aruba
a Hewlett Packard Enterprise company

IAP VPN TROUBLESHOOTING

Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST
June 27th, 2017

Presenter: Nabeel Akram

Nabeel.akram@hpe.com

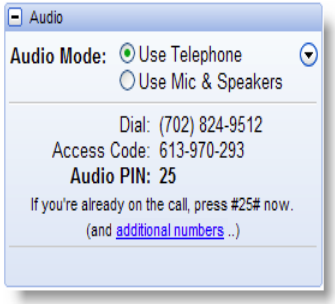
AIRHEADS COMMUNITY

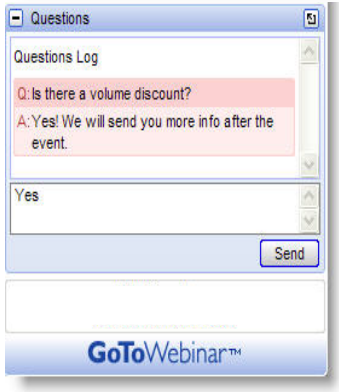
Welcome to the Technical Climb Webinar

Listen to this webinar using the computer audio broadcasting or dial in by phone.

The dial in number can be found in the audio panel, click additional numbers to view local dial in numbers.

If you experience any difficulties accessing the webinar contact us using the questions panel.



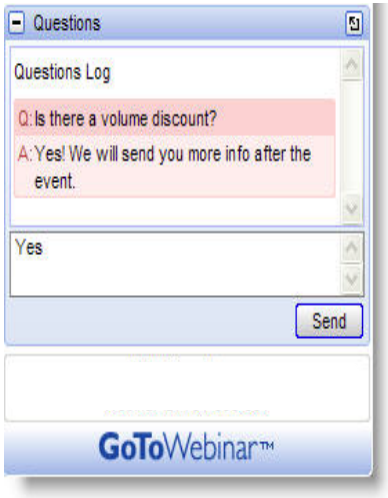


Housekeeping

This webinar will be recorded

All lines will be muted during the webinar

How can you ask questions?
Use the question panel on your screen



The recorded presentation will be posted on Arubapedia for Partners (https://arubapedia.arubanetworks.com/afp/)

IAP VPN TROUBLESHOOTING

aruba
a Hewlett Packard
Enterprise company

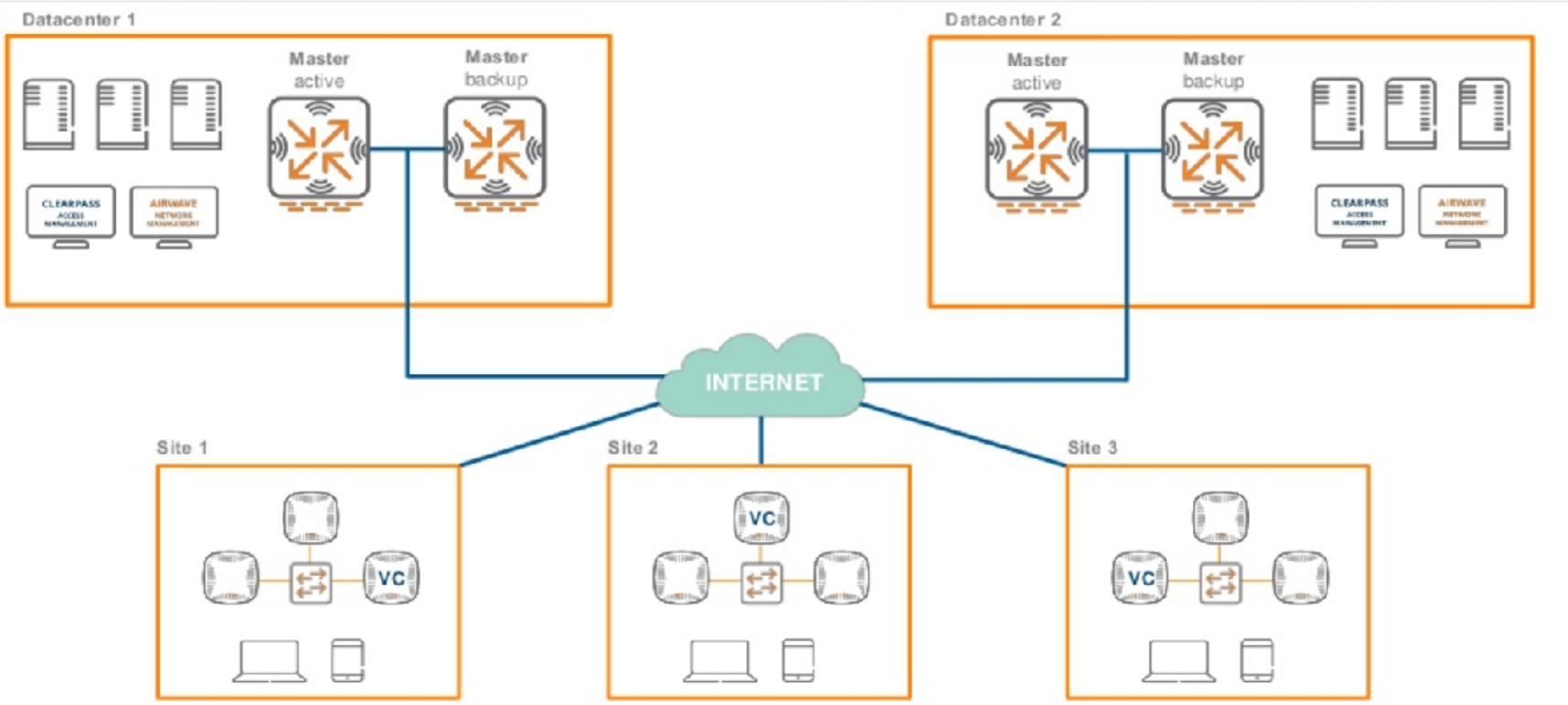
Agenda

- Introduction to RAP-NG architecture.
- BID allocation.
- Modes of Operation.
- Troubleshooting commands and debugging.
- 802.1x authentication, Radius CoA via VPN.

