

RAP Installation - Updated

August 01, 2012

Aruba Controller Release 6.1.3.2

The Controller has several “wizards” that can guide you through a variety of configuration processes. On the “Configuration” tab look for the “AP Wizard” and remember to check “remote” and “administrator-provisioned” setup options depending on your setup needs. Additional information can be obtained from the specific release “User Guide”.

Contents

Firewall NOTES	2
Recreating the Corporate Network SSID for RAP's	3
Create the RAP AP Group.....	4
Add an internal VPN Address Pool for the RAP	5
Add the RAP MAC address to the RAP Whitelist	6
Configuration of the RAP	7
Troubleshooting and Checks.....	8
User Notes – IP Addressing.....	10

Firewall NOTES

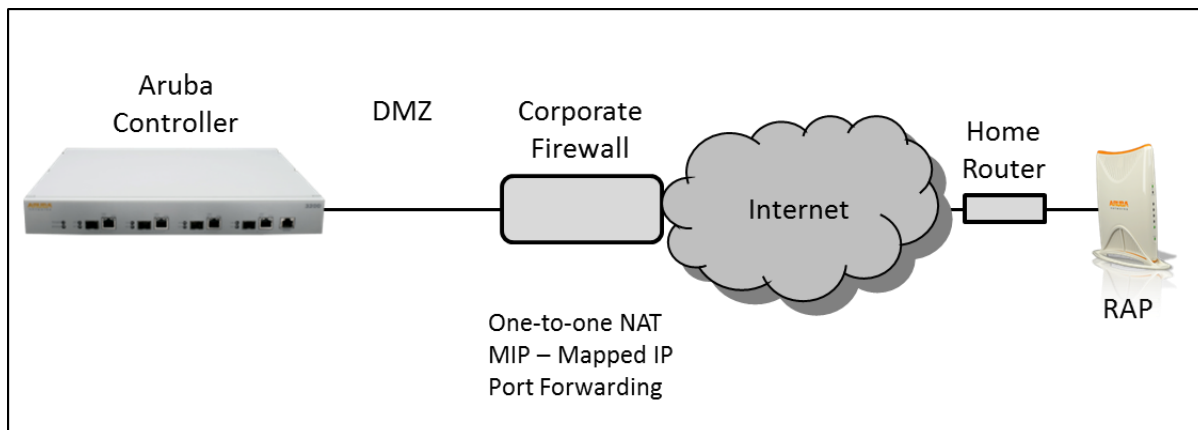
One of the most technical aspects of RAP deployment for most users (depending on their level of expertise) is the configuration of the Internet Firewall. The Aruba RAP communicates to the Aruba controller by building an IPSec tunnel to it using port 4500. You will have to configure your internet firewall /router to allow this port through and direct it to the Aruba controller from the Internet. Depending on your device and IP addresses available this can be accomplished in several ways.

One to One NAT – an external Internet routable IP address is directly translated to a private IP address on the internal DMZ. (Another vendor term used is 'MIP' for 'Mapped IP' but the same as one-to-one NAT)

Port Forwarding – configuring the internet firewall so that anytime it receives a connection request from an Internet IP address using destination port 4500 it will forward this to the IP address of the Aruba controller in the DMZ.

If the Internet Firewall / Router is already configured as a VPN concentrator you could run into difficulties – the Internet Firewall mistaking the incoming RAP IPSec connection for another of your VPN devices or IPSec clients and attempting to terminate the RAP connection to that configuration.

You must enable one of the above methods on your Internet Firewall to allow communications to from the RAP (in the public internet) to the Aruba controller (in your private network). If your organization has available Internet addresses you could program one of these to the Aruba controller ports, placing this port directly on the public internet – **ENSURE** you use caution and consider programming additional policies on the Aruba controller port to maintain security and prevent unauthorized access to the controller from the internet.



