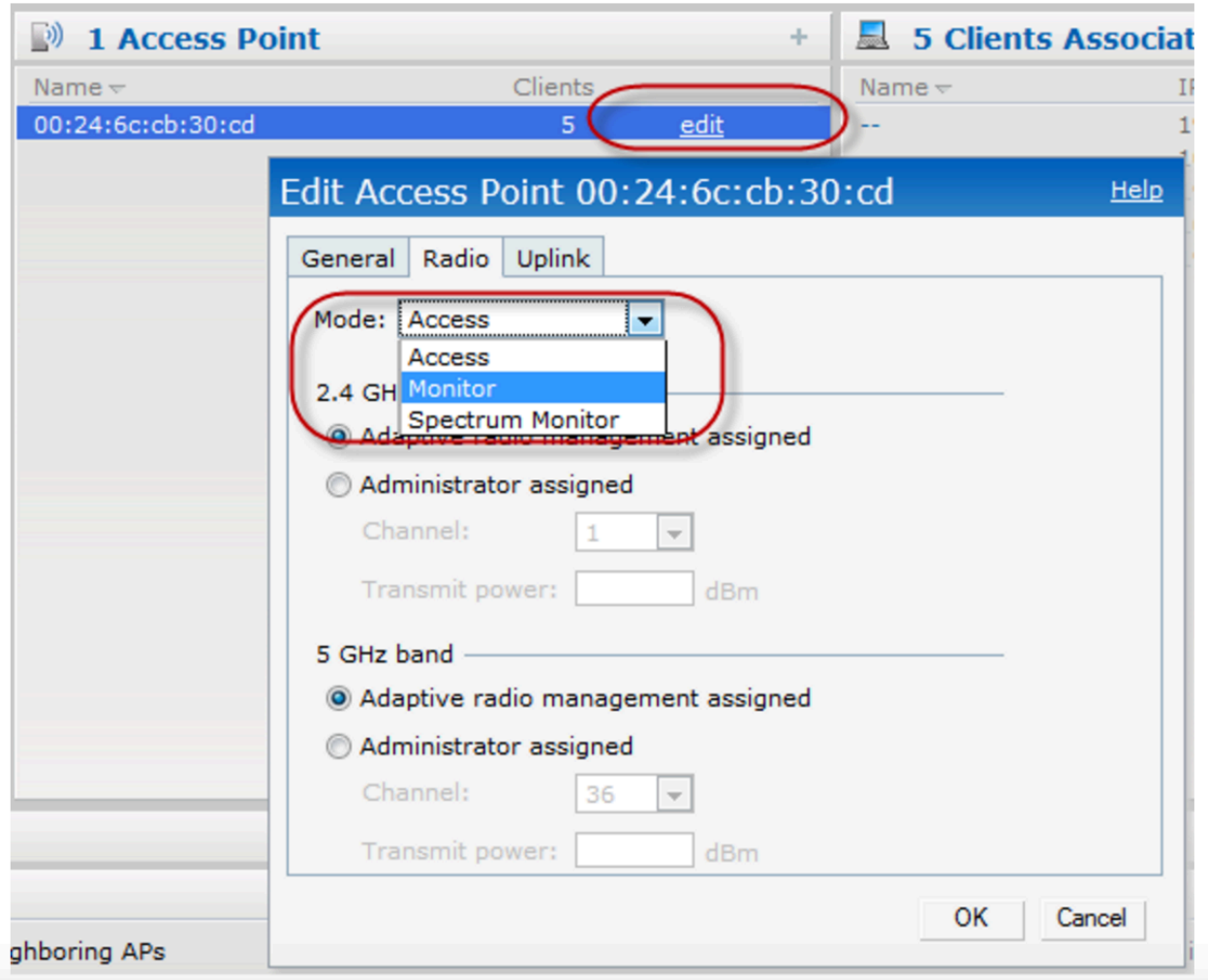
Instant AP Packet Capture.

You will need:

- An instant IAP
- Access to the GUI of the Instant AP
- Access to the commandline of the Instant AP
- A separate management station, capable of installing and running Wireshark. The management station should have the firewall disabled or be able to receive traffic from UDP 5555

Get into the IAP GUI Navigate to the AP > edit > Radio tab > Mode. Change to Monitor and click OK.

