1 Table of Contents

Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
10 May 2019	0.1	Ariya Parsamanesh	Initial creation
16 May 2019	0.2	Ariya Parsamanesh	Added the instant cluster testing

2 WiFi Uplink

This is one of the long awaited feature on Instant 11ac APs. Now with Instant version 8.5 we have it. The Wi-Fi uplink is supported on the following 11n and 11ac platforms

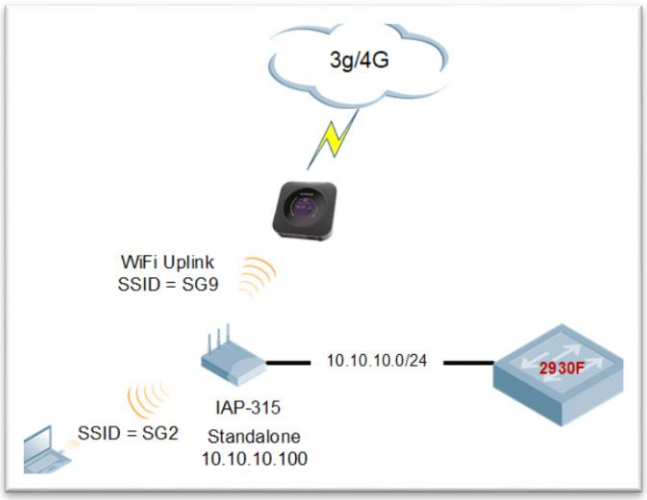
- AP-203H, AP-203R, AP-203RP, AP-207,
- AP-300 Series, AP-303H, 310 Series, 320 Series, and 330 Series access points.

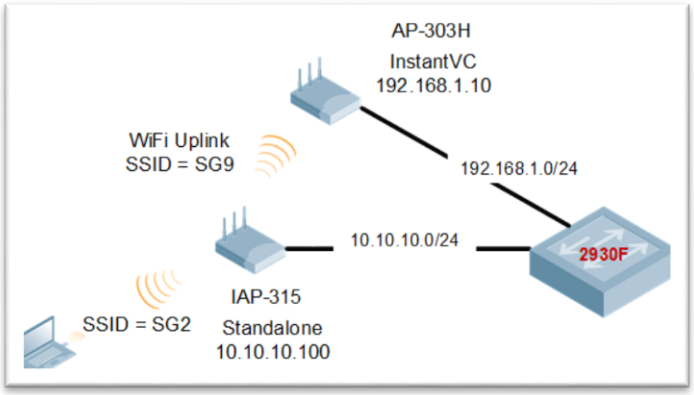
The whole aim of this feature is to use WiFi in addition to 3G/4G and Ethernet as a valid uplink. The Wi-Fi uplink allows you to connect to SSIDs with the following authentication modes

- Open
- PSK-CCMP
- PSK-TKIP encryption

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 two scenarios, one using a WiFi uplink to a WiFi hotspot and the other using WiFi uplink to connect to an existing Instant cluster.





You should note that when one enables WiFi uplink all client traffic coming out of the IAP generally will under go a NAT operation, it is meant to bridge WiFi traffic on an AP to a wireless hotspot. So in our case the WiFi client connecting to SG2 will get an VC assigned IP address from the IAP-315 that is source natted IAP-315 using its own WiFi uplink IP address.

2.1 Things you need

- Aruba Instant version 8.5.0.0 or later
- WiFi uplink device/provider or an existing Instant Cluster
- A Layer three switch and some WiFi clients