IMPORTANT - Please review the entire document before beginning your RAP deployment

Creating a new RAP Virtual AP Profile

In this example the Aruba controller has an existing 802.1x authenticated SSID broadcasting from AP's at the corporate location ("myemployee"). The existing SSID will be used as the basis to replicate the SSID on the Users RAP at home. (See Airheads Social "For the Beginner – Configuring an 802.1x WLAN with the Controller GUI")

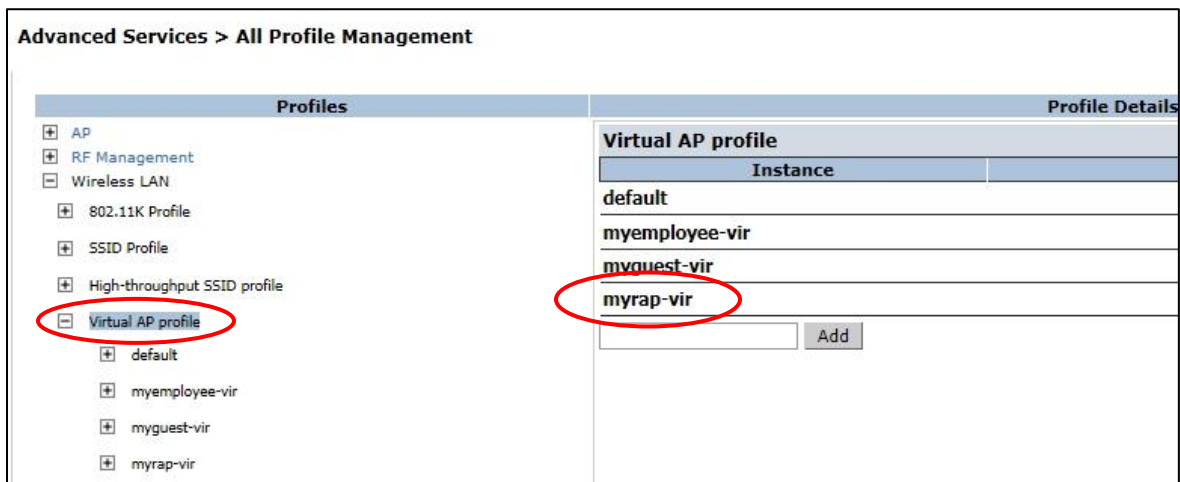
Creating a new RAP Virtual AP profile allows for future changes to the RAP (and Users connecting to it) without changing the existing Campus AP's Virtual AP profile such as; VLAN's, Remote-AP operation and Forward mode. The new RAP profile will broadcast the corporate WLAN SSID and allow a User to take their laptop home and connect to the RAP with the same Wireless Profile used at corporate. Review "User Notes – IP Addressing" at the end of this document.

In this example the RAP is configured and connected to the Master Controller through the Internet Firewall.

Go to "Configuration" > "Advanced Services" > "All Profiles"

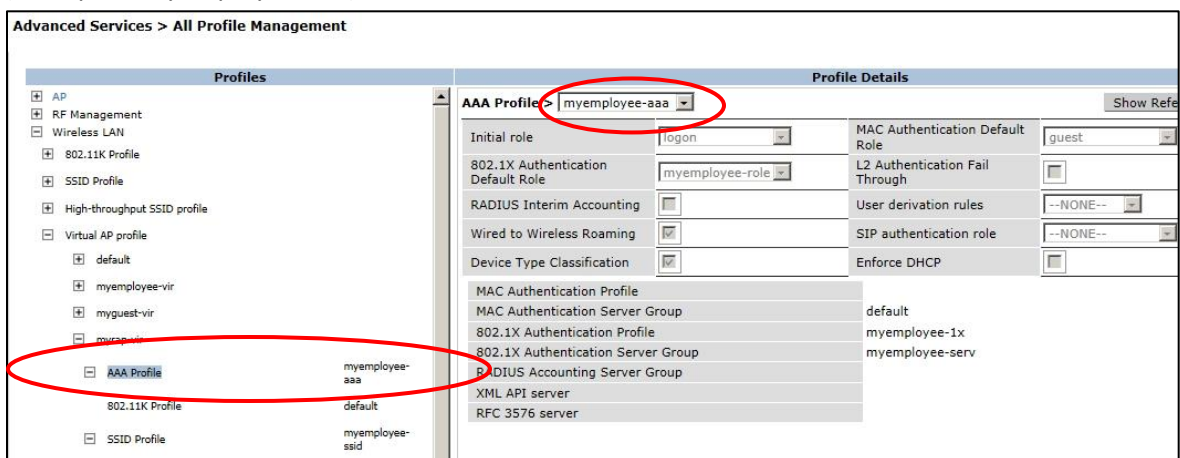
Expand the "Wireless LAN" profile and select "Virtual AP profile"

