Application Note:
Remote Packet Capture with WildPackets AiroPeek NX

Aruba Wireless Networks Application Note

Introduction

One of the powerful features provided by Aruba Wireless Networks is the ability to perform remote packet capture using Aruba's dual-purpose access points and RF Analyze software. Through a unique partnership with WildPackets, network managers are able to treat each Aruba Air Monitor and Access Point as a remote probe within WildPackets' AiroPeek NX industry-leading wireless capture and monitoring software. This application note will document the solution and provide instructions for configuring and using the system.

Features

In an Aruba wireless deployment, dual-purpose access points are deployed and automatically configured to provide either Access Point (AP) functionality or Air Monitor (AM) functionality. Air Monitors are used to enable a number of features, including automatic calibration, self-healing, wireless RMON, interference detection, rogue AP detection and destruction, wireless intrusion detection, and remote packet capture. Air Monitors can perform these functions on all channels, while APs can perform these functions only on their configured channel. APs and AMs can be deployed anywhere there is IP connectivity back to an Aruba switch – the unit will automatically locate and establish a secure connection to the switch, download its configuration, and begin operation. One implication of this is that AMs can be deployed at remote offices that have no IT staff, as long as the office has an Internet connection. Through the remote monitoring capabilities of the AM, corporate IT staff can have the same view of the remote RF environment as if they were physically present at the remote office. Naturally, this same benefit applies to buildings or floors within a local campus – rather than taking a wireless analyzer and walking to a problem area, IT staff can troubleshoot wireless problems from their own desks.

AiroPeek NX Configuration

AiroPeek NX is not sold by Aruba, and must be purchased from WildPackets or through distribution channels. Once AiroPeek NX is properly installed, a plug-in software module, the WildPackets Aruba Remote Adapter, is required to enable communications with Aruba Air Monitors and Access Points. The module can be downloaded free of charge from Aruba's customer support website at http://www.arubanetworks.com/support. Install the software by running the "setup.exe" program included with the package. The installer will automatically configure AiroPeek NX to work with Aruba equipment.

Performing Remote Packet Capture

To start a remote packet capture, open a web browser and connect to the switch. Login to RF Director. This section will discuss capturing through an Air Monitor, since this is the most common usage of the feature. Note that captures may also be done through any AP as long as the traffic to be captured is on the AP's configured channel.

If the target air monitor is already known, navigate to it by selecting RF Analze->Air Monitor, then clicking on the Air Monitor of interest. Once selected, a menu bar appears on the left side of the screen that contains a Packet Capture selection. Click on Packet Capture. The Packet Capture screen is shown in Figure 1.

Figure 1 - Packet Capture Window

To begin a packet capture, click on “New Raw Packet Capture”. Two formats are available for raw packet captures – one compatible with AiroPeek NX, and one compatible with Ethereal. Select the AiroPeek NX radio button. Next, fill in the Target IP address. This IP address is that of the station running AiroPeek NX – typically the same one currently connected to RF Director. If the channel to be monitored is known, it may be selected in the channel menu – otherwise, the AM will scan all available channels. Finally, select whether monitoring should be done on 802.11a or 802.11g frequencies (802.11b and 802.11g share the same channels). When all parameters have been filled in, click on “Start”.