Reboot the AP for the change to take effect



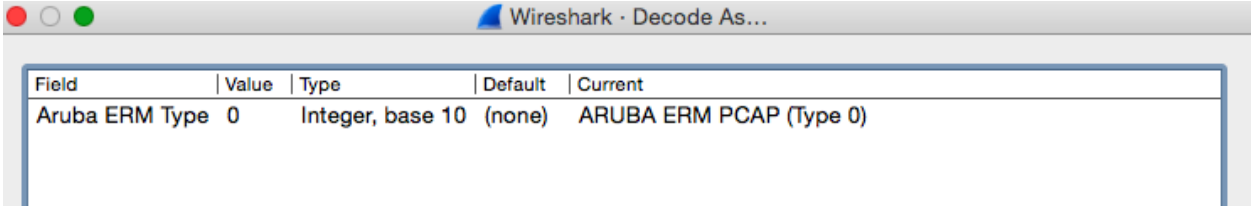
*You need to reboot for the radio change to take effect. So reboot the IAP now.

Download and install the latest version of Wireshark (https://www.wireshark.org/) on a separate management machine. It is best that machine is wired, because the packets must be streamed from the IAP to the management machine running wireshark. Make sure the management machine does not have a firewall that blocks port UDP 5555

*Things to configure in Wireshark:

Go to Analyse > Decode As:

You should see a blank list. Click on Add and select Aruba ERM, Value 0, Integer, base 10 and current is ARUBA ERM PCAP (type 0)



SSH into the IAP when it reboots. *Packet captures on Instant can only be initiated on the commandline.

Type "show pcap" to make sure that no other packet captures are already taking place:

```
IAP-135-Test# show pcap

Packet Capture Sessions at IAP-135-Test, IP 192.168.1.155
-----------------------------------------------------------
pcap-id  filter  type  intf  channel  max-pkt-size  num-pkts  status  url  target  Radio ID
-------  ------  ----  ----  -------  ------------  --------  ------  ---  ------  --------
IAP-135-Test#
```

If a pcap is running type pcap stop <bssid> <pcap-id>

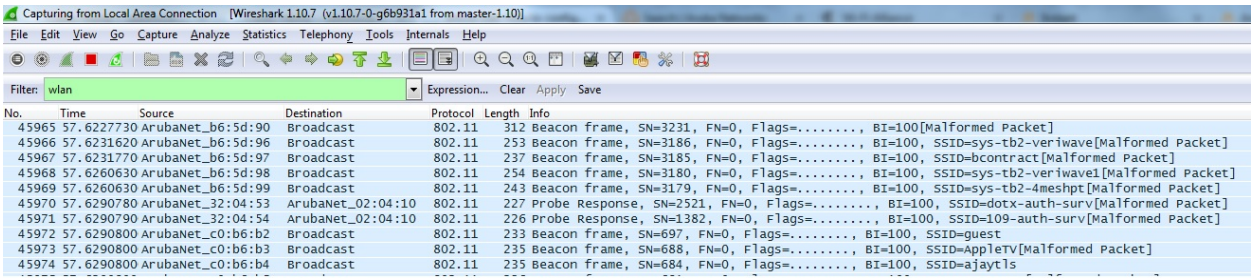
The packet capture command takes a bssid parameter, so even if you turn a radio into an AM you need to find that BSSID to start the packet capture:

Type “show ap monitor status | begin WLAN” to get the BSSID:

```
IAP-135-Test# show ap monitor status | begin WLAN
WLAN Interface
--------------
bssid              scan    monitor  probe-type  phy-type        task   channel  pkts    max-ap-cl-delay  max-sta-cl-delay  reinit-cnt  last-reinit-time
-----              ----    -------  ----------  --------        ----   -------  ----    ---------------  ----------------  ----------  ----------------
d8:c7:c8:40:10:d0  enable  enable   sap         80211a-HT-20    tuned  48       208744  supp             -                 1           8
d8:c7:c8:40:10:c0  enable  enable   am          80211b/g-HT-40  scan   2+       52622   supp             -                 1           8
```

In this case on the 802.11b/g radio the bssid is d8:c7:c8:40:10:co

Before I start my pcap, I need to start Wireshark Capture on my management PC so that I can see the stream. Start capturing on the interface that the management PC is plugged into (Local). Then I would type WLAN and press enter in the filter:



To start my pcap, I need to go back to my IAP commandline and type:

pcap start <bssid> <ip address of management station with wireshark> 5555 0 2048 <channel>

Where bssid = the bssid we got from the radio above

Ip address = ip address of the management station we installed wireshark on

5555 is the port that Wireshark is looking for the Aruba pcap traffic on

0 means we are doing traditional PCAP (1 is for omnipeek)

2048 is the max packet size

Channel is of course, the channel.

Troubleshooting:

To stop the packet capture, first find out if a pcap is running by typing “show pcap”.