Create a new Virtual AP profile for the RAP's (myrap-vir in this example)

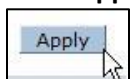


("User Notes" regarding setup of new Virtual AP profile VLAN and User IP address assignment at end of this document)

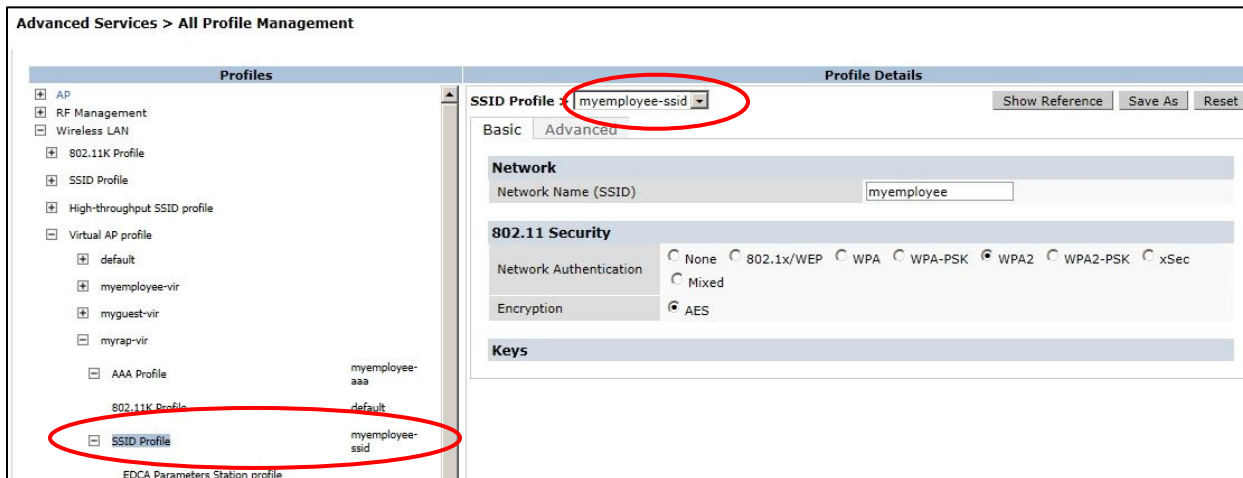
Now click on and open the new RAP virtual AP profile and assign the existing 802.1x authentication **AAA Profile** (example = myemployee-aaa) to it.



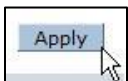
Click "Apply" at the bottom lower right of this page and "Save Configuration" when done.



Within the RAP virtual AP profile click on and assign the existing 802.1x authentication **SSID Profile** (example = myemployee-ssid) to it.



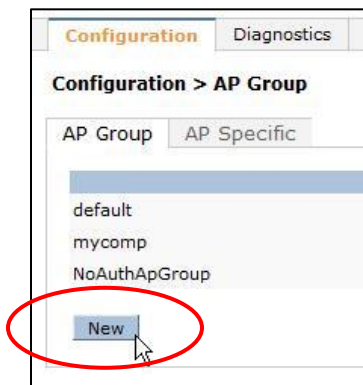
Click **“Apply”** at the bottom lower right of this page and **“Save Configuration”** when done.



Create the RAP AP Group

Setup a new AP Group for the RAP's

“Configuration” > “Wireless” > “AP Configuration” > New



Add the new AP Group Name (in this example “myRAP”)

Click “Add” to finish and “Save Configuration”



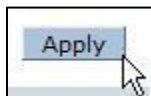
Now select the new “myRAP” AP Group, expand the “Wireless LAN” Profile > “Virtual AP” and use the pull down to add the “myrap-vir” (virtual AP profile) previously created with associated AAA and SSID profiles.