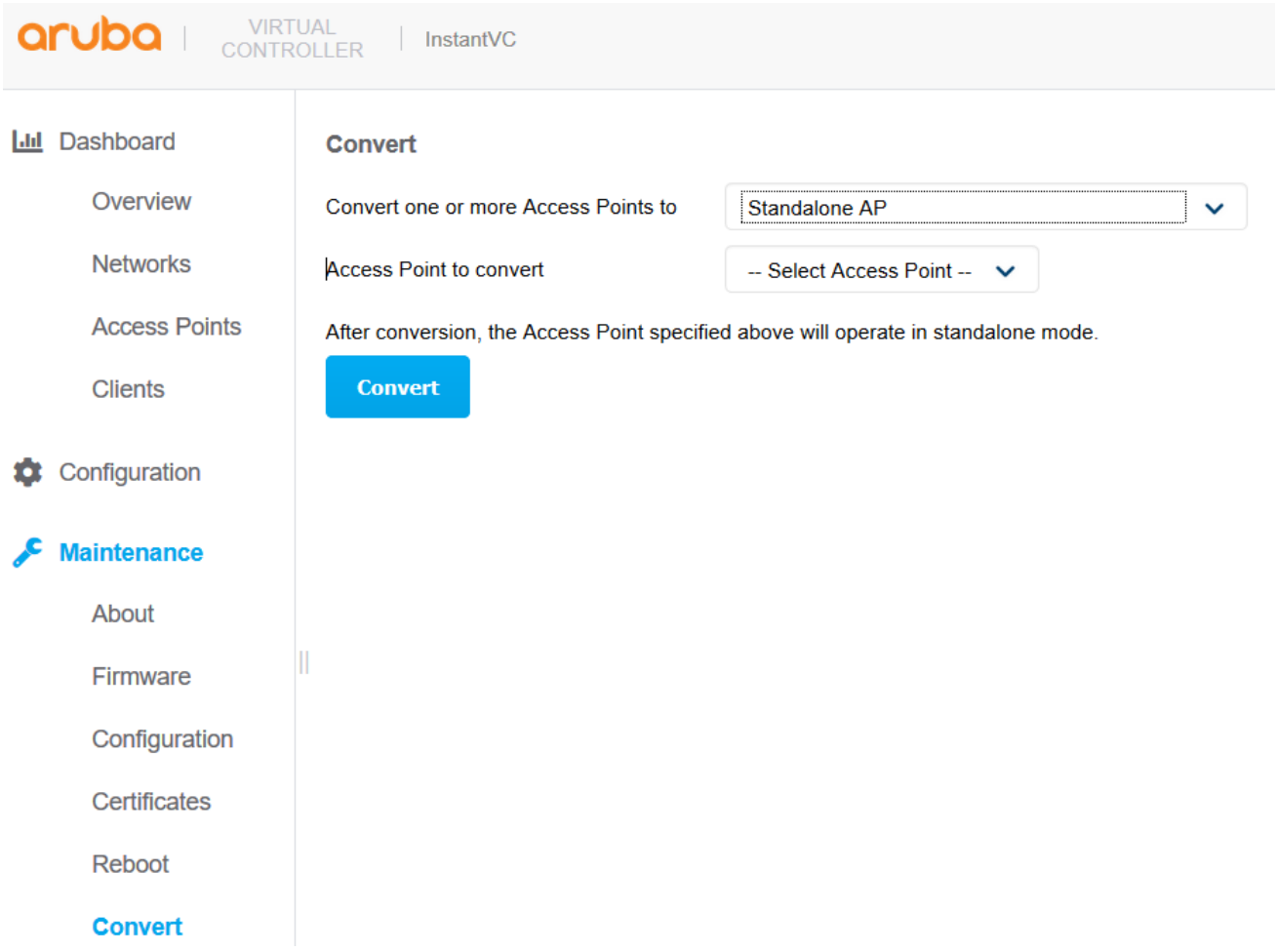
3 Instant AP Configuration

Here are the main points to note

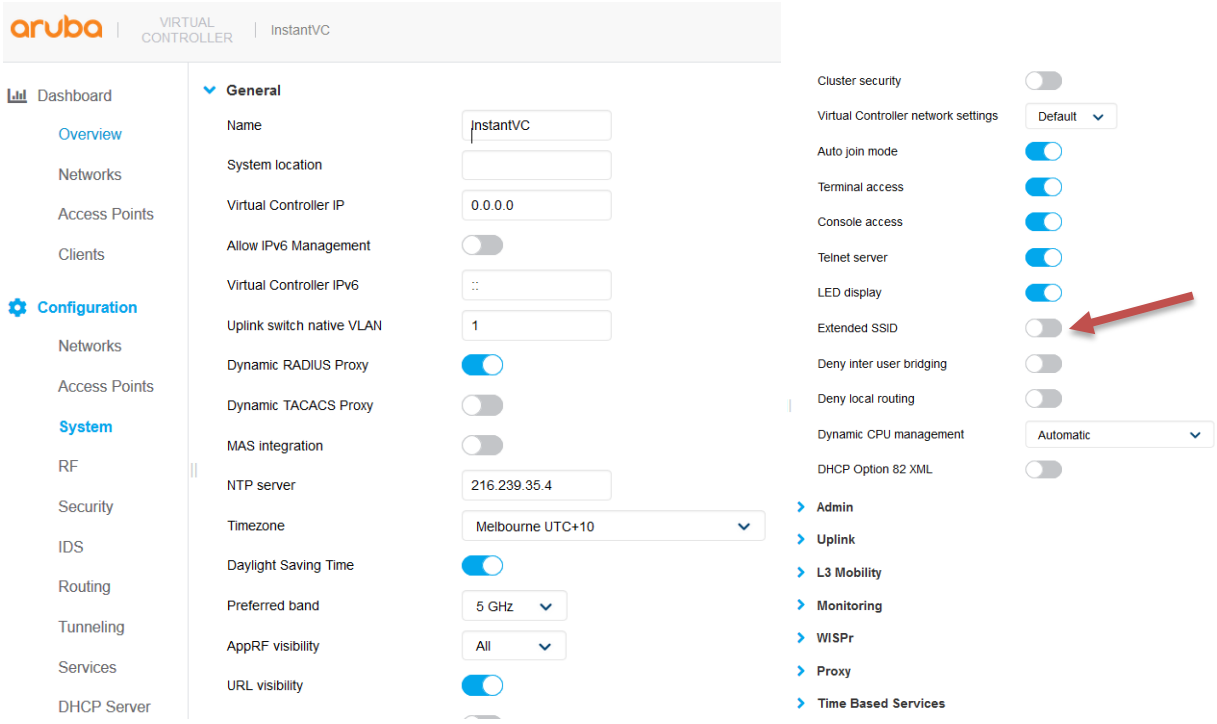
- At the moment this feature is supported on 11ac IAPs in standalone mode.
- When you configure the WiFi uplink, you need to reboot the IAPs for the changes to take effect.
- Instant Mesh and WiFi uplink are mutually exclusive, you can one or the other.
- Again for 11ac IAP if you want to WiFi uplink it to an existing IAP cluster, the instant version on the cluster needs to be 8.5.0 or later
- Currently WiFi uplink should be the main uplink with Ethernet and 3G/4G to be its backup.

3.1 Convert SSID

First you need to convert the IAP to standalone mode and reboot it.

