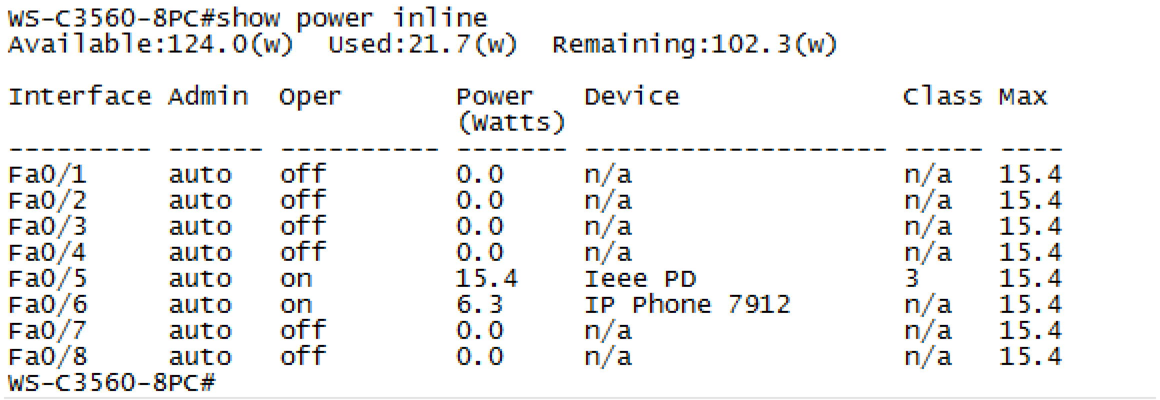
TESTING AN ARUBA IAP

Once again, I was presented the opportunity to test out a device my work borrowed me. This time: an Aruba IAP 105.

It's an Instant Access Point, which comes with a built-in virtual controller. Aruba usually makes Lightweight Access Points (LAPs) which need a central WLC or Wireless LAN Controller to function. Since this one contains the controller function inside the device, I can go experimenting. Yes, it's like a consumer-grade access point now, with a web GUI to configure it, but compared to the average consumer-grade AP, this one comes with more functionality.

First the standards: it supports 802.11a/b/g/n, with n in both 2.4 Ghz and 5 Ghz frequencies. It also supports 802.3af PoE, or an external power supply, and has support for 802.1q trunking. So as far as compatibility goes, this device supports it all.

After applying PoE to it, it boots up. Since it's an IEEE compliant power device, and I have a Cisco ILP powered IP Phone on the same switch, this gives a nice comparison:



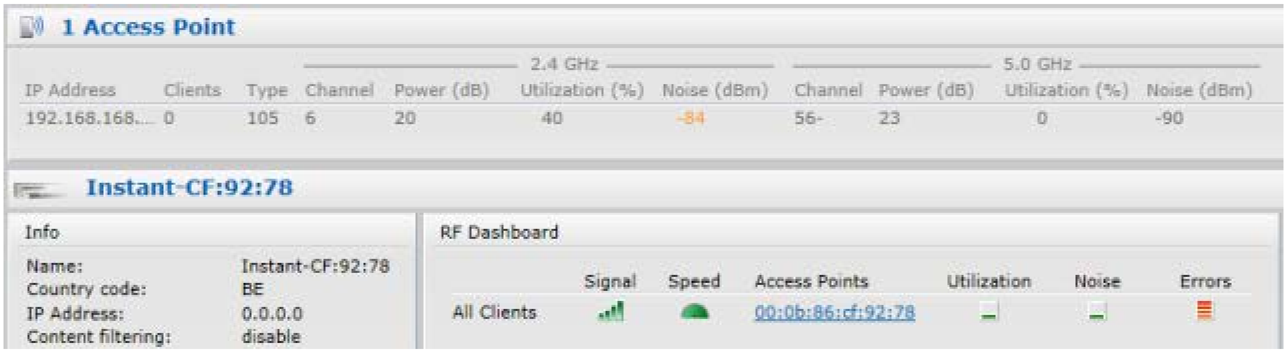
```
WS-C3560-8PC#show power inline
Available:124.0(w)  Used:21.7(w)  Remaining:102.3(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
Fa0/2     auto   off        0.0     n/a                 n/a   15.4
Fa0/3     auto   off        0.0     n/a                 n/a   15.4
Fa0/4     auto   off        0.0     n/a                 n/a   15.4
Fa0/5     auto   on         15.4    Ieee PD             3     15.4
Fa0/6     auto   on         6.3     IP Phone 7912       n/a   15.4
Fa0/7     auto   off        0.0     n/a                 n/a   15.4
Fa0/8     auto   off        0.0     n/a                 n/a   15.4
WS-C3560-8PC#
```