Configuration > AP Group > Edit "myRAP"

Profiles		Profile Details				
<input checked="" type="checkbox"/> Wireless LAN	<input checked="" type="checkbox"/> Virtual AP					
<input checked="" type="checkbox"/> myrap-vir						
<input checked="" type="checkbox"/> RF Management						
<input checked="" type="checkbox"/> AP						
<input checked="" type="checkbox"/> QoS						
<input checked="" type="checkbox"/> IDS						
<input checked="" type="checkbox"/> Mesh						

Virtual APs					
Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP enable
myrap-vir	myemployee-aaa	myemployee-ssid		tunnel	Enabled
Add a profile			default	Add	

Click “**Apply**” at the bottom lower right of this page and “Save Configuration” when done.



Add an internal VPN Address Pool for the RAP

From the “**Configuration**” > “**Advanced Services**” and enter the “**VPN Services**” menu



Go to the “Address Pools” section and select “**Add**”

Address Pools

Pool Name	Start Address
Add	

Enter a pool name and a start and end IP address that will be assigned to the RAP when connecting to and communicating with the Controller (this is for internal Controller <> RAP communications)

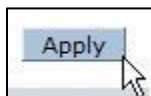
This address is used only for internal communications between the RAP and the Controller.
When the entries are completed select “**Done**”

Configuration Diagnostics Maintenance Plan Save Configuration

Advanced Services > VPN Services > IPSEC > Add Address Pool

Pool Name	RAP
Start Address	1.1.1.1
End Address	1.1.1.250

When back to the Main page (VPN Services) at the bottom lower right of this page click **“Apply”**



Add the RAP MAC address to the RAP Whitelist

Go to “Configuration” > “Wireless” > “AP Installation”



Select the “RAP Whitelist” tab



Enter the MAC address of the **RAP** and additional data related to the user and assign to the “RAP” AP Group

Wireless > AP Installation > RAP Whitelist

Provisioning Provisioning Profile RAP Whitelist Campus AP Whitelist

Search

	AP MAC Address	User Name	AP Group	AP Name	Description
<input type="checkbox"/>	00:0b:86:67:49:0c	Joe Smith	default	jsmithrap	

Add Cancel

Click **“Add”** when completed

“Save Configuration”

Configuration of the RAP

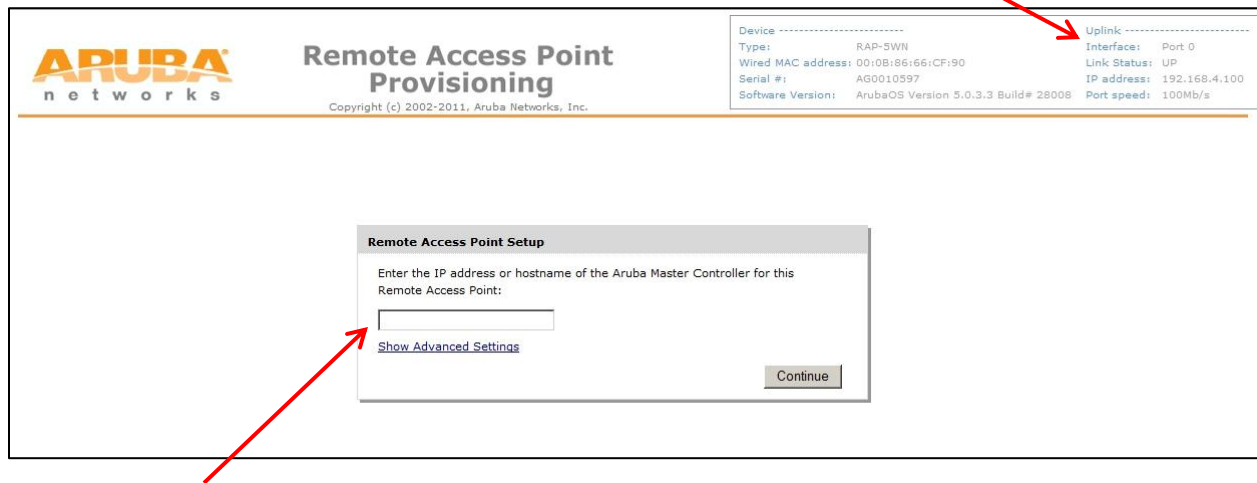
The remainder of this text is taken from the Release 6.0 User Guide page 849.