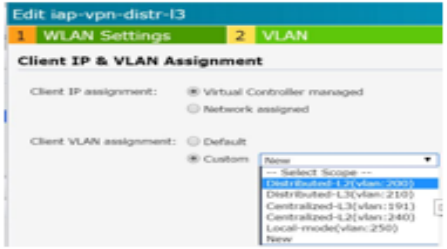
RAP-NG Architecture

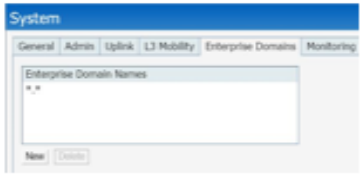
- One of the main issues associated with the classic site-site VPN is cost and complexity.
- Organizations typically need to configure and ship a branch router/VPN gateway to each location for this purpose.
- The zero-touch provisioning capability of Aruba RAPNG architecture takes care of the above steps without any IT intervention and hence eliminates the complexity and reduces the cost associated with the classic site-site IPsec VPN.
- In general, the RAPNG architecture provides the functionalities of a site-site VPN and the simplicity of a VPN server/ client architecture. This architecture has 2 components-
  - Aruba Instant APs at branch sites
  - Aruba controller at the datacenter
- The master IAP at the branch acts as the VPN endpoint and the Aruba controller at the datacenter acts as the VPN concentrator. When an IAP is setup for VPN, it forms an IPsec tunnel (using IKEv2) to the Aruba controller to secure sensitive corporate data.

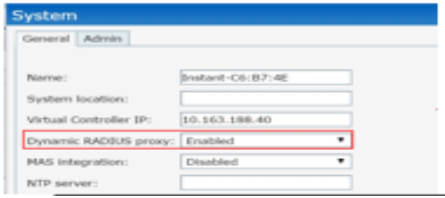
RAP-NG TOPOLOGY



Configuration Flow







VPN tab: Controller + Routing

↓

DHCP tab: DHCP scope

↓

SSID: assign VPN vlan define in DHCP scope to an SSID

↓

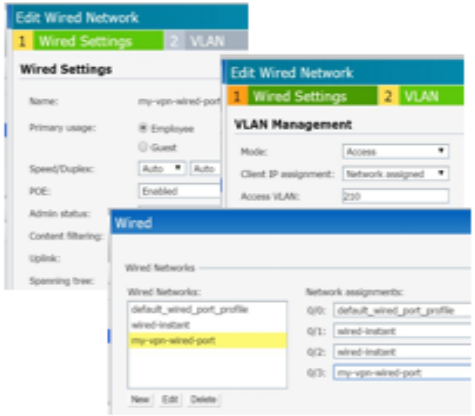
Wired tab: assign VPN vlan defined in DHCP scope to the wired profile/IAP ports (optional)

↓

System tab: Enterprise Domains(optional)

↓

System tab: Dynamic Radius Proxy(optional)



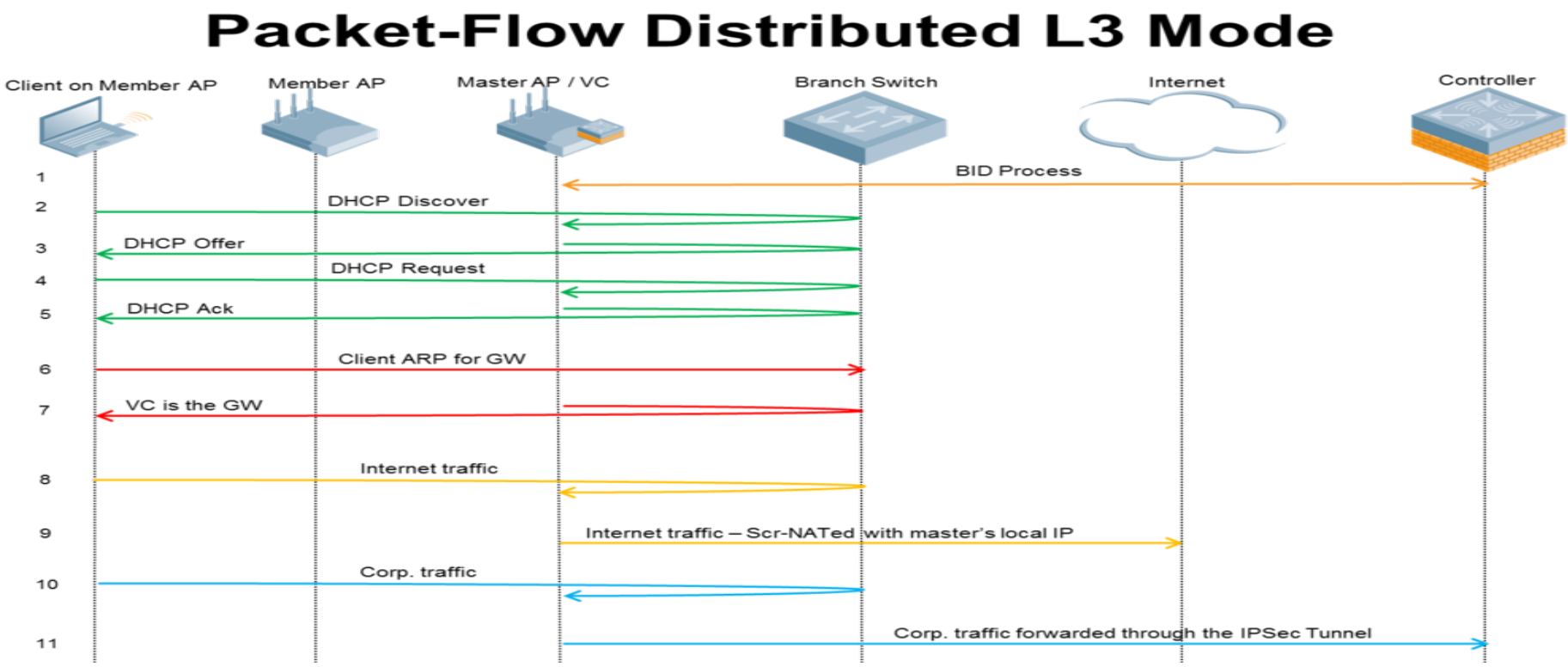
IAP VPN Modes

- **IAP VPN supports 5 operation modes**
  - Distributed L3
  - Distributed L2
  - Centralized L3
  - Centralized L2
  - Local

Distributed L3 Mode

- The most popular mode, contains broadcast and multicast traffic to the branch.
- BID allocation process is mandatory for Distributed L3/L2 mode.
- Master IAP is the DHCP server and default gateway of the clients.
- When the WAN is down, a client can renew/receive IP address.
- Client traffic to datacenter is sourced with the client's own IP address via the tunnel.
- Client traffic to Internet or local is sourced NATted with the Master IAP's local IP.
- Making the VPN pool used for inner IPs routable is essential for RFC3576 and for 802.1X if the RADIUS traffic is not source NATed at the controller and allows access to IAP WebUI from datacenter.
- Controller uses OSPF to redistribute branch routes to the upstream router. OSPF is a must for multi-controller environment and for geographical redundancy.

