Packet Capturing Options with Aruba Wireless Networks

Jcox@arubanetworks.com 18/09/2006

A number of different options for packet capture are available with Aruba's Wireless Infrastructure. Typically Packet capturing is used as a troubleshooting tool by a customer or the Aruba TAC.

Before you start you need to have ready your Aruba WLAN Controller, Access Points and Air Monitors.

You should also have ready your laptop with the Aruba Ethereal Version which should be downloaded from the Aruba Support site. When you install this we recommend WinPCap version 3.1 (not 3.2).

A short discussion of the use of each method and instructions are given. Remember that many times when secure encryption is in use we will not be able to see the contents of packets, as packets are encrypted between the Client and the Aruba WLAN Controller.

Contents

1 "Air' Packet Capture.

The Aruba Access Points and Air Monitors can both capture packets by listening on their Radio Interfaces. They can then either copy these packets to an IP address (such as your laptop), or copy the packets into their memory. You can capture packets from any AP even if it is a Remote AP.

AP

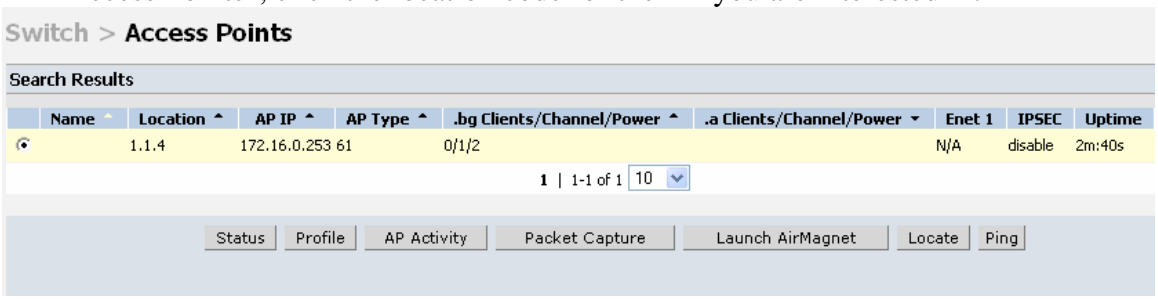
Access Points should only be used for capturing the packets to and from themselves, i.e. on their own radio channel which has been assigned by ARM. This is useful for troubleshooting connections from clients where we suspect an Air problem such as association, specific packet formation etc.

AM

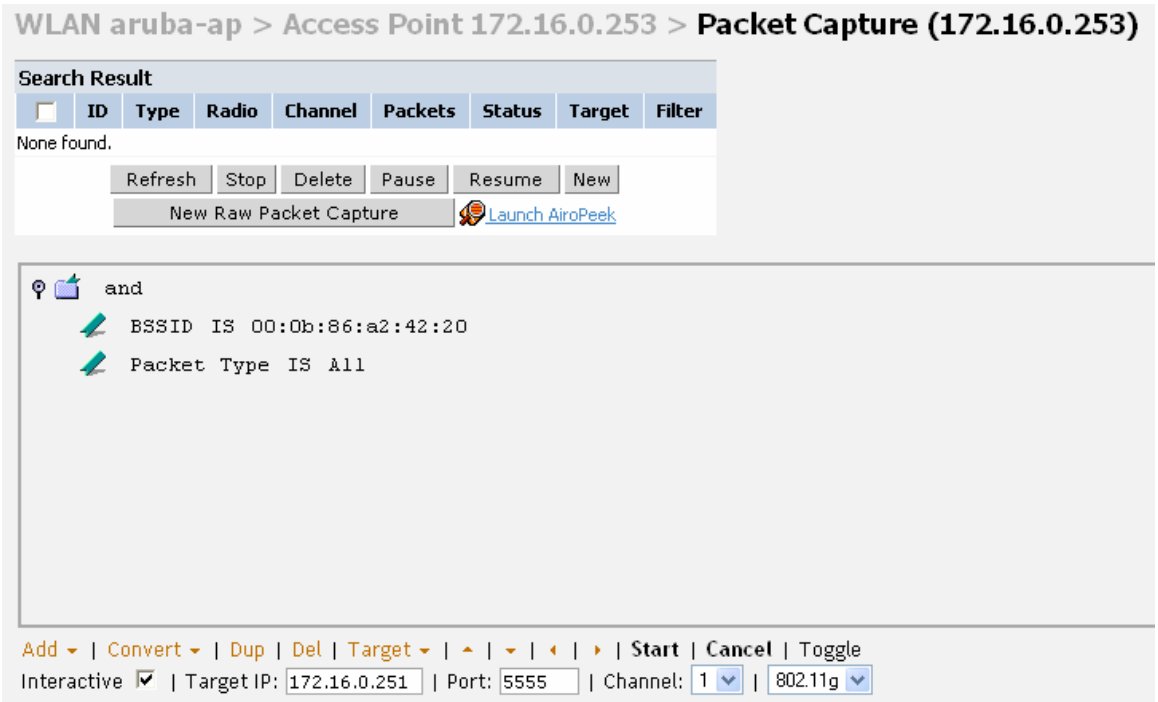
Air Monitors can 'scan' for Packets or be manually tuned to a channel. Thus an Air Monitor can capture Packets from any wifi device. This is useful when you don't want to disturb the Aruba AP, or you want to capture from a 3rd party AP. An Aruba AM which has only one radio (e.g. AP61), can be tuned to capture from 'a' or 'bg' channels