Connect the RAP Ethernet port 0 to the modem connecting to the internet - Ensure the internet modem can provide DHCP

Connect your PC to the RAP Ethernet port 1 - Ensure your PC Ethernet port is set for DHCP

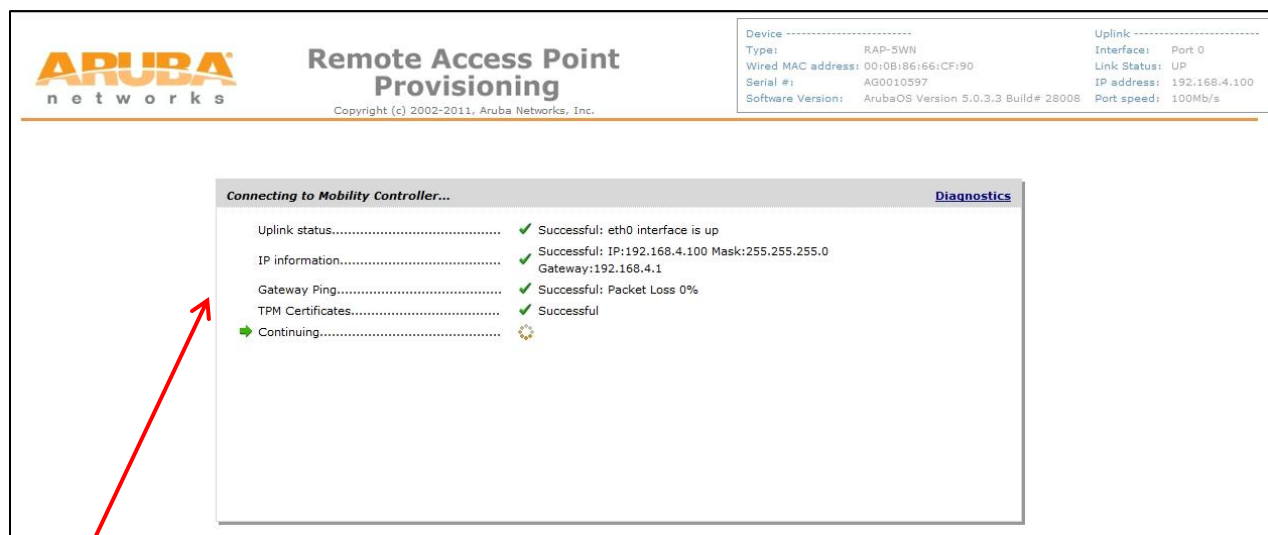
Open a web browser and connect to
<http://rapconsole.arubanetworks.com/>

Note the connection to the 'home router' – Ethernet port 0 – is UP, the RAP has an IP address (from the home router DHCP) and the RAP is running release 5.x (for connection to a release 6.x controller and upgrading)



Enter the IP address (public IP address) of the Controller reachable over the internet
Click **"Continue"**

Have the user watch the screen for information as the RAP connects to the Controller.



NOTE - "Testing connectivity to gateway"

If this step fails you do not have basic IP connectivity to the Controller!

Check your route table, start basic IP troubleshooting; ping, traceroute, etc.

Troubleshooting and Checks

(Aruba3200) #show datapath session table | include 4500 (review IPsec traffic information)

```
<Aruba3200> #show datapath session table | include 4500
192.168.4.100 192.168.10.3 17 4500 4500 0/0 0 0 0 1/3 cd FC
192.168.10.3 192.168.4.100 17 4500 4500 0/0 0 0 0 1/3 cd F
```

If no IPsec (4500) is getting to the controller no IPsec tunnel will be built, the RAP will not connect
In this example (local demo) the RAP is IP address 192.168.4.100 connecting to controller interface IP address 192.168.10.3

(Aruba3200) #show crypto isakmp sa

```
<Aruba3200> #show crypto isakmp sa
ISAKMP SA Active Session Information
-----
Initiator IP      Responder IP      Flags      Start Time      Private IP
-----
192.168.4.100    172.16.0.3        r-v2-c-R   Jul 26 17:32:01  1.1.1.3

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Aggressive Mode v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e = ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = RAP
       U = UIA; S = UIA over TCP

Total ISAKMP SAs: 1
```

In this example (local demo) the RAP isakmp is IP address 192.168.4.100 connecting to controller IP address 172.16.0.3

