

1 Table of Contents

Table of Contents

1	Table of Contents.....	1
	Revision History	1
2	WiFi Uplink.....	2
	Things you need	2
3	Existing Instant Cluster	3
	3.1 Instant Cluster Configuration	3
4	Instant AP (WiFi 5) with WiFi Uplink	4
	4.1 Disable Extended SSID	4
	4.2 WiFi Uplink Configuration	4
	4.3 Basic Testing	6
	4.4 Checking the Uplink.....	9
	4.5 Checking the WebUI	11
5	External DHCP server for Clients.....	12
	5.1 Configure Wireless network for Clients	12
	5.2 Configure Wired network for Clients.....	12
	5.3 Client Testing	13
6	Instant AP as DHCP server for Clients.....	16
	6.1 Configure Wireless network for Clients	16
	6.2 Configure Wired network for Clients.....	16
	6.3 Client Testing	16
7	WiFi Uplink with Dot1x Auth	19
	7.1 Dot1x Authenticated WiFi Uplink	19
8	Instant AP (WiFi 6) with WiFi Uplink	23
	8.1 PSK based Testing	23
	8.2 Dot1x Testing	26

Revision History

DATE	VERSION	EDITOR	CHANGES
06 Dec 2021	0.1	Ariya Parsamanesh	Initial creation
22 Dec 2021	0.2	Ariya Parsamanesh	Added the WiFi6 section

2 WiFi Uplink

In some cases where you cannot use Mesh networking, WiFi uplink could come handy. Wi-Fi uplink is supported on all WiFi6 APs as well as the following 11n/11ac.

- AP-203H, AP-203R, AP-203RP, AP-207,
- AP-300 Series, AP-303H, 310 Series, 320 Series, and 330 Series access points.

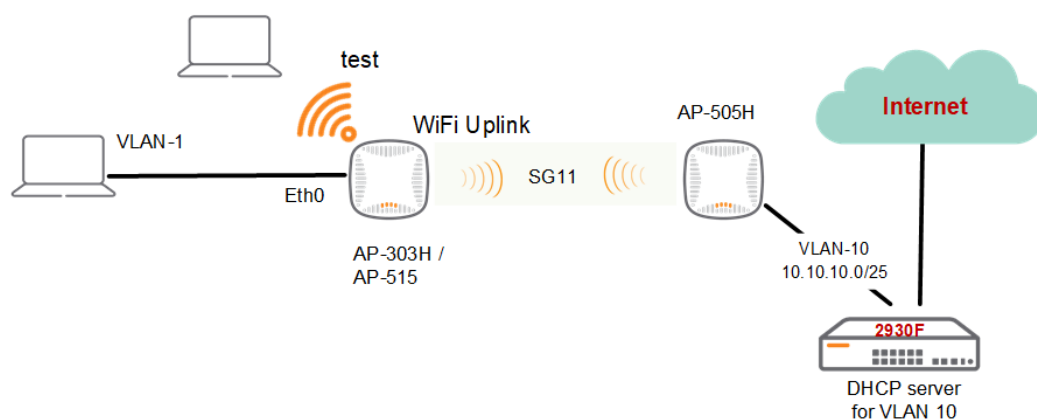
The aim of this feature is to use WiFi in addition to 3G/4G and Ethernet as a valid primary uplink. The Wi-Fi uplink allows you to connect to SSIDs with the following authentication modes

- Open
- WPA Personal
- WPA2 Personal
- WPA Enterprise (TKIP Encryption only)
- WPA2 Enterprise

Here is the lab set-up to demonstrate this feature and you should note that if your IAP has dual radios, both radios can be used to serve clients but only one of them can be used for the Wi-Fi uplink.

We are showing the following scenarios

1. AP-303H with WiFi uplink (WPA2-PSK) to connect to an existing Instant cluster (AP-505H)
 - a. add a wireless and wired client to AP-303H and test the uplink using external DHCP server
 - b. add a wireless and wired client to AP-303H and test the uplink using Instant AP's internal DHCP server
2. AP-303H with WiFi uplink (dot1x) to connect to an existing Instant cluster (AP-505H)
3. AP-515 (11ax AP) with WiFi uplink (WPA2-PSK) to an existing Instant cluster (AP-505H)
4. AP-515 (11ax AP) with WiFi uplink (dot1x) to an existing Instant cluster (AP-505H)



Things you need

- Aruba Instant version 8.8.0.0 or later
- WiFi uplink device/provider or an existing Instant Cluster
- A Layer three switch and some WiFi clients

3 Existing Instant Cluster

Here we have an existing Instant Cluster which consists of one AP-505H. This cluster is providing the WiFi network SG11 which AP-303H will use as an uplink. As stated before, this cluster is running Instant 8.9 version. Also note that you cannot combine Mesh and WiFi uplink. You can have one or the other.

3.1 Instant Cluster Configuration

Here we have just added a WLAN network called SG11 that is broadcasting on both radios 5.0GHz and 2.4GHz.

edit SG11 1 Basic 2 VLAN 3 Security 4 Access

Name & Usage

Name: SG11

Type: Wireless

Primary usage: Employee

Broadcast/Multicast

Broadcast filtering: ARP

Multicast transmission optimization: ☐

Dynamic multicast optimization: ☐

DMO channel utilization threshold: 90 %

Transmit Rates

802.11

Band: All

Allowed 5GHz radio: All

RF band 6GHz: ☐

Disable on 6GHz mesh: ☐

DTIM interval: 1 beacon

Min RSSI for probe request: 0

Min RSSI for auth request: 0

High throughput: ☒

Very high throughput: ☒

High efficiency: ☒

Client IP & VLAN Assignment

Client IP assignment: ☐ Virtual Controller managed ☒ Network assigned

Client VLAN assignment: ☒ Default ☐ Static ☐ Dynamic

Security Level

Security Level: Personal

Key management: WPA2-Personal

Passphrase format: 8-63 chars

Passphrase:

Retype:

MAC authentication: ☐

Denylisting: ☐

Enforce DHCP: ☐

Fast Roaming

802.11r: ☐

802.11k: ☐

802.11v: ☐

Access Rules

Access Rules: Unrestricted

Download roles: ☐

No restrictions on access based on destination or type of traffic

The above is a standard WLAN configuration.

4 Instant AP (WiFi 5) with WiFi Uplink

Here are the main points to note

- If you are using Instant version 8.7.x then 11ac IAPs do not need to be in standalone mode.
- For 11ac IAP to use WiFi uplink to an existing IAP cluster, the Instant version on the cluster needs to be 8.5.0 or later and for 11ax APs it should be 8.7.x
- When you configure the WiFi uplink, you need to reboot the IAPs for the changes to take effect.
- Instant Mesh and WiFi uplink are mutually exclusive.
- WiFi uplink can be either the main uplink or as a backup to Ethernet and 3G/4G uplinks.
- For deployments where only wired clients will connect to this AP through a bridged Eth port, a non-default SSID configured is mandatory or else the WiFi uplink solution won't work. If you don't want to use the SSID, you can disable it, but it must be configured.

Here we have AP-303H that uses WiFi uplink as its primary uplink. Also note that we are using Instant version 8.8.0.2. This AP will be connecting to the SG11 SSID that we configured in the previous section.

4.1 Disable Extended SSID

The screenshot shows the Aruba InstantVC configuration interface. On the left is a navigation menu with options like Dashboard, Overview, Networks, Access Points, Clients, Configuration, System, RF, Security, IDS, Routing, Tunneling, Services, and DHCP Server. The main area is divided into two columns. The left column contains the 'General' tab with fields for Name (InstantVC), System location, Virtual Controller IP (0.0.0.0), Allow IPv6 Management (disabled), Virtual Controller IPv6 (::), Uplink switch native VLAN (1), Dynamic RADIUS Proxy (enabled), Dynamic TACACS Proxy (disabled), MAS integration (disabled), NTP server (216.239.35.4), Timezone (Melbourne UTC+10), Daylight Saving Time (enabled), Preferred band (5 GHz), AppRF visibility (All), and URL visibility (enabled). The right column contains various toggle switches for Cluster security, Virtual Controller network settings (Default), Auto join mode, Terminal access, Console access, Telnet server, LED display, Extended SSID (disabled, with an orange arrow pointing to it), Deny inter user bridging, Deny local routing, Dynamic CPU management (Automatic), and DHCP Option 82 XML. Below these are expandable sections for Admin, Uplink, L3 Mobility, Monitoring, WiSPR, Proxy, and Time Based Services.

4.2 WiFi Uplink Configuration

The ESSID for my WiFi uplink is SG11 which is being advertised on 5.0GHz band but you can use 2.4GHz as well. Its mode of authentication is pre-shared key.

The screenshot shows the Aruba Virtual Controller (VC) interface for LAB2. The left sidebar contains a navigation menu with categories: Dashboard, Configuration, System, RF, Security, IDS, Routing, and Tunneling. Under Configuration, the 'Uplink' section is expanded, showing sub-sections: Management, 3G/4G, and Wifi. The 'Wifi' section is selected, displaying the following configuration fields:

- Name (SSID): SG11
- Key management: WPA2-Personal
- Band: 5 GHz
- Passphrase format: 8-63 chars
- Passphrase: NOT CHANGED

Below the Wifi section, there are expandable sections for PPPoE, AP1X, L3 Mobility, Monitoring, and WISPr.

Once you have configured this you need to reboot the IAP. But before rebooting it, you need to do couple of more configuration.

Note that currently WiFi uplink can be a primary or a backup uplink.

Next you need to re-order the uplinks for WiFi to be the first as shown below

The screenshot shows the Aruba Virtual Controller (VC) interface for InstantVC. The left sidebar is similar to the previous one, but the 'Uplink' section is expanded. The 'Management' sub-section is selected, displaying the following configuration fields:

- Enforce uplink: None
- Pre-emption: ☒
- Pre-emption interval: 300
- VPN failover timeout: 180
- Internet failover: ☐
- Internet failover IP: 8.8.8.8
- Cellular failover IP: (empty field)

Below these fields is the 'Uplink Priority List' table:

Uplink Priority List	
Wifi-sta	
eth0	
3G/4G	
↑ ↓	

Below the table, the '3G/4G' section is partially visible.