Packet Flow for Distributed L3



Verification

- **IAP status on the controller**

(A7220)#show iap table long

```
Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name            VC MAC Address     Status    Inner IP     Assigned Subnet              Assigned Vlan
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP      200.1.1.3  10.163.190.16/28,10.163.191.0/24   200

Key                                  Bid(Subnet Name)                                    Tunnel End Points
8b9....2b6f8d2c2  0(10.163.189.100-10.163.189.200,10:200),0(10.163.190.3-10.163.190.200,10)

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

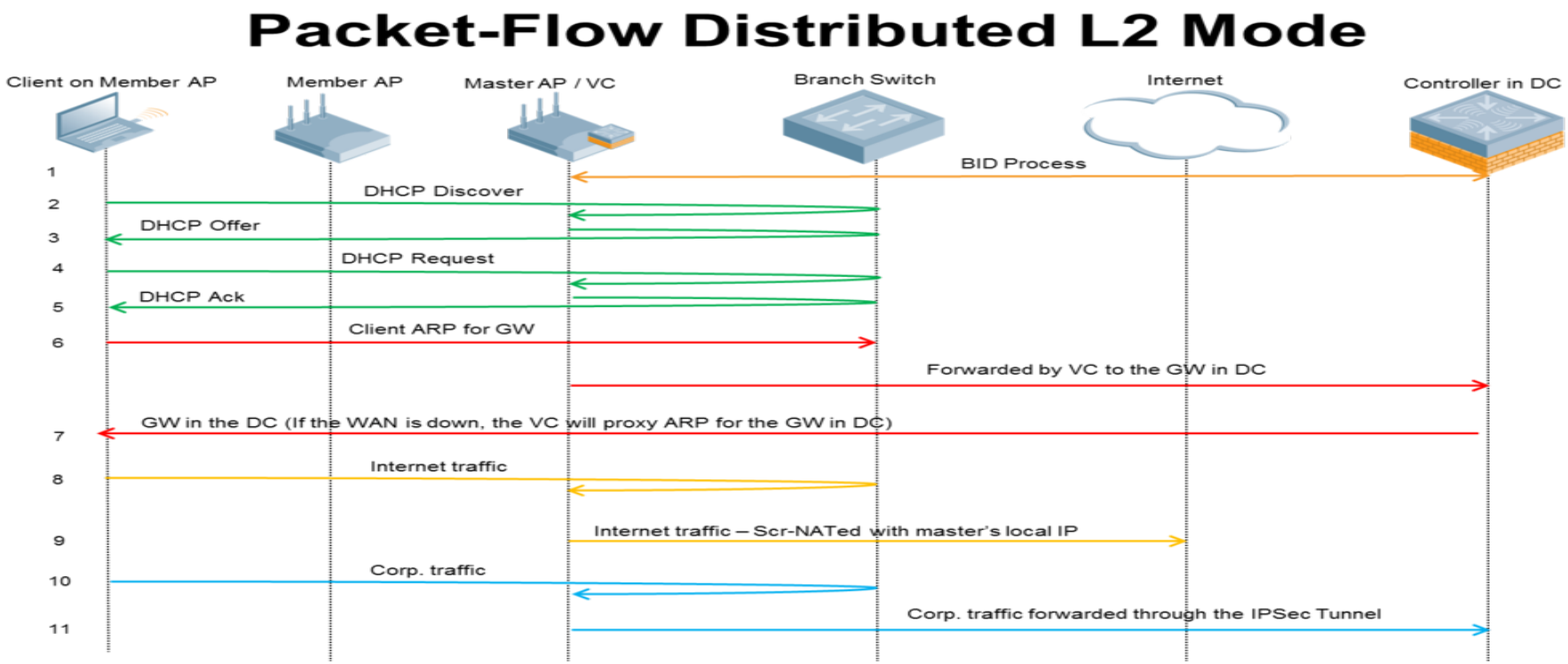
(A7220) #show iap detailed-table

