1 Table of Contents

Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
11 Nov 2019	0.1	Ariya Parsamanesh	Initial creation

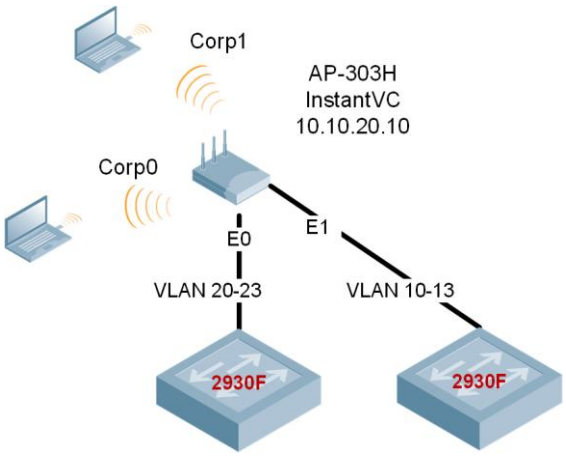
2 Segregated Networks Using Instant APs

There are a number cases for small deployments where you need to have complete segregation between two wirelesses SSIDs mapped to two separate network on separate switches. So here in this technote we'll explore how to set this up with Aruba IAPs.

This is the scenario that we want to implement.

WLAN SSID	IAP Eth interface	Native VLAN	Allowed VLANS
Corp0	E0	20	21-23
Corp1	E1	10	11-13

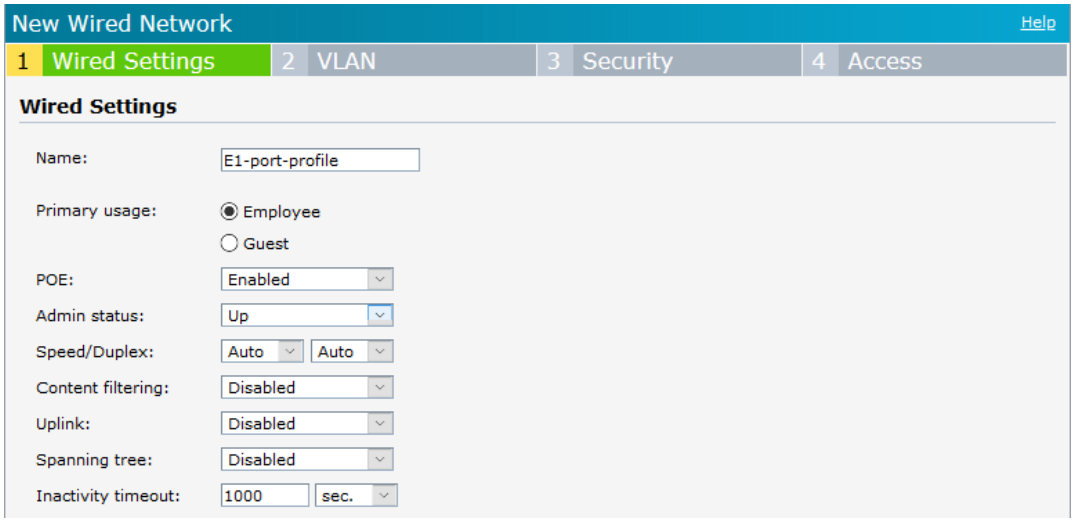
We have an AP that is broadcasting two SSIDs, but we want one of the SSIDs to be mapped to E0 and the other to E1 ports with completely separates VLANs.