And finally change the uplink setting of the AP's E0 interface to be downlink in order so that you can connect a wired client directly to it.

aruba | VIRTUAL CONTROLLER | LAB2

Dashboard

- Overview
- Networks
- Access Points
- Clients
- Mesh Devices

Configuration

- Networks
- Access Points

Access Points (1)

Name	IP Address	Mode	Spectrum
AP303H-Lab2 ★	10.10.10.23	access	disable

+ [edit icon] [delete icon]

aruba | VIRTUAL CONTROLLER | LAB2

Dashboard

- Overview
- Networks
- Access Points
- Clients
- Mesh Devices

Configuration

- Networks
- Access Points
- System

Edit Access Point AP303H-Lab2

- General
- Radio
- Installation Type
- Uplink
 - Uplink management VLAN: 1
 - Eth0 mode: Downlink
 - Eth1 mode: Downlink
 - USB port: ☒
 - PEAP User
 - Upload Certificate

Now you can reboot the AP.

4.3 Basic Testing

Here is the console log of the AP-303H when it got rebooted, I have deleted the unrelated lines

```
Booting OS partition 1
Checking image @ 0x2000000
Copying image from 0x84000000

Image is signed; verifying checksum... passed
SHA2 Signature available
Signer Cert OK
Policy Cert OK
RSA signature verified using SHA2.
Uncompressing Kernel Image ... OK
[ 0.000000]
[ 0.000000] Aruba Networks
[ 0.000000] ArubaOS Version 8.8.0.2-8.8.0.2 (build 81788 / label #81788)
[ 0.000000] Built by p4build@pr-hpn-build10 on 2021-10-07 at 18:46:06 UTC (gcc version 4.6.3)
[ 0.000000]
[ 0.000000] CPU: ARMv7 Processor [410fc075] revision 5 (ARMv7), cr=10c5387d
[ 0.015792] SMP: Total of 4 processors activated (384.00 BogoMIPS).
[ 0.051083] i2c-gpio driver registered
[ 17.796389] 3 ofpart partitions found on MTD device spi0.1
[ 17.849585] Creating 3 MTD partitions on "spi0.1":
[ 17.906864] 0x000000000000-0x000002000000 : "aos0"
[ 17.965776] 0x000002000000-0x000004000000 : "aos1"
```

```

[ 18.022928] 0x0000040000000-0x000008000000 : "ubifs"
[ 18.086989] m25p80 spi0.0: found mx25l3205d, expected n25q128a11
[ 18.193592] Found AT97SC3203 on i2c_1.8
[ 18.237662] Key type dns_resolver registered
[ 18.278093] Registering SWP/SWPB emulation handler
[ 25.738006] There is no gpio reset info
[ 25.806311]
Starting Kernel SHA1 KAT ...
[ 25.840792] Completed Kernel SHA1 KAT
[ 25.887807] Starting Kernel HMAC-SHA1 KAT ...
[ 25.937815] Starting Kernel DES KAT ...[ 25.983529] Completed Kernel DES KAT
[ 26.027255] Starting Kernel AES KAT ...
[ 26.071029] Completed Kernel AES KAT
[ 26.071029]
[ 26.134624] Starting Kernel AESGCM KAT ...
[ 26.181368] Completed Kernel AESGCM KAT
[ 26.230649] Completed Kernel HMAC-SHA1 KAT
grep: /tmp/ap-info: No such file or directory
Thu Jan 1 00:00:00 PST 1970
Populate AP type info
Domain Name: SetMeUp.arubanetworks.com
Current OEM Name : Aruba Networks
Disabling ipv6 for devices by default
AP-type has_ble_support: ONBOARD.
IPv6 capability is supported for devices
No panic info available
Enabling UDMD via nanny
Writing /dev/ttyMSM1 into /tmp/ble_port
Enabling ble_daemon and ble_relay via nanny
glenmorangie: Start hotplug
Backup ENV.
Installing glenmorangie ethernet driver
[ 42.385996] edma module_init
[ 43.227619] asap_switch: module license 'Proprietary' taints kernel.
[ 43.291228] Disabling lock debugging due to kernel taint
Enter non-FIPS mode
Cfg len is 3575
enet0 bridging detected
Mesh disabled
dual uplink platform just by config
Ethernet port 1 mode: active-standby
Eth1 works as downlink when enet1_mode is downlink
Eth0 has been enslaved into bond0 working as downlink with Eth1
Starting watchdog process...
Aruba watchdog daemon started [4 thread(s)]
training packets starting...
training packets on interface:
eth0 eth1
Index for interface eth0 is 3
MAC address for interface eth0 is 20:4c:03:5c:05:6e
Index for interface eth1 is 5
MAC address for interface eth1 is 20:4c:03:5c:05:6f
send training from interface eth0
send training from interface eth1
No reply within 1 seconds.
send training from interface eth0
send training from interface eth1
No reply within 1 seconds.
send training from interface eth0
send training from interface eth1
No reply within 1 seconds.
Recognized no echo replies from remote host after 3 tries.
Loading configuration file of length 3575...
wifi uplink detected...
Terminal access enabled...
Valid SSID detected...
touching file /tmp/ip_mode_0
do ethtool autoneg on for eth0
do ethtool autoneg on for eth2
cp: /lib/nls_base.ko: No such file or directory
cp: /lib/usbcore.ko: No such file or directory
init usb modem ...
[ 54.833367] SCSI subsystem initialized
No USB Plugged in

```

```

Skip wired uplink detection
wifi uplink is configured on 5G, and mesh will NOT be in use.
copying bootuplog ...
[ 83.327941] uol_init_driver:425 HW offload not applicable, AP will use cutting through path!
allow PAPI
set device anul0 mtu to 2000
notify asap_mod 3g no present...
Starting update SBL1 ...
SBL1 was updated already
Done.
net.aruba_asap.uplink_vlan = 1
apdot1x authentication is not enabled
skip dhcp when loop or wifi-uplink without eth detected !!!!!!!!!!!!!!!
waiting for default ip ready ...
[ 173.668800] Picked up default IP a9fe48bf, rand 48bf
[ 179.680790] Default IP is ready
Installing default ip.
Default IP comes up.
169.254.72.191 255.255.0.0
Compressing all files in the /etc/httpd directory...
[ 180.682843] ip_time_handler: Got ip and packets on bond0 Started conductor election 1-0, rand 26
Done.
Starting Webserver
bind: Transport endpoint is not connected
bind: Transport endpoint is not connected
bind: Transport endpoint is not connected
Put ntupdate to the nannylist.
AP rebooted Sun Oct 24 09:32:34 EST 2021; CLI cmd at uptime 0D 0H 17M 34S: reload
shutting down watchdog process (nanny will restart it)...
<<<<< Welcome to the Access Point >>>>>
Completed SW FIPS KAT test
Power supply mode is DC, USB Modem is not present.
User: [ 194.902841] Starting Kernel HMAC SHA1 FIPS KAT ...
[ 194.945640] Completed Kernel HMAC SHA1 FIPS KAT
[ 196.906806] Starting Kernel HMAC SHA256 FIPS KAT ...
[ 196.951675] Completed Kernel HMAC SHA256 FIPS KAT
ble_ready NOT present @init ....
[ 198.914842] Starting Kernel HMAC SHA384 FIPS KAT ...
[ 198.959715] Completed Kernel HMAC SHA384 FIPS KAT
[ 200.914836] Starting Kernel HMAC SHA512 FIPS KAT ...
[ 200.959704] Completed Kernel HMAC SHA512 FIPS KAT
Firmware AES-CCM Known Answer Test Passed
[ 233.852871] (08:46:45) !!! Init ---> Conductor
[ 233.893573] asap_send_elected_conductor: sent successfully
[ 237.141837] asap_send_elected_conductor: sent successfully
ble_ready is present @92 .... start processing msgs from APB
[ 319.597525] asap_send_elected_conductor: sent successfully

User:

```

Checking the interface IP address

```

AP303H-Lab2# sh ip int brief
Interface                IP Address / IP Netmask    Admin  Protocol
br0                      10.10.10.23 / 255.255.255.128 up      up
br0.3333                 172.31.98.1 / 255.255.254.0 up      up
AP303H-Lab2#

```

Checking that nothing is connected to any of AP303H-Lab2's ports

```

AP303H-Lab2# sh port status

Port Status
-----
Port  Type  Admin-State  Oper-State  STP-State  Dot3az  Loop-Protect  Storm-Control  Loop-Detection-TX
Loop-Detection-RX
---  ---  -----  -----  -----  -----  -----  -----  -----
-----
eth0  GE    up          down        Off        Disable  OFF          OFF            0              0
eth1  GE    up          down        Off        Disable  OFF          OFF            0              0
eth2  GE    up          down        Off        Disable  OFF          OFF            0              0
eth3  GE    up          down        Off        Disable  OFF          OFF            0              0

```

```
eth4  USB  up          down      Off      Disable  OFF      OFF      0      0
AP303H-Lab2#
```

4.4 Checking the Uplink

As you can see the uplink WiFi-sta is up as it has the highest priority.

```
AP303H-Lab2# sh uplink status
```

```
Uplink preemption          :disable
Uplink preemption interval :600
Uplink enforce             :none
Uplink wired-1            :DHCP
Internet failover          :disable
Max allowed test packet loss :10
Secs between test packets  :30
VPN failover timeout (secs) :180
Internet check timeout (secs) :10
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

```
Uplink Table
```

Type	VLAN	State	Reach	State	Prio	In Use	Interface	IP	Mask	GW
Sent	Lost	Cont	lost							
-----	----	-----	-----		----	-----	-----	--	----	--
Ethernet	1	DOWN	DOWN		0	No	br0	0.0.0.0	0.0.0.0	
0.0.0.0	0	0	0							
Cellular	0	INIT	INIT		7	No	ppp0	0.0.0.0	0.0.0.0	
0.0.0.0	0	0	0							
Wifi-sta	0	UP	UP		6	Yes	br0	10.10.10.23	255.255.255.128	
10.10.10.1	0	0	0							

```
Wired Port Table
```

Port	State	Type	Bonding (Admin/Oper/Active)
eth0	DOWN	LAN	No/Yes/Yes
eth1	DOWN	LAN	No/No/No
eth2	DOWN	LAN	No/No/No
eth3	DOWN	LAN	No/No/No

```
AP303H-Lab2#
```

There are a few new commands specifically for WiFi uplink that you should know.

```
AP303H-Lab2# sh wifi-uplink status
```

```
Configured          :YES
Enabled             :YES
State               :UP
Interfaces           :aruba001
Now                 :2021-10-24 12:41:19
SSID                 :SG11
BSSID               :d0:d3:e0:b2:41:70
Unicast/Multicast Encryption :wpa2-aes-psk wpa2-aes-psk
Link Health         :100
AID                 :1
IP Address           :10.10.10.23
Subnet Mask          :255.255.255.128
Gateway             :10.10.10.1
Associated Time      :3h:2m:42s
Associated AP Beacon Time :3h:5m:56s
```

```

Channel                :36E
RSSI                   :64
Noise Floor            :92
Phy                    :5GHz-VHT-80sgi-2ss
Maximum Speed (mbps)   :866
Overall/Tx/Rx Goodput (mbps) :16.8 13.7 19.6
Last Tx Timestamp      :2021-10-07 22:50:47
Last Rx Timestamp      :2021-10-07 22:50:47
Last Tx Rate (mbps)    :866
Last Rx Rate (mbps)    :585
Last ACK RSSI          :57
AP303H-Lab2#

```

Checking the Authentication logs for WiFi uplink.