```
Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name            VC MAC Address     Status  Inner IP   Flags  Branch (Subnet / Vlan)
----          --------------     ------ --------  -----  ----------------------
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  PD2    200
Instant-C6:B7:4E  18:64:72:c1:de:ee  N/A    200.1.1.3  PL     N/A
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  PD3    10.163.190.16/28
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  PC3    10.163.191.0/24
```

Distributed L2 Mode

- Branch subnet allocation is done via BID allocation process, it is essential to avoid subnet overlap across branches.
- The Master IAP is the DHCP server and the default gateway of the VPN clients is at the datacenter.
- Client traffic to date center is sourced with the client's own IP address.
- Client traffic to internet or local is sourced with the Master IAP's local IP.
- ARP for default gateway is forwarded to the datacenter. The master IAP will Proxy ARP for the client's gateway when WAN is down.
- Smaller user VLAN subnets are recommended to reduce the broadcast and multicast traffic across WAN link.
- Making the VPN pool used for inner IPs routable is essential for RFC3576 and for 802.1X if the RADIUS traffic is not source NATed at the controller and allows access to instant WebUI from datacenter.

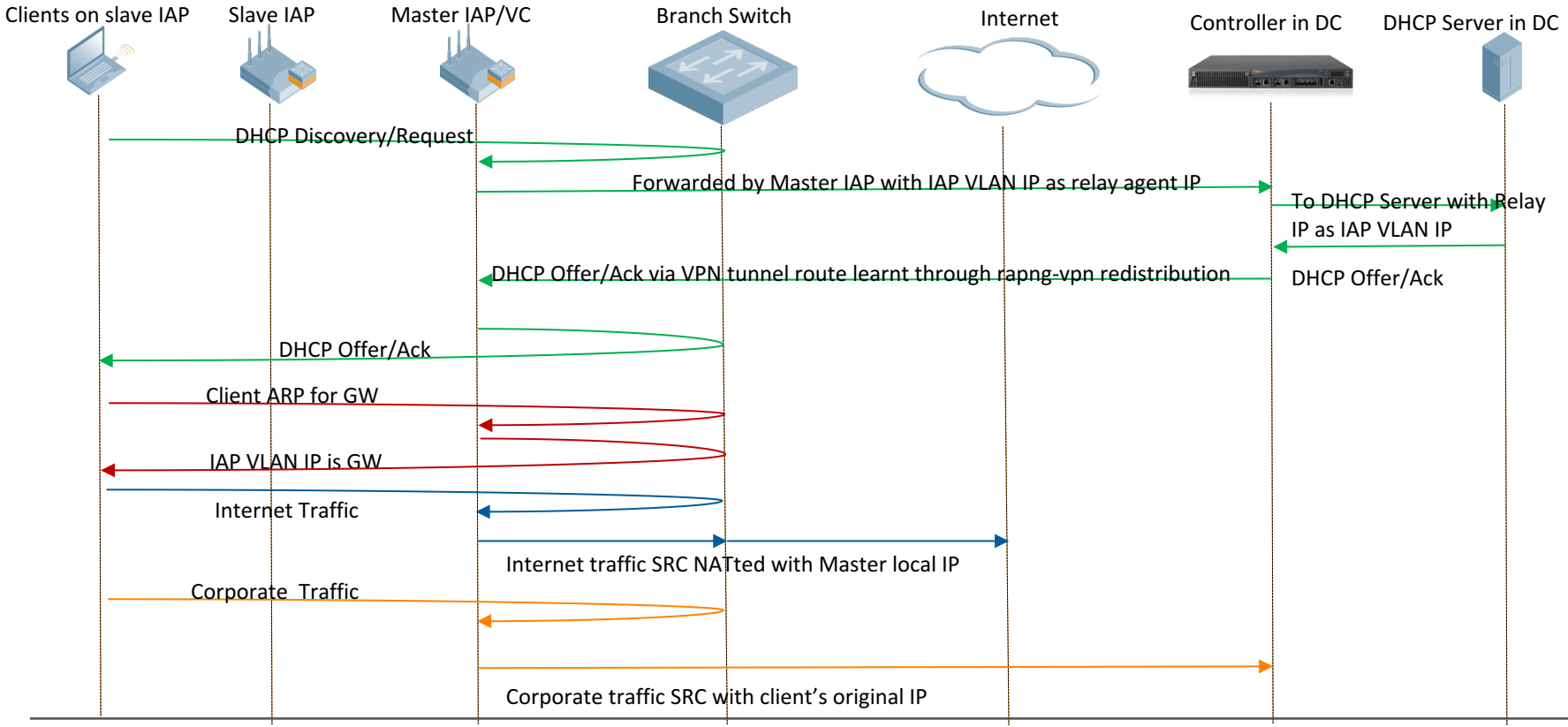
Packet Flow of Distributed L2 Mode



Centralized L3 Mode

- DHCP server is at the data center site.
- DHCP server must have route to reach the IAP-VPN client subnet.
- DHCP relay should be enabled on the IAP as DHCP server is at different subnet.
- VPN client subnet/VLAN does not exist in the data center controller.
- IAP VLAN interface IP is the gateway of the clients.
- OSPF is recommended to be enabled for the controller to route the DHCP traffic back to the IAP via VPN tunnel. Static is not practical as the IPSEC tunnel is dynamic.
- The controller itself can not be the DHCP server as the Internal server needs an VLAN interface to relay the DHCP packets while the VLAN interface could not exist in this mode.
- Client traffic to date center is sourced with the client's own IP.
- Client traffic to internet or local is sourced with Master IAP's local IP

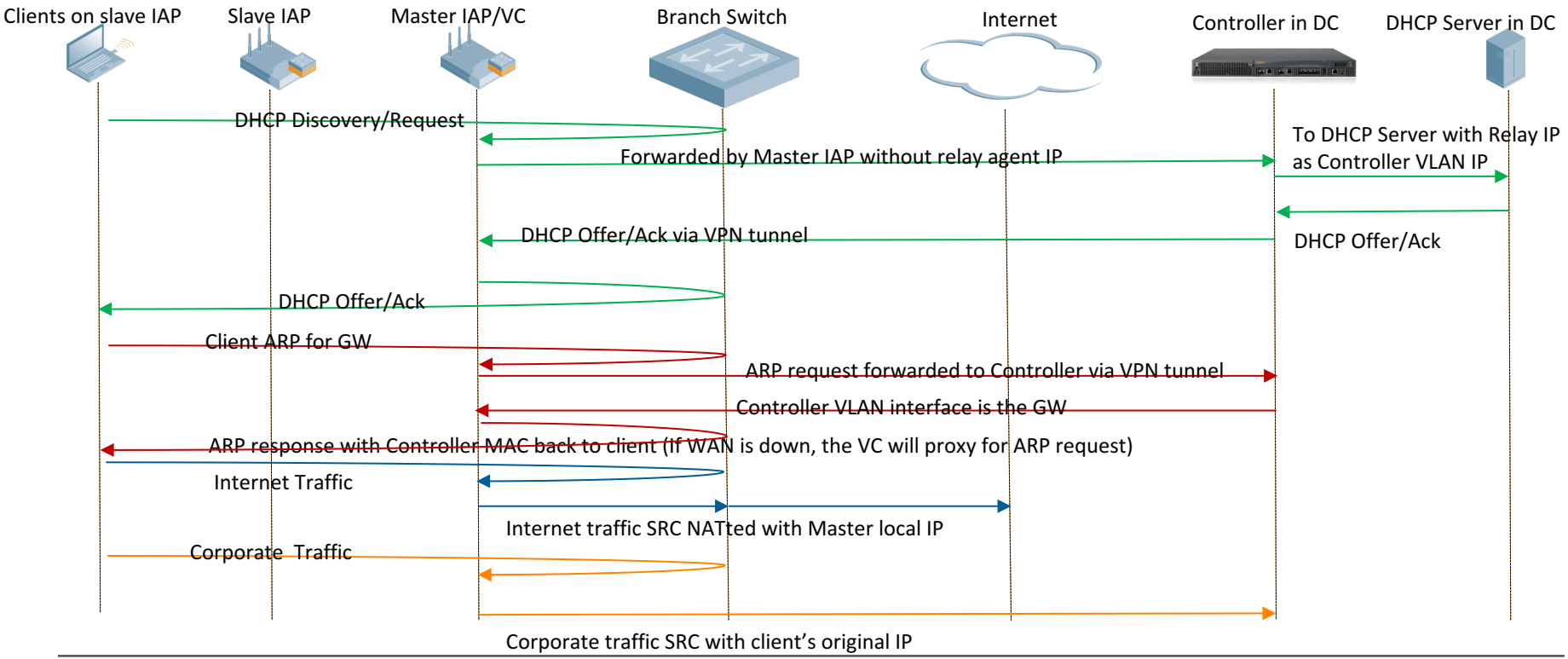
Packet flow


Clients on slave IAP
Slave IAP
Master IAP/VC
Branch Switch
Internet
Controller in DC
DHCP Server in DC
DHCP Discovery/Request
Forwarded by Master IAP with IAP VLAN IP as relay agent IP
To DHCP Server with Relay IP as IAP VLAN IP
DHCP Offer/Ack via VPN tunnel route learnt through rapng-vpn redistribution
DHCP Offer/Ack
DHCP Offer/Ack
Client ARP for GW
IAP VLAN IP is GW
Internet Traffic
Internet traffic SRC NATted with Master local IP
Corporate Traffic
Corporate traffic SRC with client's original IP

Centralized L2 Mode

- A L2 extension of datacenter VLAN/subnet.
