1 Table of Contents

Table of Contents

1 Table of Contents 1

1.1 Revision History 1
2 IAP-VPN with Aruba Instant 2

2.1 Things you need 3
3 Instant VC VPN with Centralised L2 4

3.1 Aruba Instant General Configuration 4
3.2 Aruba Instant VPN Configuration 6
3.3 Aruba Controller Configuration 8
3.4 Testing the IPSEC Tunnel – Controller 10
3.5 Testing the IPSEC Tunnel – Instant AP 13
3.6 Client Testing 15
4 3G/4G Backup 18

4.1 VPN Configuration 18
4.2 Routing Profile Configuration 18
4.3 Uplink Configuration 18
4.4 Backup Link Testing 20
4.5 Client Testing 26
5 Instant VC VPN with Distributed L3 28

5.1 DHCP Configuration 28
5.2 E1 Port Configuration 28
5.3 Testing 30

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 April 2019	0.1	Ariya Parsamanesh	Initial creation
20 April 2019	0.2	Ariya Parsamanesh	Added the DL3 section

2 IAP-VPN with Aruba Instant

This is a short design and configuration guide for configuring IPSEC VPN from Aruba Instant APs (IAP) to an Aruba VPN concentrator (VPNC) in DMZ. The main aim here is to show case two of the most common forwarding modes namely Centralised L2 and Distributed L3.

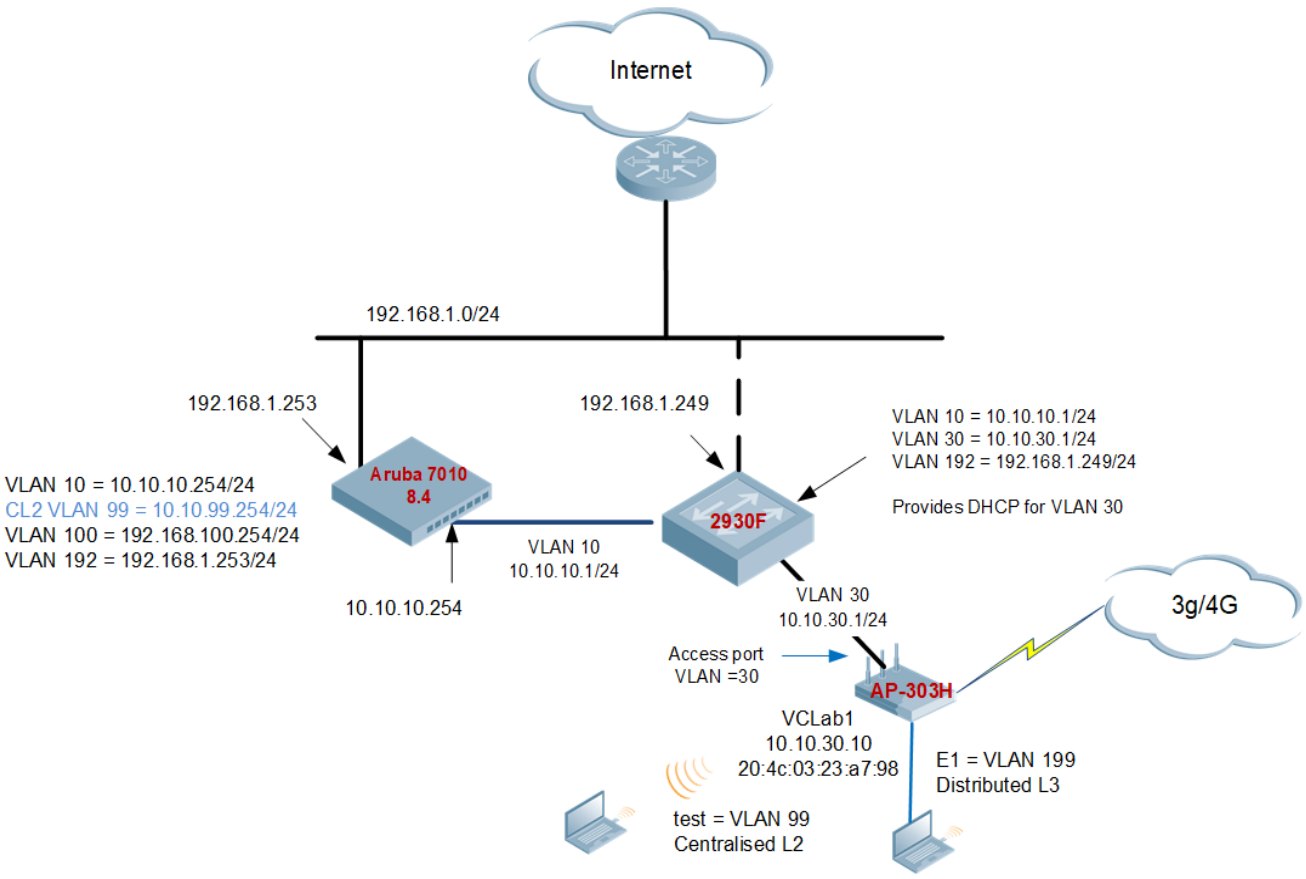
I will also demonstrate the new feature that provides pre-emption enhancement for IAP-VPN. With this feature IAPs can detect the reachability of a primary VPN over the Ethernet uplink without bringing the 3G/4G link down. Here we'll use two failover IP addresses one for each of the uplinks. (Ethernet and 3G/4G)

This document will not cover the in-depth IAP-VPN architecture, for that please refer to the "Aruba Instant Validated Reference Design".

With Centralised L2, the AP acting as Virtual Controller (VC) brings up an L2 GRE tunnel inside the IPSEC tunnel traversing the WAN to extend the VLAN to the VPNCs. Traffic going to the rest of the corporate network would be placed inside the L2 GRE tunnel, and local-breakout traffic would be source-natted. In this mode the clients will get IP addresses from the DHCP server on the controller or in the head-end network.

With Distributed L3, the AP acting as VC acts as branch gateway for those subnets. Traffic going to the rest of the corporate network would be routed through the tunnels and the DHCP services are provided by the local IAP cluster. Here the routes for branches are dynamically added to the head-end VPN controller.

For this demonstration we'll setup a TEST SSID on the IAP (operating in Centralised L2 mode) which is tunneled to Aruba controller in DMZ. We will also configure the E1 port of the IAP (AP-303H has 4x GigE ports) to be operating in Distributed L3 mode.



One of the newer features in this IAP firmware (8.4.x) is "Cellular Uplink Preemption". With this preemption enhancement for IAP-VPN, the IAPs can detect the reachability of a primary VPN over the Ethernet uplink by simultaneously keeping the secondary 3G/4G uplink stable.

2.1 Things you need

- Aruba Instant version 8.4.0.0 or later
- Aruba controller version 8.4.0.0 or later (standalone)
- A Layer three device to simulate a router shown
- Some WiFi and wired clients
- 3G/4G modem/dongle

Here are the IAP VPN branch limits for the various controller models that help in the overall design.

Controller	IAP VPN Branch Limit	Route Limit	VLAN Limit
7240	8192	32769	4094
7220	4096	32769	4094
7010	2048	32769	4094
7205	1024	16381	2048
7030	256	8189	256
7024	128	4093	128
7010	128	4093	128
7008	64	4093	128
7005	64	4093	128

You should note that IAP-VPN are completely supported on Aruba SD-Branch solution. So you could have micro branches that require just an IAP or small branches that require more than one IAP but still smaller that branches that require a branch gateways, to create VPN tunnels to the same VPNCs that are used for the Branch Gateways. This becomes a very cost effective solution.

For more information on our SD-Branch solution you can refer here.

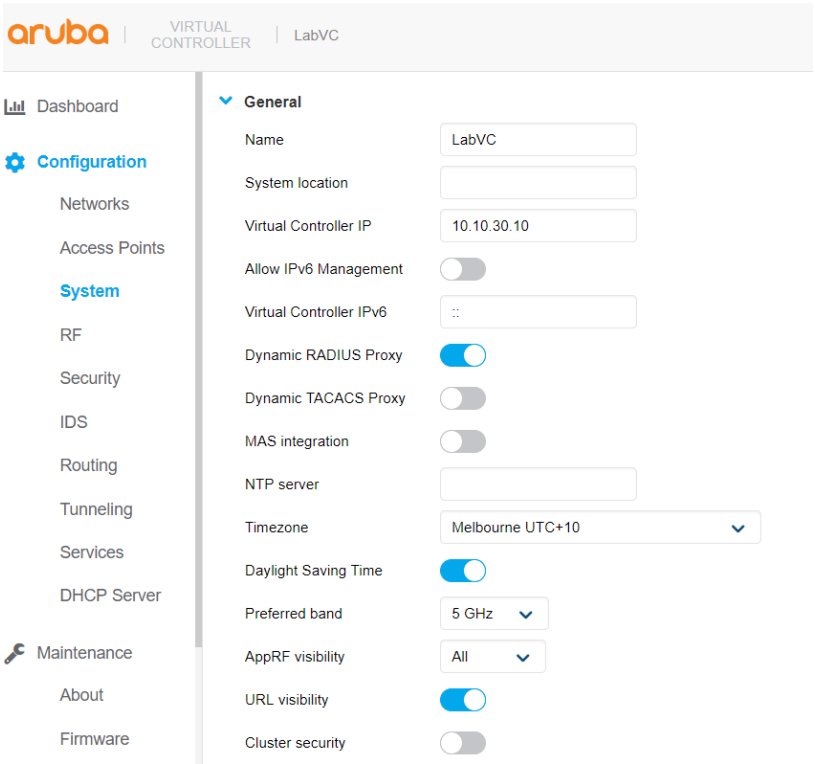
3 Instant VC VPN with Centralised L2

In an IAP-VPN solution (with Instant version 8.4.0) you need to select your Forwarding modes. The forwarding modes determine if the DHCP server and default gateway for clients are in the branch or at the VPN concentrator in datacentre or the head-end. These modes do not determine the firewall processing or traffic forwarding functionality. The virtual controller enables different DHCP pools (various assignment modes) in addition to allocating IP subnets for each branch.

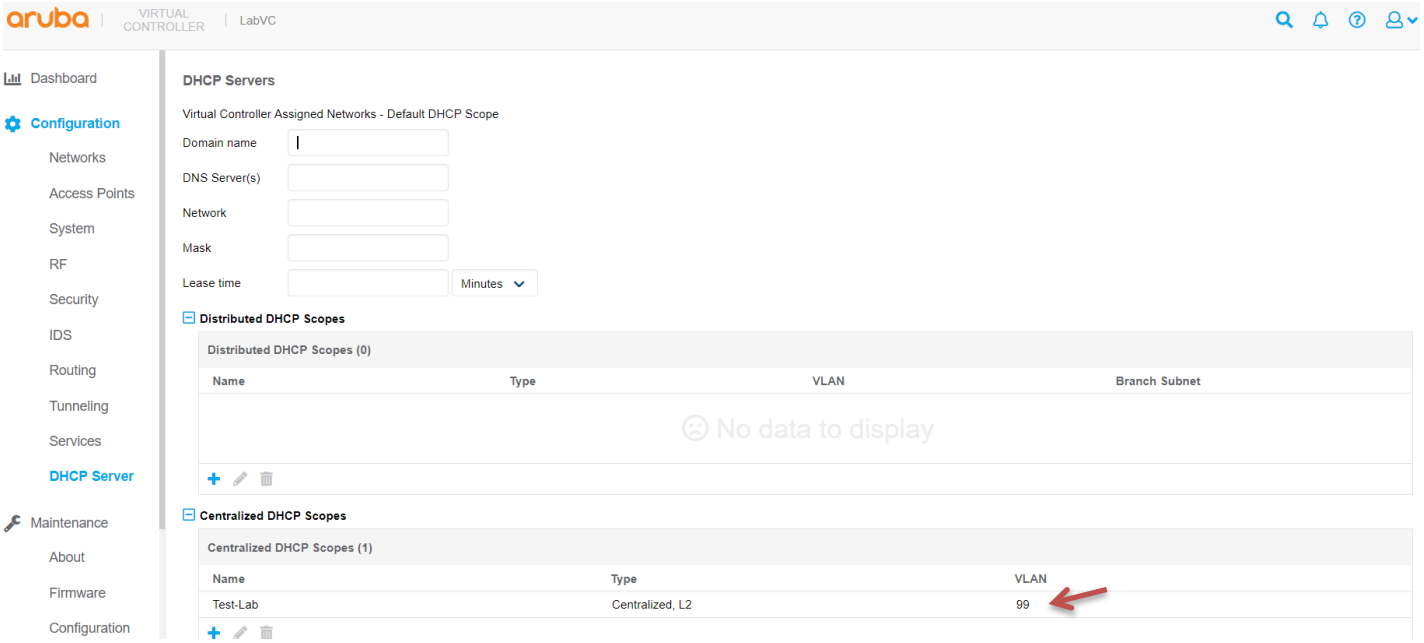
Here we'll be configuring Centralised L2 and later in the document Distributed L3.