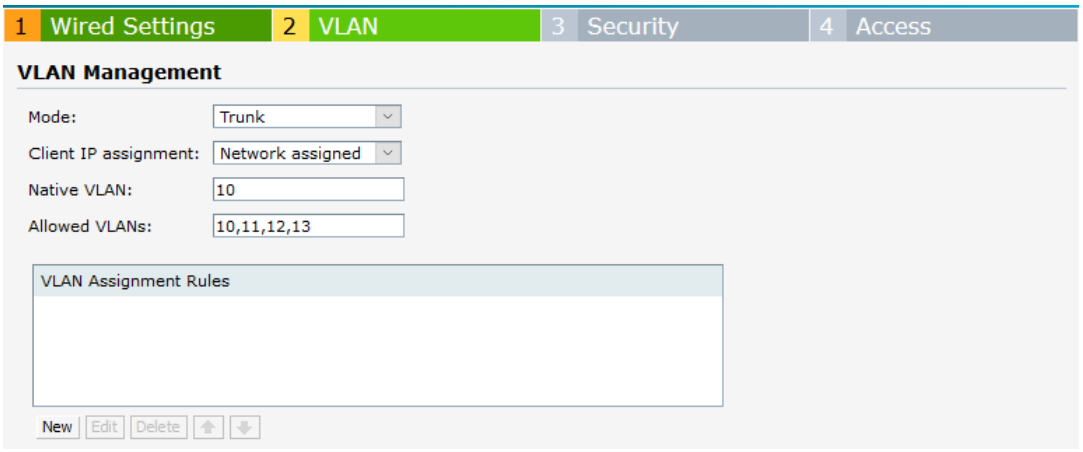


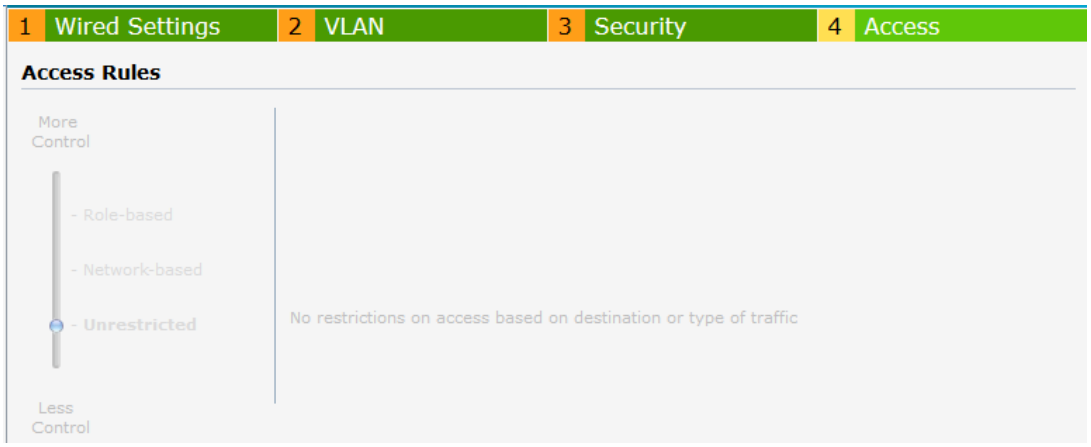
Even though Instant APs only support one wired uplink, here we are design a pseudo second wired uplink, and we need to ensure that IAP is not configured for DHCP or NAT services.

2.1 Instant AP Wired Profile Configuration

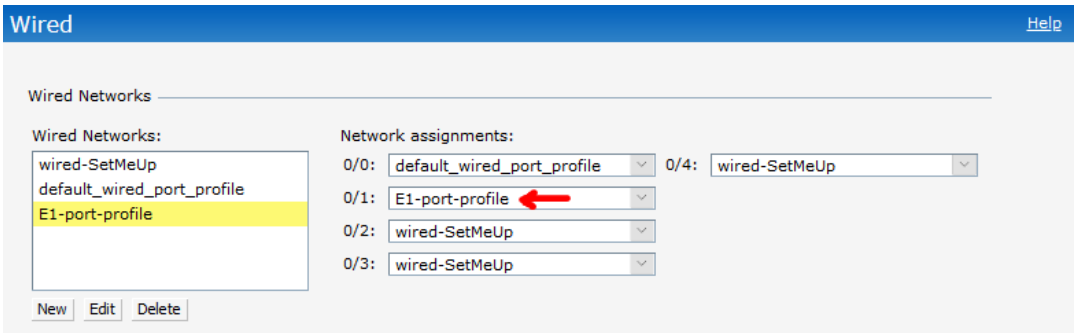
Here we'll create a new port profile for E1.