- Only recommended if streaming multicast videos or other multicast apps to remote branches are needed.
- The DHCP server & default gateway of the clients are at the datacenter site.
- ARP for default gateway is forwarded to the datacenter. The master IAP will Proxy ARP for the client's gateway when WAN is down.
- DHCP relay should be enabled on the controller VPN VLAN interface if the DHCP server is at different subnet. Do not enable DHCP relay on the IAP in this mode.
- If split-tunnel is enabled, only corporate traffic is forwarded via the VPN tunnel based on the VPN route, others will be SRC-NATted via the master IAP local IP and forwarded locally.
- If a default route 0.0.0.0/0.0.0.0 is pointed to the VPN tunnel, and it is the only route, split-tunnel will not take effect, all traffic is forwarded to the tunnel.
- If split-tunnel is disabled, all of the wireless or wired client traffic in the L2 VLAN are forwarded to the datacenter, and the routing profile is ignored.

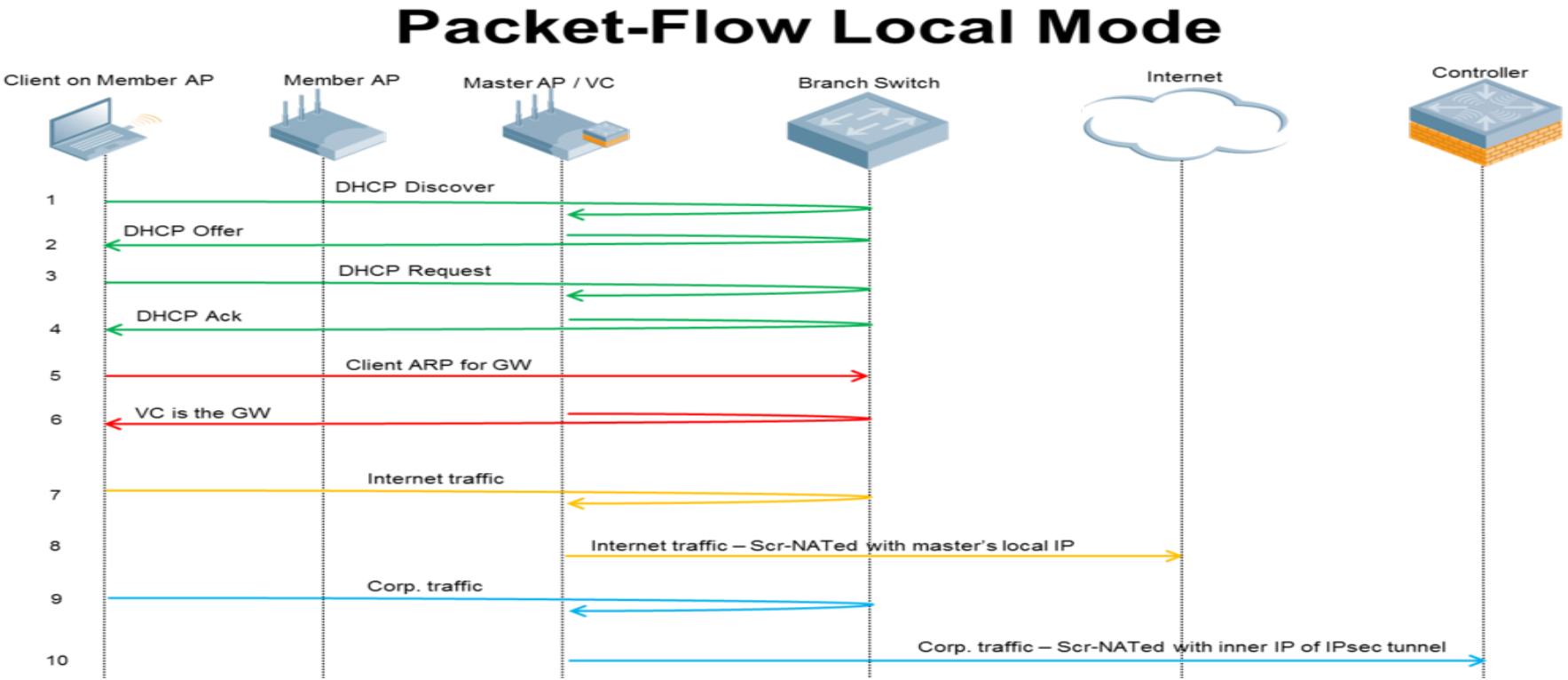
Packet flow


Clients on slave IAP
Slave IAP
Master IAP/VC
Branch Switch
Internet
Controller in DC
DHCP Server in DC
DHCP Discovery/Request
Forwarded by Master IAP without relay agent IP
To DHCP Server with Relay IP as Controller VLAN IP
DHCP Offer/Ack via VPN tunnel
DHCP Offer/Ack
DHCP Offer/Ack
Client ARP for GW
ARP request forwarded to Controller via VPN tunnel
Controller VLAN interface is the GW
ARP response with Controller MAC back to client (If WAN is down, the VC will proxy for ARP request)
Internet Traffic
Internet traffic SRC NATted with Master local IP
Corporate Traffic
Corporate traffic SRC with client's original IP

Local Mode

- Similar to the local network of a home wireless router but with VPN capabilities.
- The Master IAP is the DHCP server and the default gateway of the VPN clients.
- Client traffic to the corporate via the tunnel is source NATted via the IPSEC tunnel inner IP of the Master IAP.
- Client traffic to the local network or Internet is source NATted via the Master IAP's local IP address.
- If the VPN routing is configured as all traffic going through tunnel, then everything is NATted via the IPSEC tunnel inner IP and sent back to the corporate via the Master IAP.
- The IPSEC inner IP needs to be routable otherwise clients wont be able to reach the corporate network.
- Traffic can only be initiated by the clients, can not be initiated via a device from the corporate side.
- Ideal for branch guest networks which use a captive portal server in the datacenter.

Packet Flow


Packet-Flow Local Mode
Client on Member AP
Member AP
Master AP / VC
Branch Switch
Internet
Controller
1
DHCP Discover
2
DHCP Offer
3
DHCP Request
4
DHCP Ack
5
Client ARP for GW
6
VC is the GW
7
Internet traffic
8
Internet traffic – Scr-NATed with master's local IP
9
Corp. traffic
10
Corp. traffic – Scr-NATed with inner IP of IPsec tunnel

Verification

(A7220)#show iap table