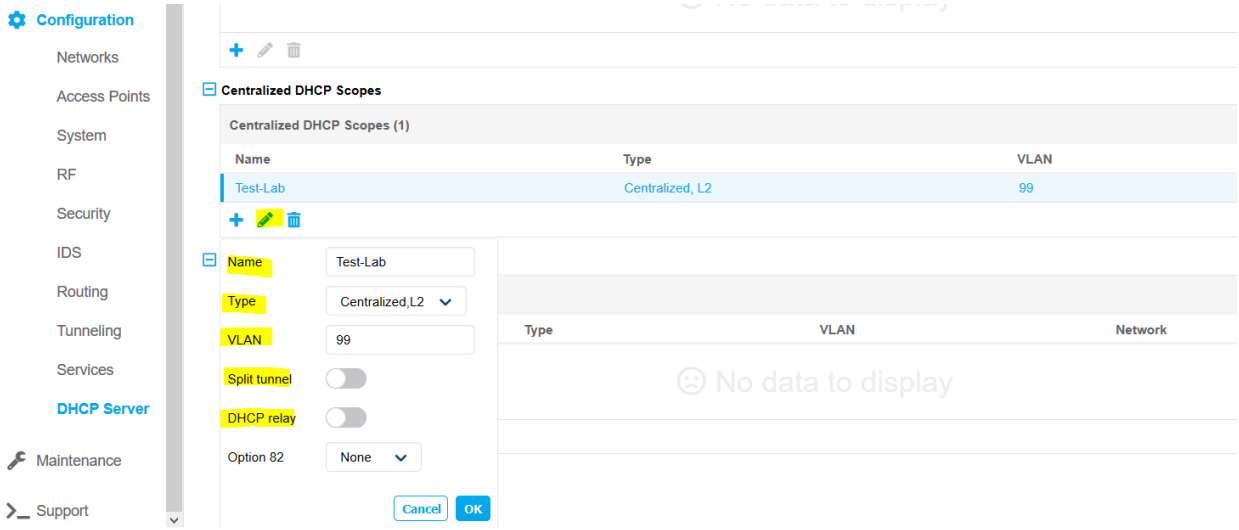
3.1 Aruba Instant General Configuration

Here is the Instant VC configuration

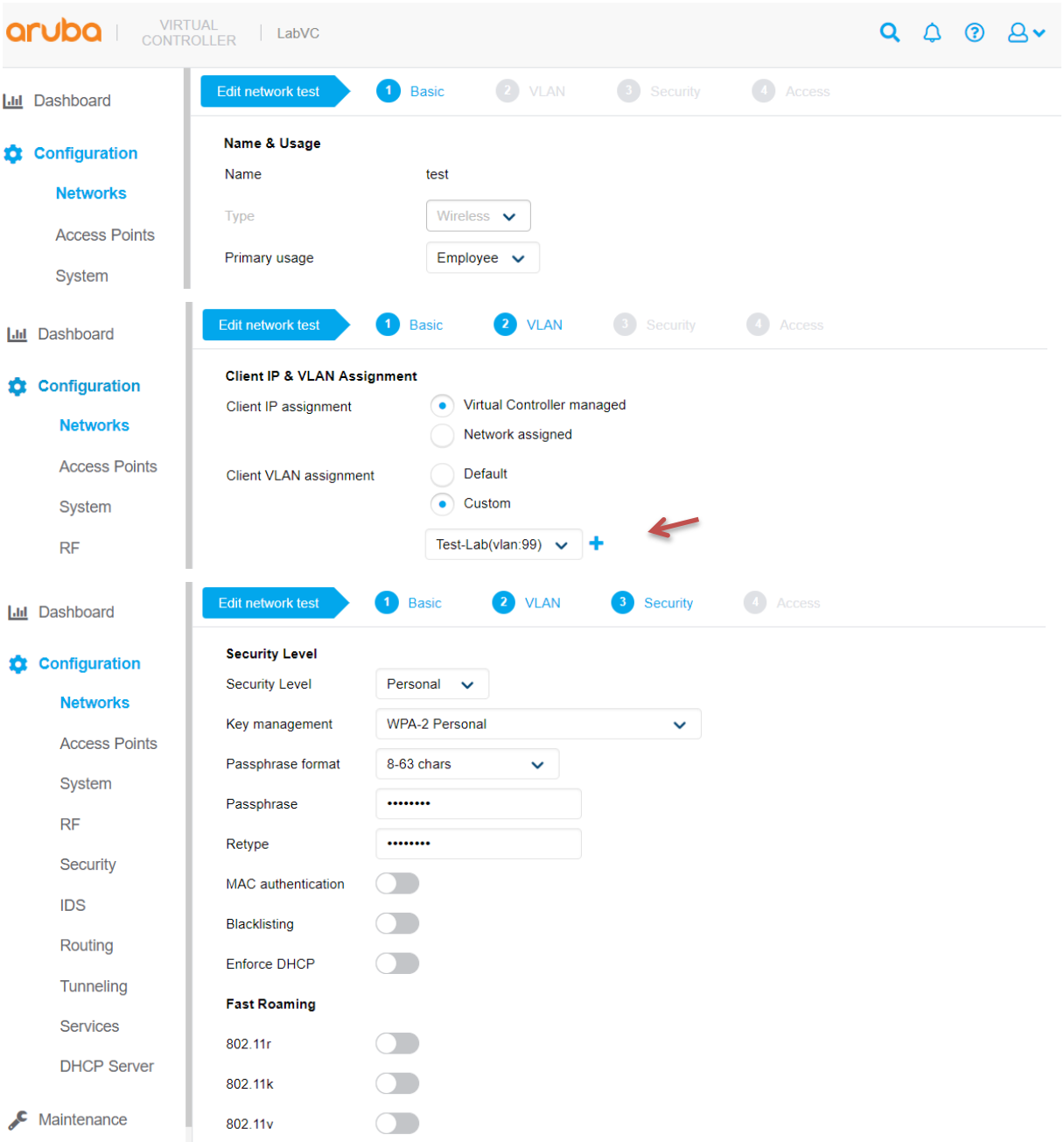


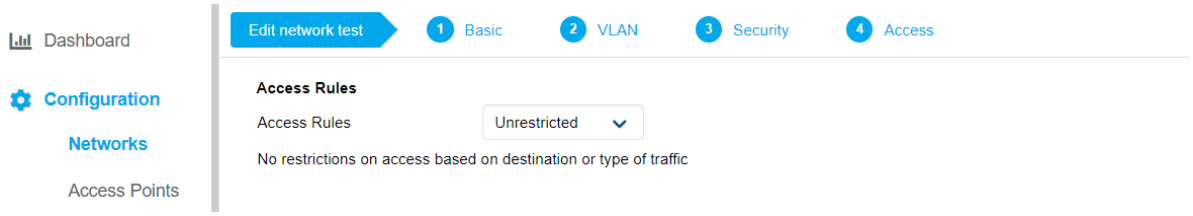
Here is the DHCP configuration and we are using Centralized L2 mode, the DHCP server and default gateway are located in the corporate network (controller or in the same L2 behind controller).





Note that we have an option to use spit tunnel functionality, but because we have disabled the split tunnel functionality all the traffic from VLAN 99, will be sent through the IPSEC Tunnel. For ease of configuration I will configure a PSK based WLAN which will be tunneled back to the DMZ.





3.2 Aruba Instant VPN Configuration

Aruba Instant VPN gives you four options:

1. Aruba IPSEC
2. Aruba GRE
3. L2TPv3
4. Manual GRE

In most of the cases you will either use Aruba IPSEC or Aruba GRE. Here we'll be covering Aruba IPSEC but wanted to give a general description of how they differ.

Aruba GRE Protocol

- It uses both IPSEC (For controller traffic like BID allocation) and GRE (For user/client traffic), once a primary host IP address is configured in the tunnel section on IAP, the IAP forms an IPSEC with controller.
- the controller will provide the following to IAP
  - management IP address of controller(10.10.10.254 in our case)
  - the available Inner IP address to IAP (10.66.66.11 in our configuration from the VPN pool)
- All the client/user traffic destined to controller will be encapsulated with GRE header from IAP with the destination IP address of the GRE packet as management IP address of controller. Now since this mgmt. IP address is not routable over Internet, this approach is generally used in MPLS network that the mgmt. IP address of the controller is reachable.

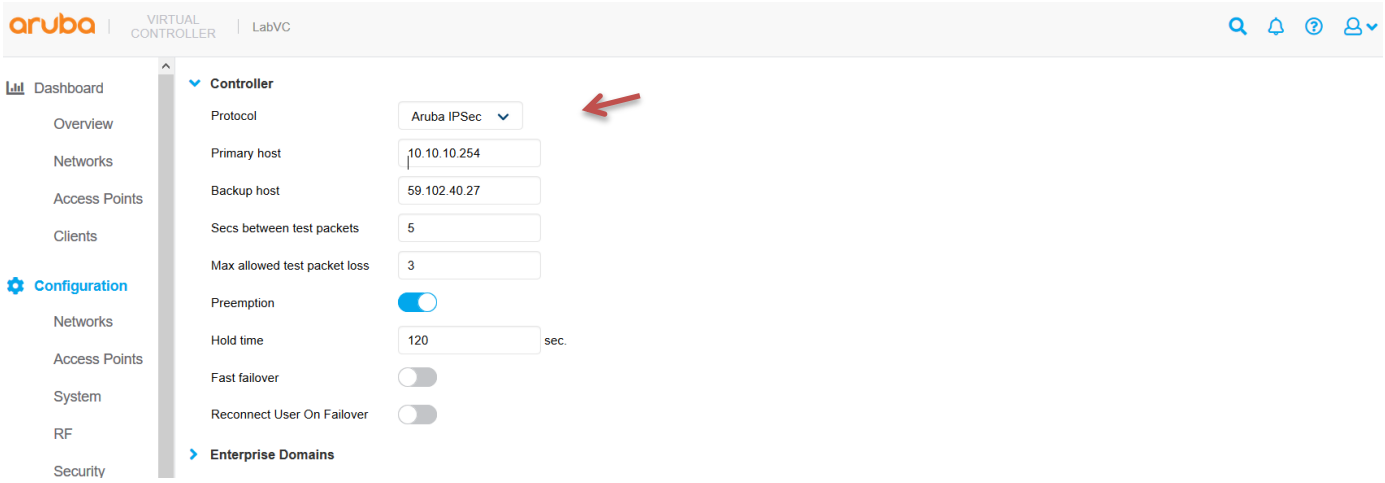
But when using Aruba IPSEC

- The main difference is that Aruba IPSEC can encapsulate the GRE packets. So as before upon establishment of IPSEC the controller will provide the mgmt. IP address of the inner IP address to the IAP.
- All the client/user (Centralised, L2) traffic destined to controller will be encapsulated with GRE header and the destination IP address of the GRE packet would be set as mgmt. IP address of controller (10.10.10.254), but the IAP further encapsulate the GRE packet with IPSEC (ESP) header and set the destination as public IP address of the controller.

3.2.1 Tunnel Configuration

Now we start the tunnel configuration (Configuration->Tunneling) and we'll choose Aruba IPSEC. In this mode the VC on behalf of the Instant cluster create an IPSEC tunnel to the VPNC.

IAPs can also verify if an active VPN connection is available by sending test packets. Once we have specified the Protocol and Primary host with either IP address or FQDN, there is a "Secs between test packets" parameter that is by default set to 5.

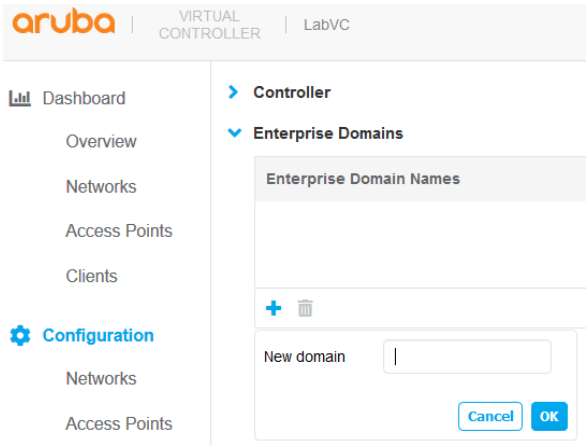


Note here that we have changed the Hold Time from default of 600 sec to 120. When we have enabled preemption and the primary host comes up, the VPN tunnel switches back to the primary host after 120 sec.

There is also a fast failover option that you can enable. This allows the IAP to create a backup VPN tunnel to the controller along with the primary tunnel. This means the backup tunnel setup time is reduced.

3.2.2 Enterprise Domains

The DNS behaviour of SSIDs and Ethernet Ports of an IAP-VPN is determined by the enterprise domain settings shown below. In the screenshot below, we could use the enterprise domains for which DNS requests would be sent to the corporate DNS servers. For all other domains, the DNS server obtained by the IAP would be used. So the DNS request from the Client for the domains not listed in the "Enterprise Domains" will be source NATed to the local DNS server of the IAP. This configuration can provide faster DNS response times, and extra privacy.