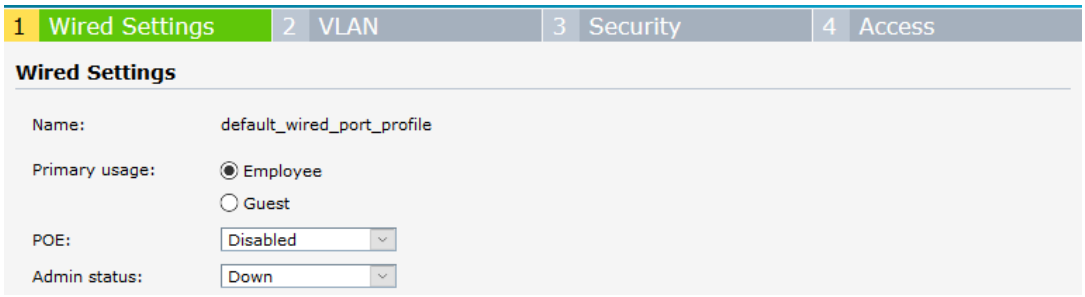


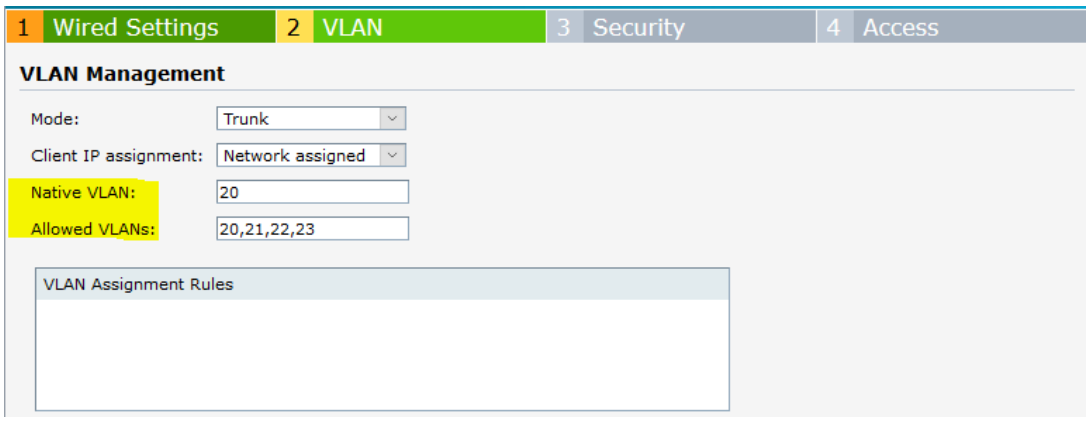


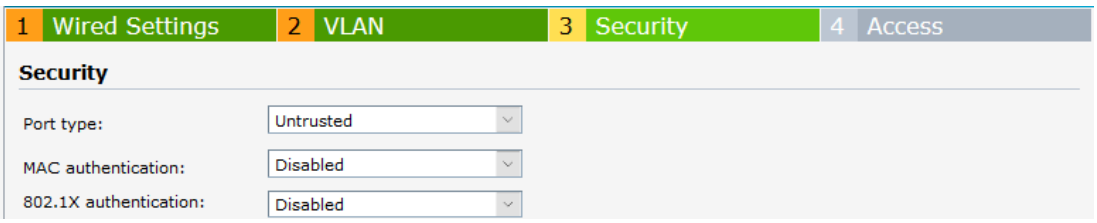
Now we'll assign it to E1 port.



