have USB 2.0 ports Is 2.0 a hard or soft requirement?

The AirPcap adapter works with USB 1.0 as well. However, since the bandwidth of USB 1.0 is very low, you might experience drops at high frame rates. We do not support USB 3.0 currently.

Is it possible to capture every packet on a WLAN?

Due to the nature of the wireless world, it is unlikely that you will ever capture all traffic. There will always be some packets missed by any wireless capture device. This is the nature of WiFi analysis and interference in the radio spectrum.

Do you support USB 3.0 ports with AirPcap?

Not officially, though AirPcap Classic and AirPcap Tx seem to work without issue on these ports. AirPcap Nx does have an issue, however, and will blue screen if you try and use it in a USB 3.0 port that is not backward-compatible.

Can AirPcap Nx sniff packets from an entire multichannel N connection from one host?

If “multichannel N connection” means “40MHz channel” (i.e. a wide channel), the answer is yes, we do support standard (20MHz) and wide channels (40MHz). If we are talking about MIMO, then the answer is yes up to 2x2.

We would like to inject packets for penetration testing using a command-line utility of some sort. Is this possible?

AirPcap Tx and AirPcap Nx have the ability to inject packets for penetration testing. You can download the AirPcap API from https://support.riverbed.com/software/wireshark.htm and look at the packet injection sample to learn more about this.

Do both the AirPcap NX adapter and AirPcap NX 3-pack allow the simultaneous capture of wireless traffic on the a/b/g/n bands?

Yes. They are exactly the same devices with the same driver. One is just a single adapter and the other is a SKU that includes three of the adapters.

Does the AirPcap 3-pack allow the monitoring and simultaneous capture from all bands as opposed to scanning the bands sequentially and only capturing packets on a specific band during the actual time that the band is being scanned?

The 3-pack allows you to capture from three different channels simultaneously and aggregate the capture streams, if you choose, into one stream that can be analyzed through the Wireshark UI.

How does the AirPcap Multi-Channel Aggregator work?

When more than one AirPcap adapter is plugged in, the AirPcap Control Panel will show one additional interface: the Multi-Channel Aggregator. The Multi-Channel Aggregator is a virtual capture interface that can be used from Wireshark or any other AirPcap-based application. Using this capture interface, the application will receive the traffic from all the installed USB AirPcap adapters, as if it was coming from a single device.

The Multi-Channel Aggregator is a virtual capture interface that can be used from Wireshark or any other AirPcap-based application. Using this capture interface, the application will receive the traffic from all the installed USB AirPcap adapters, as if it was coming from a single device.

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.

I need to be able the generate Greenfield packets to test the performance of our sensor. Can 802.11n Greenfield packets be generated?

Greenfield mode is not supported with the current Nx chipset.

Are there any channel restrictions for packet injection? We'd likely use this tool in our production tests and need to calibrate each possible channel (1-14 and all 5GHz band channels) regardless of regulatory domain.

The AirPcap Nx adapter can be programmed for universal use if necessary

Is the transmit power of the AirPcap NX configurable? Has it been calibrated? If it hasn't been calibrated, is it stable over time and reproducible?

It's not possible to configure the Tx power. It actually depends on the ship-to country, and then it's the maximum allowed in that country and we do not perform any specific calibration.

Our current production environment uses Linux and Python to control various pieces of test equipment and perform analysis. It appears that the only way to interface with the AirPcap NX is through the Windows driver, API and Windows tools. Are there any methods to script the commands going to the AirPcap NX?

There are no methods for this, no.

How is noise information computed with AirPcap adapters?

Noise information in wireless adapters is computed by the onboard chipset. The IEEE 802.11 standard defines the mechanism with which RF energy is to be measured by the adapter. This value is called the Receive Signal Strength Indicator (RSSI). The RSSI scale differs for each chip manufacturer.

In the Nx adapter for example, the noise value is computed by hardware and reported to the host when you change the frequency. The hardware reports a signal to noise value (utilizing RSSI) on a per packet basis. The signal value is then computed as signal = RSSI + noise. There is no polling involved. Also, note that the signal is a negative value, so -10 is better than -60. In general, the values returned

by the AirPcap adapters (and all adapters in general) should be taken as a rough estimate and used mainly for comparison (e.g. compare packets received from different APs by the same AirPcap adapter).