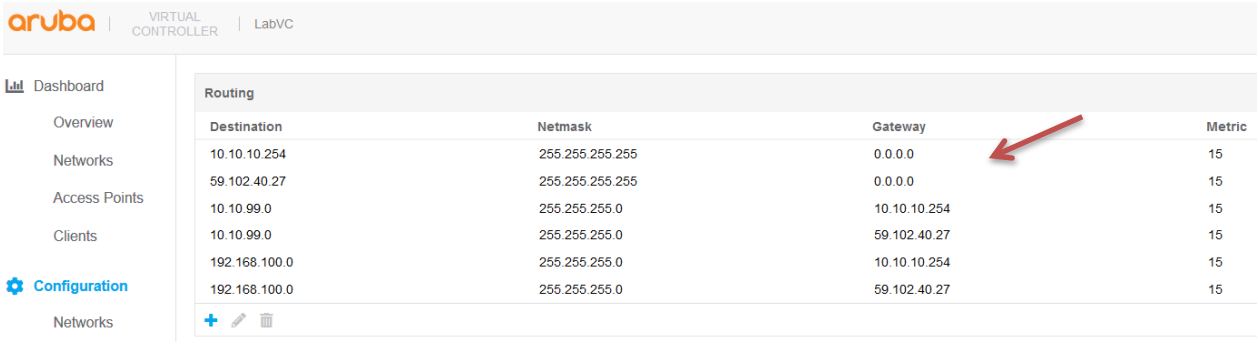


If you configure an asterisk (*) instead of a domain name in the enterprise domain list, all DNS requests are forwarded to the default DNS server of the client.

3.2.3 Routing Profile

Routing profile tells the IAP how to route the user traffic. Here you can define the corporate subnets that need to be sent through the IPSEC tunnel. Note the entries in routing profile table. (Configuration->Routing). The first two entries are using 0.0.0.0 as their gateway. This instruct the IAPs to use the default gateway they get through DHCP that is routed normally. The other entries are pointing to the primary and secondary VPN tunnels.

When you are using the cost metric for the routes, the route with the least metric value takes preference.



If you don't have the 10.10.99.0/24 routes point to the VPN controller, even though the client will get an IP address from the central DHCP scope on the controller, but it will not be able to pass traffic destine for the that subnet unless we have those routes. Just note that 192.168.100.0/24 is an interface that has defined on the VPN controller.

3.3 Aruba Controller Configuration

The controller here is running AOS version 8.4.0.1 and is in standalone mode.

```
(Aruba7010-Standalone) [mynode] #show ver

Aruba Operating System Software.
ArubaOS (MODEL: Aruba7010), Version 8.4.0.1
Website: http://www.arubanetworks.com
(c) Copyright 2019 Hewlett Packard Enterprise Development LP.
Compiled on 2019-03-19 at 08:48:39 UTC (build 69643) by p4build

ROM: System Bootstrap, Version CPBoot 1.2.1.0 (build 39183)
Built: 2013-07-26 04:57:47
Built by: p4build@re_client_39183

(Aruba7010-Standalone) [mynode] #show switches

All Switches
------------
IP Address    IPv6 Address  Name                  Location          Type        Model      Version
Status  Configuration State  Config Sync Time (sec)  Config ID
----------    ------------  ----                  --------          ----        -----      -------
------  -------------------  ----------------------  ---------
10.10.10.254  None          Aruba7010-Standalone  Building1.floor1  standalone  Aruba7010
8.4.0.1_69643  up      UPDATE SUCCESSFUL    0                     3

Total Switches:1
(Aruba7010-Standalone) [mynode] #
```

3.3.1 Network setup

First we need to configure the relevant VLANs, ensure VLAN 99 is operationally always up.

```
!
interface vlan 10
        ip address 10.10.10.254 255.255.255.0
!
interface vlan 192
        ip address 192.168.1.253 255.255.255.0
!
interface vlan 99
        ip address 10.10.99.254 255.255.255.0
        operstate up
!
interface vlan 100
        ip address 192.168.100.254 255.255.255.0
!
```

It is important to note that, when IAP cluster is configured for VPN, the VC of the cluster establishes an IPSEC tunnel (using IKEv2) with the VPNC. The IPSEC authentication and authorization between the VPNC and the IAP is based on TPM-based Aruba certificates and the RAP whitelist in VPNC.

Now we need to

1. white list the MAC address of the IAPs
2. create an IP pool for the IAPs
3. ensure that the controller IP address is the terminating the initial IPSEC tunnel needed (this is only if you are using Aruba GRE mode for IAP-VPN)

3.3.2 Whitelisting

Here we will be showing the manual way of whitelisting, which is by adding the MAC address of the IAPs to the local database of the controller.

However the recommended way is to use ClearPass as it can download the list of IAPs that are owned by an organisation directly from Aruba Activate to automate the whitelisting process. The steps for this process are

- Create a read-only account in Activate so ClearPass can get the list of IAPs.
- Configure ClearPass to periodically (1h by default) download any new devices from Activate. This is done from Administration > External Servers > Endpoint Context Servers. The list of IAPs will be added to the endpoint repository
- Create a MAC authentication service that receives auth requests from the VPNCs and authenticate them against the endpoint repository

For more information on Aruba Activate service refer here.

Here we are going to add the MAC address of the IAP to the whitelist.

```
(Aruba7010-Standalone) [mynode] #show controller-ip

Switch IP Address: 10.10.10.254
Switch IP is configured to be Vlan Interface: 10
Switch IPv6 address is not configured.

(Aruba7010-Standalone) [mynode] #
(Aruba7010-Standalone) [mynode] #whitelist-db rap add mac-address 20:4c:03:23:a7:98 ap-group default
description IAP-VPN
(Aruba7010-Standalone) [mynode] #
(Aruba7010-Standalone) [mynode] #show whitelist-db rap

AP-entry Details
----------------
Name               AP-Group  AP-Name            Full-Name  Authen-Username  Revoke-Text
AP_Authenticated  Description  Date-Added                Enabled  Remote-IP  Remote-IPv6  Cluster-
InnerIP  Cert-type
----               --------  -------            ---------  ---------------  -----------  -----------
-----  -----------  ----------                -------  ---------  -----------  ---------------  ----
-----
20:4c:03:23:a7:98  default   20:4c:03:23:a7:98                                                Provisioned
IAP-VPN      Fri Feb 15 12:04:16 2019  Yes      0.0.0.0    ::           0.0.0.0          NA

AP Entries: 1
(Aruba7010-Standalone) [mynode] #
```

Now we need trust the IAPs initiating connection.

```
(Aruba7010-Standalone) [mynode] #iap trusted-branch-db ?
add                      Configure an IAP trusted branch entry
allow-all                Allow all branches as trusted
del                      Delete an IAP trusted branch entry
del-all                  Delete all trusted branch entries

(Aruba7010-Standalone) [mynode] #iap trusted-branch-db allow-all
```

```
(Aruba7010-Standalone) [mynode] #show iap trusted-branch-db

Trusted Branch Validation: Disabled
IAP Trusted Branch Table
------------------------
Branch MAC
----------
(allow all as trusted branch)
(VMC-Standalone) [mynode] #
```

3.3.3 DHCP Service

Finally enabling DHCP on the DMZ controller and the IP local pool. Here you can also use ip-helper command and use an internal DHCP server.

```
!
ip dhcp pool vlan99
 default-router 10.10.99.254
 dns-server 10.10.99.254
 network 10.10.99.0 255.255.255.0
!
service dhcp
!
```

This is the DHCP scope that we are using for Centralise L2. Note that the VLAN ID are the exactly the same (99).

3.3.4 VPN Pool

Every IAP (Instant-VPN) that authenticates and successfully terminates an IPSEC tunnel on the VPN server module of the WLAN controller is given a valid inner IP address. This inner IP address is issued from the address pool that is configured in the VPN server module on the controller. More than one pool can be configured.

You can use the same VPN controller at the head end for SD-Branch connectivity, for IAP-VPN and VIA client VPNs.

```
!
ip local pool "IAP-pool-1" 10.66.66.11 10.66.66.20
!
user-role "default-vpn-role"
 pool l2tp "IAP-pool-1"
!
```

3.3.5 Backward Compatibility

Now it is important that if you have a mixed deployment of IAP-VPNs with different firmware version like 8.4.0 and earlier, since your controller is running 8.4 as well, you need to have this command to enable backward compatibility with the earlier IAP-VPN versions. Since the process of registration requests has changed. For more information on this please refer to the AOS 8.4 user guide

The command is "iapvpn_backward_compatible"

```
(host) [mynode] (config) #iapvpn-backward-compatible
```

3.4 Testing the IPSEC Tunnel – Controller

Before connecting the client to the TEST WLAN, you need to check if the tunnel is up.

On the controller first we check the VLAN status

```
(Aruba7010-Standalone) [mynode] #show ip interface brief

Interface                   IP Address / IP Netmask        Admin   Protocol   VRRP-IP
vlan 10                   10.10.10.254 / 255.255.255.0     up      up
vlan 1                      unassigned / unassigned        up      down
```

```
vlan 99                    10.10.99.254 / 255.255.255.0      up       up
vlan 100                 192.168.100.254 / 255.255.255.0     up       up
vlan 192                   192.168.1.253 / 255.255.255.0     up       up
loopback                      unassigned / unassigned        up       up
mgmt                          unassigned / unassigned        up       down
(Aruba7010-Standalone) [mynode] #
```

For the IAP to be listed in the table, first ISAKMP and IPSEC tunnels should be operational. This is transported over UDP/4500. Same thing here this is only the VC's AP MAC address that is shown. Also note that you'll see only one entry per IAP cluster.

Also note that if you have not assign VLAN 99 to any wired or wireless LAN in the IAP configuration, you will not get any entries in the "show iap table" command output.

```
(Aruba7010-Standalone) [mynode] #show iap table

Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name   VC MAC Address     Status  Inner IP     Assigned Subnet  Assigned Vlan
----   --------------     ------  --------     ---------------  -------------
LabVC  20:4c:03:23:a7:98  UP      10.66.66.12                   99

Total No of UP Branches   : 1
Total No of DOWN Branches : 0
Total No of Branches      : 1
(Aruba7010-Standalone) [mynode] #show crypto isakmp sa

ISAKMP SA Active Session Information
------------------------------------
Initiator IP                            Responder IP                           Flags     Start Time
Private IP                              Peer ID
------------                            ------------                           -----     ----------
----------                              -------------
10.10.30.101                            10.10.10.254                           r-v2-c-I  Feb 15
17:08:27   10.66.66.12                            CN=CNF0K2R28H::20:4c:03:23:a7:98

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Agressive Mode; v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP
       V = VIA; S = VIA over TCP; l = uplink load-balance

Total ISAKMP SAs: 1
(Aruba7010-Standalone) [mynode] #show crypto ipsec sa

IPSEC SA (V2) Active Session Information
----------------------------------------
Initiator IP                              Responder IP                             SPI(IN/OUT)
Flags Start Time        Inner IP
------------                              ------------                             ----------------
----- ---------------   --------
10.10.30.101                              10.10.10.254                             c8279600/bce7a00
UT2   Feb 15 17:08:27   10.66.66.12

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

Total IPSEC SAs: 1
(Aruba7010-Standalone) [mynode] #
```

Once you have the VPN operational you need to check the routing table as well.

```
(Aruba7010-Standalone) [mynode] #show ip route
```

```
Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink
       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
       I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 192.168.1.249 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0  [0/1] via 192.168.1.249*
S    10.10.30.0/24 [0/1] via 10.10.10.1*
C    10.10.10.0/24 is directly connected, VLAN10
C    10.10.99.0/24 is directly connected, VLAN99
C    192.168.100.0/24 is directly connected, VLAN100
C    192.168.1.0/24 is directly connected, VLAN192
C    10.66.66.12/32 is an ipsec map 10.10.30.101-10.66.66.12
(Aruba7010-Standalone) [mynode] #
```

Finally we need to check the user-roles

```
(Aruba7010-Standalone) [mynode] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC             Name               Role                    Age(d:h:m)  Auth  VPN
link      AP name    Roaming  Essid/Bssid/Phy  Profile                  Forward mode  Type  Host
Name  User Type
----------    ------------       ------             ----                    ----------  ----  -------
-      -------    -------  ---------------  -------                  ------------  ----  ---------
---------
10.10.30.101  00:00:00:00:00:00                      logon                   00:01:30    VPN
N/A                                                          tunnel
WIRELESS
10.66.66.12   00:00:00:00:00:00  20:4c:03:23:a7:98  default-vpn-role        00:01:22    VPN
10.10.30.101  N/A                                   default-iap              tunnel
WIRELESS

User Entries: 2/2
 Curr/Cum Alloc:2/15 Free:0/12 Dyn:2 AllocErr:0 FreeErr:0
(Aruba7010-Standalone) [mynode] #
```