1.1 Packet Capturing to a Laptop/PC from an AP :-

Navigate to the AP you want to packet capture from, for example from "Monitoring", "All Access Points", click the location code for the AP you are interested in.

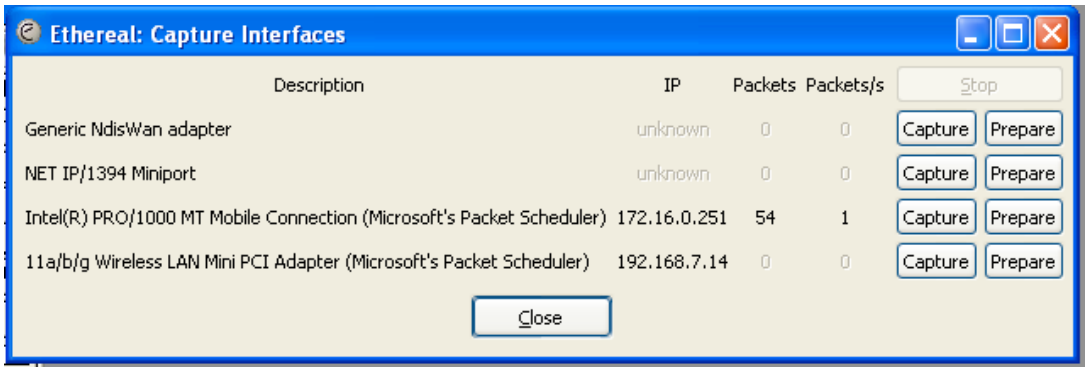


Then select the AP with the left hand radio button and click Packet Capture. If the AP has multiple Radios or there are multiple SSIDs you will be prompted to choose the bssid. Choose the bssid by clicking on it.