```

AP303H-Lab2# sh wifi-uplink connection-trace

WiFi uplink connection trace
-----

2021-10-24 09:38:36 auth      -> 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 retry=no;
tries=0; status=success
2021-10-24 09:38:36 auth      <- 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 SN=1904;
retry=no; status=0
2021-10-24 09:38:36 assoc req -> 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 retry=no;
tries=0; status=success
2021-10-24 09:38:36 assoc resp <- 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 SN=1905;
retry=no; status=0
2021-10-24 09:38:37 connection up *
bssid=d0:d3:e0:b2:41:70
2021-10-24 09:38:37 eapol-key <- 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 ver=1; len=117
2021-10-24 09:38:37 eapol-key -> 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 ver=1; len=117
2021-10-24 09:38:37 eapol-key <- 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 ver=1; len=151
2021-10-24 09:38:37 eapol-key -> 00:4e:35:7b:2c:d1 d0:d3:e0:b2:41:70 ver=1; len=95
2021-10-24 09:38:41 dhcp offer <- 00:4e:35:7b:2c:d1 f8:60:f0:c8:70:e0 xid=5da99147;
cha=00:4e:35:7b:2c:d1; gia=0.0.0.0
2021-10-24 09:38:41 dhcp ack  <- 00:4e:35:7b:2c:d1 f8:60:f0:c8:70:e0 xid=5da99147;
cha=00:4e:35:7b:2c:d1; gia=0.0.0.0
Total connection trace:11; Current time: 2021-10-24 12:42:08
AP303H-Lab2#

```

This command is used for checking the candidates for WiFi uplink.

```

AP303H-Lab2# sh wifi-uplink candidates

WiFi uplink candidates
-----

essid bssid                channel rssi encryption phy      rank up time    last update
(total updates)
-----
-----
SG11  d0:d3:e0:b2:41:70  36E      64    WPA2-psk    VHT-2ss  64/0  3h:9m:14s  2021-10-24
12:44:37 (217642)
Total candidates:1; Current time: 2021-10-24 12:44:37
AP303H-Lab2#

```

Displaying the WiFi uplink config

```

AP303H-Lab2# sh wifi-uplink config

ESSID                :SG11
Cipher Suite         :wpa2-ccmp-psk

```

```

Passphrase      :*****
Passphrase Size :9
Band            :dot11a
AP303H-Lab2#

```

Another useful command is to check the connection history and connection trace.

```

AP303H-Lab2# sh wifi-uplink connection-history

WiFi uplink connection history
-----
timestamp          essid    bssid          channel  rssi  result
-----
2021-10-24 09:38:36 SG11      d0:d3:e0:b2:41:70 36E      62    SUCCESS
Total connection times:1; Current time: 2021-10-24 12:45:34

AP303H-Lab2#

```

Lastly here we see that the Instant AP is in cluster mode, you don't need to convert it to standalone mode.

```

AP303H-Lab2# sh swarm mode

Swarm Mode      :Cluster
AP303H-Lab2#

AP303H-Lab2# sh ver
Aruba Operating System Software.
ArubaOS (MODEL: 303H), Version 8.8.0.2
Website: http://www.arubanetworks.com
(c) Copyright 2021 Hewlett Packard Enterprise Development LP.
Compiled on 2021-10-07 at 18:46:06 UTC (build 81788) by p4build
FIPS Mode :disabled

AP uptime is 3 hours 13 minutes 35 seconds
Reboot Time and Cause: AP rebooted Sun Oct 24 09:32:34 EST 2021; CLI cmd at uptime 0D 0H 17M
34S: reload

AP303H-Lab2#

```

4.5 Checking the WebUI

First let's check the Aruba Instant Cluster (AP-505H) that is broadcasting SG11, note the BSS address.

The screenshot shows the Aruba Instant Cluster WebUI. On the left is a navigation menu with options like Dashboard, Overview, Networks, Access Points, Clients, Mesh Devices, Configuration, and Networks. The main content area is titled 'Wireless (1) Wired (0)' and shows a table of wireless clients. The table has columns for Name, IP Address, MAC address, OS, ESSID, Access Point, Channel, Type, Role, IPv6 Address, Signal, and Speed (Mbps). The first row shows AP303H-Lab2 with IP 10.10.10.23, MAC 00:4e:35:7b:2c:d1, OS NOFP, ESSID SG11, Access Point AP505H-Lab1, Channel 36E, Type AC, Role SG11, IPv6 Address --, Signal 61, and Speed 780. Below the table, there is an 'Info' section for the selected AP, showing details like Name, IP Address, MAC address, OS, ESSID, Access Point, Type, and Role. To the right of the Info section is an 'RF Dashboard' with a graph showing Signal, Speed, and Errors over time.

And now checking the AP-303H cluster that is using SG11 as WiFi uplink.

The screenshot shows the Aruba Instant Cluster WebUI. On the left is a navigation menu with options like Dashboard, Overview, Networks, Access Points, Clients, Mesh Devices, Configuration, and Networks. The main content area is titled 'Access Points (1)' and shows a table of access points. The table has columns for Name, IP Address, Mode, Clients, Type, Channel, Power, Utilization, Noise, Channel, Power, Utilization, Noise, Channel, Power, Utilization, and Noise. The first row shows AP303H-Lab2 with IP 10.10.10.23, Mode access, Clients 0, Type 303H(ind...), Channel 36E, Power 12 dBm, Utilization 6%, Noise -92 dBm, Channel 1, Power 9 dBm, Utilization 20%, Noise -91 dBm, Channel -, Power -, Utilization -, and Noise -. Below the table, there is an 'Info' section for the selected AP, showing details like SSID, Band, RSSI, Encryption, Channel, and Noise Floor. To the right of the Info section is an 'RF Dashboard' with a graph showing Signal, Speed, and Errors over time.

5 External DHCP server for Clients

Here we'll configure AP303H-Lab to use the external DHCP server for its wired and wireless clients.

5.1 Configure Wireless network for Clients

This is the SSID for the wireless clients on AP303H-Lab2

The first screenshot shows the 'Basic' configuration tab for a network named 'test'. The 'Type' is set to 'Wireless' and 'Primary usage' is 'Employee'. The second screenshot shows the 'VLAN' tab, where 'Client IP assignment' is set to 'Network assigned' and 'Client VLAN assignment' is 'Default'. The third screenshot shows the 'Security' tab, with 'Security Level' set to 'Personal', 'Key management' to 'WPA2-Personal', and 'Passphrase format' to '8-63 chars'. The fourth screenshot shows the 'Access' tab, with 'Access Rules' set to 'Unrestricted' and 'Download roles' disabled.

5.2 Configure Wired network for Clients

This is the wired network for the clients that can connect directly to E0 port on AP303H-Lab2

The first screenshot shows the 'Basic' configuration tab for a new network named 'E0-Net'. The 'Type' is set to 'Wired' and 'Primary usage' is 'Employee'. The second screenshot shows the 'VLAN' tab, where 'Mode' is 'Access', 'Client IP assignment' is 'Network assigned', and 'Native VLAN' is '1'. The third screenshot shows the 'Security' tab, where 'Port type' is 'Untrusted', 'MAC authentication' is disabled, and '802.1X authentication' is disabled.

New Network → 1 Basic 2 VLAN 3 Security 4 Access 5 Assignment

Access Rules

Access Rules: Unrestricted

Download roles: ☐

No restrictions on access based on destination or type of traffic

New Network → 1 Basic 2 VLAN 3 Security 4 Access 5 Assignment

0/0: E0-Net

0/1: wired-SetMeUp

0/2: wired-SetMeUp

0/3: wired-SetMeUp

0/4: wired-SetMeUp

5.3 Client Testing

And when we connect a WiFi client to test network, we see that it gets an IP address from the external DHCP server and has full connectivity. Remember that AP-303H is not source NATing the client's IP address 10.10.10.25

aruba | VIRTUAL CONTROLLER | LAB2

Dashboard

Overview Networks Access Points

Wireless (1) Wired (0)

Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role	IPv6 Address	Signal	Speed (Mbps)
SpectreLab	10.10.10.25	f0:d5:bf:4b:67:11	Win 10	test	AP303H-Lab2	36E	AC	test	fe80::e86b:ceb9:86c6:b5eb...	50	526

Now when we connect a WiFi client to “test” which is the SSID that AP-303H is advertising, we see that it is getting an IP address from the standalone IAP and it is getting source NAT as indicated by the output of the “show datapath session” command.

```
AP303H-Lab2# sh clients

Client List
-----
Name      IP Address  MAC Address  OS      ESSID  Access Point  Channel  Type  Role  IPv6 Address
Signal    Speed (mbps)
-----
SpectreLab 10.10.10.25 f0:d5:bf:4b:67:11 Win 10  test  AP303H-Lab2  36E      AC    test
fe80::e86b:ceb9:86c6:b5eb 48 (good) 585 (good)
Number of Clients :1
Info timestamp    :7258
AP303H-Lab2#
AP303H-Lab2#
AP303H-Lab2#

AP303H-Lab2# sh ip int brief
Interface      IP Address / IP Netmask  Admin  Protocol
br0            10.10.10.23 / 255.255.255.128  up     up
br0.3333       172.31.98.1 / 255.255.254.0   up     up
AP303H-Lab2#

AP303H-Lab2# sh datapath session
Datapath Session Table Entries
-----
Flags: F - fast age, S - src NAT, N - dest NAT
       D - deny, R - redirect, Y - no syn
       H - high prio, P - set prio, T - set ToS
       C - client, M - mirror, V - VOIP
       I - Deep inspect, U - Locally destined
       s - media signal, m - media mon, a - rtp analysis
       E - Media Deep Inspect, G - media signal
       A - Application Firewall Inspect
```