Here is the session table on the 7010 controller, you'll see that the 4500/UDP is between 10.10.10.254 and 10.10.30.100 This is NAT-T which transports IPSEC over UDP.

```
(Aruba7010-Standalone) [mynode] #show datapath session table

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
       Q - Real-Time Quality analysis
       u - Upstream Real-Time Quality analysis
       I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal
       r - Route Nexthop, h - High Value
       A - Application Firewall Inspect
       J - SDWAN Default Probe stats used as fallback
       B - Permanent, O - Openflow
       L - Log

Source IP or MAC  Destination IP  Prot SPort DPort Cntr     Prio ToS Age Destination TAge Packets    Bytes      Flags
CPU ID
----------------- --------------- ---- ----- ----- -------- ---- --- --- ----------- ---- ---------- ---------- ---------------

192.168.1.253     192.168.1.132   6    22    54927 0/0      0    4   0   0/0/1       552  262        34277                 11
10.10.30.100      10.10.10.254    1    0     2048  1/15794  0    0   0   0/0/0       3cd  442        37128      FCI        13
10.10.10.254      10.10.30.100    17   4500  59823 0/0      0    0   11  0/0/0       3cb  13         7336       F          11
192.168.1.132     192.168.1.253   6    54927 22    1/15784  0    0   0   0/0/1       552  357        25327      C          11
10.10.10.254      10.10.30.100    1    0     0     0/0      0    0   0   0/0/0       3ce  443        37212      FI         11
10.66.66.12       10.10.10.254    47   0     0     0/0      0    48  0   tunnel 11   3cb  1661       168733     FC         12
```

```
10.10.30.100      10.10.10.254    17   59823 4500   0/0      0    48  0   0/0/0       3cc  1698       295200     FC              12
10.10.10.254      10.66.66.12     47   0     0      0/0      0    4   0   tunnel 11   3cb  1391       210618     F               12

(Aruba7010-Standalone) [mynode] #
```

```
(Aruba7010-Standalone) [mynode] #show datapath tunnel

+----+-------+-------------------------------------------------------+
|SUM/|       |                                       |               |
|CPU |  Addr | Description                                    Value |
+----+-------+-------------------------------------------------------+
|    | [004] | Tunnel FIB stale                                 1 |
+----+-------+-------------------------------------------------------+
|    |       |                                                       |
| G  | [000] | Current Entries                                 12 |
| G  | [002] | High Water Mark                                 12 |
| G  | [003] | Maximum Entries                               5120 |
| G  | [004] | Total Entries                                   16 |
| G  | [007] | Max link length                                  2 |
| G  | [009] | Tunnel FIB recompute                             1 |
+----+-------+-------------------------------------------------------+

Datapath Tunnel Table Entries
-----------------------------

Flags: E - Ether encap,  I - Wi-Fi encap,  R - Wired tunnel,  F - IP fragment OK
       W - WEP,  K - TKIP,  A - AESCCM,  G - AESGCM,  M - no mcast src filtering
       S - Single encrypt,  U - Untagged,  X - Tunneled node,  1(cert-id) - 802.1X Term-PEAP
       2(cert-id) - 802.1X Term-TLS,  T - Trusted,  L - No looping, d - Drop Bcast/Unknown Mcast,
       D - Decrypt tunnel,  a - Reduce ARP packets in the air, e - EAPOL only
       C - Prohibit new calls, P - Permanent, m - Convert multicast, B - Bgw peer uplink tunnel
       n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
       V - enforce user vlan(open clients only), x - Striping IP, z - Datazone
       H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t - Cluster s-AAC tunnel
       c - IP Compression, g - PAN GlobalProtect Tunnel, w - Tunneled Node Heartbeat
       B - Cluster A-SAC Mcast, G - Cluster S-SAC Mcast, l - Tunneled Node user tunnel
       f - Static GRE Tunnels, k- keepalive enabled, Y - Convert BC/MC to Unicast

 #          Source       Destination    Prt  Type  MTU   VLAN       Acls                    BSSID          Decaps     Encaps
Heartbeats Flags            EncapKBytes  DecapKBytes
------  --------------  --------------  ---  ----  ----  ---- ----------------------  ----------------- ---------- ---------- --
-------- --------------- ------------- -----------
14       SPIC8279600 in  10.10.10.254    50   IPSE  1500  0    routeDest 0000     0                            4519          0
T                0           0
13       SPI0BCE7A00out  10.10.30.101    50   IPSE  1500  0    routeDest 0000     0                               0       4455
T                0           0
11       10.10.10.254    10.66.66.12     47   1     1200  0    0   0    13   0    0     00:00:00:00:00:00        108          50
0 EFPR
12       10.10.10.254    10.66.66.12     47   9000  1200  0    0   0    0    0    0     00:00:00:00:00:00       4395          0
4395 TEP
(Aruba7010-Standalone) [mynode] #
```

3.5 Testing the IPSEC Tunnel – Instant AP

From the Instant AP you can issue the following commands to see the status of the VPN back to the DMZ controller.

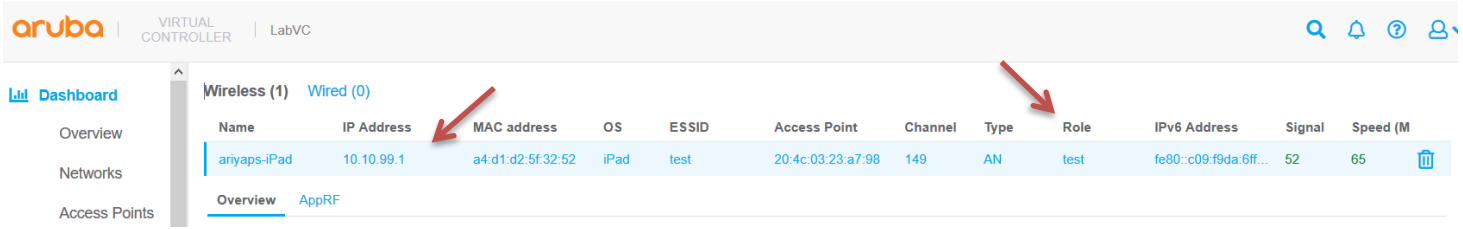
```
20:4c:03:23:a7:98# sh vpn status

profile name:default
--------------------------------------------------
current using tunnel                                :primary tunnel
current tunnel using time                           :1 hour 17 minutes 55 seconds
ipsec is preempt status                             :disable
ipsec is fast failover status                       :disable
ipsec hold on period                                :600s
ipsec tunnel monitor frequency (seconds/packet)     :5
ipsec tunnel monitor timeout by lost packet cnt     :6

ipsec      primary tunnel crypto type               :Cert
ipsec      primary tunnel peer address              :10.10.10.254
ipsec      primary tunnel peer tunnel ip            :10.10.10.254
ipsec      primary tunnel ap tunnel ip              :10.66.66.12
ipsec      primary tunnel using interface           :tun0
ipsec      primary tunnel using MTU                 :1230
ipsec      primary tunnel profile index             :0
ipsec      primary tunnel current sm status         :Up
ipsec      primary tunnel tunnel status             :Up
ipsec      primary tunnel tunnel retry times        :3
ipsec      primary tunnel tunnel uptime             :1 hour 17 minutes 55 seconds
```

```
ipsec      backup tunnel crypto type            :Cert
ipsec      backup tunnel peer address           :N/A
ipsec      backup tunnel peer tunnel ip         :N/A
ipsec      backup tunnel ap tunnel ip           :N/A
ipsec      backup tunnel using interface        :N/A
ipsec      backup tunnel using MTU              :N/A
ipsec      backup tunnel current sm status      :Init
ipsec      backup tunnel tunnel status          :Down
ipsec      backup tunnel tunnel retry times     :0
ipsec      backup tunnel tunnel uptime          :0
20:4c:03:23:a7:98#
20:4c:03:23:a7:98# sh vpn tunnels

Tunnel Flags: M = Master IAP; S = Slave IAP; P = Primary Tunnel
              B = Backup Tunnel; R = Registered; H = Heartbeat Enable

Tunnel Info for peer address 10.10.10.254 (default)
---------------------------------------------------
Type                                Value
----                                -----
Source IP                           10.66.66.12
Destination IP                      10.10.10.254
End IP                              10.10.10.254
Default GW                          0.0.0.0
Use count                           0
Ifindex                             23
Ifname                              tun0
GRE If                              gre0
Profile index                       0
Flags                               MPRH
Retry count for Register Request    0
Last Heartbeat                      20237
Heartbeat Encap/Decap               4724(seq 4724)/4724(seq 4724)
GRE Encap/Decap                     7056/4855
For DHCP Profile                    Test-Lab
 Retry count for Vlan Add Request   0
 Old Subnet Status                  Normal
 Existing Subnet Status             Registered
20:4c:03:23:a7:98#
20:4c:03:23:a7:98#
20:4c:03:23:a7:98# sh vpn config

Concentrator
------------
Type                            Value
----                            -----
VPN Primary Server              10.10.10.254
VPN Backup Server
VPN Preemption                  disable
VPN Fast Failover               disable
VPN Hold Time                   600
VPN Monitor Pkt Send Freq       5
VPN Monitor Pkt Lost Cnt        6
VPN Ikepsk                      7891be2e1777dd48c7356d1bbe948469
VPN Username
VPN Password                    7ef1137a242497bb3de0894e48191ce7
GRE outside vpn                 disable
GRE Per AP Tunnel               disable
GRE Type                        1
GRE Primary Server
GRE Primary IP Address          0.0.0.0
GRE Backup Server
GRE Backup IP Address           0.0.0.0
GRE Reconnect User On Failover  enable
GRE Reconnect Time On Failover  60
Reconnect User On Failover      disable
```

```
Reconnect Time On Failover      60

Routing Table
--------------
Destination  Netmask  Gateway  Metric  Type  Flag
-----------  -------  -------  ------  ----  ----

Number of Route Entries   :0

Route Flags: A = Active; D = in Datapath; M = to Master

20:4c:03:23:a7:98#
```

3.6 Client Testing

Now we get the WiFi client connects to the TEST WLAN, it should get an IP address from the central controller in the DMZ and be put into the default role as previously configured.



Here is the DHCP binding table on the central controller.

```
(Aruba7010-Standalone) [mynode] #show ip dhcp binding

lease 10.10.99.1 {
  Lease starts : Fri Mar 22 10:32:32 2019
  Lease ends : Fri Mar 22 22:32:32 2019
  Client Last Transaction Time : Fri Mar 22 10:32:32 2019
  binding state active;
  next binding state free;
  hardware ethernet a4:d1:d2:5f:32:52;
}

(Aruba7010-Standalone) *[mynode] #
```

The users now should be in the controller's user's table but they will be listed as wired clients.

```
(Aruba7010-Standalone) [mynode] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
    IP              MAC             Name              Role                  Age(d:h:m)  Auth  VPN
link      AP name    Roaming  Essid/Bssid/Phy  Profile                  Forward mode  Type  Host
Name  User Type
----------    ------------       ------             ----                  ----------  ----  -------
10.10.30.100  00:00:00:00:00:00                     logon                 00:00:20    VPN
N/A                                                        tunnel
WIRELESS
10.10.99.1    a4:d1:d2:5f:32:52                     default-iap-user-role  00:00:08
tunnel 13  Wired                    default-iap-aaa-profile  tunnel                          WIRED
10.66.66.12   00:00:00:00:00:00  20:4c:03:23:a7:98  default-vpn-role       00:00:19    VPN
10.10.30.100  N/A                                  default-iap             tunnel
WIRELESS

User Entries: 3/3
 Curr/Cum Alloc:3/4 Free:0/1 Dyn:3 AllocErr:0 FreeErr:0
(Aruba7010-Standalone) [mynode] #
```

Now from the WiFi laptop (10.10.99.1) we'll start pinging the wired laptop (10.10.99.254) and the pings succeeds since there are routes for 10.10.99.0/24 in the routing table of the IAP.

```
20:4c:03:23:a7:98# sh routing

Routing Table
-------------
Destination     Netmask           Gateway        Metric  Type    Flag
-----------     -------           -------        ------  ----    ----
10.10.10.254    255.255.255.255   0.0.0.0        15      Local   AD
59.102.40.27    255.255.255.255   0.0.0.0        15      Local   AD
10.10.99.0      255.255.255.0     10.10.10.254   15      Tunnel  AD
10.10.99.0      255.255.255.0     59.102.40.27   15      Tunnel
192.168.100.0   255.255.255.0     10.10.10.254   15      Tunnel  AD
192.168.100.0   255.255.255.0     59.102.40.27   15      Tunnel

Number of Route Entries   :6
Route Flags: A = Active; D = in Datapath; M = to Master

20:4c:03:23:a7:98#
```