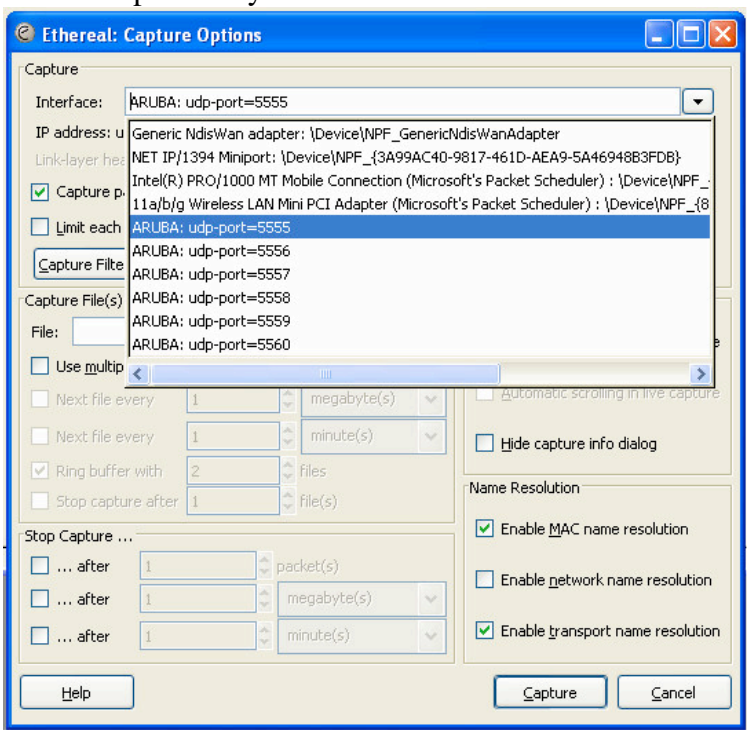


You will then enter your PC IP address in the Target IP box, and the Port such as 5555.Click start, and packets are now being sent to that target IP.

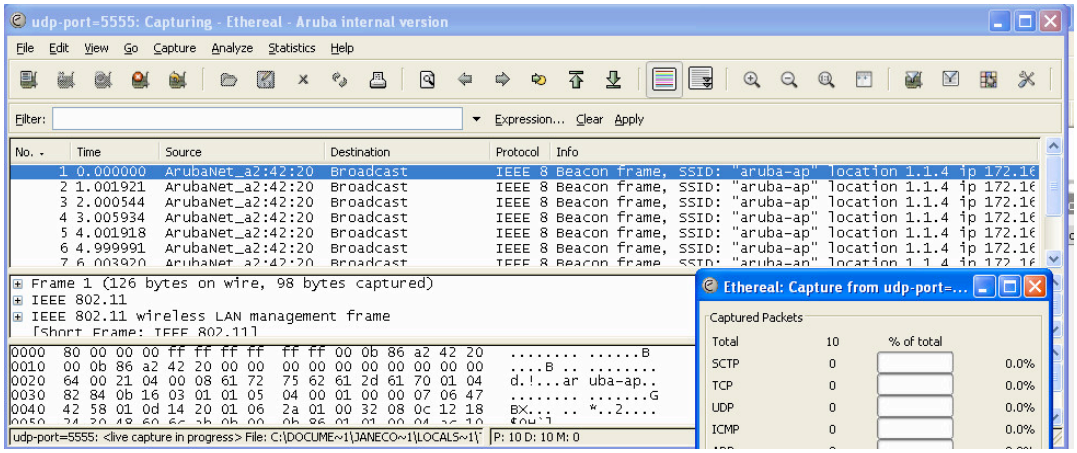
On your laptop start the Aruba version of Ethereal. Click Capture and Interfaces. You will see packets active on your Ethernet Interface



Click 'Prepare' on your Ethernet Interface



Now you can select which of the Aruba Ports to capture on. Select 5555 as we are copying to the port from the AP !. Set all other Ethereal options as you choose.

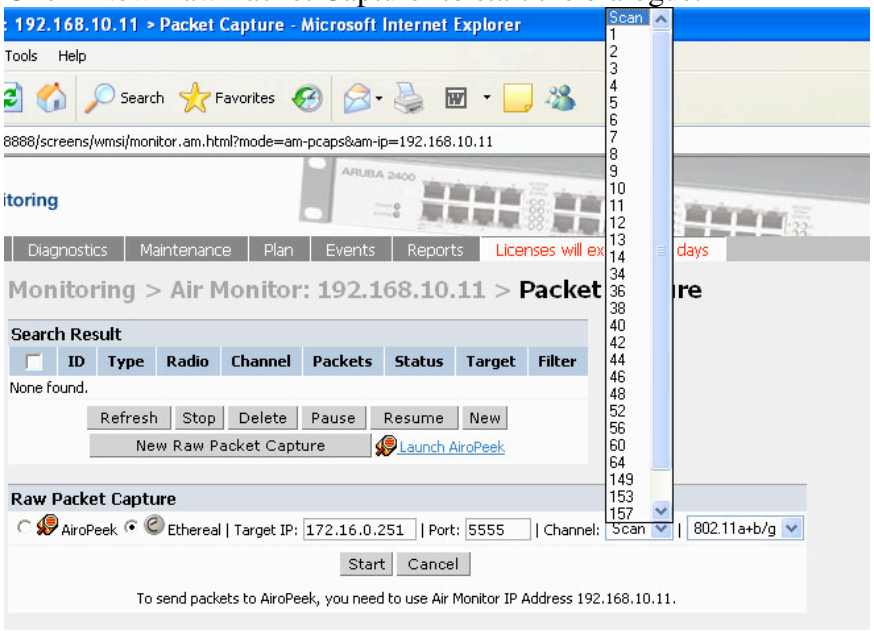


You will then see packets as usual. You can save these in the usual way with File, Save, save as <file>.pcap.