(Aruba3200) #show crypto ipsec sa

```
<Aruba3200> #show crypto ipsec sa
IPSEC SA <U2> Active Session Information
-----
Initiator IP      Responder IP      SPI(IN/OUT)      Flags Start Time      Inner IP
-----
192.168.4.100    172.16.0.3        b22fef00/8ae57d00 UT2   Jul 26 17:32:02  1.1.1.3

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2

Total IPSEC SAs: 1
```

(Aruba3200) #show ap association ap-group <ap group name>

```
show ap association ap-group myrap
Flags: W: WMM client, A: Active, K: 802.11K client, B: Band Steerable
PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz
<n>ss: <n> spatial streams

Association Table
-----
Name      bssid      mac      auth  assoc  aid  l-in  essid      vlan-id  tunnel-id  phy      assoc. time  num assoc  Flags
-----
jsmithrap 00:1a:1e:43:30:40 f8:7b:7a:68:f5:da y      y      1    3      myemployee 1        0x1089     g-HI-20-1ss 1m:4s      1        WA
Num Clients: 1
```


(Aruba3200) #show user

(Aruba3200) #show user ip x.x.x.x (ip address of rap user)

```
<Aruba3200> #show user-table
Users
-----
IP          MAC          Name      Role      Age<d:h:m>  Auth  UPN link  AP name  Roaming  Essid/Bssid/Phy  Profile
-----
192.168.40.254 f8:7b:7a:68:f5:da mrube     myemployee-role 00:00:01  802.1x  jsmithrap Wireless  myemployee/00:1a:1e:43:30:40/g-HI myemployee
-aaa tunnel

User Entries: 1/1
<Aruba3200> #show user-table ip 192.168.40.254

Name: mrube, IP: 192.168.40.254, MAC: f8:7b:7a:68:f5:da, Role:myemployee-role, ACL:50/0, Age: 00:00:01
Authentication: Yes, status: successful, method: 802.1x, protocol: EAP-PEAP, server: Internal
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: default for authentication type 802.1x
VLAN Derivation: unknown
Idle timeouts: 0, ICMP requests sent: 0, replies received: 0, Valid ARP: 0
Mobility state: Wireless, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 L3 Mob: 0
Flags: internal=0, trusted_ap=0, delete=0, l3auth=0, l2=1 mba=0
Flags: innerip=0, outerip=0, guest=0, station=0, download=1, nodatapath=0, wispr=0
Auth fails: 0, phy_type: g-HI, reauth: 0, BW Contract: up:0 down:0, user-how: 1
Vlan default: 1, Assigned: 10, Current: 10 vlan-how: 0
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, Proxyarp=0, Flags=0x0
Tunnel=0, SlotPort=0x1043, Port=0x1089 (tunnel 9)
Role assigned: n/a, UPN: n/a, Dot1x: Name: myemployee-role role-how: 1
Essid: myemployee, Bssid: 00:1a:1e:43:30:40 AP name/group: jsmithrap/myrap Phy-type: g-HI
Radacct sessionID:n/a
Radacct Traffic In 24/1864 Out 0/0 (0:24/0:0:0:1864,0:0/0:0:0:0)
Timers: arp-reply 0, spoof-reply 0, reauth 0
Profiles AAA:myemployee-aaa, dot1x:myemployee-1x, mac: CP: def-role:'logon' sip-role:'' via-auth-profile:''
ncfg flags udr 0, mac 0, dot1x 0
Born: 1343336064 (Thu Jul 26 15:54:24 2012)

<Aruba3200> #
```

If everything else appears correct but the rap group has an authorization profile it may not connect (Thanks to CJoseph)

“Make sure that there is no AP authorization Profile accidentally attached to that ap-group:”

```
<Aruba3200> #
<Aruba3200> #show ap ap-group ap-name myRAP
AP with name "myRAP" not found.

<Aruba3200> #show ap ap-group ap-name jsmithrap
AP group "myRAP"

Parameter                                     Value
-----
Virtual AP                                   myrap-vir
802.11a radio profile                       default
802.11g radio profile                       default
Ethernet interface 0 port configuration     default
Ethernet interface 1 port configuration     default
Ethernet interface 2 port configuration     shutdown
Ethernet interface 3 port configuration     shutdown
Ethernet interface 4 port configuration     shutdown
AP system profile                           myrap-ap-sys
VoIP Call Admission Control profile         default
802.11a Traffic Management profile          N/A
802.11g Traffic Management profile          N/A
Regulatory Domain profile                  default
RF Optimization profile                    default
RF Event Thresholds profile                default
IDS profile                                default
Mesh Radio profile                         default
Mesh Cluster profile                       N/A
Provisioning profile                       N/A
AP authorization profile                   N/A

<Aruba3200> #
```