```
Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name           VC MAC Address     Status  Inner IP   Assigned Subnet                Assigned Vlan
----           --------------     ------  --------   ---------------                -------------
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  10.163.190.16/28,10.163.191.0/24   200,240
```

(A7220) #show iap detailed-table

```
Trusted Branch Validation: Disabled
IAP Branch Table
----------------
Name           VC MAC Address     Status  Inner IP   Flags  Branch (Subnet / Vlan)
----           --------------     ------  --------   -----  ----------------------
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  PD2    200
Instant-C6:B7:4E  18:64:72:c1:de:ee  N/A    200.1.1.3  PL     N/A
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  PD3    10.163.190.16/28
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  PC3    10.163.191.0/24
```

Summary

Features	IAP VPN Modes				
	Local mode	**Centralized L2**	**Centralized L3**	**Distributed L2**	**Distributed L3**
DHCP Server	VC	DHCP server in the Datacenter	DHCP server in the Datacenter	VC	VC
Default GW for Clients	VC	Controller or a router in the Datacenter	VC	Controller or a router in the Datacenter	VC
Corporate Traffic	Scr-NATed by VC with the inner IP of IPsec tunnel	L2 reachable (forwarded by VC through the IPsec tunnel)	Routed (routed by VC through the IPsec tunnel)	L2 reachable (forwarded by VC through the IPsec tunnel)	Routed (routed by VC through the IPsec tunnel)
Internet Traffic	Scr-NATed with Master APs local IP	Scr-NATed with Master APs local IP	Scr-NATed with Master APs local IP	Scr-NATed with Master APs local IP	Scr-NATed with Master APs local IP
Branch Access from Datacenter	No	Yes	Yes	Yes	Yes
Authentication survivability feature for 802.1X	Yes	Yes	Yes	Yes	Yes

“debug pkt” Command

- **It is a very useful command for VPN troubleshooting.**
- **As VPN client traffic may go out via tunnel interface or IAP local IP, the majority of VPN cases are related to that the traffic may not go out through the right interface or may not source with the right IP as what we have expected. “debug pkt” & “debug pkt dump” will give us those details such as egress interface, ingress interface & packet source IP.**

```
18:64:72:c1:de:ee# debug pkt type ?
<type1>    arp/pppoe/mobility/icmp/tcp/udp/gre/dhcp/dns/radius/http/https/all

18:64:72:c1:de:ee# debug pkt type dhcp
18:64:72:c1:de:ee# debug pkt dump
Received packet from aruba001 (timestamp 2639373626)
#mac: etype 0800 smac 0c:8b:fd:62:79:6f dmac ff:ff:ff:ff:ff:ff
 #ip: sip 0.0.0.0, dip 255.255.255.255, proto 17, dscp 24, fragment ok, last fragment,
fragment offset 0
   #udp: sport 68 dport 67 len 309
    #dhcp: message-type: request
         hardware type: 1, len: 6, hops: 0
         txn id: 0x158b2f36, seconds elapsed: 0
         boot flags: 0x8000
         client mac: 0c:8b:fd:62:79:6f
         magic cookie: 0x63825363
    #dhcp-option: requested-ip: 115.1.1.46
```

Commands to Find Subnet Info in Distributed Mode

- **In Distributed Mode, the VPN client IP subnet info, such as IP subnet, IP range, netmask, default gateway, etc., are all allocated by the controller dynamically after BID process.**
- **There are a few DHCP commands on IAP to check out client subnet info.**

```
18:64:72:c1:de:ee# show dhcp-allocation
#profile: Distributed-L2
{
    vlan-id=200
    dhcp-range=10.163.189.112,10.163.189.117,255.255.255.0,14400s
    dhcp-option=1,255.255.255.0
    dhcp-option=3,10.163.189.1
    dhcp-option=6,10.1.10.10
    dhcp-option=15,arubanetworks.com
```

```
18:64:72:c1:de:ee# show dhcp
DHCP Subnet Table
-----------------
VLAN  Type  Subnet       Mask           Gateway      Mode              Rolemap
----  ----  ------       ----           -------      ----              -------
200   l2    0.0.0.0      255.255.255.255  0.0.0.0      remote,full-tunnel
250   nat   115.1.1.0     255.255.255.0    115.1.1.1    local,split-tunnel
210   l3    10.163.190.16  255.255.255.240  10.163.190.17  local,split-tunnel
191   l3    10.163.191.0   255.255.255.0    10.163.191.1   remote,split-tunnel
```