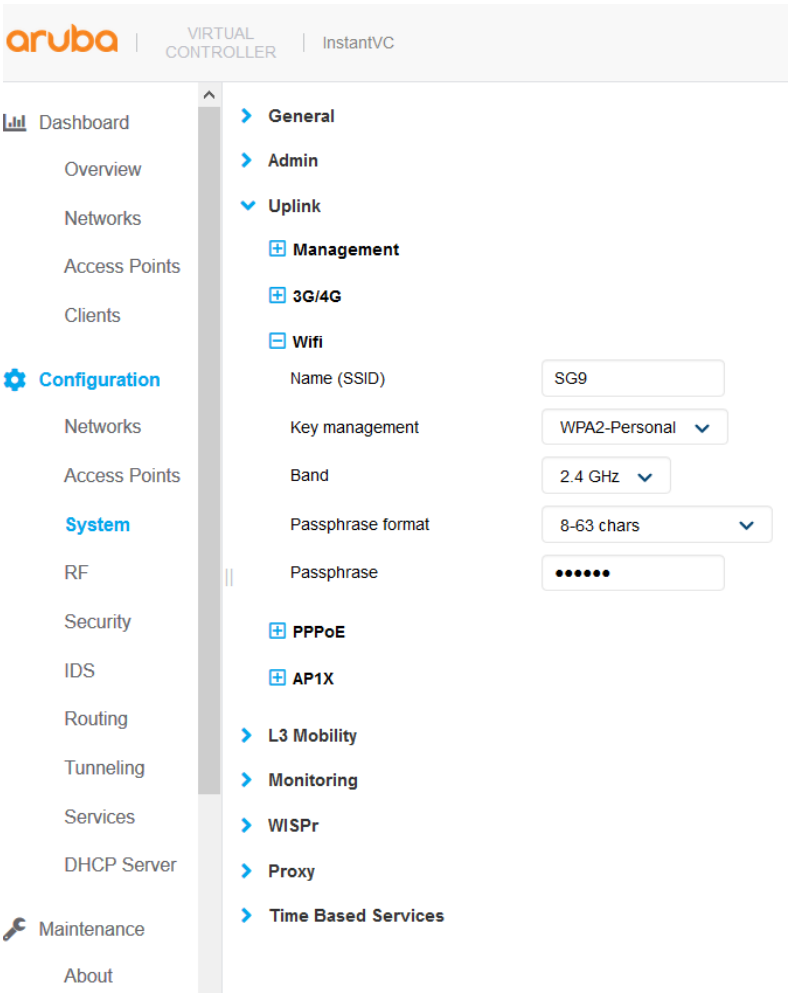


3.2 Disable Extended SSID



3.3 Uplink Configuration

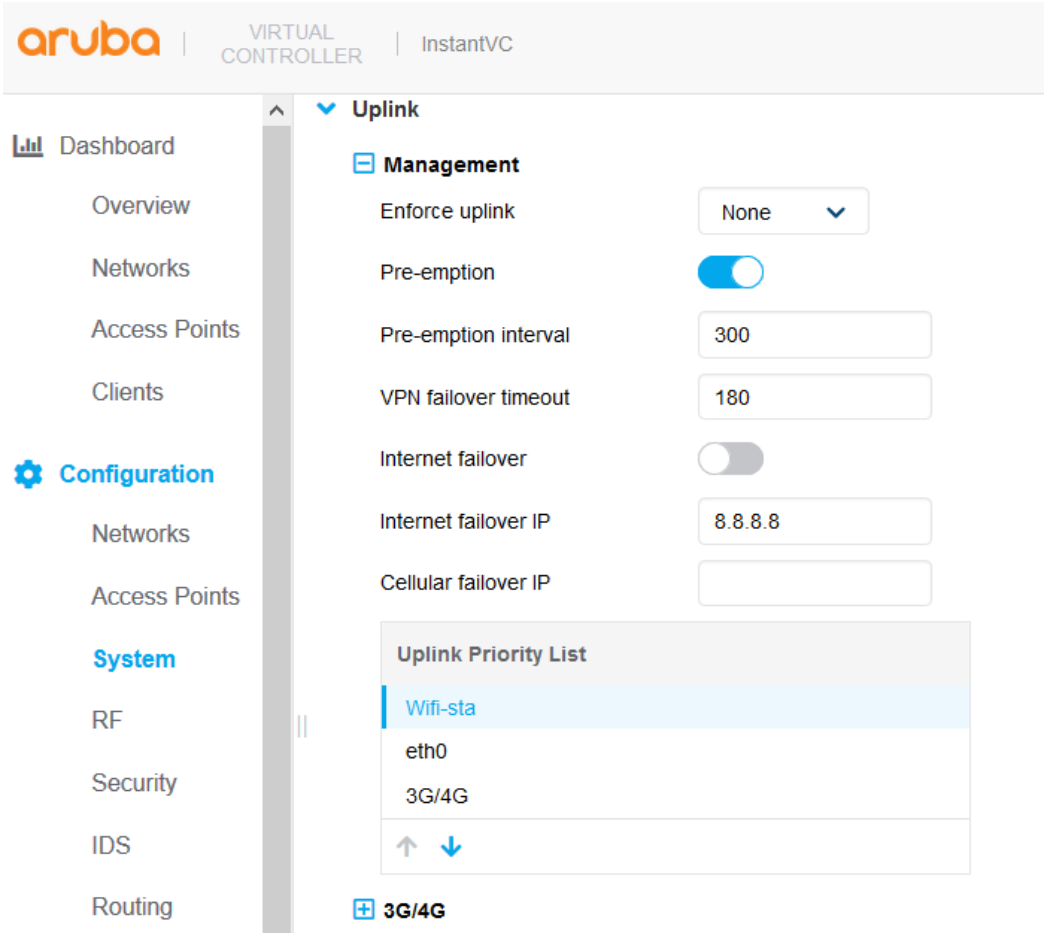
The ESSID for my WiFi uplink is SG9 which his being advertised on 2.4GHz band but you can use 5GHz as well.



Once you have configured this you need to reboot the IAP.

Note that currently we support WiFi uplink as a primary uplink and not backup to either 3G/4G or Ethernet. In the upcoming relases this will be supported as well.

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



Once you have configured this and clicked on save button, you need to reboot the IAP.

3.4 Testing

Here is the console log of the IAP when it got rebooted, I have deleted the unrelated lines

```
APBoot 1.5.5.7 (build 56398)
Built: 2016-09-08 at 14:21:29

Hit <Enter> to stop autoboot:  0
Booting OS partition 0
Checking image @ 0x0
Copying image from 0x44000000

Image is signed; verifying checksum... passed
SHA2 Signature available
Signer Cert OK

Loading configuration file of length 11195...
wifi uplink detected...
Terminal access enabled...
Telnet server enabled...
Valid SSID detected...
touching file /tmp/ip_mode_0
[   57.327991] ADDRCONF(NETDEV_UP): bond0: link is not ready
[   57.387503] Kernel watchdog refresh ended on core 1.
do ethtool autoneg on for bond0
[   57.453358] bond0: Link down
eth1 admin down
SIOCGIFFLAGS: No such device
```

```
init usb modem ...
[   57.622368] Kernel watchdog refresh ended on core 0.
insmod: cannot insert `/lib/slhc.ko': File exists (-1): File exists
insmod: cannot insert `/lib/ppp_generic.ko': File exists (-[   57.788597] usbcore: registered new interface
driver usbserial
1): File exists
No USB Plugged in
wifi uplink is configured on 2G, and mesh will NOT be in use.[   83.153264] uol: module license 'Proprietary'
taints kernel.
[   83.239300] Disabling lock debugging due to kernel taint

apdot1x authentication is not enabled
Starting DHCP
Getting an IP address...
Jan  1 00:01:05 udhcpc[4905]: udhcpc (v0.9.9-pre) started
Jan  1 00:01:05 udhcpc[4905]: send_discover: pkt num 0, secs 0
Jan  1 00:01:05 udhcpc[4905]: Sending discover...
Jan  1 00:01:07 udhcpc[4905]: send_selecting: pkt num 0, secs 512
Jan  1 00:01:07 udhcpc[4905]: Sending select for 10.10.10.100...
Jan  1 00:01:07 udhcpc[4905]: Lease of 10.10.10.100 obtained, lease time 86400
[   88.950359] ip_time_handler: Got ip and packets on bond0 Started master election 5-0, rand 27
10.10.10.100 255.255.255.0 10.10.10.1
Compressing all files in the /etc/httpd directory...
Done.
Starting Webserver
bind: Transport endpoint is not connected
bind: Transport endpoint is not connected
bind: Transport endpoint is not connected
NTP server 216.239.35.4 from configuration.

[  123.381162] SERIAL NUMBER:  : wifi0
[  123.381162]
[  123.457200] wmi_service_ready_event_rx:  WMI UNIFIED SERVICE READY event
[  123.610184] wmi_ready_event_rx:  WMI UNIFIED READY event
[  123.662417] target uses HTT version 2.2; host uses 2.2
[  123.774101] aruba_mods_radio_attach: dev:<wifi0> ic:d6480540 osdev:d67adc10 phy:2
[  123.851327] wifi0: Base BSSID c8:b5:ad:3c:ae:30, 16 available BSSID(s) processor ID: 0
[  123.946048] bond0 address=c8:b5:ad:cb:ca:e2
[  123.996094] br0 address=c8:b5:ad:cb:ca:e2
[  124.043955] wifi0: AP type AP-315, radio 0, max_bssids 16
[  124.108559] aruba_mods_radio_attach() INT  setting antenna polarization to 0 radio 0
[  124.201343] Resetting spectral chainmask to Rx chainmask
[  124.368509] Resetting spectral chainmask to Rx chainmask
[  124.419900] Init the PCAP for radio0 offload 1.
[  124.474101] aruba_mods_radio_attach: radio: 0, init txq work cpu: core-0
[  124.554076] PCI: enabling device 0000:03:00.0 (0140 -> 0142)
[  124.622024] ath_pci 0000:03:00.0: ath DEBUG: sc=0xd8023400
[  125.893470] Startup Mode-0 set
[  125.917869] htt_peer_map_timer_init Enter pdev d6564000 hrtimer d65669b0
[  125.997688]
[  125.997688]  htt_alloc_peer_map_mem : Alloc Success : host q vaddr d65b3000 paddr 57ab3000
[  126.114401]
[  126.114401]  htt_alloc_peer_map_mem : Flush Interval Configured to 256 pkts
[  126.216994] ol_txrx_pdev_attach: 2500 tx desc's allocated ; range starts from d6580000
[  126.311371]
[  126.311371] SERIAL NUMBER:  : wifi1
[  126.311371]
[  126.387285] wmi_service_ready_event_rx:  WMI UNIFIED SERVICE READY event
[  126.541955] wmi_ready_event_rx:  WMI UNIFIED READY event
[  126.594189] target uses HTT version 2.2; host uses 2.2
[  126.600687] ol_ath_smart_ant_attach: Firmware doest not support Smart Antenna.
[  126.600687] ol_ath_smart_ant_attach: Hardware doest not support Smart Antenna.
[  126.831802] aruba_mods_radio_attach: dev:<wifi1> ic:d5b80540 osdev:d8023410 phy:2
[  126.918119] wifi1: Base BSSID c8:b5:ad:3c:ae:20, 16 available BSSID(s) processor ID: 0
[  127.012839] bond0 address=c8:b5:ad:cb:ca:e2
[  127.062855] br0 address=c8:b5:ad:cb:ca:e2
[  127.110746] wifi1: AP type AP-315, radio 1, max_bssids 16
[  127.175351] aruba_mods_radio_attach() INT  setting antenna polarization to 0 radio 1
[  127.268103] Resetting spectral chainmask to Rx chainmask
[  127.331615] Resetting spectral chainmask to Rx chainmask
[  127.395438] Init the PCAP for radio1 offload 1.
[  127.449609] aruba_mods_radio_attach: radio: 1, init txq work cpu: core-1
[  127.536707]  pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
[  127.616026]  pktlog_init: Initializing Pktlog for AR900B, pktlog_hdr_size = 16
```

```
[  127.734926] usbcore: registered new interface driver usbserial
[  127.793814] usbcore: registered new interface driver usbserial_generic
[  127.873133] USB Serial support registered for generic
[  127.930896] usbserial: USB Serial Driver core
[  127.985723] usbcore: registered new interface driver cp210x
[  128.051077] USB Serial support registered for cp210x
[  128.121149] usbcore: registered new interface driver cdc_eem
AP rebooted Tue May 14 11:53:10 UTC 2019; CLI cmd at uptime 0D 0H 42M 16S: reload
shutting down watchdog process (nanny will restart it)...

        <<<<<       Welcome to the Access Point     >>>>>

[  176.998719] VAP device aruba002 created osifp: (d65b7540) os_if: (d5070000)
[  178.825929] VAP device aruba102 created osifp: (dc67f540) os_if: (d51b0000)
[  179.764354] wlan_mlme_app_ie_delete: appie is NULL. Do nothing.
[  180.955888] wlan_mlme_app_ie_delete: appie is NULL. Do nothing.
[  182.051671] wmi_unified_set_psmode:set psmode=1
[  182.094970] wmi_unified_set_psmode:set psmode=0
[  182.151640] VAP device aruba101 created osifp: (d50f9540) os_if: (d4978000)
[  184.814276] ieee80211_connection_state_connecting_entry:701, enter.....,sm->candidate_aplist_index = 0
[  184.914401] wlan_assoc_sm_start:914, enter......
[  184.969572] ieee80211_assoc_state_init_event:149, enter....., event 0
[  185.054233] ieee80211_assoc_state_join_event:204, goto AUTH
[  185.114339] wlan_mlme_auth_request:354, enter >>>>>>>>>>
[  185.190315] aruba_set_vdev_rawmode at line 8768, retv = 22
[  185.243517] aruba_configure_fw_mode 8805
[  185.290565] ieee80211_assoc_state_assoc_event:340, ASSOC sucess and transition to RUN state
[  187.453577] asap_firewall_device_update, firewall dev changed to aruba101, addr changed to
c8:b5:ad:3c:ae:21
[  189.098562] asap_send_elected_master: sent successfully
[  210.826366] VAP device aruba002 created osifp: (d5744540) os_if: (dbf08000)
[  211.126616] VAP device aruba102 created osifp: (d50fc540) os_if: (dbb10000)
```