!!**DO NOT capture your own PC traffic wirelessly. You will capture a packet which is sent to you wireless then copied to be sent to you, then copied…you will have to restart your PC to escape. !!**

1.2 Packet Capturing from an AM :-

Same as above except that you will navigate to All Air Monitors to choose the AM. Click 'New Raw Packet Capture' to start the dialogue.

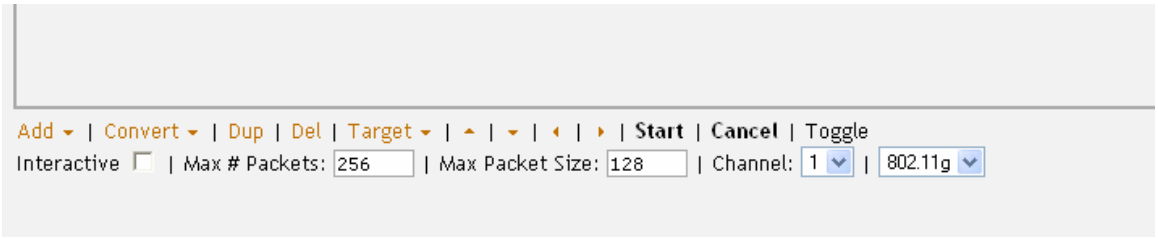


Fill in the screen as before. You can scan (the Air Monitor will scan between channels), or select a particular channel to monitor. Note that the FULL channel range is available for all Aruba AP types. Click "Start" and proceed as before.

1.3 Packet Capture to an AP memory.

Packets can be temporarily saved on the AP, to be retrieved later rather than copying them to your PC. Note the Aruba APs have limited memory for this !.

In the Packet Capture on the AP, uncheck the ‘Interactive’ Option.



Click ‘Start’ as before. Once you reach the maximum packets, or click ‘stop’ a “Download’ url option will appear. You can either click the ‘Download’ now or navigate back to the AP later to get the packets. The packets are held in AP memory and will disappear upon AP reboot

2 Port Monitoring

In common with many network switches you can copy packets from one Aruba Ethernet Port to another. (Sometimes this is called a span port). This is useful for checking data which is coming into/out of the Aruba switch from the rest of the network. Also you can copy AP input/output, if an AP is connected to an Ethernet Port.

I have found this useful for example to check that the Aruba switch was sending DHCP requests to a Server and not receiving replies.

2.1 Port Monitoring Example

In this example we want to copy traffic FROM port 5 TO port 13 . You will notice that the 'show port monitor' command can be used to check status

```
(Aruba2400) (config) #interface fastethernet 1/13

(Aruba2400) (config-if)#port ?
monitor                 Monitor another interface

(Aruba2400) (config-if)#port monitor ?
fastethernet            FastEthernet IEEE 802.3
gigabitethernet         Gigabitethernet Interface

(Aruba2400) (config-if)#port monitor fastethernet 1/5

(Aruba2400) #show port monitor

Monitor Port       Port being Monitored
------------       --------------------
fastethernet 1/13  fastethernet 1/5
```

Once the monitor is started you can connect your laptop/PC to port 13, and start an Ethereal session , in this case simply capturing from your Ethernet card. Use PCAP as usual.
Remember to switch off the monitor !!

```
(Aruba2400) (config) #interface fastethernet 1/5
(Aruba2400) (config-if)#no port monitor fastethernet 1/13
```

3 Controller Packet Capture

Lastly, Packet Capture can be launched on the Aruba Controller itself. This can copy packets that are essentially going to or from the Aruba switch e.g. to or from the VLAN 1 IP address.

The packets are copied from the Aruba Control Processor so you will not see the entire traffic, as with the Port Monitor. You will see packets such as Radius Packets. You will not see some packets such as Heartbeats to the AP as these are formed lower down in a separate processor. You will not see any user-server traffic.