```
18:64:72:c1:de:ee# show dhcps
Distributed DHCP Scopes
Name          Type          VLAN  Netmask  Default Router  DNS Server  Domain Name   Lease Time  IP Address Range          Client Count
Distributed-L3  Distributed,L3  210   0.0.0.0  0.0.0.0    10.1.10.10  arubanetworks.com  14400      10.163.190.3-10.163.190.200  10
DHCP Option  Reserve First  Reserve Last  Branch ID     Branch Netmask   Branch Router  DHCP Host
                4             0             10.163.190.16  255.255.255.240  10.163.190.17
```

Command for IAP Status & Branch KEY & BID

(A7220) **#show iap table long**

```
Name           VC MAC Address     Status  Inner IP   Assigned Subnet              Assigned Vlan
instant-CE:22:E6  04:bd:88:ce:22:e6  UP     200.1.1.9  10.163.190.32/28             200
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.3  10.163.190.16/28,10.163.191.0/24  200

Key                                                              Bid(Subnet Name)
b6d88c73015e3d905edf9c5e6b3955f103a569a2edd73574a7  1(10.163.190.3-10.163.190.200,10),1(10.163.189.100-10.163.189.200,10:200)
8b9aee28019ede132fa5ae76969da095ed4e794682b6f8d2c2  0(10.163.189.100-10.163.189.200,10:200),0(10.163.190.3-10.163.190.200,10)
```

(A7220**) #show iap detailed-table**

```
Trusted Branch Validation: Disabled
IAP Branch Table
Name           VC MAC Address     Status  Inner IP    Flags  Branch (Subnet / Vlan)
----           --------------     ------  --------    -----  ----------------------
instant-CE:22:E6  04:bd:88:ce:22:e6  UP     200.1.1.9   PD3    10.163.190.32/28
instant-CE:22:E6  04:bd:88:ce:22:e6  UP     200.1.1.9   PD2    200
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.10  PC2    200
Instant-C6:B7:4E  18:64:72:c1:de:ee  N/A    200.1.1.10  PL     N/A
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.10  PD3    10.163.190.16/28
Instant-C6:B7:4E  18:64:72:c1:de:ee  UP     200.1.1.10  PC3    10.163.191.0/24

Total No of UP Branches   : 2
Total No of DOWN Branches : 0
Total No of Branches      : 2
```

Trusted Branches

- **Since AOS 6.4+ and IAP 4.0+, only IAPs managed by Aruba Central or Airwave can form VPN tunnel to a controller and they are not allowed to if they are locally managed.**
- **For IAP pre-4.0 VPN deployments or locally-managed IAPs to work, the IAP mac address needs to be added into IAP trusted DB:**

(A7200)**#iap trusted-branch-db add mac-address**
(A7200)**#iap trusted-branch-db allow-all**

- **Check if the clients are in the trusted-db:**

(A7220) **#show iap trusted-branch-db**

Trusted Branch Validation: Disabled
IAP Trusted Branch Table

Branch MAC
(allow all as trusted branch)

Other useful commands

- **Show datapath route**
  - Datapath routing table is a key table for how and via which interface the IAP forwards the VPN clients' traffic.

```
18:64:72:c1:de:ee# show datapath route
IP          Mask          Gateway       Cost  VLAN  Flags
0.0.0.0     0.0.0.0       15.1.1.1      0     0
10.0.0.0    255.0.0.0     10.163.188.38 0     0     T
15.1.1.0    255.255.255.0 15.1.1.252    0     1     L
192.168.1.0 255.255.255.0 192.168.1.1   0     3333  D
```

- **Show datapath session**
  - Datapath session table is useful for checking if the traffic is NATted.

```
18:64:72:c1:de:ee# show datapath session | in .33
10.163.189.33   74.125.28.147  6  62462 443  0  0  24 1  local   120 SRC  ====➔traffic to internet or local network is SRC NATTed
10.163.188.111  10.163.189.33  1  80    0    0  0  0  1  dev13   38  FI   ======➔traffic to 10.0.0.0 will not be NATted
```

- **Show vpn status/config/tunnels**
- **Show run | begin bid**
  - Bid is assigned when the IAP cluster came up for the first time and saved into configuration. Do not copy configuration with BID to a new cluster, otherwise it may cause duplicate BID.

Case Studies

- **Symptom**
  - All the VPN traffic is sent via the IPSEC tunnel to the datacenter, but the VPN route is not optimal route for some servers in the branch.
- **Reason**
  - Default route of VPN has pointed to the datacenter controller, it excludes the possibility for accessing some servers locally in the branch.
- **Solution**
  - To reach a server through the IAP local route instead of the VPN tunnel, we can add specific route for the server pointing to gateway “0.0.0.0” in the VPN routing profile.

Clients on Slave IAP Fail to Get IP

- **Symptom**
  - VPN Clients on Master IAP work fine, but clients on slave IAPs could not get IP.
- **Reason**
  - In an IAP cluster only the master AP forms the VPN tunnel to the controller. All the VPN traffic in non default VLAN on slave IAPs have to be sent to the master IAP with VLAN tagging. If the slave IAP uplink port is an access port, all the VPN traffic will be dropped, the VPN client will fail to get IP.
- **Solution**
  - The uplink port of IAPs should be configures as trunk ports and the ports should allow the VPN VLANs.

VPN Tunnel Not Come Up After Upgrading

- **Symptom**
  - After IAP cluster upgraded to release 4.2, IAP VPN failed to come up.
- **Reason**
  - Since AOS 6.4+ and IAP 4.0+, only IAPs managed by Aruba Central or Airwave can form VPN tunnel to a controller and is not allowed to if they are locally managed.
- **Solution**
  - Adding all the IAP mac addresses into IAP trust DB in the controller.