Now we can ping from one client to the other. As you can see there is no NAT at all.

```
(Aruba7010-Standalone) *[mynode] #show datapath session table | include 10.10.99
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
       Q - Real-Time Quality analysis
       u - Upstream Real-Time Quality analysis
       I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal
       r - Route Nexthop, h - High Value
       A - Application Firewall Inspect
       J - SDWAN Default Probe stats used as fallback
       B - Permanent, O - Openflow
       L - Log

Source IP or MAC  Destination IP  Prot SPort DPort Cntr     Prio ToS Age Destination TAge Packets    Bytes      Flags
CPU ID
----------------- --------------- ---- ----- ----- -------- ---- --- --- ----------- ---- ---------- ---------- ---------------

10.10.99.1        10.10.99.254    1    3     2048  1/15794 0    0   0   tunnel 13   3    1          84         FCI            12
10.10.99.1        10.10.99.254    1    2     2048  1/15794 0    0   0   tunnel 13   4    1          84         FCI            12
10.10.99.1        10.10.99.254    1    1     2048  1/15794 0    0   0   tunnel 13   5    1          84         FCI            12
10.10.99.1        10.10.99.254    1    0     2048  1/15794 0    0   0   tunnel 13   6    1          84         FCI            12
10.10.99.1        10.10.99.254    1    4     2048  1/15794 0    0   0   tunnel 13   2    1          84         FCI            12
10.10.99.1        10.10.99.254    1    5     2048  1/15794 0    0   0   tunnel 13   1    1          84         FCI            12
10.10.99.254      10.10.99.1      1    4     0     0/0     0    0   0   tunnel 13   2    1          84         FI             11
10.10.99.254      10.10.99.1      1    5     0     0/0     0    0   0   tunnel 13   1    1          84         FI             11
10.10.99.254      10.10.99.1      1    3     0     0/0     0    0   0   tunnel 13   3    1          84         FI             11
10.10.99.254      10.10.99.1      1    2     0     0/0     0    0   1   tunnel 13   4    1          84         FI             11
10.10.99.254      10.10.99.1      1    1     0     0/0     0    0   1   tunnel 13   5    1          84         FI             11
10.10.99.254      10.10.99.1      1    0     0     0/0     0    0   1   tunnel 13   6    1          84         FI             11

(Aruba7010-Standalone) [mynode] #
```

And here is the "show datapath session" output when the client pings 192.168.100.254

```
(Aruba7010-Standalone) [mynode] #show datapath session | include 192.168.100

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
       Q - Real-Time Quality analysis
       u - Upstream Real-Time Quality analysis
       I - Deep inspect, U - Locally destined
       E - Media Deep Inspect, G - media signal
       r - Route Nexthop, h - High Value
       A - Application Firewall Inspect
       B - Permanent, O - Openflow
       L - Log


192.168.100.254   10.10.99.1      1    5     0      0/0     0    0   1   tunnel 13   12   1          84         FI             11
192.168.100.254   10.10.99.1      1    4     0      0/0     0    0   1   tunnel 13   13   1          84         FI             11
192.168.100.254   10.10.99.1      1    14    0      0/0     0    0   0   tunnel 13   9    1          84         FI             11
```

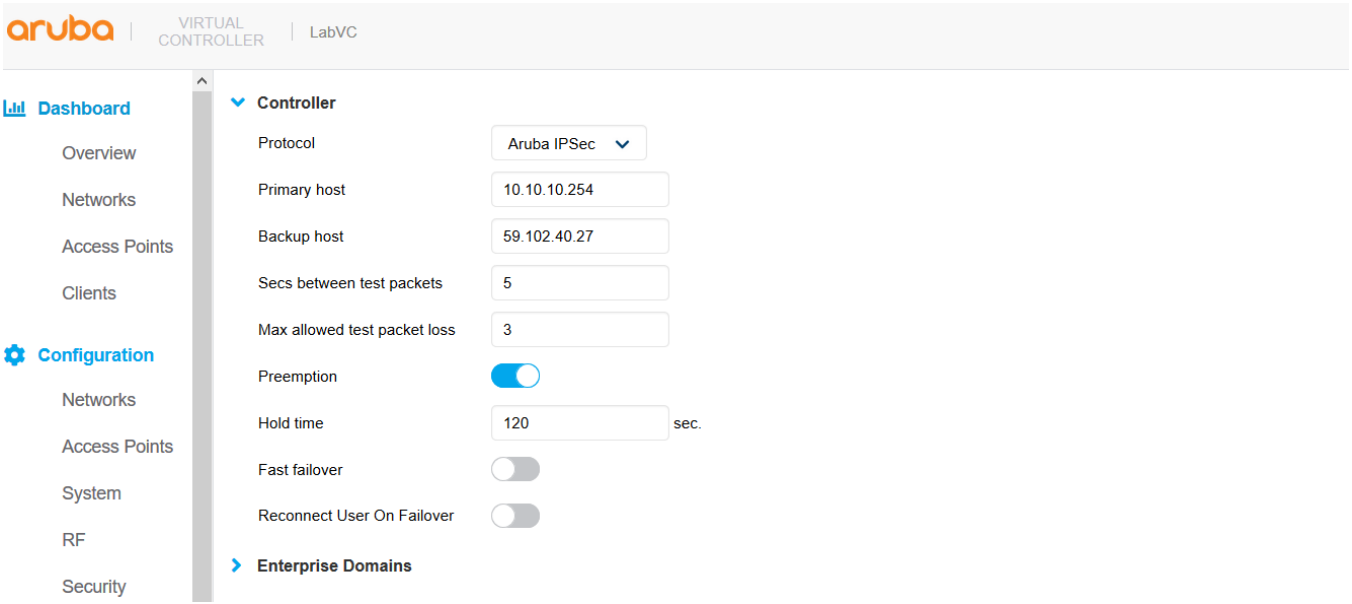
```
192.168.100.254   10.10.99.1      1    13    0      0/0     0    0   0   tunnel 13   a    1          84          FI              11
192.168.100.254   10.10.99.1      1    7     0      0/0     0    0   1   tunnel 13   10   1          84          FI              11
192.168.100.254   10.10.99.1      1    12    0      0/0     0    0   0   tunnel 13   b    1          84          FI              11
192.168.100.254   10.10.99.1      1    6     0      0/0     0    0   1   tunnel 13   11   1          84          FI              11
192.168.100.254   10.10.99.1      1    0     0      0/0     0    0   1   tunnel 13   17   1          84          FI              11
192.168.100.254   10.10.99.1      1    10    0      0/0     0    0   1   tunnel 13   d    1          84          FI              11
192.168.100.254   10.10.99.1      1    1     0      0/0     0    0   1   tunnel 13   16   1          84          FI              11
192.168.100.254   10.10.99.1      1    11    0      0/0     0    0   1   tunnel 13   c    1          84          FI              11
192.168.100.254   10.10.99.1      1    8     0      0/0     0    0   1   tunnel 13   f    1          84          FI              11
192.168.100.254   10.10.99.1      1    2     0      0/0     0    0   1   tunnel 13   17   1          84          FI              11
192.168.100.254   10.10.99.1      1    9     0      0/0     0    0   1   tunnel 13   10   1          84          FI              11
192.168.100.254   10.10.99.1      1    3     0      0/0     0    0   1   tunnel 13   16   1          84          FI              11
10.10.99.1        192.168.100.254 1    8     2048   1/15794 0    0   1   tunnel 13   11   1          84          FCI             12
10.10.99.1        192.168.100.254 1    2     2048   1/15794 0    0   1   tunnel 13   17   1          84          FCI             12
10.10.99.1        192.168.100.254 1    9     2048   1/15794 0    0   1   tunnel 13   10   1          84          FCI             12
10.10.99.1        192.168.100.254 1    3     2048   1/15794 0    0   1   tunnel 13   16   1          84          FCI             12
10.10.99.1        192.168.100.254 1    0     2048   1/15794 0    0   1   tunnel 13   19   1          84          FCI             12
10.10.99.1        192.168.100.254 1    10    2048   1/15794 0    0   1   tunnel 13   f    1          84          FCI             12
10.10.99.1        192.168.100.254 1    1     2048   1/15794 0    0   1   tunnel 13   18   1          84          FCI             12
10.10.99.1        192.168.100.254 1    11    2048   1/15794 0    0   1   tunnel 13   e    1          84          FCI             12
10.10.99.1        192.168.100.254 1    13    2048   1/15794 0    0   1   tunnel 13   c    1          84          FCI             12
10.10.99.1        192.168.100.254 1    7     2048   1/15794 0    0   1   tunnel 13   12   1          84          FCI             12
10.10.99.1        192.168.100.254 1    12    2048   1/15794 0    0   1   tunnel 13   d    1          84          FCI             12
10.10.99.1        192.168.100.254 1    6     2048   1/15794 0    0   1   tunnel 13   13   1          84          FCI             12
10.10.99.1        192.168.100.254 1    14    2048   1/15794 0    0   1   tunnel 13   e    1          84          FCI             12

(Aruba7010-Standalone) [mynode] #
```

4 3G/4G Backup

Here we'll configure a 3G/4G Backup uplink and make use of the new pre-emption enhancement method for IAP-VPN wherein Instant APs can detect the reachability of a primary VPN over the Ethernet uplink without bringing the 3G/4G link down. Here we'll use two failover IP addresses one for each of the uplinks. (Ethernet and 3G/4G)

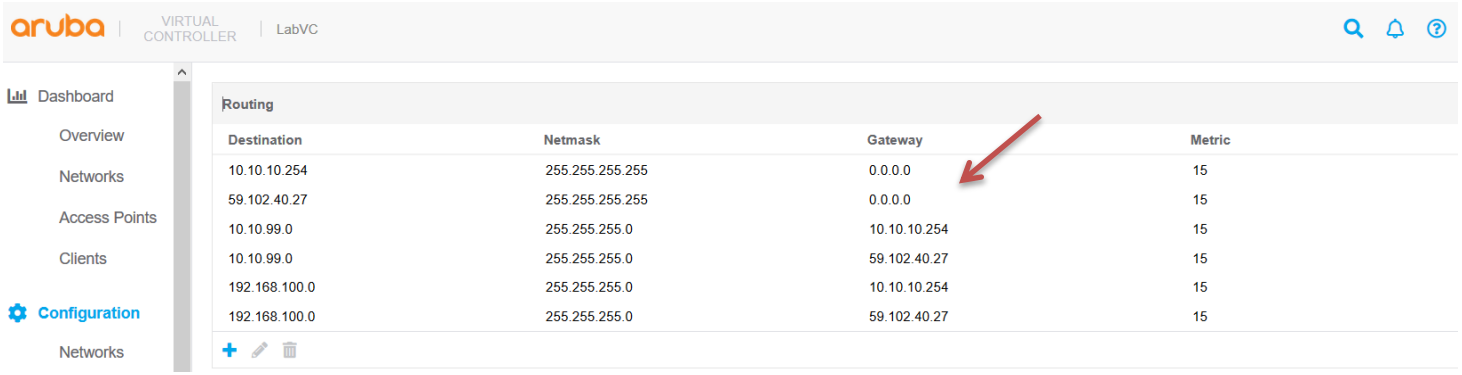
4.1 VPN Configuration

Now we have added the backup controller's IP address. Under Configuration->Tunnel



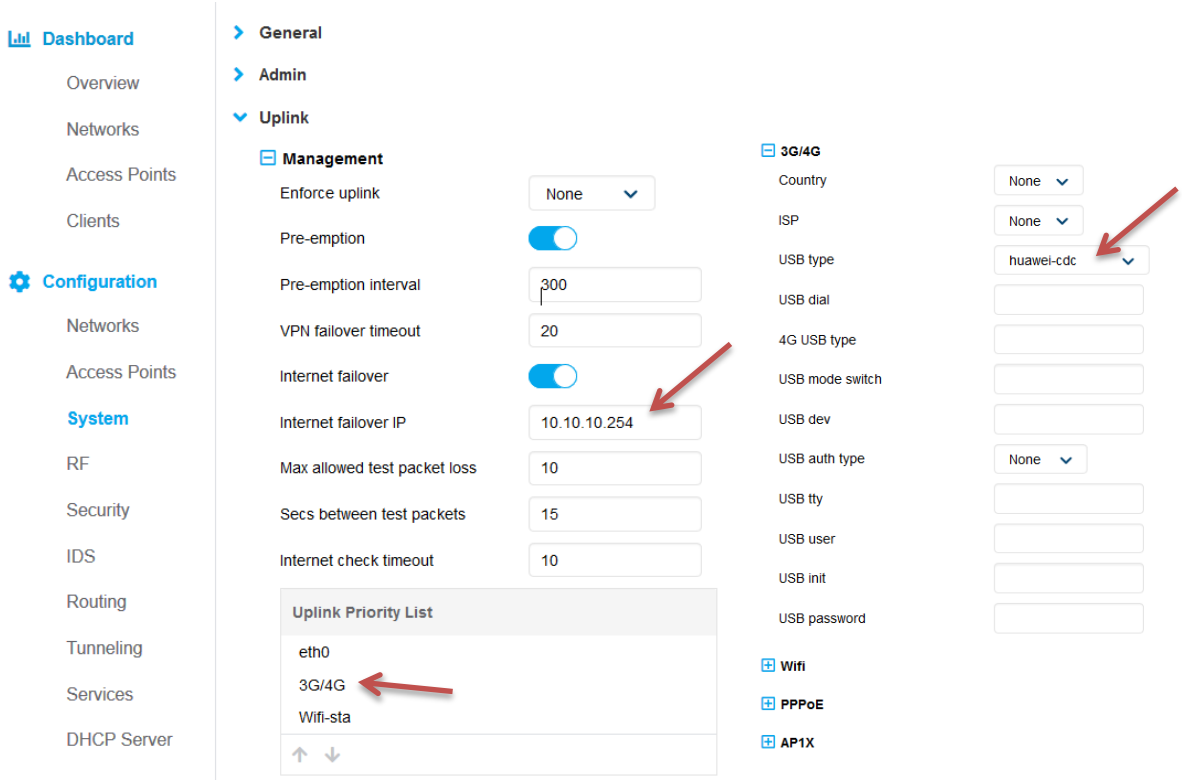
4.2 Routing Profile Configuration

Just recapping the already configured routing profile.