```

L - ALG session
O - Session is programmed through SDN/Openflow controller
p - Session is marked as permanent
h - Https redirect error page
X - Http/https redirect for dpi denied session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor, t - time based, i - in flow
Flow Offload Blacklist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel
R - L3 route

```

Source IP	Destination IP	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge	Packets	Bytes	Flags
Offload flags													
192.168.1.130	10.10.10.23	17	53	57454	0	0	0	1	local	53	1	3a	FI
139.99.236.185	10.10.10.23	17	123	52128	0	0	0	1	local	51	2	98	F
10.10.10.23	192.168.1.130	17	56549	53	0	0	0	1	local	54	1	56	FCI
10.10.10.23	192.168.1.130	17	53977	53	0	0	0	1	local	54	1	56	FCI
192.168.1.121	10.10.10.23	6	60239	4343	0	0	0	1	dev25	55	b	6aa	FC
192.168.1.121	10.10.10.23	6	60240	4343	0	0	0	1	dev25	55	8	65b	FC
192.168.1.121	10.10.10.23	6	60241	4343	0	0	0	1	dev25	55	9	690	FC
192.168.1.121	10.10.10.23	6	60254	4343	0	0	0	1	dev25	2c	8	62c	FC
10.10.10.25	8.255.44.248	6	50617	443	0	0	0	1	dev27	43f	2d25	95b15	FC
192.168.1.130	10.10.10.23	17	53	58653	0	0	0	1	local	53	1	7a	FI
40.100.149.226	10.10.10.25	6	443	50644	0	0	0	11	dev27	351	11	252c	
10.10.10.23	139.99.236.185	17	52128	123	0	0	0	1	local	51	10	4c0	FC
192.168.1.130	10.10.10.23	17	53	50358	0	0	0	1	local	53	1	67	FI

Now connecting the wired client to the E0 port of AP303H-Lab2

aruba VIRTUAL CONTROLLER LAB2						
Dashboard						
Overview						
Wireless (1) Wired (1)						
Networks						
Access Points						
Clients						
Name	IP Address	MAC address	OS	AP	Port	
AriyaP	10.10.10.24	f0:de:f1:64:0a:82	Win 10	AP303H-Lab2	0/0	

And checking it from the CLI as well.

```
AP303H-Lab2# sh clients wired
```

```
Wired Client List
```

Name	IP Address	MAC Address	OS	Network	Access Point	Role	IPv6 Address
Speed (mbps)							
AriyaP	10.10.10.24	f0:de:f1:64:0a:82	Win 10	eth0	AP303H-Lab2	E0-Net	--
Info timestamp		:7824					

```
AP303H-Lab2#
```

And again we have full connectivity between these clients and outside network.

```
AP303H-Lab2# sh datapath session
```

```
Datapath Session Table Entries
```

```

-----
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
L - ALG session
O - Session is programmed through SDN/Openflow controller
p - Session is marked as permanent
h - Https redirect error page

```

X - Http/https redirect for dpi denied session
 RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor, t - time based, i - in flow
 Flow Offload Blacklist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel
 R - L3 route

Source IP Offload flags	Destination IP	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge	Packets	Bytes	Flags
23.206.199.145	10.10.10.24	6	443	52239	0	0	0	3	dev8	fa	d	267d	
23.206.199.34	10.10.10.24	6	80	52229	0	0	0	0	dev8	1d0	5	360	F
20.198.162.78	10.10.10.24	6	443	52181	0	0	0	15	dev8	4c1	1	1cf	A
10.10.10.25	52.168.112.67	6	50734	443	0	0	0	4	dev27	146	a	f5c	C
10.10.10.24	224.0.0.22	2	2	2	0	0	0	1	dev8	70	5	c8	FC
10.10.10.24	239.255.255.250	17	53238	1900	0	0	0	0	dev8	70	6	3de	FC
10.10.10.25	104.97.230.134	6	50724	443	0	0	0	1	dev27	243	a	52f	FC
10.10.10.25	40.100.149.226	6	50736	443	0	0	0	3	dev27	11d	9	dd3	C
10.10.10.23	139.99.236.185	17	61887	123	0	0	0	1	local	9d	10	4c0	FC
10.10.10.24	204.79.197.254	6	52196	443	0	0	0	8	dev8	284	e	5b7	C
10.10.10.23	220.158.215.21	17	123	123	0	0	46	1	local	7d	1	4c	FC
10.10.10.24	142.250.70.131	6	52240	443	0	0	0	0	dev8	43	f	a4d	FC
13.107.21.200	10.10.10.24	6	443	52202	0	0	0	7	dev8	278	10	223b	
13.107.21.200	10.10.10.24	6	443	52201	0	0	0	0	dev8	27c	1d	2307	F
10.10.10.24	204.79.197.222	6	52199	443	0	0	0	8	dev8	282	d	7ae	C
139.99.236.185	10.10.10.23	17	123	61887	0	0	0	1	local	9d	3	e4	F
10.10.10.25	10.10.10.24	1	17	0	0	0	0	0	dev8	36	1	3c	FI
10.10.10.25	10.10.10.24	1	16	0	0	0	0	0	dev8	3c	1	3c	FI
10.10.10.25	10.10.10.24	1	11	0	0	0	0	1	dev8	55	1	3c	FI
10.10.10.25	10.10.10.24	1	13	0	0	0	0	0	dev8	4b	1	3c	FI
10.10.10.25	10.10.10.24	1	12	0	0	0	0	1	dev8	50	1	3c	FI
10.10.10.25	10.10.10.24	1	15	0	0	0	0	0	dev8	41	1	3c	FI
10.10.10.25	10.10.10.24	1	14	0	0	0	0	0	dev8	46	1	3c	FI
F0:D5:BF:4B:67:11		0806			0	0	0	1	dev27	51	1	800	F
220.158.215.21	10.10.10.23	17	123	123	0	0	0	1	local	7d	1	4c	F
104.97.230.134	10.10.10.24	6	443	52222	0	0	0	1	dev8	1fb	d	1cda	F
104.97.230.134	10.10.10.24	6	443	52218	0	0	0	1	dev8	1fc	d	1elb	F
10.10.10.24	13.107.21.200	6	52202	443	0	0	0	8	dev8	28c	11	f16	C
13.107.18.254	10.10.10.24	6	443	52198	0	0	0	0	dev8	296	12	205c	F
10.10.10.23	13.211.226.240	6	56920	443	0	0	0	4	local	2e6	2f	2cf0	C

AP303H-Lab2#

Finally checking the session table on AP505H-Lab1 for the wired client (10.10.10.24) and wireless client (10.10.10.25)

AP505H-Lab1#

AP505H-Lab1# sh datapath sess | incl 10.10.10.24

1.1.1.1	10.10.10.24	1	24	0	0	0	0	0	dev29	20	1	3c	FI
1.1.1.1	10.10.10.24	1	25	0	0	0	0	0	dev29	16	1	3c	FI
1.1.1.1	10.10.10.24	1	22	0	0	0	0	0	dev29	34	1	3c	FI
1.1.1.1	10.10.10.24	1	23	0	0	0	0	0	dev29	2a	1	3c	FI
10.10.10.24	1.1.1.1	1	25	2048	0	0	0	0	dev29	16	1	3c	FCI
10.10.10.24	1.1.1.1	1	24	2048	0	0	0	0	dev29	20	1	3c	FCI
10.10.10.24	1.1.1.1	1	23	2048	0	0	0	0	dev29	2a	1	3c	FCI
10.10.10.24	1.1.1.1	1	22	2048	0	0	0	0	dev29	34	1	3c	FCI
34.107.221.82	10.10.10.24	6	80	50360	0	0	0	1	dev29	5a	1	34	A
34.107.221.82	10.10.10.24	6	80	50359	0	0	0	1	dev29	5a	1	34	A

AP505H-Lab1#

AP505H-Lab1# sh datapath sess | incl 10.10.10.25

1.1.1.1	10.10.10.25	1	28	0	0	0	0	0	dev29	19	1	3c	FI
1.1.1.1	10.10.10.25	1	26	0	0	0	0	0	dev29	2e	1	3c	FI
1.1.1.1	10.10.10.25	1	27	0	0	0	0	0	dev29	23	1	3c	FI
1.1.1.1	10.10.10.25	1	25	0	0	0	0	0	dev29	38	1	3c	FI
10.10.10.25	1.1.1.1	1	25	2048	0	0	0	0	dev29	38	1	3c	FCI
10.10.10.25	1.1.1.1	1	27	2048	0	0	0	0	dev29	23	1	3c	FCI
10.10.10.25	1.1.1.1	1	26	2048	0	0	0	0	dev29	2e	1	3c	FCI
10.10.10.25	1.1.1.1	1	28	2048	0	0	0	0	dev29	19	1	3c	FCI
23.206.199.144	10.10.10.25	6	443	50749	0	0	0	0	dev29	29	3	97	F
10.10.10.25	23.206.199.144	6	50749	443	0	0	0	0	dev29	29	4	a0	FC

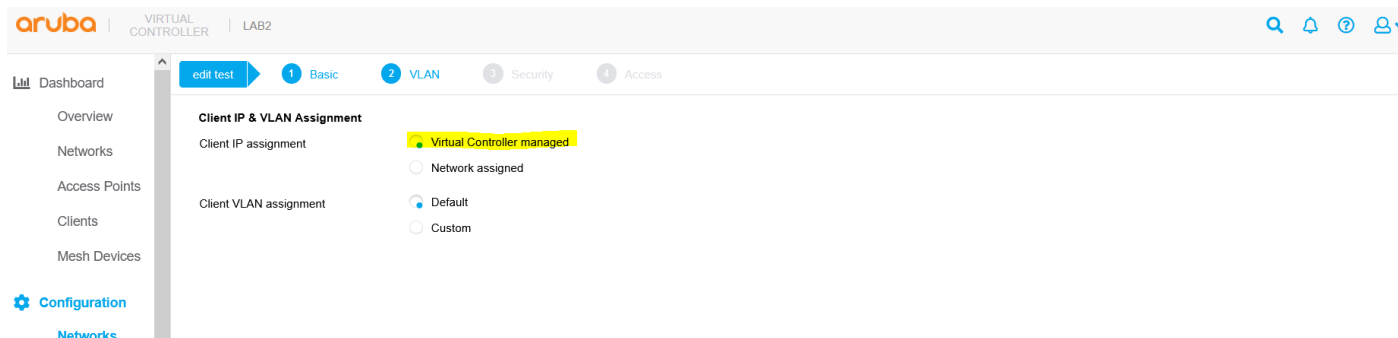
AP505H-Lab1#

6 Instant AP as DHCP server for Clients

Here we'll configure AP303H-Lab to use the Instant's internal DHCP service for its wired and wireless clients.

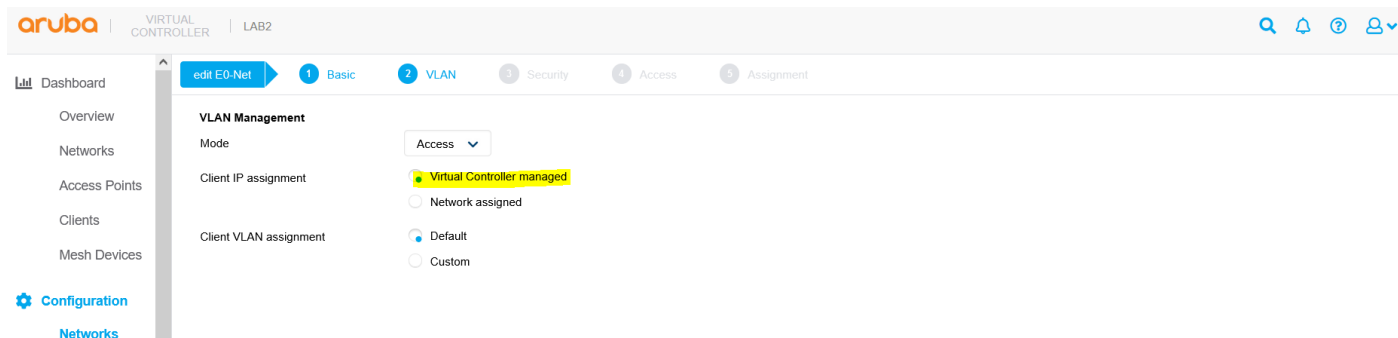
6.1 Configure Wireless network for Clients

We'll just modify the same wireless network on AP303H-Lab2. The only thing that changes is the client IP assignment as shown below.



6.2 Configure Wired network for Clients

And the same thing goes for the wired network that we previously configured on AP303H-Lab2

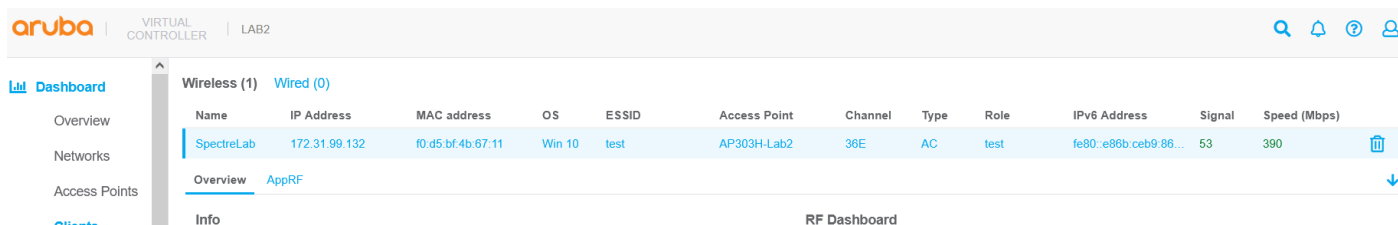


Now both these networks will use Instant AP's internal DHCP scope