```
(A7200)#iap trusted-branch-db add mac-address
or
(A7200)#iap trusted-branch-db allow-all
```

Only single branch works due to conflicting BID

- **Symptom**
  - One IAP branch works, but the other fails.
- **Reason**
  - Two IAP clusters were in the same cluster in the past and have been assigned the same BID which was pushed into the configuration permanently. Duplicate BID caused the second up running IAP cluster fail to work.
- **Solution**
  - Delete one of the IAP clusters and force it to renegotiate a new BID.

Deleting a Branch

- **We can use the following command to delete a branch:**

```
(A7220) #show iap table long
----------------
Name   VC MAC Address     Status  Inner IP   Assigned Subnet     Assigned Vlan  Key
instant-CE:22:E6  04:bd:88:ce:22:e6  UP  200.1.1.9  10.163.190.32/28  200          b6d88c73015e3d905edf9c5e6b3955f103a569a2edd73574a7
```

(A7220) **#iap del branch-key** b6d88c73015e3d905edf9c5e6b3955f103a569a2edd73574a7

- **Before a branch is deleted, the branch needs to be in the "Down" state.**

```
(A7220) #show crypto ipsec sa


IPSEC SA (V2) Active Session Information
-----------------------------------
Initiator IP     Responder IP     SPI(IN/OUT)       Flags Start Time       Inner IP
------------     ------------     ----------------  ----- ---------------  --------
10.163.188.41    10.163.188.38    1459d300/4a29ef00  UT2   Dec  7 10:32:44   200.1.1.3
10.163.188.253   10.163.188.38    6b56c000/c09b8e00  UT2   Dec  7 11:04:57   10.163.188.253
10.163.145.46    10.163.188.38    7bddf400/7610e100  UT2   Dec  7 10:31:24   200.1.1.9
```

(A7220) **#clear crypto ipsec sa peer** 10.163.145.46

Client Traffic not Follow Routing Profile

- **Symptom**
  - Centralized L2 VPN client traffic are all forwarded to the datacenter instead of following the route configuration in the VPN routing profile.
- **Reason**
  - In the CL2 mode configuration, split-tunnel is disabled and it forces all client traffic getting into “full-tunnel” mode and being forwarded via tunnel to the datacenter and the routing profile is ignored completely.

```
18:64:72:c1:de:ee# show dhcp subnets

DHCP Subnet Table
-----------------
VLAN  Type  Subnet       Mask          Gateway      Mode            Rolemap
----  ----  ------       ----          -------      ----            -------
200   l2    0.0.0.0      255.255.255.255  0.0.0.0      remote,full-tunnel
250   nat   115.1.1.0     255.255.255.0    115.1.1.1     local,split-tunnel
191   l3    10.163.191.0  255.255.255.0    10.163.191.1  remote,split-tunnel
```

- **Solution**
  - Enable split-tunnel mode in the CL2 configuration, the client traffic will follow the routes defined in the VPN routing profile.

Local mode users unable to access DC resources

- **Symptom**
  - Local mode VPN users could not reach servers in the datacenter.
- **Reason**
  - Local mode VPN user traffic is Natted via the tunnel inner IP when they are sent to the datacenter. However the inner IP is not routable IP in the datacenter network and it causes the servers' responding traffic get dropped.
- **Solution**
  - Make the controller local L2TP pool for IAP VPN routable.

Clients Traffic Lost after Failover

- **Symptom**
  - VPN clients are in distributed L3 mode, they are working fine with primary controller, but could not send traffic after failover to the backup controller.

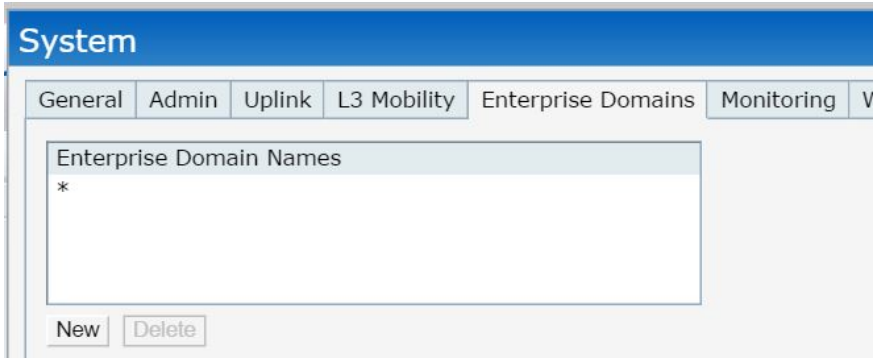
- **Reason**
  - Static routes do not work for multiple controllers environment for redundancy. Without OSPF, the backup datacenter wont be able to learn the routes of the DL3 client subnets, the client's traffic will break after failover happens.

- **Solution**
  - Enable OSPF on the primary and the backup VPN controllers.

```
#show run | begin "router o"
router ospf
router ospf router-id 10.163.188.38
router ospf area 0.0.0.0
router ospf redistribute rapng-vpn
```

Client's DNS Server not Being Used

- **Symptom**
  - VPN clients' own DNS server IP is not being used for name resolution as expected, all DNS traffic is forwarded to the IAP's uplink DNS server.
- **Reason**
  - The default behavior of name resolution for IAP VPN clients is to proxy all client's DNS traffic with IAP's own DNS server instead of using the clients' own DNS server.
- **Solution**
  - Define the domain names which needs to use the clients' DNS under "Enterprise Domains" tab of "System". To use the clients' DNS server for all name resolution, add "*" under "Enterprise Domains" tab.



Centralized L2 Client not able to Get IP

- **Symptom**
  - Centralized L2 clients are assigned to a dedicated VLAN in the controller, but they could not get IP addresses.
- **Reason**
  - There are no physical ports belong to the VPN client VLAN in the controller, the VLAN is in the “down” state. The controller wont be able to forward any traffic in a “down” state VLAN.
- **Solution**
  - Add “operstate up” command under the VPN VLAN interface in the controller. It will bring up the VLAN.

Dot1x Auth Fails due to DRP Disabled

- **Symptom**
  - 802.1x VPN users fail authentication against the radius server in the datacenter.

- **Reason**
  - DRP is not enabled. Only when DRP is enabled, the radius packets of clients are sourced with master IAP's inner IP, otherwise, the client's own IP address is used as the source IP in centralized modes. As the client's IP is not valid radius client IP configured in the radius server, all authentication will fail.

- **Solution**
  - Enable "DRP" under "System" tab. Also recommend enabling source NAT for all radius traffic under "default-vpn-role" to controller IP, then only controller IP needs to be configured as radius client in the radius server, otherwise each IAP inner IP needs to be configured in the radius server.

RFC 3576 COA not Working

- **Symptom**
  - Radius server is at the datacenter, all dot1x users traffic is SRC-NATted via the controller IP, and dot1x users work fine, but RFC 3576 COA function is not working
- **Reason**
  - RFC 3576 COA messages are initiated by the radius server, the server needs to send COA messages directly to the radius clients (IAP master Inner IP). NAT wont work here.
- **Solution**
  - Make the IAP inner IP routable and disable NAT on the controller side.

THANK YOU!

aruba
a Hewlett Packard
Enterprise company