Checking the system log entries

```
c8:b5:ad:cb:ca:e2# sh log sys 30

Apr 27 02:01:26  cli[5676]: <341174> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  No current uplink, pick
the highest one - Wifi-sta Wifi-sta.
Apr 27 02:01:26  cli[5676]: <341175> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Connecting with current
uplink - Wifi-sta.
Apr 27 02:01:26  cli[5676]: <341263> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  enable uplink Wifi-sta.
Apr 27 02:01:26  cli[5676]: <341167> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Uplink Wifi-sta type
Wifi-sta, state LOAD->PROBE.
Apr 27 02:01:34  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  recv wifi-uplink linkup
Apr 27 02:01:34  cli[5676]: <341181> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Uplink Wifi-sta, setup
ip for uplink - Wifi-sta.
Apr 27 02:01:34  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  About to setup ip for
wifi uplink
Apr 27 02:01:36  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  /etc/setup_ip_swarm
Wifi-sta 1
Apr 27 02:01:36  cli[5676]: <341166> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Get interface br0 ip:
192.168.43.49/255.255.255.0.
Apr 27 02:01:36  cli[5676]: <341167> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Uplink Wifi-sta type
Wifi-sta, state PROBE->UP.
Apr 27 02:01:36  cli[5676]: <341185> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Retrieving ip address
from br0, ip 192.168.43.49, mask 255.255.255.0.
Apr 27 02:01:36  cli[5676]: <341274> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|  Update election ip from
br0, election ip 192.168.43.49/255.255.255.0.
Apr 27 02:01:36  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|
build_my_ip_address:setting this as new IP address for swarm
Apr 27 02:01:36  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@10.10.10.100 cli|
build_my_ip_address_stage2:setting this as new IP address for swarm/clients
May 14 11:58:16  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@192.168.43.49 cli|  Sending out drt-check
request to Activate
May 14 11:58:19  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@192.168.43.49 cli|  Activate response for
'drt-check': new_drt='1.0_70076' payload='1.0_70076 http://d2vxf1j0rhr3p0.cloudfront.net/drtfiles/reg-data-
1.0_70076.dat^M '
May 14 11:58:19  cli[5676]: <341004> <WARN> |AP c8:b5:ad:cb:ca:e2@192.168.43.49 cli|  The DRT vesion in
payload from Activate is 1.0_70076, DRT url is http://d2vxf1j0rhr3p0.cloudfront.net/drtfiles/reg-data-
1.0_70076.dat

c8:b5:ad:cb:ca:e2#
```

Note that the IP address 10.10.10.100 is provided initually throughon Eth0 since the IAP is connected to active Ethernet interface on VLAN 10.

Checking the interface IP address

```
c8:b5:ad:cb:ca:e2# sh ip int b
Interface                          IP Address / IP Netmask       Admin  Protocol
br0                              192.168.43.49 / 255.255.255.0     up     up
br0.3333                           172.31.98.1 / 255.255.254.0     up     up
c8:b5:ad:cb:ca:e2#
```

3.5 Checking the Uplink

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

```
c8:b5:ad:cb:ca:e2# sh uplink status

Uplink preemption             :enable
Uplink preemption interval    :300
Uplink enforce                :none
Ethernet uplink bond0        :DHCP
Uplink Table
------------
Type      State  Priority  In Use
----      -----  --------  ------
eth0      UP     10        No
Wifi-sta  UP     9         Yes
3G/4G     INIT   11        No
Internet failover                        :disable
Max allowed test packet loss             :10
Secs between test packets                :30
VPN failover timeout (secs)              :180
Internet check timeout (secs)            :10
ICMP pkt sent        :0
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
c8:b5:ad:cb:ca:e2#
```

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

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink status

Configured                  :YES
Enabled                     :YES
Interfaces                  :aruba101
Now                         :2019-05-14 12:08:22
SSID                        :SG9
BSSID                       :32:07:4d:4a:e5:66
Unitcast/Multicast Encryption:wpa2-aes-psk wpa2-aes-psk
Link Health                 :100
AID                         :1
Associated Time             :11m:11s
```