Now we also ensure that the "default_wired_port_profile" is configured correctly as well







Here is the show command to check the configuration.

```
20:4c:03:17:a0:4c# show wired-port-settings

Wired Port Profiles
-------------------
Name                        VLAN Mode  Allowed VLANs  Native VLAN  Admin Status  Role
Speed  Duplex  POE  In Use  Authentication Method  STP  Trusted
----                        ---------  -------------  -----------  ------------  ----

wired-SetMeUp               Access     all            guest        Up            wired-SetMeUp
auto   auto    No   Yes     None                   No   No


default_wired_port_profile  Trunk      20,21,22,23    20           Down
default_wired_port_profile  auto   full    No   Yes     None                   No   No

E1-port-profile             Trunk      10,11,12,13    10           Up            E1-port-profile
auto   auto    Yes  Yes     None                   No   Yes
Port Profile Assignments
------------------------
Port  Profile Name
----  ------------
0     default_wired_port_profile
1     E1-port-profile
2     wired-SetMeUp
3     wired-SetMeUp
4     wired-SetMeUp
20:4c:03:17:a0:4c#
```

Important thing to note is that the VLANs for E0 and E1 should not overlap otherwise IAP has no way of knowing which port to use.

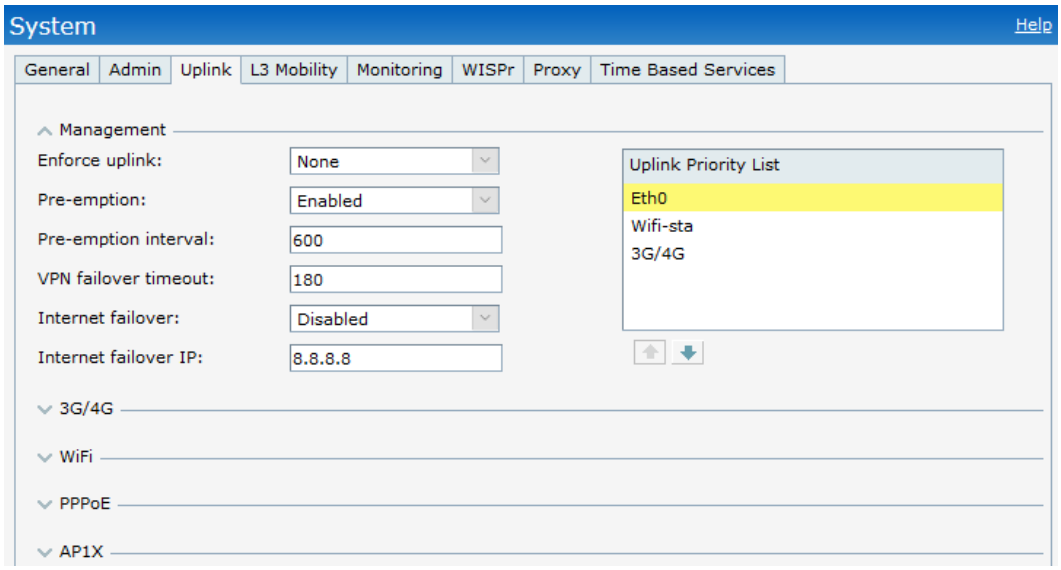
2.2 Wireless Configuration

Here we'll create two WLANs Corp0 and Corp1

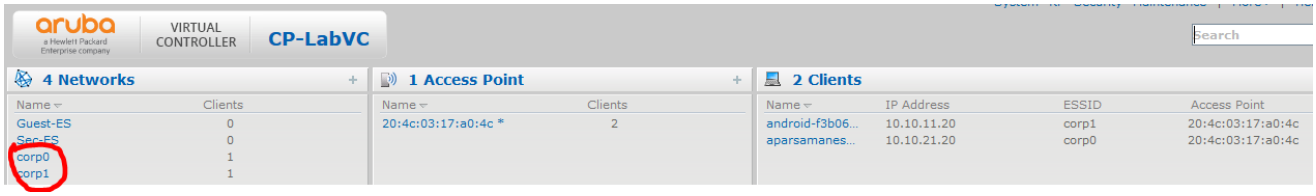
```
wlan ssid-profile corp0
 enable
 index 2
 type employee
 essid corp0
 wpa-passphrase bad428ffcb91810207a479d466f3ae8910ae732dc0750d8f
 opmode wpa2-psk-aes
 max-authentication-failures 0
 vlan 21
 rf-band all
 captive-portal disable
 dtim-period 1
 broadcast-filter arp
 dmo-channel-utilization-threshold 90
 local-probe-req-thresh 0
 max-clients-threshold 64

wlan ssid-profile corp1
 enable
 index 3
 type employee
 essid corp1
 wpa-passphrase 8aaeb0d3fa292ef769140914c8eb056b10d352889ef2581b
 opmode wpa2-psk-aes
 max-authentication-failures 0
 vlan 11
 rf-band all
 captive-portal disable
 dtim-period 1
 broadcast-filter arp
 dmo-channel-utilization-threshold 90
 local-probe-req-thresh 0
 max-clients-threshold 64
```