I know that AirPcap captures Wi-Fi 802.11 traffic. I am looking for a similar product to capture mobile broadband (2G/3G/4G) traffic from a USB dongle, preferably for Windows 7 environment. Do you have a product for this?

Our adapters are for 802.11 WLAN traffic only today and we have no plans currently to offer a similar product in the mobile broadband space.

Can AirPcap sniff a wireless network protected with WPA/WPA2 without the passphrase?

The short answer to your question is “yes” if you’re using Wireshark and WPA/WPA2 Personal (pre-shared key) encryption. You need to make sure that "Wireshark" is selected as "Decryption Mode" in the wireless toolbar. Alternatively, go to Edit > Preferences > Protocols > IEEE 802.11 for a more comprehensive configuration screen. Wireshark will then automatically decrypt the WPA-encrypted packets, and show them in clear text in the decoding panes. If decryption is disabled, you will just see the 802.11 headers and then encrypted information. If decryption is enabled, you will see the 802.11 headers and then IP, TCP and so on. For some more information about 802.11decryption, you can refer to the following wiki page: http://wiki.wireshark.org/HowToDecrypt802.11.

Remember that you need to catch the WPA handshake when a workstation first connects to the access point to see decrypted traffic as well. If you’re not seeing decrypted packets, the most likely cause is either the decryption key information is not set or, in the case of WPA, the initial four-way handshake negotiated between the access point and its peer was not captured.

If you have verified that the encryption keys have been installed correctly, the other most likely reason preventing you from seeing the decoded traffic is the placement of the analyzer with respect to the access point and its peers. If the Wireshark analyzer misses any of the initial WPA/WPA2 EAPOL handshake packets used to establish the pairwise transient key (PTK) between the AP and its peer, Wireshark will not be able to decrypt that conversation. Try relocating the analyzer closer between the AP and peer. Also, you will not be able to decrypt traffic from existing conversations established before the analyzer started capturing/decrypting packets. Here is a quick overview of the four-way key: http://en.wikipedia.org/wiki/IEEE_802.11i-2004#The_Four-Way_Handshake. You should see EAPOL in the protocol column in Wireshark. Also, just to keep the terms straight, you need to decrypt the packet first before the data can be 'decoded' (various protocol statistics displayed).

Note that WPA/WPA2 Personal (pre-shared key) decryption is supported while WPA/WPA2 Enterprise is not since it requires the use of a 3rd party authenticator (ex a Radius server) which cannot be queried by the analyzer for any keys issued. This would obviously defeat the extra security level of Enterprise mode.

Do AirPCap Tx/Nx have API support to transmit and receive raw 802.11 frames at the same time? Can I build up my own raw 802.11 frames and transmit through AirPCap Tx/Nx through a software API/SDK? And can I simulate multiple WiFi adapters through a single AirPCap Tx/Nx device by sending 802.11 frames with different WiFi MAC addresses? My software will handle the simulation.

Yes, this is all possible through API use.

About Riverbed

Riverbed delivers performance for the globally connected enterprise. With Riverbed, enterprises can successfully and intelligently implement strategic initiatives such as virtualization, consolidation, cloud computing, and disaster recovery without fear of compromising performance. By giving enterprises the platform they need to understand, optimize and consolidate their IT, Riverbed helps enterprises to build a fast, fluid and dynamic IT architecture that aligns with the business needs of the organization. Additional information about Riverbed (NASDAQ: RVBD) is available at **www.riverbed.com**.

Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Tel: (415) 247-8800
www.riverbed.com

Riverbed Technology Ltd.
One Thames Valley
Wokingham Road, Level 2
Bracknell. RG42 1NG
United Kingdom
Tel: +44 1344 401900

Riverbed Technology Pte. Ltd.
391A Orchard Road #22-06/10
Ngee Ann City Tower A
Singapore 238873
Tel: +65 6508-7400

Riverbed Technology K.K.
Shiba-Koen Plaza, Bldg. 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990