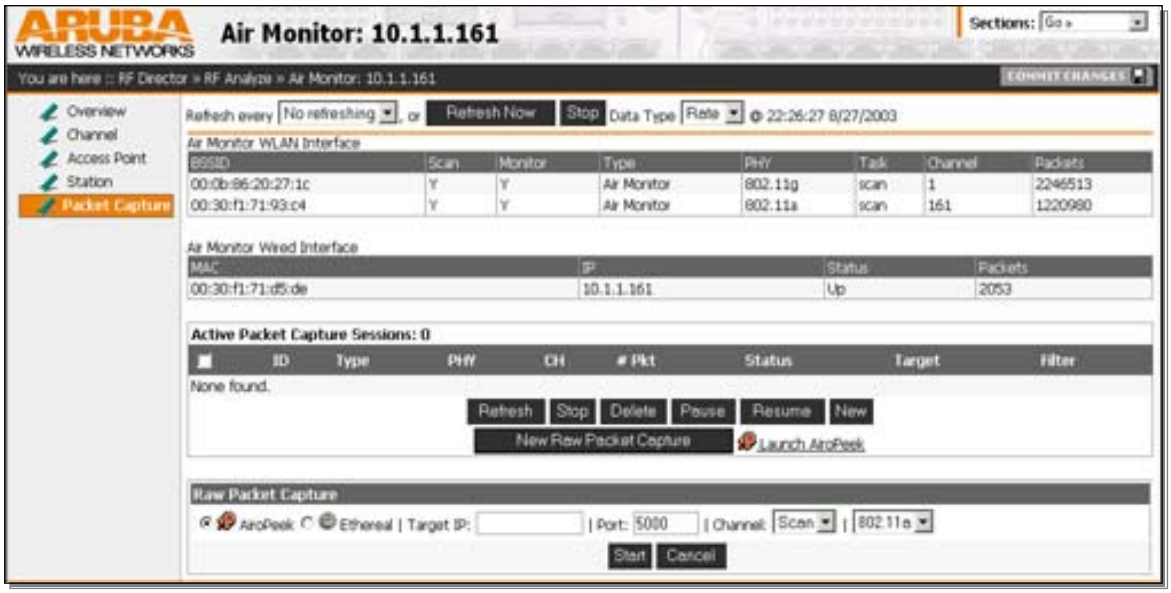

Figure 2 - Raw Packet Capture

The new packet capture will appear under the Active Packet Capture Sessions, and the status will show “in-progress”. Once this has happened, all 802.11 packets seen by the selected Air Monitor will be encapsulated inside a UDP datagram and sent to the target IP address specified. The capture will continue until stopped by the user.

If AiroPeek NX is not already running, it may be launched by clicking on the “Launch AiroPeek NX” link. Once AiroPeek NX launches, a new packet capture may be started by clicking “New Packet Capture.” If the Aruba Remote Adapter has been installed correctly, the adapter list will include “Module: Aruba Remote Adapter” as shown in Figure 3.

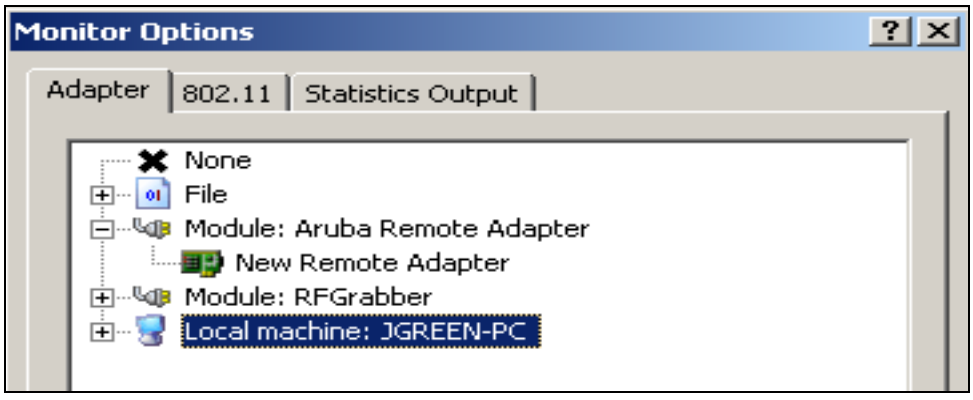

Figure 3 - AiroPeek NX Adapter Selection

If the AM/AP sending the packet capture is not listed under the Aruba module, create a new entry for it by double-clicking on “New Remote Adapter” and filling in the IP address of the Air Monitor. This address can be found at the top of the RF Director screen where the packet capture was started. The Aruba Remote Adapter provides filtering capability to capture packets only from a specific AM/AP. This allows a user to have multiple

packet captures running at the same time, and ensure that AiroPeek NX displays traffic from only the correct one. By creating a new remote adapter with the IP address of the target AM/AP, AiroPeek NX will display only traffic coming from that AM/AP. Multiple packet captures may be displayed simultaneously by starting new AiroPeek NX captures and selecting a different remote adapter.

The 802.11 tab under "Capture Options" has no effect during an Aruba remote capture. Traffic to be captured is selected by the AM/AP, so pre-processing filters such as channel, BSSID, and ESSID are not used by AiroPeek NX. All other triggers and filters are available.

To stop the packet capture within AiroPeek NX, first click on "Stop Aruba Capture". Note that this only tells AiroPeek NX to stop the capture – to tell the AM/AP to stop capturing, return to the RF Director screen where the capture was configured, select the checkbox next to the active capture session, and click on "Stop."

Locating the Target AM

If the AM/AP in the area to be monitored is not known (for example, a user calls from a conference room to report a wireless problem), RF Analyze provides several other mechanisms for locating the correct AM/AP. The simplest way is to select RF Analyze->User. This screen will display a table that can be sorted by username, MAC address, IP address, and other parameters. When the desired user is found, click on the magnifying glass symbol next to that user's MAC address. A screen similar to that shown in Figure 4 will appear.

Figure 4 - RF Analyze

As shown in this screen, four different APs/AMs can see this user, with the signal strength shown under the RSSI column. The signal strength is highest for AP 1.1.1, most likely the AP that this user is currently associated with. The signal strength is also relatively strong on AM 1.1.7, indicating that a good packet capture can be done from this AM. Click on either 1.1.1 or 1.1.7 to bring up the AM view of the station, as shown in Figure 5.