```
Associated AP Beacon Time    :16m:47s
Channel                      :11
RSSI                         :74
Noise Floor                  :96
Phy                          :2.4GHz-VHT-20sgi-2ss
Maximum Speed (mbps)         :144
Overall/Tx/Rx Goodput (mbps) :34.9 22.9 49.9
Last Tx Timestamp            :2019-04-27 02:11:20
Last Rx Timestamp            :2019-04-27 02:11:20
Last Tx Rate (mbps)          :52
Last Rx Rate (mbps)          :130
Last ACK RSSI                :71
c8:b5:ad:cb:ca:e2#
```

Checking the Authentiction logs for WiFi uplink.

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink auth

------------------------------------------------------------------------
wifi uplink auth log:
------------------------------------------------------------------------
[5853]<DEBUG>1556294443.043244: wpa_supplicant v2.6
[5853]<DEBUG>1556294443.043369: random: Trying to read entropy from /dev/random
[5853]<INFO>1556294443.043463: Successfully initialized wpa_supplicant
[5853]<DEBUG>1556294489.360465: Priority group 1
[5853]<DEBUG>1556294489.360527:    id=0 ssid='SG9'
[5853]<DEBUG>1556294489.360652: Add interface aruba101 to a new radio N/A
[5853]<DEBUG>1556294489.360777: aruba101: Own MAC address: c8:b5:ad:3c:ae:21
[5853]<DEBUG>1556294489.360840: aruba_driver_set_key 0x5f1484 0x5f153c
[5853]<DEBUG>1556294489.360933: set key: alg 0 key_id 0 tx 0 addr (nil) seq_len 0 key_len 0
[5853]<DEBUG>1556294489.361027: aruba_driver_set_key 0x5f1484 0x5f153c
[5853]<DEBUG>1556294489.361121: set key: alg 0 key_id 1 tx 0 addr (nil) seq_len 0 key_len 0
[5853]<DEBUG>1556294489.361214: aruba_driver_set_key 0x5f1484 0x5f153c
[5853]<DEBUG>1556294489.361277: set key: alg 0 key_id 2 tx 0 addr (nil) seq_len 0 key_len 0
[5853]<DEBUG>1556294489.361402: aruba_driver_set_key 0x5f1484 0x5f153c
[5853]<DEBUG>1556294489.361464: set key: alg 0 key_id 3 tx 0 addr (nil) seq_len 0 key_len 0
[5853]<DEBUG>1556294489.361558: aruba101: RSN: flushing PMKID list in the driver

[5853]<DEBUG>1556294492.465869: aruba101: State: DISCONNECTED -> ASSOCIATED
[5853]<DEBUG>1556294492.465963: aruba101: Associated to a new BSS: BSSID=32:07:4d:4a:e5:66
[5853]<DEBUG>1556294492.466025: aruba101: Select network based on association information
[5853]<DEBUG>1556294492.466088: aruba_driver_get_ssid 0x5f1484 0x5f153c
[5853]<DEBUG>1556294492.466150: aruba101: Network configuration found for the current AP
[5853]<DEBUG>1556294492.466244: aruba101: WPA: Using WPA IE from AssocReq to set cipher suites
[5853]<DEBUG>1556294492.466307: aruba101: WPA: Selected cipher suites: group 16 pairwise 16
key_mgmt 2 proto 2
[5853]<DEBUG>1556294492.466369: aruba101: WPA: clearing AP WPA IE
[5853]<DEBUG>1556294492.466432: aruba101: WPA: clearing AP RSN IE
[5853]<DEBUG>1556294492.466494: aruba101: WPA: using GTK CCMP
[5853]<DEBUG>1556294492.466588: aruba101: WPA: using PTK CCMP
[5853]<DEBUG>1556294492.466650: aruba101: WPA: using KEY_MGMT WPA-PSK
[5853]<DEBUG>1556294492.466713: WPA: Set own WPA IE default - hexdump(len=22): 30 14 01 00 00 0f
ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 00 00

[5853]<DEBUG>1556294492.495454: aruba101: Event EAPOL_RX (24) received
[5853]<DEBUG>1556294492.495547: aruba101: RX EAPOL from 32:07:4d:4a:e5:66
[5853]<DEBUG>1556294492.495610: aruba101: IEEE 802.1X RX: version=2 type=3 length=151
[5853]<DEBUG>1556294492.495672: aruba101:   EAPOL-Key type=2
[5853]<DEBUG>1556294492.495766: aruba101:   key_info 0x13ca (ver=2 keyidx=0 rsvd=0 Pairwise
Install Ack MIC Secure Encr)
[5853]<DEBUG>1556294492.495829: aruba101:   key_length=16 key_data_length=56
[5853]<DEBUG>1556294492.495891:   replay_counter - hexdump(len=8): 00 00 00 00 00 00 00 02
```

```
[5853]<DEBUG>1556294492.496047:   key_nonce - hexdump(len=32): 57 f3 b7 87 e0 af 0c bd 81 39 7d
6a a3 1c 0e a7 ef 5a df a1 e1 85 b2 3b 49 ee 94 d0 a8 76 00 d6
[5853]<DEBUG>1556294492.496391:   key_iv - hexdump(len=16): 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00
[5853]<DEBUG>1556294492.496672:   key_rsc - hexdump(len=8): 00 00 00 00 00 00 00 00
[5853]<DEBUG>1556294492.496828:   key_id (reserved) - hexdump(len=8): 00 00 00 00 00 00 00 00
[5853]<DEBUG>1556294492.496985:   key_mic - hexdump(len=16): c2 6d 9d cb b2 c9 2a db 0d c7 ec 5c
e3 14 5b d7
[5853]<DEBUG>1556294492.497234: RSN: encrypted key data - hexdump(len=56): 8b e5 09 4e 93 36 09
9c c2 36 c8 31 27 1e ca 09 f2 81 a0 50 80 81 42 90 5a b3 e0 2b 55 ae 97 94 c9 28 48 81 53 7e 48
bc 3a 7e 16 fd 74 15 de 06 63 51 46 40 7a 81 dd 6f
[5853]<DEBUG>1556294492.497828: WPA: decrypted EAPOL-Key key data - hexdump(len=48): 30 14 01 00
00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 0c 00 dd 16 00 0f ac 01 01 00 86 14 3a 8a bc ad
1f 83 24 0e 22 36 10 73 98 0d dd 00
[5853]<DEBUG>1556294492.498390: aruba101: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
[5853]<DEBUG>1556294492.498484: aruba101: WPA: RX message 3 of 4-Way Handshake from
32:07:4d:4a:e5:66 (ver=2)
[5853]<DEBUG>1556294492.498547: WPA: IE KeyData - hexdump(len=48): 30 14 01 00 00 0f ac 04 01 00
00 0f ac 04 01 00 00 0f ac 02 0c 00 dd 16 00 0f ac 01 01 00 86 14 3a 8a bc ad 1f 83 24 0e 22 36
10 73 98 0d dd 00
[5853]<DEBUG>1556294492.500577: aruba101: WPA: Installing PTK to the driver
[5853]<DEBUG>1556294492.500640: aruba_driver_set_key 0x5f1484 0x5f153c
[5853]<DEBUG>1556294492.500702: set key: alg 3 key_id 0 tx 1 addr 0x5fb594 seq_len 6 key_len 16
[5853]<DEBUG>1556294492.501046: EAPOL: External notification - portValid=1
[5853]<DEBUG>1556294492.501139: aruba101: State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE
[5853]<DEBUG>1556294492.501202: RSN: received GTK in pairwise handshake - hexdump(len=18): 01 00
86 14 3a 8a bc ad 1f 83 24 0e 22 36 10 73 98 0d
[5853]<DEBUG>1556294492.501421: WPA: Group Key - hexdump(len=16): 86 14 3a 8a bc ad 1f 83 24 0e
22 36 10 73 98 0d
[5853]<DEBUG>1556294492.501639: aruba101: WPA: Installing GTK to the driver (keyidx=1 tx=0
len=16)
[5853]<DEBUG>1556294492.501702: WPA: RSC - hexdump(len=6): 00 00 00 00 00 00
[5853]<DEBUG>1556294492.501827: aruba_driver_set_key 0x5f1484 0x5f153c
[5853]<DEBUG>1556294492.501920: set key: alg 3 key_id 1 tx 0 addr 0x9988c seq_len 6 key_len 16
[5853]<INFO>1556294492.502358: aruba101: WPA: Key negotiation completed with 32:07:4d:4a:e5:66
[PTK=CCMP GTK=CCMP]
[5853]<DEBUG>1556294492.502420: aruba101: Cancelling authentication timeout
[5853]<DEBUG>1556294492.502483: aruba101: State: GROUP_HANDSHAKE -> COMPLETED
[5853]<INFO>1556294492.502577: aruba101: CTRL-EVENT-CONNECTED - Connection to 32:07:4d:4a:e5:66
completed [id=0 id_str=]
[5853]<DEBUG>1556294492.502764: EAPOL: External notification - portValid=1
[5853]<DEBUG>1556294492.502826: EAPOL: External notification - EAP success=1
[5853]<DEBUG>1556294492.502889: EAPOL: SUPP_PAE entering state AUTHENTICATING
[5853]<DEBUG>1556294492.502951: EAPOL: SUPP_BE entering state SUCCESS
[5853]<DEBUG>1556294492.503014: EAP: EAP entering state DISABLED
[5853]<DEBUG>1556294492.503076: EAPOL: SUPP_PAE entering state AUTHENTICATED
[5853]<DEBUG>1556294492.503108: EAPOL: Supplicant port status: Authorized
[5853]<DEBUG>1556294492.503170: EAPOL: SUPP_BE entering state IDLE
[5853]<DEBUG>1556294492.503233: EAPOL authentication completed - result=SUCCESS
[5853]<DEBUG>1556294498.375398: 32:07:4d:4a:e5:66(2462): nss 2; snr 0; nf 0; level -18; rssi 71
[5853]<DEBUG>1556294498.577522: 32:07:4d:4a:e5:66(2462): nss 2; snr 0; nf 0; level -18; rssi 71
[5853]<DEBUG>1556294498.777397: 32:07:4d:4a:e5:66(2462): nss 2; snr 0; nf 0; level -18; rssi 71
[5853]<DEBUG>1556294498.977491: 32:07:4d:4a:e5:66(2462): nss 2; snr 0; nf 0; level -18; rssi 71
[5853]<DEBUG>1556294500.136816: 32:07:4d:4a:e5:66(2462): nss 2; snr 0; nf 0; level -18; rssi 71
c8:b5:ad:cb:ca:e2#
```