2.3 Uplink configuration

This is just to show we have not made any changes to the default configuration.



2.4 Testing



Here we can see the clients are on different subnets and are completely isolated from one another.

```
20:4c:03:17:a0:4c# sh client

Client List
-----------
Name                        IP Address    MAC Address         OS  ESSID  Access Point
Channel  Type  Role    IPv6 Address                Signal     Speed (mbps)
----                        ----------    -----------         --  -----  ------------
-------  ----  ----    ------------                ------     ------------
aparsamanesh-t400           10.10.21.20   00:21:6a:47:8c:9c       corp0
20:4c:03:17:a0:4c  52+       AN     corp0  --                            52(good)
300(good)
android-f3b06cc9a661b537    10.10.11.20   9c:02:98:8c:8a:47       corp1
20:4c:03:17:a0:4c  1         GN     corp1  fe80::9e02:98ff:fe8c:8a47  43(good)
52(good)
Number of Clients    :2
Info timestamp       :6388
20:4c:03:17:a0:4c#
20:4c:03:17:a0:4c#
192.168.1.130     10.10.11.20     17   53    57229 0    0    0   0   dev26       1b   1
51    FI
10.10.21.20       192.168.1.130   17   58972 53    0    0    0   1   dev23       2c   0
0     FCI
20:4c:03:17:a0:4c#
20:4c:03:17:a0:4c#
20:4c:03:17:a0:4c#
20:4c:03:17:a0:4c# 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
---------------   --------------  ---- ----- ----- ---- ---- --- --- ----------- ---- -------
-----  -----
10.10.11.20       8.8.8.8         17   31745 53    0    0    0   0   dev26       4f   1
3f    FCI
```

```
10.10.11.20       8.8.8.8          17   50562 53    0    0    0    0   dev26       1a   2
94    FCI
8.8.8.8           10.10.11.20      17   53    50562 0    0    0    0   dev26       1a   0
0     FYI
77.234.41.236     10.10.21.20      6    80    1511  0    0    0    1   dev23       64   0
0     Y
10.10.21.20       255.255.255.255 17   1494  43440 0    0    0    0   dev23       6    0
0     FYCIEm
8.8.8.8           10.10.11.20      17   53    31745 0    0    0    1   dev26       4f   0
0     FYI
10.10.11.20       8.8.8.8          17   61649 53    0    0    0    0   dev26       1d   2
7e    FCI
10.10.11.20       8.8.8.8          17   23058 53    0    0    0    0   dev26       1d   2
80    FCI
8.8.8.8           10.10.11.20      17   53    34747 0    0    0    1   dev26       51   0
0     FYI
255.255.255.255   10.10.21.20      17   43440 1494  0    0    0    0   dev23       6    0
0     FYIEm
10.10.21.20       77.234.41.236    6    1511  80    0    0    0    0   dev23       64   1
40    YC
10.10.11.20       8.8.8.8          17   45110 53    0    0    0    0   dev26       1f   2
82    FCI
20:4c:03:17:a0:4c#
```

Note that the LAN switches connected to each of the IAP's Eth ports should only allow those specific VLANs.