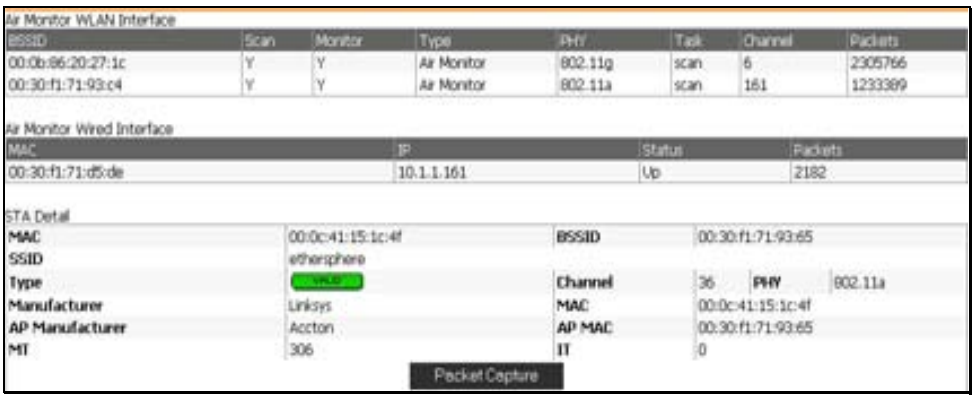

Figure 5 - AM STA View

From this screen, click on the Packet Capture button to bring up the packet capture window.

Three types of packet captures are possible from this window. The first is a raw packet capture, exactly like that described in the previous section. In the raw capture mode, anything received by the AM/AP will be sent to the capture station. As of this writing, only raw packet captures may be done with AiroPeek NX, because AiroPeek NX contains built-in advanced filtering capabilities of its own. The second type of packet capture is known as "interactive." In this mode, which is not currently compatible with AiroPeek NX, a filter may be applied on the AM so that only packets of interest are sent to the monitoring station. The restriction in this mode is that only the first 256 bytes of the packet are captured. This type of packet capture is more useful for capture software without advanced filtering capabilities. A third type of capture is known as batch mode. In this mode, filters are applied on the AM as in interactive mode, but packets are stored on the AM and are made available for download to the monitoring station after the capture has completed. This mode is appropriate when low-speed lines are used between the monitor and the capture station so that the capture does not overwhelm the entire line. Of the three modes, raw capture is the most powerful, since it consists of real-time monitoring with full packets being sent to the monitoring station. Any desired filtering may be done in AiroPeek NX while the capture is in progress, or after a capture has ended.

Configuring Capture Port

The Aruba Remote Adapter works by encapsulating all 802.11 frames inside a UDP packet, and streaming them to UDP port 5000 on the capture station. If port 5000 is already used by another application, or if it is blocked by a firewall, an alternate port may be configured.

To configure an alternate port in AiroPeek NX, click on the Tools menu, and then select Options. On the left side, highlight Analysis Modules. The Aruba Remote Adapter will be listed under the Analysis Module column. Click on Aruba Remote Adapter to highlight it, then click on Options to change the port number. This screen is shown in Figure 6 below.

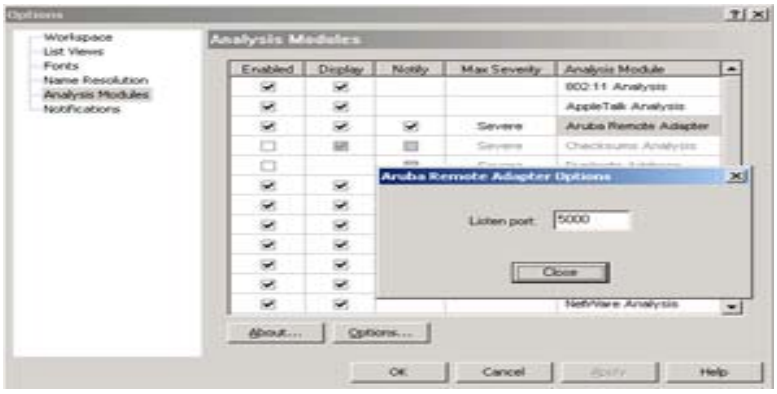

Figure 6 - Remote Adapter UDP Port

In RF Director, the UDP port number may be specified any time a new capture is created. This option is located immediately after the target IP address when setting up a new capture.

Caveats

With Release 1.0 of the Aruba Remote Adapter for AiroPeek NX, certain caveats exist that the network administrator should be aware of. Some of these will be addressed in future releases.

- Time stamps on received packets come from the local PC where AiroPeek NX is running, not from the AM/AP where the capture took place.
- There is currently no way to stop a capture with a single mouse click – captures must be stopped in AiroPeek NX and in RF Director separately.
- Only raw packet captures are supported with AiroPeek NX today. Pre-processing of captured packets by the AP/AM is not available.
- It is not advisable to perform a packet capture on a wireless-connected PC that is in the vicinity of the AP/AM doing the capture. This will geometrically increase utilization on the channel, since any capture traffic sent to the monitoring station will itself be monitored and captured. The capture station should be located either on a wired network, or in a completely separate part of the wireless network.

Summary

The partnership between Aruba Wireless Networks and WildPackets is of great value to network managers. Many already use AiroPeek NX for its powerful network analysis capabilities, and with the addition of the free WildPackets Aruba Remote Adapter, a complete troubleshooting and analysis solution that scales to the needs of the distributed enterprise is finally available.