This shows the IAP as a Class 3 power device, and the IP Phone as Cisco proprietary. The IP Phone gets a slight advantage here as it can tell by CDP how much it needs, thus drawing less power budget. I did not detect any CDP or LLDP support for the Aruba IAP by the way.

Back to the IAP: after booting up and receiving an IP through DHCP, it sends out a default network. After connecting to it, I'm automatically redirected to the login page (Windows 7 even shows an event message 'Please open your browser'). After entering the default login and password I'm asked in which country I am, likely to comply with local radio regulations.

The main page in the web GUI show some graphs, indicating signal strength, throughput, and number of users connected. Clicking around, I discover noise levels, transmission errors, even individual reports for each client device, as well as a mobility trail, to check the roaming patterns between multiple access points. As I only have one, there's no useful information there.

The noise levels do indicate a problem:



1 Access Point

			2.4 GHz				5.0 GHz			
IP Address	Clients	Type	Channel	Power (dB)	Utilization (%)	Noise (dBm)	Channel	Power (dB)	Utilization (%)	Noise (dBm)
192.168.168....	0	105	6	20	40	-84	56-	23	0	-90

Instant-CF:92:78

Info

Name:	Instant-CF:92:78
Country code:	BE
IP Address:	0.0.0.0
Content filtering:	disable

RF Dashboard

	Signal	Speed	Access Points	Utilization	Noise	Errors
All Clients	📶	◓	00:0b:86:cf:92:78	▁	▁	🟥

Reason: there are several other access points nearby, one of which is on the same channel 6 as the Aruba. After setting the channel static to 11 (it was automatically searching first), the problem did go away.

Apart from that, there's also an IDS tab that showed more details about other access points in the area: how far away they are, channel, 802.11 mode, connected clients,… Strangely enough, my own AP is the only one marked as 'rogue'. Since it's also the only AP to be in the physically same network as the Aruba, I assume it has some mechanism of finding out unauthorized APs. Maybe it has found the AP's MAC address in the same VLAN?

As far as configuring SSIDs goes, it have plenty of options too: multiple VLANs are supported, each with it's own security features. There's support for WPA, WPA2, WPA2 through RADIUS, MAC filtering, also optionally through RADIUS, 802.1x WEP, and open network. There's also the option to do a redirect to a login webpage, either hosted on the IAP itself or on an external web server. Network access can be done either through NAT on the IAP, direct access to the uplink (access port) or VLAN tagged to a trunk link. The last one is very useful and what it's usually all about: by mapping different SSIDs to different VLANs, and connecting the Aruba IAP with a trunk link, one can give access to different subnets through one AP. The authentication (usually by RADIUS) then checks whether access to a certain VLAN is allowed or not. On top of that, it's possible to set up a per-SSID access list to deny access to certain resources or networks from the IAP.

I did ran into a few unexpected problems. First was that my 802.11n capable laptop could not pick up any 5 Ghz signal, only 802.11n on 2.4 Ghz worked. Second was setting up the trunk link, which didn't work at first until I realized I was acting too quickly and 'spanning-tree portfast' is not the same as 'spanning-tree portfast trunk', making the trunk link go through STP states.

And in case you were wondering: yes, the signal strength of the device is great. I had no stability issues, connecting went fast and reliable.

Source : http://reggle.wordpress.com/2012/01/08/testing-an-aruba-iap/