4.3 Uplink Configuration

Here we should ensure 3g/4G is the second in the uplink priority list and since we are using Huawei E3372 dongle, we need to choose the shown USB type.



In the uplink configuration, there are two related IP addresses that can be set.

1. One is “failover-internet-ip [ip-address]”, the default value is 8.8.8.8.
2. The other is “failover-internet-ip-for-cellular-uplink [ip-address]”

When “failover-internet-ip-for-cellular-uplink” is not set, it will be same as the value of “failover-internet-ip”.

The configuration for this scenario is as follows:

1. Enable both of pre-emption and failover-internet in uplink.
2. Two VPN configured, primary is 10.10.10.254, the backup is 59.102.40.27
3. failover-internet-ip-for-cellular-uplink 59.102.40.27
4. failover-internet-ip 10.10.10.254

Note that “failover-internet-ip-for-cellular-uplink” command is only in CLI.

```
!
uplink
 preemption
 preemption interval 300
 enforce none
 failover-internet
 failover-internet-ip 10.10.10.254
 failover-internet-ip-for-cellular-uplink 59.102.40.27
 failover-internet-pkt-lost-cnt 10
 failover-internet-pkt-send-freq 15
 failover-vpn-timeout 20
 uplink-priority ethernet 8
 uplink-priority wifi 10
 uplink-priority cellular 9
!
```

4.4 Backup Link Testing

We need to reboot the IAP for all the 3G/4G to take effect and the USB to be recognized on startup. Also ensure that the AP-303H is powered by 802/3at power source so that the USB dongle is power up.

Here is the relevant console boot up messages.

```
extended ssid config detected...
Terminal access enabled...
Valid SSID detected...
touching file /tmp/ip_mode_0
do ethtool autoneg on for eth0
eth1 admin down
init usb modem ...
[   39.784818] SCSI subsystem initialized
[   39.819731] eth0: GMAC Link is up with phy_speed=1000
USB Plugged in: Vendor_ID=12d1 Product_ID=155e
convert usb type from huawei-cdc to 12
USB is provisioned
Extra delay required for E3276/E3372 modem
Comm USB Plugged in: Vendor_ID=12d1 Product_ID=155e
[   69.868579] lxz device is Balong device bcdDevice=102,InterfaceSubClass=d
SIOCGIFFLAGS: No such device
Mesh is DISABLED on this device.
extended ssid is activated on the platform ...[   74.517290] uol_init_driver:261 HW
offload not applicable, AP will use cutting through path!

copying bootuplog ...
allow PAPI
set device anul0 mtu to 2000
notify asap_mod 3g present...
Starting update SBL1 ...
SBL1 was updated already
Done.
apdot1x authentication is not enabled
Starting DHCP
```

To be able to check if the IAP has been powered up by 802.3at, you can use this command.

```
20:4c:03:23:a7:98# show ap debug system-status | begin "Power Status"
Power Status
------------
Item                         Value
----                         -----
Power Supply                 : POE-AT
LLDP Power                   : Successfully negotiated at 15.8W
Current Operational State    : PSE disabled, USB port enabled (Overridden by LLDP)
```

Now once the IAP has booted up we need to check the 3G/4G modem with following commands.

```
20:4c:03:23:a7:98# sh cell config
Comm USB Plugged in: Vendor_ID=12d1 Product_ID=155e

Cellular configuration
----------------------
Type            Value
----            -----
4g-usb-type
usb-type        huawei-cdc
usb-dev
usb-tty
usb-init
```

```
usb-auth-type
usb-user
usb-passwd
usb-dial
usb-modeswitch
modem-isp
modem-country

Supported Modem Types
---------------------
Modem Type      Driver Used
----------      -----------
option          option
acm             acm
airprime        airprime
hso             hso
sierra-evdo     sierra-evdo
sierra-gsm      sierra-gsm
pantech-uml290  pantech-3g
novatal-mc551   ether-3g
sierra-net      sierra-net
franklin-u770   rndis-u770
rndis-l800      rndis-l800
huawei-cdc      huawei-cdc
novatel-u620    novatel-u620
pantech-uml295  rndis-uml295
sierra-gobi     sierra-gobi
zte-mf832       zte-cdc

Supported Country list
----------------------
Country list
------------

Supported ISP list
------------------
ISP list
--------

modem status summary:USB modem attached without driver load
20:4c:03:23:a7:98#
```

Now checking the status with the command below, we need to get the highlight result.

```
20:4c:03:23:a7:98# sh cell status

Cellular Status
---------------
card     detect      link      SIM PIN
----     ------      ----      -------
Present  Not-detect  Linkdown  Disable

plugin counter   :0
plugout counter   :0
cellular history log not available
20:4c:03:23:a7:98#
20:4c:03:23:a7:98#
20:4c:03:23:a7:98# show uplink status

Uplink pre-emption            :enable
Uplink pre-emption interval   :300
Uplink enforce                :none
Ethernet uplink eth0          :DHCP
Uplink Table
------------
```

```
Type      State  Priority  In Use
----      -----  --------  ------
eth0      UP     8         Yes
Wifi-sta  INIT   10        No
3G/4G     LOAD   9         No
Internet failover                        :enable
Internet failover IP                     :10.10.10.254
Internet failover IP for cellular uplink :59.102.40.27
Max allowed test packet loss             :10
Secs between test packets                :15
VPN failover timeout (secs)              :20
Internet check timeout (secs)            :10
ICMP pkt sent        :28
ICMP pkt lost        :0
Continuous pkt lost  :0
VPN down time        :0
AP1X type:NONE
Certification type:NONE
Validate server:NONE
20:4c:03:23:a7:98#
```

Checking the VPN tunnels to ensure the Primary VPN is up.

```
20:4c:03:23:a7:98# sh vpn status

profile name:default
-----------------------------------------------
current using tunnel                            :primary tunnel
current tunnel using time                       :3 minutes 43 seconds
ipsec is preempt status                         :enable
ipsec is fast failover status                   :disable
ipsec hold on period                            :120s
ipsec tunnel monitor frequency (seconds/packet) :5
ipsec tunnel monitor timeout by lost packet cnt :6

ipsec     primary tunnel crypto type            :Cert
ipsec     primary tunnel peer address           :10.10.10.254
ipsec     primary tunnel peer tunnel ip         :10.10.10.254
ipsec     primary tunnel ap tunnel ip           :10.66.66.18
ipsec     primary tunnel using interface        :tun0
ipsec     primary tunnel using MTU              :1230
ipsec     primary tunnel profile index          :0
ipsec     primary tunnel current sm status      :Up
ipsec     primary tunnel tunnel status          :Up
ipsec     primary tunnel tunnel retry times     :1
ipsec     primary tunnel tunnel uptime          :3 minutes 43 seconds

ipsec      backup tunnel crypto type            :Cert
ipsec      backup tunnel peer address           :59.102.40.27
ipsec      backup tunnel peer tunnel ip         :0.0.0.0
ipsec      backup tunnel ap tunnel ip           :0.0.0.0
ipsec      backup tunnel using interface        :
ipsec      backup tunnel using MTU              :0
ipsec      backup tunnel profile index          :0
ipsec      backup tunnel current sm status      :Down
ipsec      backup tunnel tunnel status          :Down
ipsec      backup tunnel tunnel retry times     :0
ipsec      backup tunnel tunnel uptime          :0
20:4c:03:23:a7:98#
```

And lastly checking the interfaces, we should now have ppp interface for our 3g/4G modem.

```
20:4c:03:23:a7:98# sh ip int brief
Interface                      IP Address / IP Netmask       Admin  Protocol
```

```
br0                              10.10.30.100 / 255.255.255.0     up      up
br0.3333                          172.31.98.1 / 255.255.254.0     up      up
ppp0                                0.0.0.0 / 0.0.0.0             down    down
20:4c:03:23:a7:98#
20:4c:03:23:a7:98# sh ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.10.30.1      0.0.0.0         UG        0 0          0 br0
10.10.10.254    0.0.0.0         255.255.255.255 UH        0 0          0 tun0
10.10.10.254    10.10.30.1      255.255.255.255 UGH       0 0          0 br0
10.10.30.0      0.0.0.0         255.255.255.0   U         0 0          0 br0
10.10.99.0      10.10.30.1      255.255.255.0   UG        0 0          0 br0
59.102.40.27    10.10.30.1      255.255.255.255 UGH       0 0          0 br0
172.31.98.0     0.0.0.0         255.255.254.0   U         0 0          0 br0.3333
192.168.100.0   10.10.30.1      255.255.255.0   UG        0 0          0 br0
20:4c:03:23:a7:98#
```

We are going to simulate the primary VPN failure, be removing the Ethernet cable from Gig0/0/0 interface of the VPN controller. This will ensure that the Eth0 of the IAP is still up and operational.

Here are the console messages on the IAP. This interface is used for establishing of the Primary VPN. About 15 sec the 3G/4G will come up. This is based on “sec between test packets=5” and the number of test packets = 3.

```
20:4c:03:23:a7:98# [  297.978217] Thu Dec 13 03:10:31 2018 ppp_device_event: dev ppp0 is
up, is_3g:0, is_4g:1, is_pppoe_uplink:0
[  309.801414] asap_send_elected_master: sent successfully

20:4c:03:23:a7:98#
```

Checking the cellular status

```
20:4c:03:23:a7:98# sh cell status

Cellular Status
---------------
card     detect      link    SIM PIN
----     ------      ----    -------
Present  Not-detect  Linkup  Disable

Cellular Link Status
--------------------
Parameter                 Value
---------                 -----
USB Modem State            Active
USB Uplink RSSI(in dBm)    -91
Current Network Service    4G-LTE
plugin counter   :0
plugout counter   :0
2018-12-13 14:10:42,Cellular uplink is up with IP 10.96.149.79

20:4c:03:23:a7:98#
```

Checking the interfaces, now we should see ppp interface up and running.

```
20:4c:03:23:a7:98# sh ip int b
Interface                          IP Address / IP Netmask       Admin  Protocol
br0                              10.10.30.100 / 255.255.255.0    up     up
br0.3333                          172.31.98.1 / 255.255.254.0    up     up
ppp0                             10.96.149.79 / 255.255.255.224  up     up
20:4c:03:23:a7:98#
```

Here is the routing table

```
20:4c:03:23:a7:98# show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.96.149.65    0.0.0.0         UG        0 0          0 ppp0
10.10.10.254    0.0.0.0         255.255.255.255 UH        0 0          0 tun0
10.10.10.254    10.96.149.65    255.255.255.255 UGH       0 0          0 ppp0
10.10.10.254    10.10.30.1      255.255.255.255 UGH       0 0          0 br0
10.10.30.0      0.0.0.0         255.255.255.0   U         0 0          0 br0
10.10.99.0      10.96.149.65    255.255.255.0   UG        0 0          0 ppp0
10.96.149.64    0.0.0.0         255.255.255.224 U         0 0          0 ppp0
59.102.40.27    10.96.149.65    255.255.255.255 UGH       0 0          0 ppp0
59.102.40.27    10.96.149.65    255.255.255.255 UGH       0 0          0 ppp0
172.31.98.0     0.0.0.0         255.255.254.0   U         0 0          0 br0.3333
192.168.100.0   10.96.149.65    255.255.255.0   UG        0 0          0 ppp0
20:4c:03:23:a7:98#
```

Checking the VPN tunnels

```
20:4c:03:23:a7:98# sh vpn status

profile name:default
-------------------------------------------------
current using tunnel                            :backup tunnel
current tunnel using time                       :1 minute 56 seconds
ipsec is preempt status                         :enable
ipsec is fast failover status                   :disable
ipsec hold on period                            :120s
ipsec tunnel monitor frequency (seconds/packet) :5
ipsec tunnel monitor timeout by lost packet cnt :3

ipsec     primary tunnel crypto type            :Cert
ipsec     primary tunnel peer address           :10.10.10.254
ipsec     primary tunnel peer tunnel ip         :0.0.0.0
ipsec     primary tunnel ap tunnel ip           :0.0.0.0
ipsec     primary tunnel using interface        :
ipsec     primary tunnel using MTU              :0
ipsec     primary tunnel profile index          :0
ipsec     primary tunnel current sm status      :Down
ipsec     primary tunnel tunnel status          :Down
ipsec     primary tunnel tunnel retry times     :2
ipsec     primary tunnel tunnel uptime          :0

ipsec      backup tunnel crypto type            :Cert
ipsec      backup tunnel peer address           :59.102.40.27
ipsec      backup tunnel peer tunnel ip         :10.10.10.254
ipsec      backup tunnel ap tunnel ip           :10.66.66.15
ipsec      backup tunnel using interface        :tun0
ipsec      backup tunnel using MTU              :1230
ipsec      backup tunnel profile index          :0
ipsec      backup tunnel current sm status      :Up
ipsec      backup tunnel tunnel status          :Up
ipsec      backup tunnel tunnel retry times     :1
ipsec      backup tunnel tunnel uptime          :1 minute 56 seconds
20:4c:03:23:a7:98#tunnel uptime          :1 minute 56 seconds
20:4c:03:23:a7:98#
```