This is useful for diagnosing Radius not working problems, and in cases such as with a 6000 with Gigabit ports where you cannot physically insert your laptop into the data path.

3.1 Starting a Packet Capture on the Controller.

```
(Aruba2400) #packet-capture tcp all

(Aruba2400) #packet-capture udp all
(Aruba2400) #show packet-capture

Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering for all TCP ports enabled.
Packet filtering for all UDP ports enabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.


Packet Capture Defaults(across switches and reboots if saved)
=============================================================
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.

(Aruba2400) #
```

You will note that you can see the status of a packet capture with the ‘show packet-capture’ command.

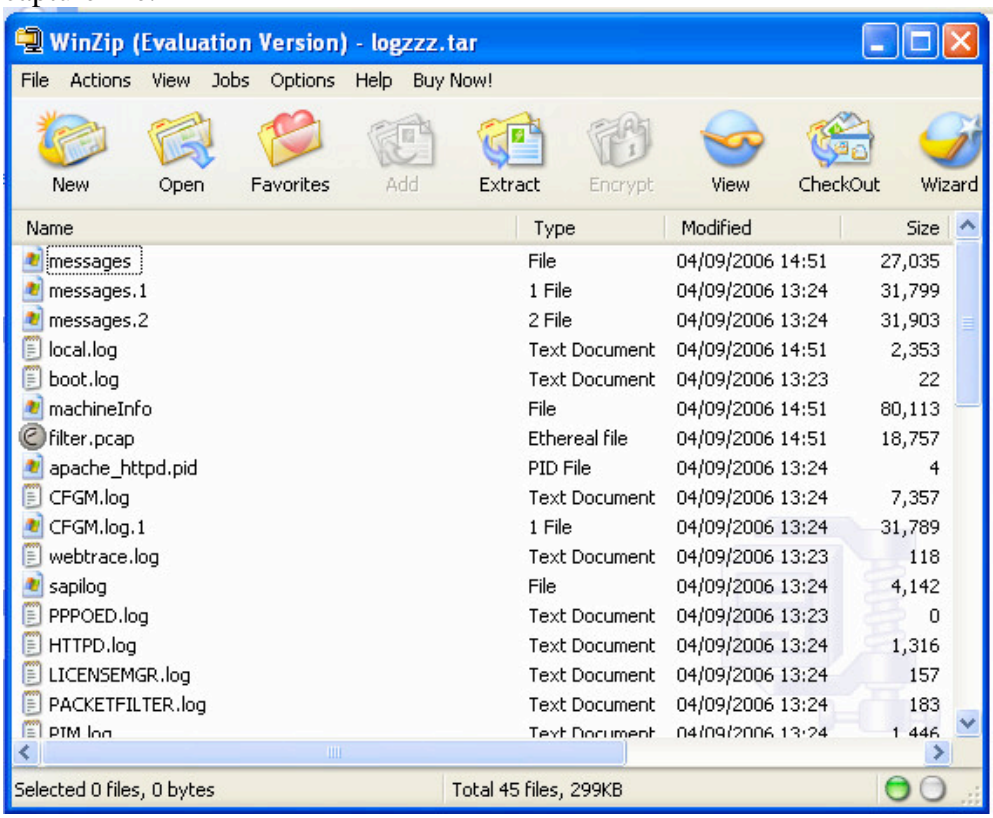
Once you have finished you need to copy the packet capture off the WLAN Controller for analysis :-

```
(Aruba2400) #tar logs
(Aruba2400) #dir

-rw-r--r--   1 root    root       17190 Aug 10 02:55 aug10.cfg
-rw-r--r--   1 root    root       16451 Aug 10 05:45 default.cfg
-rw-r--r--   1 root    root      344064 Sep  4 05:51 logs.tar


(Aruba2400) #copy flash: logs.tar tftp: 172.16.0.251 logszzz.tar
(Aruba2400) #
```

If you look in the logs.tar file, you will see a file called 'filter.pcap', which is the packet capture file.



Don't forget to turn off packet capturing when finished.

```
(Aruba2400) #packet-capture tcp disable

(Aruba2400) #packet-capture udp disable
```