```
AP303H-Lab2# sh ip int brief
Interface                IP Address / IP Netmask    Admin  Protocol
br0                      10.10.10.23 / 255.255.255.128 up      up
br0.3333                 172.31.98.1 / 255.255.254.0 up      up
AP303H-Lab2#
```

6.3 Client Testing

When we connect a WiFi client to test network, we see that it gets a private IP address from AP-303H and has full connectivity. Remember that AP-303H is source NATing the IP address 172.31.99.132 with the IP address that it got from the WiFi uplink.



Now when we connect a WiFi client to “test” which is the SSID that AP303H-Lab2 is advertising, we see that it is getting an IP address from its internal DHCP and it is getting source NAT as indicated by the output of the “show datapath session” command.

```
AP303H-Lab2# sh clients
```

```
Client List
```

```
-----
Name          IP Address      MAC Address      OS      ESSID  Access Point  Channel  Type  Role
IPv6 Address      Signal      Speed (mbps)
----          -
-----
SpectreLab  172.31.99.132  f0:d5:bf:4b:67:11  Win 10  test   AP303H-Lab2   36E      AC    test
fe80::e86b:ceb9:86c6:b5eb  52 (good)  351 (good)
Number of Clients   :1
Info timestamp      :10923
```

```
AP303H-Lab2#
```

```
AP303H-Lab2# sh ip int brief
```

```
Interface          IP Address / IP Netmask      Admin  Protocol
br0                 10.10.10.23 / 255.255.255.128  up     up
br0.3333            172.31.98.1 / 255.255.254.0   up     up
```

```
AP303H-Lab2#
```

```
AP303H-Lab2# sh data
```

```
Datapath Session Table Entries
```

```
-----
```

```
Flags: F - fast age, S - src NAT, N - dest NAT
D - deny, R - redirect, Y - no syn
H - high prio, P - set prio, T - set ToS
C - client, M - mirror, V - VOIP
I - Deep inspect, U - Locally destined
s - media signal, m - media mon, a - rtp analysis
E - Media Deep Inspect, G - media signal
A - Application Firewall Inspect
L - ALG session
O - Session is programmed through SDN/Openflow controller
p - Session is marked as permanent
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to master, t - time based
```

Source IP	Destination IP	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge	Packets	Bytes	Flags
40.100.151.130													
172.31.99.132	192.168.1.130	17	61107	53	0	0	0	1	dev27	3	1	50	FSCIA
172.31.99.132	20.43.111.112	6	50784	443	0	0	0	0	dev27	3	1f	c5c	SC
172.31.99.132	192.168.1.130	17	60526	53	0	0	0	0	dev27	6	1	4f	FSCIA
172.31.99.132	192.168.1.130	17	59850	53	0	0	0	0	dev27	2	1	40	FSCIA
172.31.99.132	192.168.1.130	17	59403	53	0	0	0	0	dev27	3	1	3c	FSCIA
172.31.99.132	192.168.1.130	17	58840	53	0	0	0	0	dev27	2	1	4b	FSCIA
172.31.99.132	192.168.1.130	17	58562	53	0	0	0	0	dev27	3	1	3c	FSCIA
172.31.99.132	34.98.75.36	6	50786	443	0	0	0	0	dev27	3	b	600	SC
172.31.99.132	192.168.1.130	17	58482	53	0	0	0	0	dev27	1	1	3c	FSCIA
172.31.99.132	192.168.1.130	17	58169	53	0	0	0	0	dev27	1e	1	3f	FSCIA
172.31.99.132	117.18.237.29	6	50773	80	0	0	0	0	dev27	1d	4	19c	SC
172.31.99.132	117.18.237.29	6	50771	80	0	0	0	0	dev27	1e	6	2d4	FSC
172.31.99.132	117.18.237.29	6	50790	80	0	0	0	0	dev27	2	4	254	SC
172.31.99.132	34.117.237.239	6	50792	443	0	0	0	0	dev27	1	4	2b1	SC
172.31.99.132	192.168.1.130	17	65457	53	0	0	0	0	dev27	1	1	53	FSCIA
172.31.99.132	34.107.221.82	6	50783	80	0	0	0	0	dev27	3	4	1d9	SC
172.31.99.132	34.107.221.82	6	50789	80	0	0	0	0	dev27	2	4	1db	SC

```
AP303H-Lab2#
```

Now connecting the wired client to the E0 port of AP303H-Lab2

aruba		VIRTUAL CONTROLLER		LAB2			
Dashboard		Wireless (1)		Wired (1)			
Overview		Name		IP Address		MAC address	
Networks		AriyaP		172.31.98.235		f0:de:f1:64:0a:82	
Access Points				OS		AP	
Clients				Win 10		AP303H-Lab2	
						Port	
						0/0	

And checking it from the CLI as well.

```
AP303H-Lab2# sh clients wired
```

Wired Client List

Name	IP Address	MAC Address	OS	Network	Access Point	Role	IPv6 Address	Speed (mbps)
AriyaP	172.31.98.235	f0:de:f1:64:0a:82	Win 10	eth0	AP303H-Lab2	E0-Net	--	-

Info timestamp :11384

```
AP303H-Lab2#
```

```
AP303H-Lab2# sh port status
```

Port Status

Port	Type	Admin-State	Oper-State	STP-State	Dot3az	Loop-Protect	Storm-Control	Loop-Detection-TX	Loop-Detection-RX
eth0	GE	up	up	Off	Disable	OFF	OFF	0	0
eth1	GE	up	down	Off	Disable	OFF	OFF	0	0
eth2	GE	up	down	Off	Disable	OFF	OFF	0	0
eth3	GE	up	down	Off	Disable	OFF	OFF	0	0
eth4	USB	up	down	Off	Disable	OFF	OFF	0	0

```
AP303H-Lab2#
```

Again, both the clients Wired (172.31.98.235) and wireless (172.31.99.132) have full connectivity between themselves as well. Here below is the session table when I was pinging 172.31.99.132 from 172.31.98.235