Now checking the controller status

```
(Aruba7010-Standalone) [mynode] #show iap table

Trusted Branch Validation: Disabled
```

```
IAP Branch Table
----------------
Name   VC MAC Address     Status  Inner IP     Assigned Subnet  Assigned Vlan
----   --------------     ------  --------     ---------------  -------------
LabVC  20:4c:03:23:a7:98  UP      10.66.66.15                   99

Total No of UP Branches   : 1
Total No of DOWN Branches : 0
Total No of Branches      : 1
(Aruba7010-Standalone) [mynode] #
(Aruba7010-Standalone) [mynode] #show crypto isakmp sa

ISAKMP SA Active Session Information
------------------------------------
Initiator IP                          Responder IP                            Flags
Start Time        Private IP                            Peer ID
------------                          ------------                            -----
----------        ----------                            -------------
10.10.30.100                          10.10.10.254                            r-v2-c-I
Mar 22 11:12:44     -                                   CN=CNF0K2R28H::20:4c:03:23:a7:98
1.152.174.155                         192.168.1.253                           r-v2-c-I
Mar 22 11:15:47   10.66.66.15                           CN=CNF0K2R28H::20:4c:03:23:a7:98

Flags: i = Initiator; r = Responder
       m = Main Mode; a = Agressive Mode; v2 = IKEv2
       p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
       x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
       3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP
       V = VIA; S = VIA over TCP; l = uplink load-balance

Total ISAKMP SAs: 2
(Aruba7010-Standalone) [mynode] #
(Aruba7010-Standalone) [mynode] #
(Aruba7010-Standalone) [mynode] #show crypto ipsec sa


IPSEC SA (V2) Active Session Information
----------------------------------------
Initiator IP                              Responder IP
SPI(IN/OUT)        Flags Start Time        Inner IP
------------                              ------------                          ------
----------   ----- ---------------   --------
1.152.174.155                             192.168.1.253
a3c5ad00/2e59fb00  UT2   Mar 22 11:15:47   10.66.66.15

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

Total IPSEC SAs: 1
(Aruba7010-Standalone) [mynode] #
```

And the routing table

```
(Aruba7010-Standalone) [mynode] #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink
       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
       I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 192.168.1.1 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0  [0/1] via 192.168.1.1*
```

```
S    10.10.30.0/24 [0/1] via 10.10.10.1*
C    10.10.10.0/24 is directly connected, VLAN10
C    10.10.99.0/24 is directly connected, VLAN99
C    192.168.100.0/24 is directly connected, VLAN100
C    192.168.1.0/24 is directly connected, VLAN192
C    10.66.66.15/32 is an ipsec map 1.152.174.155-10.66.66.15
(Aruba7010-Standalone) [mynode] #
```

4.5 Client Testing

We can start the client testing by connecting to the TEST WLAN, it should get an IP address from the central controller in the DMZ and be put into the default role as previously configured.

```
20:4c:03:23:a7:98# sh clients

Client List
-----------
Name          IP Address  MAC Address        OS  ESSID  Access Point       Channel  Type  Role  IPv6
Address              Signal    Speed (mbps)
----          ----------  -----------        --  -----  ------------       -------  ----  ----  ----
--------              ------    ------------

ariyaps-iPad  10.10.99.1  a4:d1:d2:5f:32:52      test   20:4c:03:23:a7:98  149      AN    test
fe80::c09:f9da:6ff5:f179  48(good)  52(good)
Number of Clients   :1
Info timestamp      :839
20:4c:03:23:a7:98#
```

We need to check the VPN tunnels form Instant AP side

```
20:4c:03:23:a7:98# sh vpn tunnels

Tunnel Flags: M = Master IAP; S = Slave IAP; P = Primary Tunnel
              B = Backup Tunnel; R = Registered; H = Heartbeat Enable

Tunnel Info for peer address 10.10.10.254 (default)
---------------------------------------------------
Type                              Value
----                              -----
Source IP                         10.66.66.15
Destination IP                    10.10.10.254
End IP                            59.102.40.27
Default GW                        10.96.149.65
Use count                         2
Ifindex                           24
Ifname                            tun0
GRE If                            gre0
Profile index                     0
Flags                             MBRH
Retry count for Register Request  0
Last Heartbeat                    913
Heartbeat Encap/Decap             533(seq 533)/533(seq 533)
GRE Encap/Decap                   873/637
For DHCP Profile                  Test-Lab
 Retry count for Vlan Add Request  0
 Old Subnet Status                Normal
 Existing Subnet Status           Registered
20:4c:03:23:a7:98#
```

Checking to see if the WiFi user is shown on the VPNC

```
(Aruba7010-Standalone) [mynode] #show user
This operation can take a while depending on number of users. Please be patient ....

Users
```

```
-----
    IP              MAC             Name              Role                    Age(d:h:m)  Auth  VPN
link       AP name    Roaming  Essid/Bssid/Phy  Profile                   Forward mode  Type  Host
Name  User Type
----------     ------------       ------             ----                    ----------  ----  ------
--       -------    -------  ---------------  -------                  ------------  ----  ---------
---------
10.66.66.15    00:00:00:00:00:00  20:4c:03:23:a7:98  default-vpn-role       00:00:10    VPN
1.152.174.155  N/A                                 default-iap              tunnel
WIRELESS
10.10.99.1     a4:d1:d2:5f:32:52                   default-iap-user-role  00:00:04
tunnel 13  Wired                    default-iap-aaa-profile  tunnel                          WIRED
1.152.174.155  00:00:00:00:00:00                   logon                  00:00:10    VPN
N/A                                                        tunnel
WIRELESS

User Entries: 3/3
 Curr/Cum Alloc:3/9 Free:1/6 Dyn:4 AllocErr:0 FreeErr:0
(Aruba7010-Standalone) [mynode] #
```

Finally we'll start to ping 192.168.100.254 from the WiFi client and observe the datapath on the VPNC.

```
(Aruba7010-Standalone) [mynode] #show datapath session | include 192.168.100
192.168.100.254   10.10.99.1      1    5     0      0/0     0    0   1   tunnel 13   5    1       84    FI   11
192.168.100.254   10.10.99.1      1    4     0      0/0     0    0   1   tunnel 13   6    1       84    FI   11
192.168.100.254   10.10.99.1      1    7     0      0/0     0    0   0   tunnel 13   3    1       84    FI   11
192.168.100.254   10.10.99.1      1    6     0      0/0     0    0   1   tunnel 13   4    1       84    FI   11
192.168.100.254   10.10.99.1      1    0     0      0/0     0    0   1   tunnel 13   a    1       84    FI   11
192.168.100.254   10.10.99.1      1    10    0      0/0     0    0   0   tunnel 13   0    1       84    FI   11
192.168.100.254   10.10.99.1      1    1     0      0/0     0    0   1   tunnel 13   9    1       84    FI   11
192.168.100.254   10.10.99.1      1    8     0      0/0     0    0   0   tunnel 13   2    1       84    FI   11
192.168.100.254   10.10.99.1      1    2     0      0/0     0    0   1   tunnel 13   8    1       84    FI   11
192.168.100.254   10.10.99.1      1    9     0      0/0     0    0   0   tunnel 13   1    1       84    FI   11
192.168.100.254   10.10.99.1      1    3     0      0/0     0    0   1   tunnel 13   7    1       84    FI   11
10.10.99.1        192.168.100.254 1    8     2048   1/15794 0    0   1   tunnel 13   2    1       84    FCI  10
10.10.99.1        192.168.100.254 1    2     2048   1/15794 0    0   1   tunnel 13   8    1       84    FCI  10
10.10.99.1        192.168.100.254 1    9     2048   1/15794 0    0   1   tunnel 13   1    1       84    FCI  10
10.10.99.1        192.168.100.254 1    3     2048   1/15794 0    0   1   tunnel 13   9    1       84    FCI  10
10.10.99.1        192.168.100.254 1    0     2048   1/15794 0    0   1   tunnel 13   c    1       84    FCI  10
10.10.99.1        192.168.100.254 1    10    2048   1/15794 0    0   0   tunnel 13   2    1       84    FCI  10
10.10.99.1        192.168.100.254 1    1     2048   1/15794 0    0   1   tunnel 13   b    1       84    FCI  10
10.10.99.1        192.168.100.254 1    11    2048   1/15794 0    0   0   tunnel 13   1    1       84    FCI  10
10.10.99.1        192.168.100.254 1    7     2048   1/15794 0    0   1   tunnel 13   5    1       84    FCI  10
10.10.99.1        192.168.100.254 1    6     2048   1/15794 0    0   1   tunnel 13   6    1       84    FCI  10
10.10.99.1        192.168.100.254 1    5     2048   1/15794 0    0   1   tunnel 13   7    1       84    FCI  10
10.10.99.1        192.168.100.254 1    4     2048   1/15794 0    0   1   tunnel 13   8    1       84    FCI  10
(Aruba7010-Standalone) [mynode] #
```

The last part here is test the pre-emption process. For this we reconnect the Ethernet cable to Gig0/0/0 interface of the VPNC to ensure that Primary VPN is reachable. It will take about 7-8 minutes and the 3G/4G interface will come down and primary VPN reestablished.

```
20:4c:03:23:a7:98# sh ip int brief
Interface                 IP Address / IP Netmask       Admin  Protocol
br0                       10.10.30.100 / 255.255.255.0  up     up
br0.3333                  172.31.98.1 / 255.255.254.0   up     up
ppp0                      0.0.0.0 / 0.0.0.0             down   down
20:4c:03:23:a7:98#
```

We have the VPN Hold time = 120 sec and we also have the Pre-emption interval of 300 sec. So all up it should take about 7-8 mins for the VPN revert back to the primary site when the

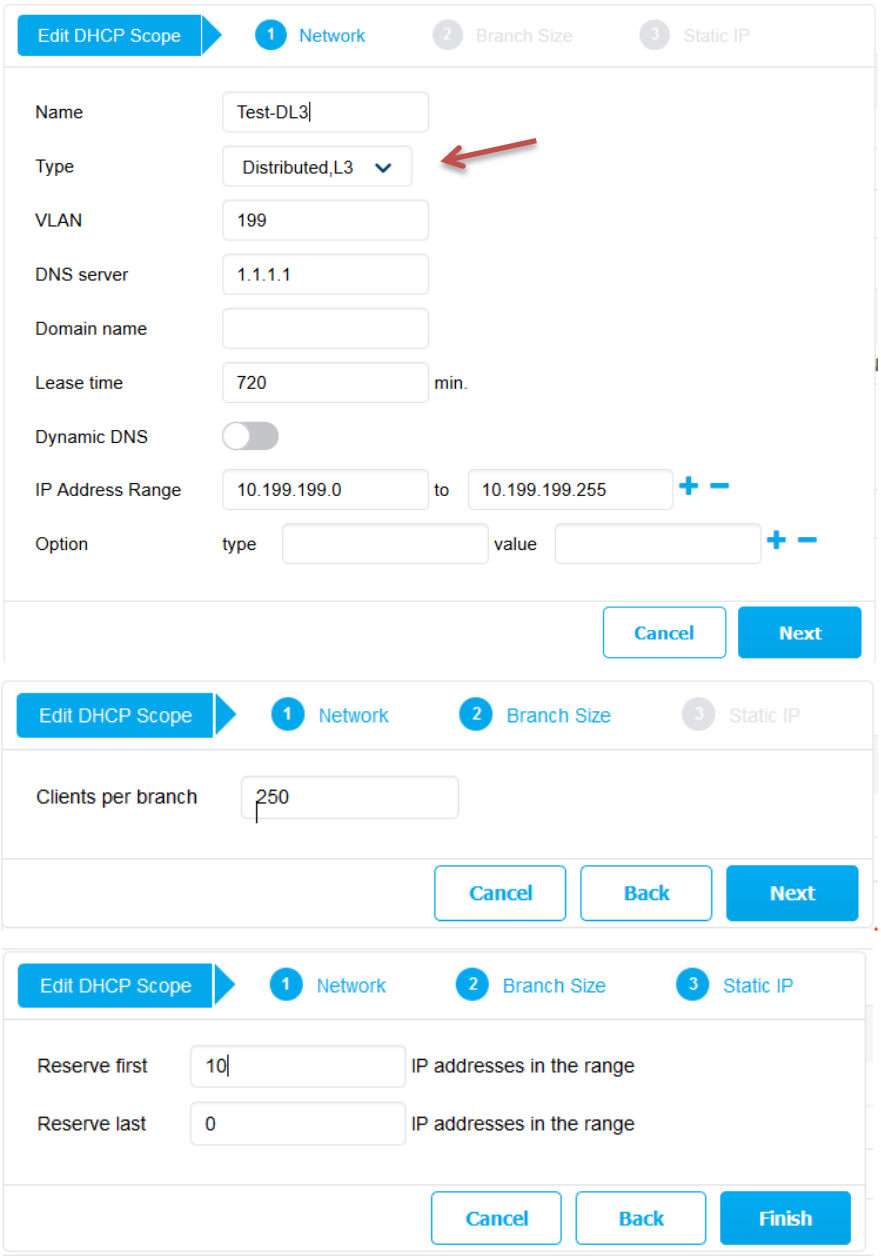
5 Instant VC VPN with Distributed L3

With IAP-VPN you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch.