Once the RAP is up and running

(Aruba3200) #show ap image version ap-name <name>

```
<Aruba3200> #show ap image version ap-name jsmithrap
AP Image Versions On Controller
6.1.3.2(p4build@corsica)#33796 Fri May 25 13:25:45 PDT 2012
6.1.3.2(p4build@corsica)#33796 Fri May 25 13:09:12 PDT 2012

Access Points Image Version
AP      Running Image Version String      Flash (Production) Image Version String      Flash (Provisioning/Backup) Image Version Stri
ng      Matches  Num Matches  Num Mismatches  Bad Checksums  Bad Provisioning Checksums  Image Load Status
-----
1.1.1.3 6.1.3.2(p4build@corsica)#33796 Fri May 25 13:09:12 PDT 2012 6.1.3.2(p4build@corsica)#33796 Fri May 25 13:09:12 PDT 2012 5.0.4.3(p4build@corsica)#31056 Wed Nov 9 14:41
:32 PST 2011 Yes 2 0 0 0 Done

<Aruba3200> #
```

Shows RAP version image production and backup

User Notes – IP Addressing

The information above provides the basic steps necessary for the connection of a RAP on the Aruba controller but do not address the network details when a User connects to the RAP SSID - in particular IP address assignment to the User when connecting to the Corporate SSID or RAP SSID.

The methodology for creation of a new RAP Virtual AP profile is to allow for a different IP address assignment to the User when connected at the RAP SSID vs. the User connecting at the corporate location SSID. This is keeping within typical IT organizations best practices.

In this example VLAN 500 has been created and assigned to the controller's port 1/3. VLAN 500 has been assigned as the VLAN for the new RAP Virtual AP profile. When a User connects to the RAP SSID (and associated Virtual AP profile) and is authenticated the User will receive an IP address from the DHCP server serving VLAN 500 (the 192.168.10.x subnet).

Network > VLAN ID

VLAN ID | VLAN Pool | Spanning-tree

VLAN ID	IPv4 Address	IPv4 Net Mask	IPv6 Address	Associated Ports
1	172.16.0.3	255.255.255.0	fe80::b:8600:161:d	GE1/0-2, Pc0-7
10	192.168.40.3	255.255.255.0	fe80::b:8600:a61:d	
100	192.168.100.3	255.255.255.0		
500	192.168.10.3	255.255.255.0	fe80::b:8601:f461:	GE1/3

Add a VLAN | Add/Edit Bulk VLANs | Delete Bulk VLANs

Virtual AP profile > myrap-vir Show Reference Save As Reset

Virtual AP enable	<input checked="" type="checkbox"/>	Allowed band	all
VLAN	500	Forward mode	tunnel
Deny time range	--NONE--	Mobile IP	<input checked="" type="checkbox"/>
HA Discovery on-association	<input type="checkbox"/>	DoS Prevention	<input type="checkbox"/>
Station Blacklisting	<input checked="" type="checkbox"/>	Blacklist Time	3600 sec
Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>	Dynamic Multicast Optimization (DMO) Threshold	6
Authentication Failure Blacklist Time	3600 sec	Strict Compliance	<input type="checkbox"/>
VLAN Mobility	<input type="checkbox"/>	Preserve Client VLAN	<input type="checkbox"/>
Remote-AP Operation	standard	Drop Broadcast and Multicast	<input type="checkbox"/>
Convert Broadcast ARP requests to unicast	<input checked="" type="checkbox"/>	Disable conversion multicast RA packets to unicast	<input type="checkbox"/>
Deny inter user traffic	<input type="checkbox"/>	Band Steering	<input type="checkbox"/>
Steering Mode	prefer-5ghz		