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

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink candidates

WiFi uplink candidates
----------------------
```

```
essid  bssid              channel  rssi  encryption  phy      rank  up time  last update (total
updates)
-----  -----              -------  ----  ----------  ---      ----  -------  --------------------
-------
SG9    32:07:4d:4a:e5:66  11       70    WPA2-psk    VHT-2ss  70/0  28m:27s  2019-05-14
12:20:02(23464)
Total candidates:1;  Current time: 2019-05-14 12:20:02
c8:b5:ad:cb:ca:e2#
```

displaying the WiFi uplink config

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink config

ESSID           :SG9
Cipher Suite    :wpa2-ccmp-psk
Passphrase      :******
Band            :dot11g
c8:b5:ad:cb:ca:e2#
```

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

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink connection-history

WiFi uplink connection history
------------------------------
timestamp            essid  bssid              channel  rssi  result
---------            -----  -----              -------  ----  ------
2019-05-14 11:57:09  SG9    32:07:4d:4a:e5:66  11       71    SUCCESS
2019-05-14 12:15:08  SG9    32:07:4d:4a:e5:66  11       75    SUCCESS
Total connection times:2;  Current time: 2019-05-14 12:22:02
c8:b5:ad:cb:ca:e2#

c8:b5:ad:cb:ca:e2# sh wifi-uplink connection-trace

WiFi uplink connection trace
----------------------------
2019-05-14 11:57:10  auth            ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  retry=no;
tries=0; status=success
2019-05-14 11:57:10  auth            <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  SN=3906;
retry=no; status=0
2019-05-14 11:57:10  assoc req       ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  retry=no;
tries=0; status=success
2019-05-14 11:57:10  assoc resp      <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  SN=3907;
retry=no; status=0
2019-05-14 11:57:10  connection up   *
bssid=32:07:4d:4a:e5:66
2019-05-14 11:57:10  eapol-key       <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=2; len=95
2019-05-14 11:57:10  eapol-key       ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=1; len=117
2019-05-14 11:57:10  eapol-key       <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=2; len=151
2019-05-14 11:57:10  eapol-key       ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=1; len=95
2019-05-14 12:15:06  connection loss  *
bssid=32:07:4d:4a:e5:66
2019-05-14 12:15:06  connection down  *
2019-05-14 12:15:08  auth            ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  retry=no;
tries=0; status=failed
2019-05-14 12:15:08  auth            <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  SN=2491;
retry=no; status=0
2019-05-14 12:15:08  assoc req       ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  retry=no;
tries=0; status=success
2019-05-14 12:15:09  assoc resp      <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  SN=2495;
retry=no; status=0
```

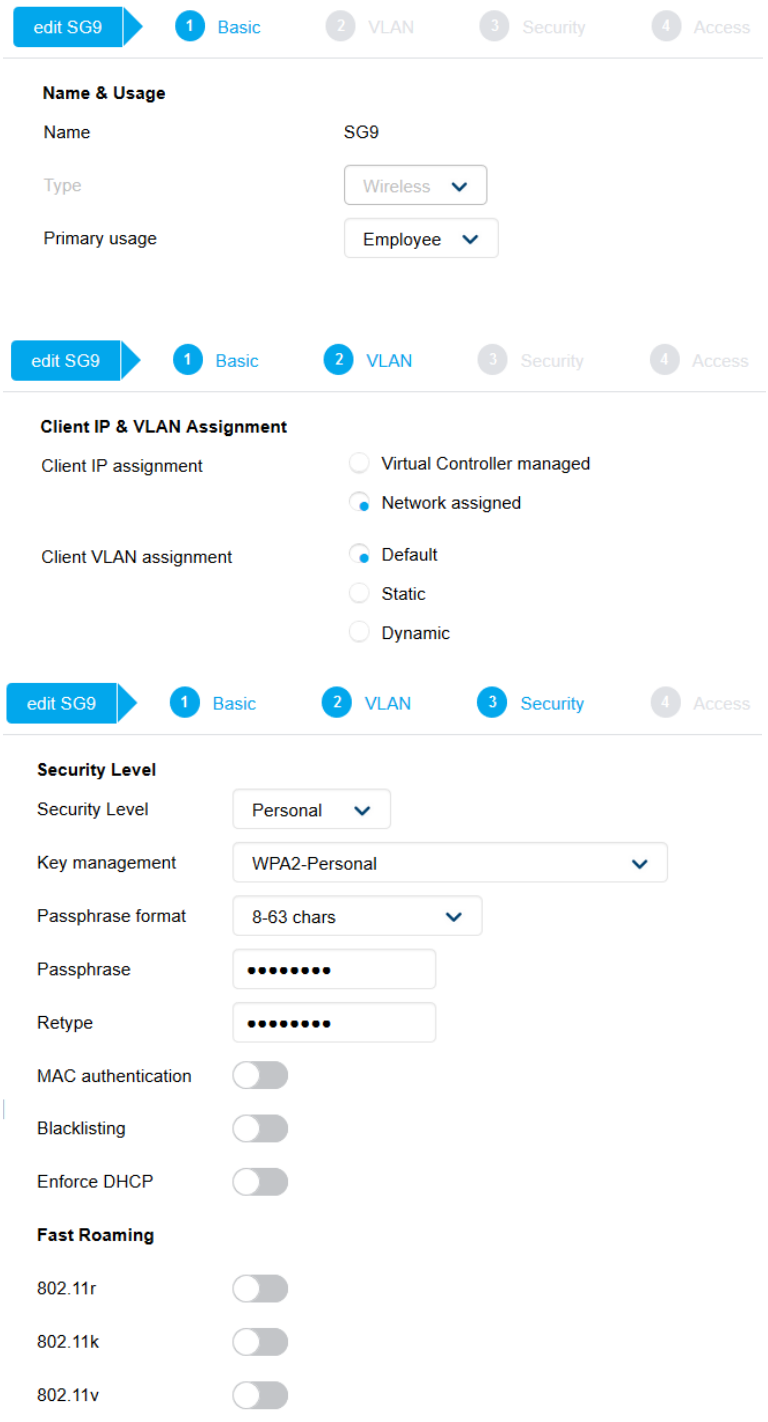
```
2019-05-14 12:15:09  connection up    *
bssid=32:07:4d:4a:e5:66
2019-05-14 12:15:09  eapol-key       <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=2; len=95
2019-05-14 12:15:09  eapol-key       ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=1; len=117
2019-05-14 12:15:09  eapol-key       <-  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=2; len=151
2019-05-14 12:15:09  eapol-key       ->  c8:b5:ad:3c:ae:21  32:07:4d:4a:e5:66  ver=1; len=95
Total connection trace:20;  Current time: 2019-05-14 12:23:11