```
AP303H-Lab2# sh datapath session | incl 172.31.9
```

172.31.99.132	35.165.184.220	6	50804	443	0	0	0	2	dev27	c56	c	7c2	SC
172.31.98.235	172.31.99.132	1	37	2048	0	0	0	1	dev8	30	1	3c	FCI
172.31.98.235	172.31.99.132	1	38	2048	0	0	0	1	dev8	2b	1	3c	FCI
172.31.98.235	172.31.99.132	1	39	2048	0	0	0	1	dev8	26	1	3c	FCI
172.31.98.235	172.31.99.132	1	40	2048	0	0	0	0	dev8	21	1	3c	FCI
172.31.99.132	172.31.98.235	1	38	0	0	0	0	1	dev8	2b	1	3c	FI
172.31.99.132	172.31.98.235	1	39	0	0	0	0	1	dev8	26	1	3c	FI
172.31.99.132	172.31.98.235	1	37	0	0	0	0	1	dev8	30	1	3c	FI
172.31.99.132	172.31.98.235	1	40	0	0	0	0	1	dev8	21	1	3c	FI
172.31.98.235	20.197.71.89	6	61523	443	0	0	0	17	dev8	54f	d	be3	SC
172.31.98.235	224.0.0.251	17	5353	5353	0	0	0	1	dev8	5e	5	151	FC
172.31.98.235	224.0.0.22	2	2	2	0	0	0	1	dev8	5e	5	c8	FC
172.31.98.235	239.255.255.250	17	52474	1900	0	0	0	0	dev8	5e	6	3de	FC
172.31.99.132	20.198.162.76	6	50764	443	0	0	0	14	dev27	1046	16	fa3	SC
172.31.99.132	20.198.162.76	6	50769	443	0	0	0	1	dev27	e85	f	b1b	SC
172.31.99.132	35.244.181.201	6	50828	443	0	0	0	0	dev27	26f	f	690	SC
172.31.98.235	224.0.0.252	17	62658	5355	0	0	0	1	dev8	5e	1	34	FCA
172.31.98.235	13.107.5.88	6	61525	443	0	0	0	3	dev8	f1	e	5ce	SC

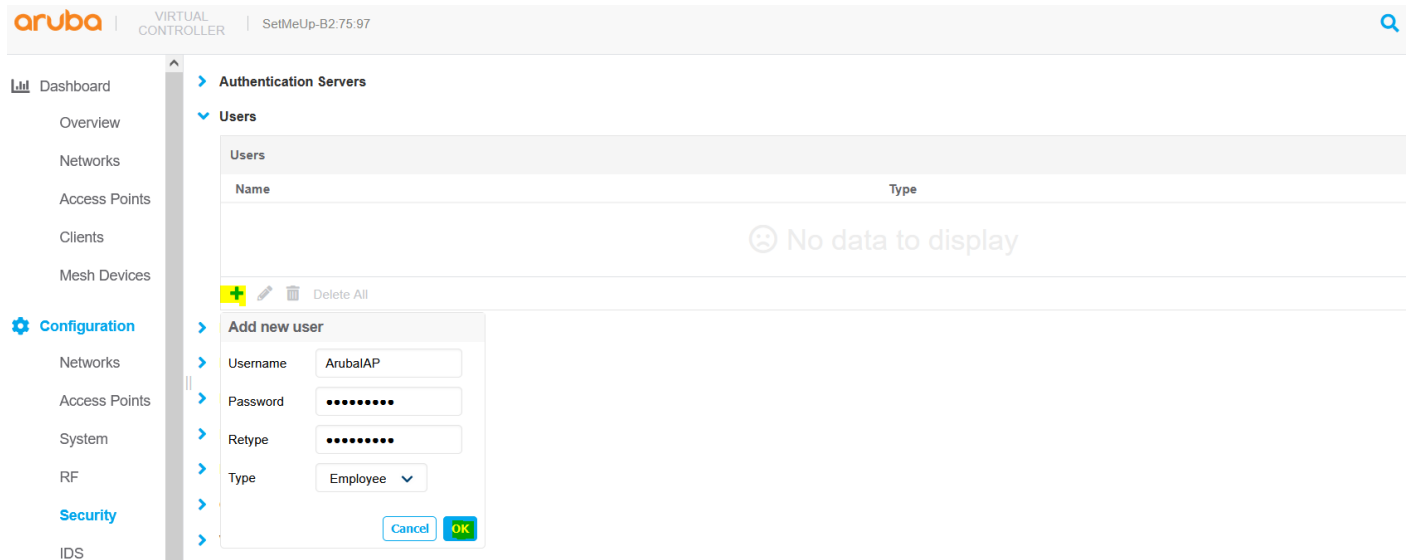
```
AP303H-Lab2#
```

7 WiFi Uplink with Dot1x Auth

Here we'll configure dot1x authentication for our previously PSK based WiFi uplink network. This solution could be used for deployments where you don't want to use an external RADIUS server such as ClearPass.

7.1 Dot1x Authenticated WiFi Uplink

On the AP-505H we'll change the security setting to WPA2-Enterprise and using Internal DB as authentication server (you can also use any external RADIUS server like ClearPass). This is shown below.

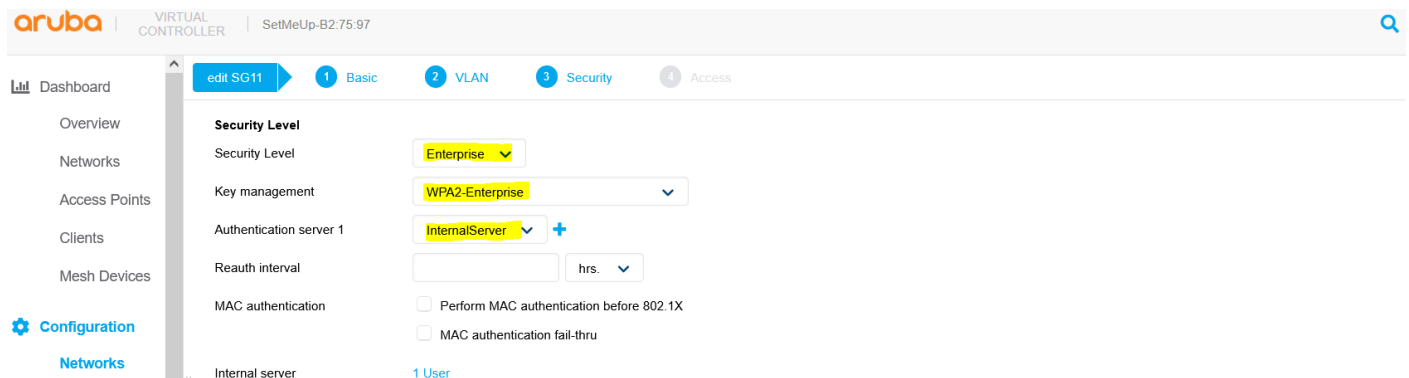


The screenshot shows the Aruba Virtual Controller interface. The left sidebar has a 'Configuration' section with 'Security' highlighted. The main area is titled 'Authentication Servers' and 'Users'. A modal dialog 'Add new user' is open, showing fields for Username (ArubaAP), Password (masked), Retype (masked), and Type (Employee). There are 'Cancel' and 'OK' buttons at the bottom of the dialog.



The screenshot shows the Aruba Virtual Controller interface after adding the user. The 'Users' table now contains one entry: 'ArubaAP' with Type 'Employee'. The 'Add new user' dialog is no longer visible. The left sidebar shows 'Configuration' with 'Security' highlighted.

Then we'll reconfigure the security component of the SG11 WLAN network.



The screenshot shows the Aruba Virtual Controller interface with the 'Security' configuration for SG11. The 'Security Level' is set to 'Enterprise'. The 'Key management' is set to 'WPA2-Enterprise'. The 'Authentication server 1' is set to 'InternalServer'. The 'Reauth interval' is set to 'hrs'. The 'MAC authentication' section has two checkboxes: 'Perform MAC authentication before 802.1X' and 'MAC authentication fail-thru', both of which are unchecked. The 'Internal server' section shows a link to '1 User'.

Now on the AP-303H which is using WiFi Uplink we need to change the mode of and type of dot1x authentication

Aruba Virtual Controller | LAB2

Configuration > Uplink > Wifi

Name (SSID): SG11

Key management: WPA2-Enterprise

Band: 5 GHz

AP1X type: PEAP

Username: ArubaIAP

Password: [Masked]

Validate server: ☐

When you make any changes here, you need to reboot the AP303H-Lab2. Now when the AP reboots, it will make a successful dot1x authentication for its WiFi uplink.

Aruba Virtual Controller | SetMeUp-5C:05:6E

Dashboard > Access Points (1)

Name	IP Address	Mode	Clients	Type	Radio 0				Radio 1				Radio 2			
					Channel	Power	Utilization	Noise	Channel	Power	Utilization	Noise	Channel	Power	Utilization	Noise
AP303H-Lab2	10.10.10.23	access	0	303H(ind...	36E	12 dBm	4%	-92 dBm	1	6 dBm	18%	-89 dBm	-	-	-	-

Overview | Client Match | AppRF | Spectrum | Cellular | **Wi-Fi Uplink**

SSID	SG11	Encryption	wpa2-aes-enterprise wpa2-aes-enterprise
Band	5GHz-VHT-80sgl-2ss	Channel	36E
RSSI	57	Noise Floor	-92 (dBm)

And we have a wired client that successfully connects

aruba

VIRTUAL CONTROLLER

SetMeUp-5C:05:6E

Dashboard

Overview

Networks

Access Points

Clients

Wireless (0)

Wired (1)

Name	IP Address	MAC address	OS	AP	Port
AriyaP	10.10.10.25	f0:de:f1:64:0a:82	Win 10	AP303H-Lab2	0/0

Here is the config and status of the WiFi uplink

```
AP303H-Lab2# sh wifi-uplink config
ESSID                :SG11
Cipher Suite         :wpa2-ccmp
Wifilx               :wifilx peap ArubaIAP *****
Passphrase           :
Band                 :dot11a

AP303H-Lab2# sh wifi-uplink status
Configured           :YES
Enabled              :YES
State                :UP
Interfaces           :aruba001
Now                  :2021-10-27 12:19:56
SSID                 :SG11
BSSID                :d0:d3:e0:b2:41:70
Unicast/Multicast Encryption :wpa2-aes-enterprise wpa2-aes-enterprise
```

```

Link Health           :99
AID                   :1
IP Address             :10.10.10.23
Subnet Mask            :255.255.255.128
Gateway               :10.10.10.1
Associated Time        :7m:23s
Associated AP Beacon Time :2h:6m:2s
Channel               :36E
RSSI                   :56
Noise Floor           :92
Phy                   :5GHz-VHT-80sgi-2ss
Maximum Speed (mbps)  :866
Overall/Tx/Rx Goodput (mbps) :83.3 127.6 38.4
Last Tx Timestamp      :2021-08-16 10:17:10
Last Rx Timestamp      :2021-08-16 10:17:10
Last Tx Rate (mbps)    :866
Last Rx Rate (mbps)    :866
Last ACK RSSI          :51

```

AP303H-Lab2#

Now checking the uplink status

AP303H-Lab2# sh uplink status

```

Uplink preemption      :enable
Uplink preemption interval :120
Uplink enforce         :none
Uplink wired-1         :DHCP
Internet failover      :disable
Max allowed test packet loss :10
Secs between test packets :30
VPN failover timeout (secs) :180
Internet check timeout (secs) :10
AP1X type:NONE
Certification type:NONE
Validate server:NONE

```

Uplink Table

Type	VLAN	State	Reach	State	Prio	In Use	Interface	IP	Mask	GW
Sent	Lost	Cont	lost							
Ethernet	1	DOWN	DOWN		0	No	br0	0.0.0.0	0.0.0.0	--
0.0.0.0	0	0	0							
Cellular	0	INIT	INIT		7	No	ppp0	0.0.0.0	0.0.0.0	
0.0.0.0	0	0	0							
Wifi-sta	0	UP	UP		6	Yes	wuplink0	10.10.10.23	255.255.255.128	
10.10.10.1	0	0	0							

Wired Port Table

Port	State	Type	Bonding (Admin/Oper/Active)
eth0	UP	LAN	No/Yes/Yes
eth1	DOWN	LAN	No/No/No
eth2	DOWN	LAN	No/No/No
eth3	DOWN	LAN	No/No/No

AP303H-Lab2#

Here is some additional info and the wired client.

AP303H-Lab2# sh ip int b

Interface	IP Address / IP Netmask	Admin	Protocol
-----------	-------------------------	-------	----------