Here we'll use Distributed L3, in this mode, the virtual controller (VC) for the IAP cluster acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the virtual controller is configured with a unique subnet and a corresponding scope.

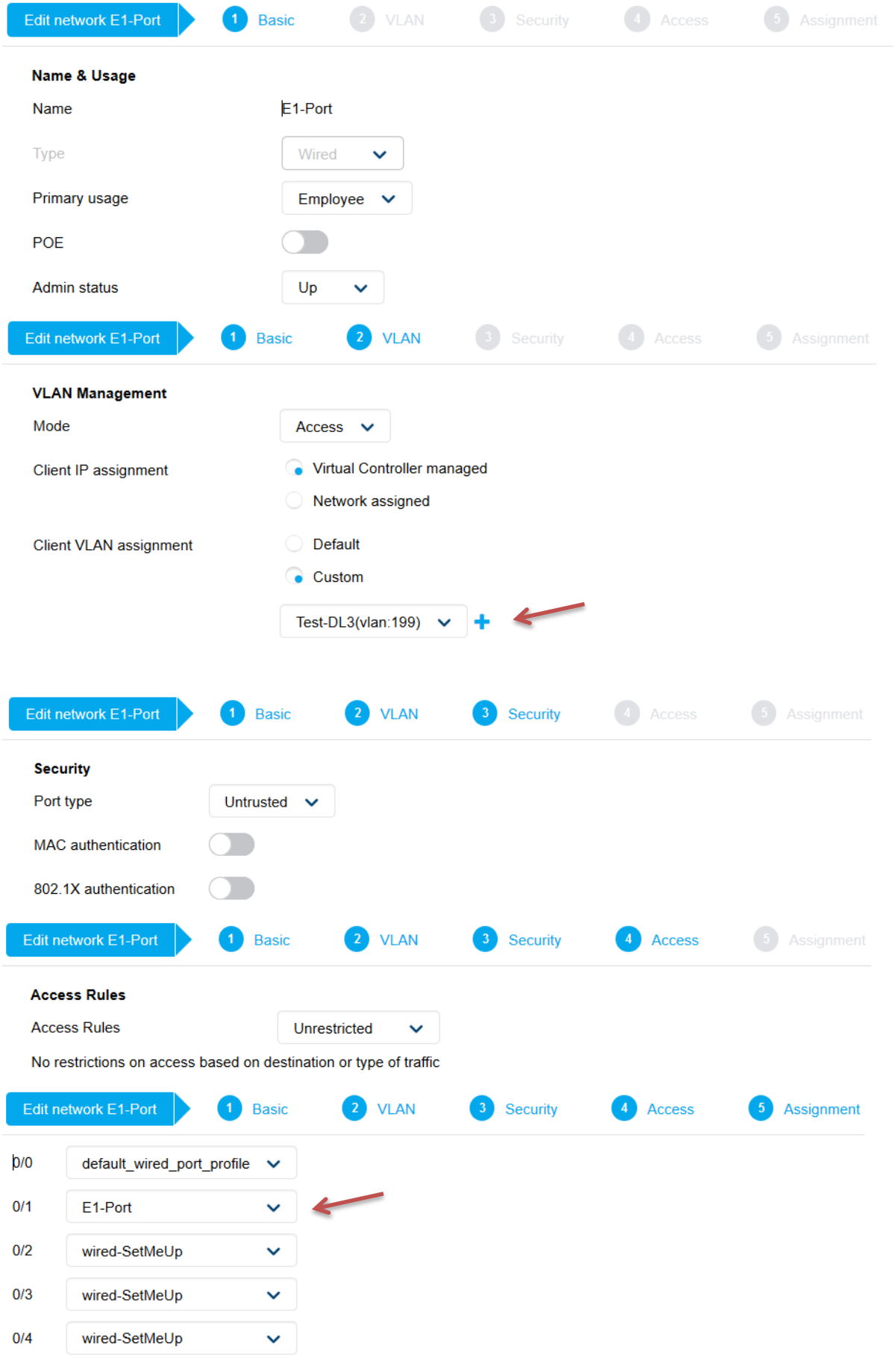
5.1 DHCP Configuration

Starting with configuring a DHCP scope



5.2 E1 Port Configuration

Here we will configure E1 port so that it uses distributed-L3 DHCP VLAN.


Edit network E1-Port
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment
Name & Usage
Name
E1-Port
Type
Wired
Primary usage
Employee
POE
Admin status
Up
Edit network E1-Port
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment
VLAN Management
Mode
Access
Client IP assignment
Virtual Controller managed
Network assigned
Client VLAN assignment
Default
Custom
Test-DL3(vlan:199)
Edit network E1-Port
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment
Security
Port type
Untrusted
MAC authentication
802.1X authentication
Edit network E1-Port
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment
Access Rules
Access Rules
Unrestricted
No restrictions on access based on destination or type of traffic
Edit network E1-Port
1 Basic
2 VLAN
3 Security
4 Access
5 Assignment
0/0
default_wired_port_profile
0/1
E1-Port
0/2
wired-SetMeUp
0/3
wired-SetMeUp
0/4
wired-SetMeUp

5.3 Testing

As soon as we have configured the distrubted-L3 DHCP scope, assuming the VPN is already established we should see it on the controller side.

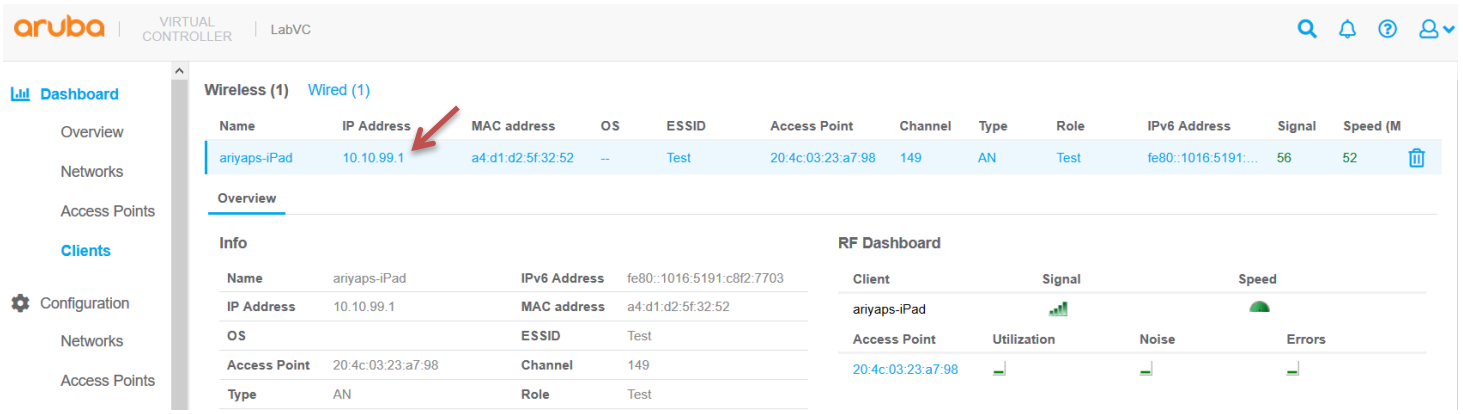
```
(Aruba7010-Standalone) [mynode] #show iap table long

Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name    VC MAC Address      Status  Inner IP     Assigned Subnet  Assigned Vlan  Key
Bid(Subnet Name)                     Tunnel End Points
----    --------------      ------  --------     ---------------  -------------  ---
----------------                     -----------------
LabVC   20:4c:03:23:a7:98   UP      10.66.66.26                   99
e0e971e901dd3e3a9d3bb19536fad013fbd2681b064f5b180f  0(10.10.100.0-10.10.100.255,250)

Total No of UP Branches   : 1
Total No of DOWN Branches : 0
Total No of Branches      : 1

(Aruba7010-Standalone) [mynode]#
(Aruba7010-Standalone) [mynode]#show iap detailed-table long

Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name    VC MAC Address      Status  Inner IP     Flags  Branch (Subnet / Vlan)  Key
Bid   Subnet Range                  Client count
----    --------------      ------  --------     -----  ----------------------  ---
---   ------------                  ------------
LabVC   20:4c:03:23:a7:98   UP      10.66.66.12  PC2    99
50b4dffe019145cedff55f8799d77464414c8a564642c07f65  N/A  N/A                          N/A
LabVC   20:4c:03:23:a7:98   UP      10.66.66.12  PD3    10.199.199.0/24
50b4dffe019145cedff55f8799d77464414c8a564642c07f65  0    10.199.199.0-10.199.199.255  250

Flags: P = Primary Tunnel; B = Backup Tunnel; C = Centralized; U = Unassigned;
D = Distributed; L = Local; 3 = Routed(L3); 2 = Bridged(L2);

Total No of UP Branches   : 1
Total No of DOWN Branches : 0
Total No of Branches      : 1

(Aruba7010-Standalone) [mynode] #
```

So once there is an entry in for PD3 that should also get reflected in the routing table of the controller.

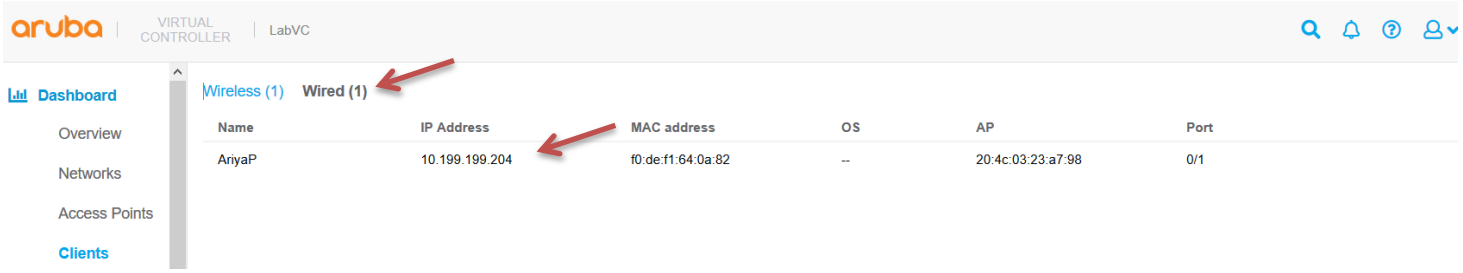
```
(Aruba7010-Standalone) [mynode] #show ip route

Codes: C - connected, O - OSPF, R - RIP, S - static, B - Bgw peer uplink
       M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
       I - Ike-overlay, N - not redistributed

Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 192.168.1.1 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0  [0/1] via 192.168.1.1*
S     10.10.30.0/24 [0/1] via 10.10.10.1*
V     10.199.199.0/24 [0/10] ipsec map 10.10.30.100-10.66.66.12
C     10.10.10.0/24 is directly connected, VLAN10
C     10.10.99.0/24 is directly connected, VLAN99
C     192.168.100.0/24 is directly connected, VLAN100
```

```
C    192.168.1.0/24 is directly connected, VLAN192
C    10.66.66.12/32 is an ipsec map 10.10.30.100-10.66.66.12

(Aruba7010-Standalone) [mynode] #
```

Now when we connect the wired client to the E1 port of the AP-303H, it gets an IP address from VLAN 199. From the WebUI of the Instant AP you see the Centralised L2 client that is connected to the Test SSID.



When you click on the Wired link, you should be able to see the wired client on DL3 scope



Now we can successfully ping 192.68.100.254 from the wired client. Note that earlier we had created a routing profile entry for this subnet point it through the IPSEC tunnel.

```
(Aruba7010-Standalone) [mynode] #show datapath session | include 199
192.168.100.254   10.199.199.204  1    5     0      0/0     0    0   0   tunnel 11   6    1
60          FI              11
192.168.100.254   10.199.199.204  1    6     0      0/0     0    0   0   tunnel 11   5    1
60          FI              11
192.168.100.254   10.199.199.204  1    7     0      0/0     0    0   0   tunnel 11   4    1
60          FI              11
192.168.100.254   10.199.199.204  1    8     0      0/0     0    0   0   tunnel 11   3    1
60          FI              11
10.199.199.204    192.168.100.254 1    8     2048   1/15794 0    0   0   tunnel 11   3    1
60          FCI             12
10.199.199.204    192.168.100.254 1    6     2048   1/15794 0    0   0   tunnel 11   5    1
60          FCI             12
10.199.199.204    192.168.100.254 1    7     2048   1/15794 0    0   0   tunnel 11   4    1
60          FCI             12
10.199.199.204    192.168.100.254 1    5     2048   1/15794 0    0   1   tunnel 11   6    1
60          FCI             12

(Aruba7010-Standalone) [mynode] #
```