c8:b5:ad:cb:ca:e2#
```

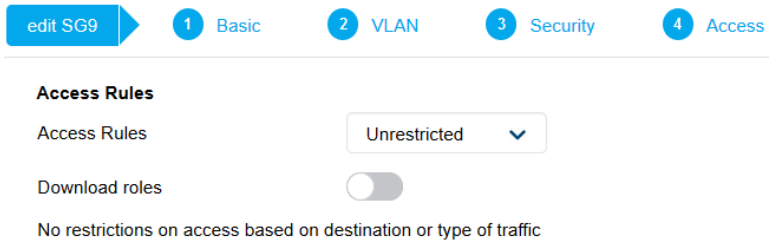
4 WiFi Uplink to Existing Instant Cluster

Here we are demonstrating that a standalone 11ac IAP can have a WiFi uplink to an existing Instant cluster. You need to ensure that the Instant cluster is also running version 8.5 or later. Also note that you cannot combine Mesh and WiFi uplink. You can have one or the other.

4.1 Instant Cluster Configuration

Here we have just added a WLAN network called SG9 that is broadcasting only on 2.4GHz. This is because the existing standalone IAP is configured to connect to SG9 WLAN on 2.4GHz band.





4.2 Testing

First let's check the Aruba Instant Cluster that is broadcasting SG9, note the BSS address.

```
BLDG-A-ATV1# sh ap bss-table

Aruba AP BSS Table
------------------
bss                ess  port  ip              phy    type  ch/EIRP/max-EIRP  cur-cl  ap name
in-t(s)  tot-t         flags
---                ---  ----  --              ---    ----  ----------------  ------  -------
-------  -----         -----
24:f2:7f:d5:fa:d0  SG1  ?/?   192.168.1.121   a-VHT  ap    36E/23.0/23.0     4       BLDG-A-ATV1
0        5d:6h:52m:2s
24:f2:7f:d5:fa:c0  SG1  ?/?   192.168.1.121   g-HT   ap    1/9.0/22.1        1       BLDG-A-ATV1
0        5d:6h:52m:1s
24:f2:7f:d5:fa:c1  SG9  ?/?   192.168.1.121   g-HT   ap    1/9.0/22.1        1       BLDG-A-ATV1
0        1h:16m:31s

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:3
Num Associations:6

Flags:       K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = OWE Transition mode OWE
BSS; o = OWE Transition mode Open BSS; M = WPA3-SAE mixed mode BSS
BLDG-A-ATV1#
```

Now we go to the standalone IAP to check the uplink.

```
c8:b5:ad:cb:ca:e2# sh uplink status

Uplink preemption             :enable
Uplink preemption interval    :300
Uplink enforce                :none
Ethernet uplink bond0        :DHCP
Uplink Table
------------
Type      State  Priority  In Use
----      -----  --------  ------
eth0      UP     10        Yes
Wifi-sta  Probe   9         No
3G/4G     INIT   11        No
Internet failover                       :disable
Max allowed test packet loss            :10
Secs between test packets               :30
VPN failover timeout (secs)             :180
Internet check timeout (secs)           :10
```

```
ICMP pkt sent        :0
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE

c8:b5:ad:cb:ca:e2#
c8:b5:ad:cb:ca:e2# sh ip int b
Interface                        IP Address / IP Netmask       Admin  Protocol
br0                            10.10.10.100 / 255.255.255.0    up     up
br0.3333                        172.31.98.1 / 255.255.254.0    up     up
c8:b5:ad:cb:ca:e2#
```

Note the IP address of br0, it is from the Eth0 which is on VLAN 10.

Then we see these messages on the standalone IAP's console, looks like the uplink has just associated.

```
[  660.321805] wlan_mlme_app_ie_delete: appie is NULL. Do nothing.
[  661.505841] wlan_mlme_app_ie_delete: appie is NULL. Do nothing.
[  662.603030] wmi_unified_set_psmode:set psmode=1
[  662.646516] wmi_unified_set_psmode:set psmode=0
[  662.702030] VAP device aruba101 created osifp: (dc4d9540) os_if: (d50d8000)
[  665.718306] ieee80211_connection_state_connecting_entry:701, enter......,sm-
>candidate_aplist_index = 0
[  665.818369] wlan_assoc_sm_start:914, enter......
[  665.873602] ieee80211_assoc_state_init_event:149, enter......, event 0
[  666.160293] ieee80211_assoc_state_join_event:204, goto AUTH
[  666.214526] wlan_mlme_auth_request:354, enter >>>>>>>>>>
[  666.288659] aruba_set_vdev_rawmode at line 8768, retv = 22
[  666.343705] aruba_configure_fw_mode 8805
[  666.390690] ieee80211_assoc_state_assoc_event:340, ASSOC sucess and transition to RUN state
[  668.456544] asap_firewall_device_update, firewall dev changed to aruba101, addr changed to
c8:b5:ad:3c:ae:21
[  669.808622] asap_send_elected_master: sent successfully
```

Now lets run some of the WiFi uplink commands

```
c8:b5:ad:cb:ca:e2# sh uplink status

Uplink preemption             :enable
Uplink preemption interval    :300
Uplink enforce                :none
Ethernet uplink bond0        :DHCP
Uplink Table
------------
Type      State  Priority  In Use
----      -----  --------  ------
eth0      UP     10        No
Wifi-sta  UP     9         Yes
3G/4G     INIT   11        No
Internet failover                       :disable
Max allowed test packet loss            :10
Secs between test packets               :30
VPN failover timeout (secs)             :180
Internet check timeout (secs)           :10
ICMP pkt sent        :0
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0
AP1X type:NONE
Certification type:NONE
```

```
Validate server:NONE
c8:b5:ad:cb:ca:e2#
```

As soon the standalone IAP has a successful WiFi uplink and gets an IP address, it will replace its previous IP address it got from Eth0.