```
br0          169.254.72.191 / 255.255.0.0    up    up
br0.3333     172.31.98.1 / 255.255.254.0    up    up
wuplink0     10.10.10.23 / 255.255.255.128 up    up
```

```
AP303H-Lab2# sh clients wired
```

Wired Client List

Name	IP Address	MAC Address	OS	Network	Access Point	Role	IPv6 Address
Speed (mbps)							
----	-----	-----	--	-----	-----	----	-----
AriyaP	10.10.10.25	f0:de:f1:64:0a:82	Win 10	eth0	AP303H-Lab2	E0-Net	--
Info timestamp	:885						

```
AP303H-Lab2#
```

8 Instant AP (WiFi 6) with WiFi Uplink

Now we'll configure the same thing with AP-505H. It is the same as AP-303H.

We need to

1. Disable the Extended SSID
2. Configuration WiFi uplink for PSK or dot1x
3. And ensure that the uplink priority list has the WiFi-sta at the top if you want it to be the primary uplink.
4. Configure some WiFi and Wired network for testing

8.1 PSK based Testing

Here are the screenshots to show that AP-515 successfully connected to its primary WiFi uplink. We are using WPA2-PSK based authentication.

The screenshot shows the Aruba Virtual Controller interface. On the left is a navigation menu with options: Dashboard, Overview, Networks, Access Points, Clients, Mesh Devices, and Configuration. The main area displays 'Access Points (1)' with a table for AP515-Lab1. The table has columns for Name, IP Address, Mode, Clients, Type, and three radio sections (Radio 0, Radio 1, Radio 2). The 'Wi-Fi Uplink' tab is selected, showing details for SSID (SG11), Band (5GHz-VHT-80sgt-2ss), RSSI (55), Encryption (wpa2-aes-psk wpa2-aes-psk), Channel (149E), and Noise Floor (-95 (dBm)).

```
AP515-Lab1# sh ip int b
Interface                               IP Address / IP Netmask      Admin  Protocol
br0                                     0.0.0.0 / 0.0.0.0            up     up
br0.3333                               172.31.98.1 / 255.255.254.0  up     up
wuplink0                               10.10.10.22 / 255.255.255.128  up     up
```

AP515-Lab1#

```
AP515-Lab1# sh uplink status
```

```
Uplink preemption           :enable
Uplink preemption interval  :600
Uplink enforce               :none
Uplink wired-1              :DHCP
Internet failover            :disable
Max allowed test packet loss :10
Secs between test packets    :30
VPN failover timeout (secs)  :180
Internet check timeout (secs):10
AP1X type:NONE
Certification type:NONE
Validate server:NONE
```

Uplink Table

Type	VLAN	State	Reach State	Prio	In Use	Interface	IP	Mask	GW
Sent	Lost	Cont	lost						
Ethernet	1	DOWN	DOWN	0	No	br0	0.0.0.0	0.0.0.0	--
0.0.0.0	0	0	0						
Cellular	0	INIT	INIT	7	No	ppp0	0.0.0.0	0.0.0.0	
0.0.0.0	0	0	0						

```
Wifi-sta 0 UP UP 6 Yes wuplink0 10.10.10.22 255.255.255.128
10.10.10.1 0 0 0
```

Wired Port Table

```
-----
Port  State  Type  Bonding (Admin/Oper/Active)
-----
eth0  DOWN   WAN   Yes/Yes/Yes
eth1  DOWN   WAN   Yes/Yes/Yes
```

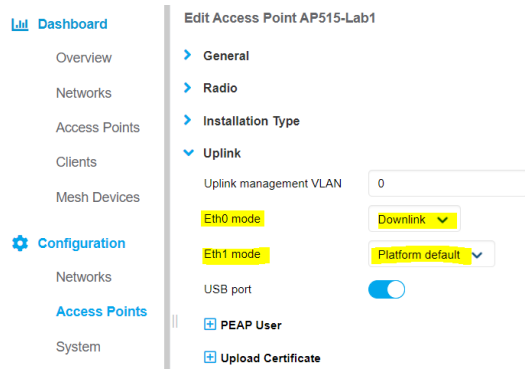
AP515-Lab1#

AP515-Lab1# sh wifi-uplink status

```
Configured           :YES
Enabled              :YES
State                :UP
Interfaces            :aruba000
Now                  :2021-10-27 14:18:29
SSID                  :SG11
BSSID                 :d0:d3:e0:b2:41:70
Unicast/Multicast Encryption :wpa2-aes-psk wpa2-aes-psk
Link Health           :99
AID                   :1
IP Address             :10.10.10.22
Subnet Mask            :255.255.255.128
Gateway               :10.10.10.1
Associated Time        :5m:2s
Associated AP Beacon Time :17m:38s
Channel                :149E
RSSI                   :55
Noise Floor            :95
Phy                    :5GHz-VHT-80sgi-2ss
Maximum Speed (mbps)   :866
Overall/Tx/Rx Goodput (mbps) :150 119.1 720.6
Last Tx Timestamp      :2021-08-16 10:13:39
Last Rx Timestamp      :2021-08-16 10:13:42
Last Tx Rate (mbps)    :866
Last Rx Rate (mbps)    :866
Last ACK RSSI          :55
```

AP515-Lab1#

Here we'll quickly cover the configuration of Wired network for E0 of AP-515. The first thing is to ensure it's the mode for E0 and 1 are as shown below.



Then as we per our wired configuration on AP-303H, we'll do the same thing here.

aruba
VIRTUAL CONTROLLER
SetMeUp-C9:2B:30

Dashboard
Overview
Networks
Access Points
Clients
Mesh Devices
Configuration
Networks

edit E0-Net
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment

Name & Usage

Name
E0-Net

Type
Wired

Primary usage
Employee

POE

Admin status
Up

aruba
VIRTUAL CONTROLLER
SetMeUp-C9:2B:30

Dashboard
Overview
Networks
Access Points
Clients
Mesh Devices
Configuration
Networks

edit E0-Net
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment

VLAN Management

Mode
Access

Client IP assignment
Virtual Controller managed
Network assigned

Native VLAN
1

VLAN Assignment Rules

No data to d

aruba
VIRTUAL CONTROLLER
SetMeUp-C9:2B:30

Dashboard
Overview
Networks
Access Points
Clients
Mesh Devices
Configuration
Networks

edit E0-Net
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment

Security

Port type
Untrusted

MAC authentication

802.1X authentication

aruba
VIRTUAL CONTROLLER
SetMeUp-C9:2B:30

Dashboard
Overview
Networks
Access Points
Clients
Mesh Devices
Configuration
Networks

edit E0-Net
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment

Access Rules

Access Rules
Unrestricted

Download roles

No restrictions on access based on destination or type of traffic

aruba
VIRTUAL CONTROLLER
SetMeUp-C9:2B:30

Dashboard
Overview
Networks
Access Points
Clients
Mesh Devices
Configuration
Networks

edit E0-Net
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment

0/0
E0-Net

0/1
wired-SetMeUp

0/2
wired-SetMeUp

0/3
wired-SetMeUp

0/4
wired-SetMeUp

Next we'll connect a wired client to AP515-Lab1's E0.

aruba | VIRTUAL CONTROLLER | SetMeUp-C9:2B:30

Dashboard

Overview

Networks

Access Points

Info

Name	SetMeUp-C9:2B:30	Country code	AU
Virtual Controller IP	0.0.0.0	Management	Local
Conductor	10.10.10.22	IPv6 Address	--
Uplink type	Wifi-sta	Uplink status	UP

aruba | VIRTUAL CONTROLLER | SetMeUp-C9:2B:30

Dashboard

Overview

Networks

Access Points

Clients

Wireless (0) Wired (1)

Name	IP Address	MAC address	OS	AP	Port
AriyaP	10.10.10.25	f0:de:f1:64:0a:82	Win 10	AP515-Lab1	0/0

```
AP515-Lab1# sh clients wired
```

Wired Client List

Name	IP Address	MAC Address	OS	Network	Access Point	Role	IPv6 Address	Speed (mbps)
AriyaP	10.10.10.25	f0:de:f1:64:0a:82	Win 10	eth0	AP515-Lab1	E0-Net	--	-

Info timestamp :1817

```
AP515-Lab1#
```

```
AP515-Lab1# sh port status
```

Port Status

Port	Type	Admin-State	Oper-State	STP-State	Dot3az	Loop-Protect	Storm-Control	Loop-Detection-TX
eth0	2.5GE	up	up	N/A	Disable	OFF	OFF	0
eth1	GE	up	down	N/A	Disable	OFF	OFF	0
eth2	USB	up	down	N/A	Disable	OFF	OFF	0

```
AP515-Lab1#
```

8.2 Dot1x Testing

Here is the screenshot to show that AP-515 successfully connected to its primary WiFi uplink. We are using dot1x based authentication.

aruba | VIRTUAL CONTROLLER | SetMeUp-C9:2B:30

Dashboard

Overview

Networks

Access Points

Clients

Mesh Devices

Configuration

Access Points (1)

Name	IP Address	Mode	Clients	Type	Channel	Power	Utilization	Noise	Channel	Power	Utilization	Noise	Channel	Power	Utilization	Noise
AP515-Lab1	10.10.10.22	access	0	515(undo)	52E	12 dBm	1%	-96 dBm	1	9 dBm	11%	-93 dBm	-	-	-	-

Overview Client Match Cellular Wi-Fi Uplink

SSID	SG11	Encryption	wpa2-aes-enterprise wpa2-aes-enterprise
Band	5GHz-VHT-80sgi-2ss	Channel	52E
RSSI	53	Noise Floor	-96 (dBm)