```
c8:b5:ad:cb:ca:e2# sh ip int b
Interface                          IP Address / IP Netmask       Admin  Protocol
br0                              192.168.1.126 / 255.255.255.0     up     up
br0.3333                           172.31.98.1 / 255.255.254.0     up     up
c8:b5:ad:cb:ca:e2#
```

Checking the status of the uplink again.

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink status

Configured                    :YES
Enabled                       :YES
Interfaces                    :aruba101
Now                           :2019-05-15 18:34:55
SSID                          :SG9
BSSID                         :24:f2:7f:d5:fa:c1
Unitcast/Multicast Encryption:wpa2-aes-psk wpa2-aes-psk
Link Health                   :100
AID                           :1
Associated Time               :1m:29s
Associated AP Beacon Time     :5d:5h:45m:8s
Channel                       :1
RSSI                          :47
Noise Floor                   :94
Phy                           :2.4GHz-HT-20sgi-2ss
Maximum Speed (mbps)          :144
Overall/Tx/Rx Goodput (mbps) :12.8 11.2 14.3
Last Tx Timestamp             :2019-04-27 02:10:59
Last Rx Timestamp             :2019-04-27 02:11:02
Last Tx Rate (mbps)           :104
Last Rx Rate (mbps)           :144
Last ACK RSSI                 :43
c8:b5:ad:cb:ca:e2#
```

Now lets check the connection history and trace

```
c8:b5:ad:cb:ca:e2# sh wifi-uplink connection-his

WiFi uplink connection history
------------------------------
timestamp            essid  bssid              channel  rssi  result
---------            -----  -----              -------  ----  ------
2019-05-15 18:33:25  SG9    24:f2:7f:d5:fa:c1  1        44    SUCCESS
2019-05-15 18:33:25  SG9    24:f2:7f:d5:fa:c1  1        50    SUCCESS
Total connection times:2;  Current time: 2019-05-15 19:40:55


c8:b5:ad:cb:ca:e2# sh wifi-uplink connection-trace

WiFi uplink connection trace
----------------------------
```

```
2019-05-15 18:33:26  auth             ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  retry=no;
tries=0; status=success
2019-05-15 18:33:26  auth             <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  SN=161; retry=no;
status=0
2019-05-15 18:33:26  assoc req        ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  retry=no;
tries=0; status=success
2019-05-15 18:33:26  assoc resp       <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  SN=162; retry=no;
status=0
2019-05-15 18:33:26  connection up    *
bssid=24:f2:7f:d5:fa:c1
2019-05-15 18:33:26  eapol-key        <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=117
2019-05-15 18:33:26  eapol-key        ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=117
2019-05-15 18:33:26  eapol-key        <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=151
2019-05-15 18:33:26  eapol-key        ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=95
2019-05-15 19:13:43  connection loss  *
bssid=24:f2:7f:d5:fa:c1
2019-05-15 19:13:43  connection down  *
2019-05-15 19:13:43  auth             ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  SN=0; retry=no;
status=0
2019-05-15 19:13:43  auth             <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  SN=1524;
retry=no; status=0
2019-05-15 19:13:43  assoc req        ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  retry=no;
tries=0; status=success
2019-05-15 19:13:44  assoc resp       <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  SN=1525;
retry=no; status=0
2019-05-15 19:13:44  connection up    *
bssid=24:f2:7f:d5:fa:c1
2019-05-15 19:13:44  eapol-key        <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=117
2019-05-15 19:13:44  eapol-key        ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=117
2019-05-15 19:13:44  eapol-key        <-  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=151
2019-05-15 19:13:44  eapol-key        ->  c8:b5:ad:3c:ae:21  24:f2:7f:d5:fa:c1  ver=1; len=95
Total connection trace:20;  Current time: 2019-05-15 19:41:06
c8:b5:ad:cb:ca:e2#
```

Here note that "`c8:b5:ad:3c:ae:21`" is the MAC address of the standalone IAP "`24:f2:7f:d5:fa:c1`" is the BSS address for SG9 from the instant Cluster.

Here is the client list on the Instant cluster and we see the standalone IAP. Check its MAC address.

```
BLDG-A-ATV1# show client

Client List
-----------
Name              IP Address     MAC Address        OS       ESSID  Access Point  Channel  Type
Role          IPv6 Address                              Signal    Speed (mbps)
----              ----------     -----------        --       -----  ------------  -------  ----  -
---           ------------                                 ------    ------------
DESKTOP-VUTSS58  192.168.1.124  18:56:80:16:c3:d5  Win 10   SG1    BLDG-A-ATV1   36E      AC
SG1           fd14:5f94:8156:2600:f5d9:49fc:fc6c:f151  27(good)  263(good)
                 192.168.1.126  c8:b5:ad:3c:ae:21           SG9    BLDG-A-ATV1   1        GN
SG9           --                                         50(good)  144(good)
Number of Clients   :2
Info timestamp      :458102
BLDG-A-ATV1#
```

Now when we connect a WiFi client to SG2 which is the SSID that standalone IAP is advertising, we see that it is getting an IP adress from the standalone IAP and it is getting source NAT as indicatd by the output of the "show datapath session" command.

```
c8:b5:ad:cb:ca:e2# sh client

Client List
```

```
-----------
Name          IP Address    MAC Address        OS    ESSID  Access Point       Channel  Type
Role  IPv6 Address               Signal    Speed (mbps)
----          ----------    -----------        --    -----  ------------       -------  ----  ---
-  ------------               -------    ------------
ariyaps-iPad  172.31.99.33  a4:d1:d2:5f:32:52  iPad  SG2    c8:b5:ad:cb:ca:e2  149      AN    SG2
fe80::1016:5191:c8f2:7703  68(good)  52(good)
Number of Clients   :1
Info timestamp      :6221
c8:b5:ad:cb:ca:e2#
c8:b5:ad:cb:ca:e2# sh ip int b
Interface                        IP Address / IP Netmask       Admin  Protocol
br0                            192.168.1.126 / 255.255.255.0    up     up
br0.3333                        172.31.98.1 / 255.255.254.0     up     up
c8:b5:ad:cb:ca:e2#

c8:b5:ad:cb:ca:e2# 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
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    192.168.1.126   6    443   59088 0    0    0   24  dev24       7a9  0       0
N
192.168.1.126     192.168.1.128   17   161   58527 0    0    0   0   dev23       28   0       0
FY
192.168.1.126     192.168.1.124   17   2054  61168 0    0    0   1   dev23       49   0       0
FY
192.168.1.128     192.168.1.126   17   58527 161   0    0    0   1   dev23       28   0       0
FYC
17.252.252.85     192.168.1.126   6    443   59075 0    0    0   13  dev24       165c 0       0
N
172.31.99.33      40.100.151.130  6    59088 443   0    0    0   25  dev24       7a9  0       0
SC
172.31.99.33      17.252.252.85   6    59075 443   0    0    0   13  dev24       165c 0       0
SC
192.168.1.124     192.168.1.126   17   61168 2054  0    0    0   1   dev23       49   0       0
FYC

c8:b5:ad:cb:ca:e2#
```