```
AP515-Lab1# sh ip int b
```

Interface	IP Address / IP Netmask	Admin	Protocol
br0	0.0.0.0 / 0.0.0.0	up	up
br0.3333	172.31.98.1 / 255.255.254.0	up	up
wuplink0	10.10.10.22 / 255.255.255.128	up	up

AP515-Lab1#

AP515-Lab1# sh uplink status

Uplink preemption :enable
Uplink preemption interval :600
Uplink enforce :none
Uplink wired-1 :DHCP
Internet failover :disable
Max allowed test packet loss :10
Secs between test packets :30
VPN failover timeout (secs) :180
Internet check timeout (secs) :10
AP1X type:NONE
Certification type:NONE
Validate server:NONE

Uplink Table

Type	VLAN	State	Reach	State	Prio	In Use	Interface	IP	Mask	GW
Sent	Lost	Cont	lost							
-----	----	-----	-----	-----	----	-----	-----	--	----	--
Ethernet	1	DOWN	DOWN		0	No	br0	0.0.0.0	0.0.0.0	
0.0.0.0	0	0	0							
Cellular	0	INIT	INIT		7	No	ppp0	0.0.0.0	0.0.0.0	
0.0.0.0	0	0	0							
Wifi-sta	0	UP	UP		6	Yes	wuplink0	10.10.10.22	255.255.255.128	
10.10.10.1	0	0	0							

Wired Port Table

Port	State	Type	Bonding (Admin/Oper/Active)
----	-----	-----	-----
eth0	DOWN	WAN	Yes/Yes/Yes
eth1	DOWN	WAN	Yes/Yes/Yes

AP515-Lab1#

AP515-Lab1# sh wifi-uplink status

Configured :YES
Enabled :YES
State :UP
Interfaces :aruba000
Now :2021-10-27 13:05:47
SSID :SG11
BSSID :d0:d3:e0:b2:41:70
Unicast/Multicast Encryption :wpa2-aes-enterprise wpa2-aes-enterprise
Link Health :99
AID :1
IP Address :10.10.10.22
Subnet Mask :255.255.255.128
Gateway :10.10.10.1
Associated Time :4m:4s
Associated AP Beacon Time :11m:28s
Channel :52E
RSSI :53
Noise Floor :96
Phy :5GHz-VHT-80sgi-2ss
Maximum Speed (mbps) :866
Overall/Tx/Rx Goodput (mbps) :150.9 123.2 684.2
Last Tx Timestamp :2021-10-27 13:05:46

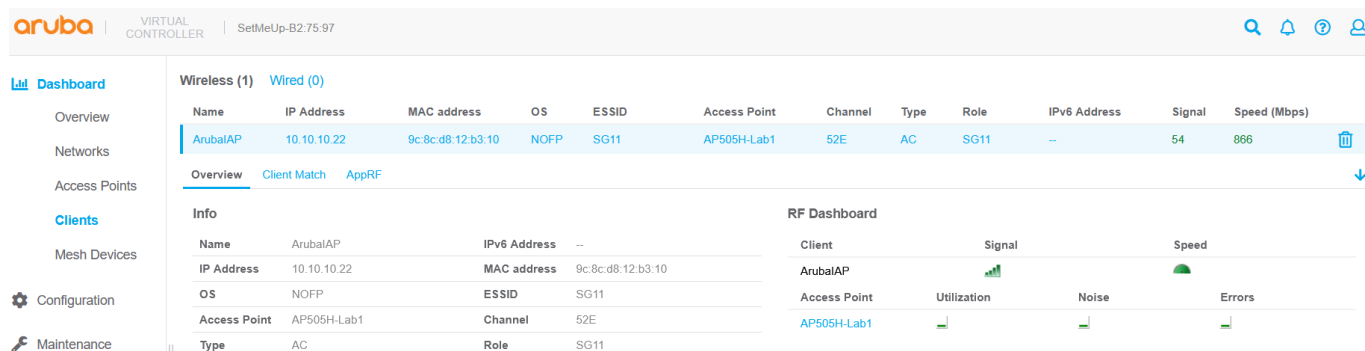
```

Last Rx Timestamp      :2021-10-27 13:05:46
Last Tx Rate (mbps)    :866
Last Rx Rate (mbps)    :866
Last ACK RSSI          :55

```

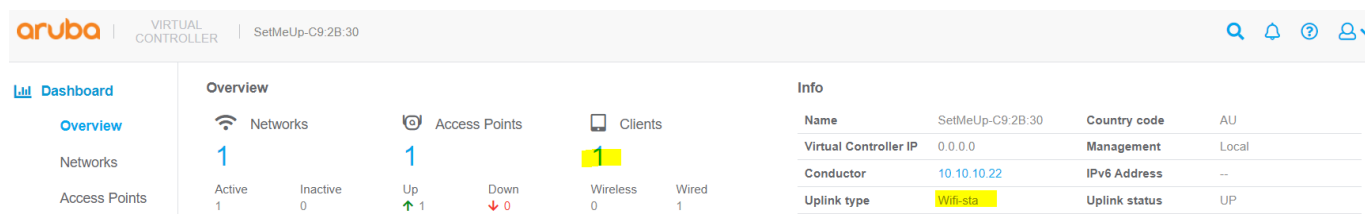
AP515-Lab1#

And here is the view from the Instant Cluster that AP515-Lab1 has connected to.

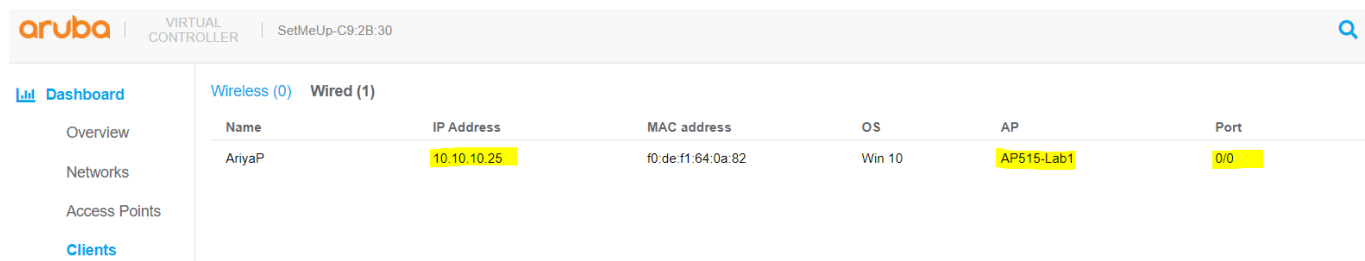


The screenshot shows the Aruba Instant Cluster web interface. The top header includes the Aruba logo, 'VIRTUAL CONTROLLER', and the controller name 'SetMeUp-B2:75:97'. The left sidebar has a 'Clients' menu item highlighted. The main content area shows a table of wireless clients. One client, 'ArubaAP', is listed with IP address 10.10.10.22, MAC address 9c:8c:d8:12:b3:10, OS NOFP, and ESSID SG11. It is connected to access point AP505H-Lab1 on channel 52E. The client's role is SG11, and it has a signal strength of 54 and a speed of 866 Mbps. Below the table, there is an 'Info' section for the selected client, showing details like IP address, MAC address, OS, ESSID, access point, channel, and role. To the right, an 'RF Dashboard' shows signal and speed metrics for the client and access point.

And here is when we have connected the wired client to AP515-Lab1.



The screenshot shows the Aruba Instant Cluster web interface. The top header includes the Aruba logo, 'VIRTUAL CONTROLLER', and the controller name 'SetMeUp-C9:2B:30'. The left sidebar has an 'Overview' menu item highlighted. The main content area shows an 'Overview' section with a summary of network statistics: 1 active network, 1 inactive network, 1 up access point, 0 down access points, 0 wireless clients, and 1 wired client. Below this, there is an 'Info' section for the selected client, showing details like Name, Virtual Controller IP, Conductor, and Uplink type. The client is connected to access point AP505H-Lab1 on channel 52E.



The screenshot shows the Aruba Instant Cluster web interface. The top header includes the Aruba logo, 'VIRTUAL CONTROLLER', and the controller name 'SetMeUp-C9:2B:30'. The left sidebar has a 'Clients' menu item highlighted. The main content area shows a table of wireless clients. One client, 'AriyaP', is listed with IP address 10.10.10.25, MAC address f0:de:f1:64:0a:82, OS Win 10, and AP AP515-Lab1. It is connected to access point AP515-Lab1 on port 0/0. The client's role is E0-Net, and it has a signal strength of 0/0 and a speed of 0/0 Mbps. Below the table, there is an 'Info' section for the selected client, showing details like IP address, MAC address, OS, AP, and Port.

```
AP515-Lab1# sh clients wired
```

```
Wired Client List
```

```

-----
Name      IP Address  MAC Address  OS      Network  Access Point  Role    IPv6 Address  Speed (mbps)
-----
AriyaP    10.10.10.25 f0:de:f1:64:0a:82 Win 10  eth0     AP515-Lab1    E0-Net  --            -
Info timestamp      :1817

```

```
AP515-Lab1# sh data
```

```
datapath      Datapath information
datatunnelcert
```

```
AP515-Lab1# sh datap session
```

```
Datapath Session Table Entries
```

```

-----
Flags: F - fast age, S - src NAT, N - dest NAT
       D - deny, R - redirect, Y - no syn
       H - high prio, P - set prio, T - set ToS
       C - client, M - mirror, V - VOIP
       I - Deep inspect, U - Locally destined
       s - media signal, m - media mon, a - rtp analysis
       E - Media Deep Inspect, G - media signal

```

A - Application Firewall Inspect
 L - ALG session
 O - Session is programmed through SDN/Openflow controller
 p - Session is marked as permanent
 h - Https redirect error page
 X - Http/https redirect for dpi denied session

RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor, t - time based, i - in flow

Flow Offload Denylist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel

R - L3 route

Source IP	Destination IP	Prot	SPort	Dport	Cntr	Prio	ToS	Age	Destination	TAge	Packets	Bytes	Flags
Offload flags													
10.10.10.25	20.197.71.89	6	55743	443	0	0	0	5	dev8	163	c	9b7	C
192.168.1.121	10.10.10.22	6	61654	4343	0	0	0	1	dev24	e	6	308	FC
192.168.1.121	10.10.10.22	6	61655	4343	0	0	0	1	dev24	e	6	308	FC
192.168.1.121	10.10.10.22	6	61658	4343	0	0	0	1	dev24	e	7	6ca	FC
192.168.1.121	10.10.10.22	6	61659	4343	0	0	0	1	dev24	e	8	6cb	FC
192.168.1.121	10.10.10.22	6	61656	4343	0	0	0	1	dev24	e	6	308	FC
192.168.1.121	10.10.10.22	6	61657	4343	0	0	0	1	dev24	e	7	68a	FC
10.10.10.25	20.198.162.76	6	55741	443	0	0	0	8	dev8	28f	c	bbc	C
20.198.162.76	10.10.10.25	6	443	55741	0	0	0	8	dev8	28f	d	14d4	
10.10.10.22	192.168.1.121	6	4343	61657	0	0	0	0	dev24	e	c	2439	F
10.10.10.22	192.168.1.121	6	4343	61656	0	0	0	0	dev24	e	4	135	F
10.10.10.22	192.168.1.121	6	4343	61659	0	0	0	0	dev24	e	8	8e4	F
10.10.10.22	192.168.1.121	6	4343	61658	0	0	0	0	dev24	e	d	26e4	F

AP515-Lab1#