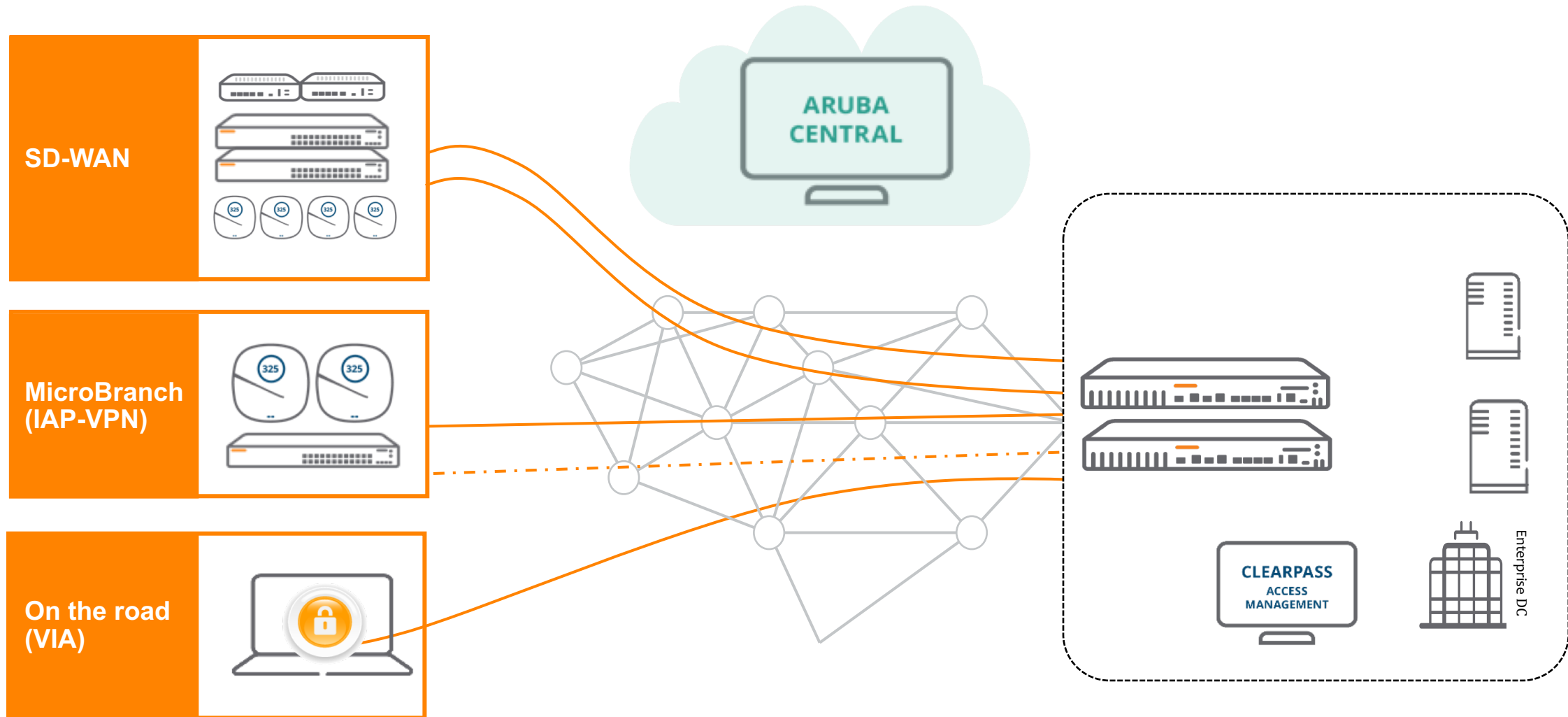


Aruba SD-WAN

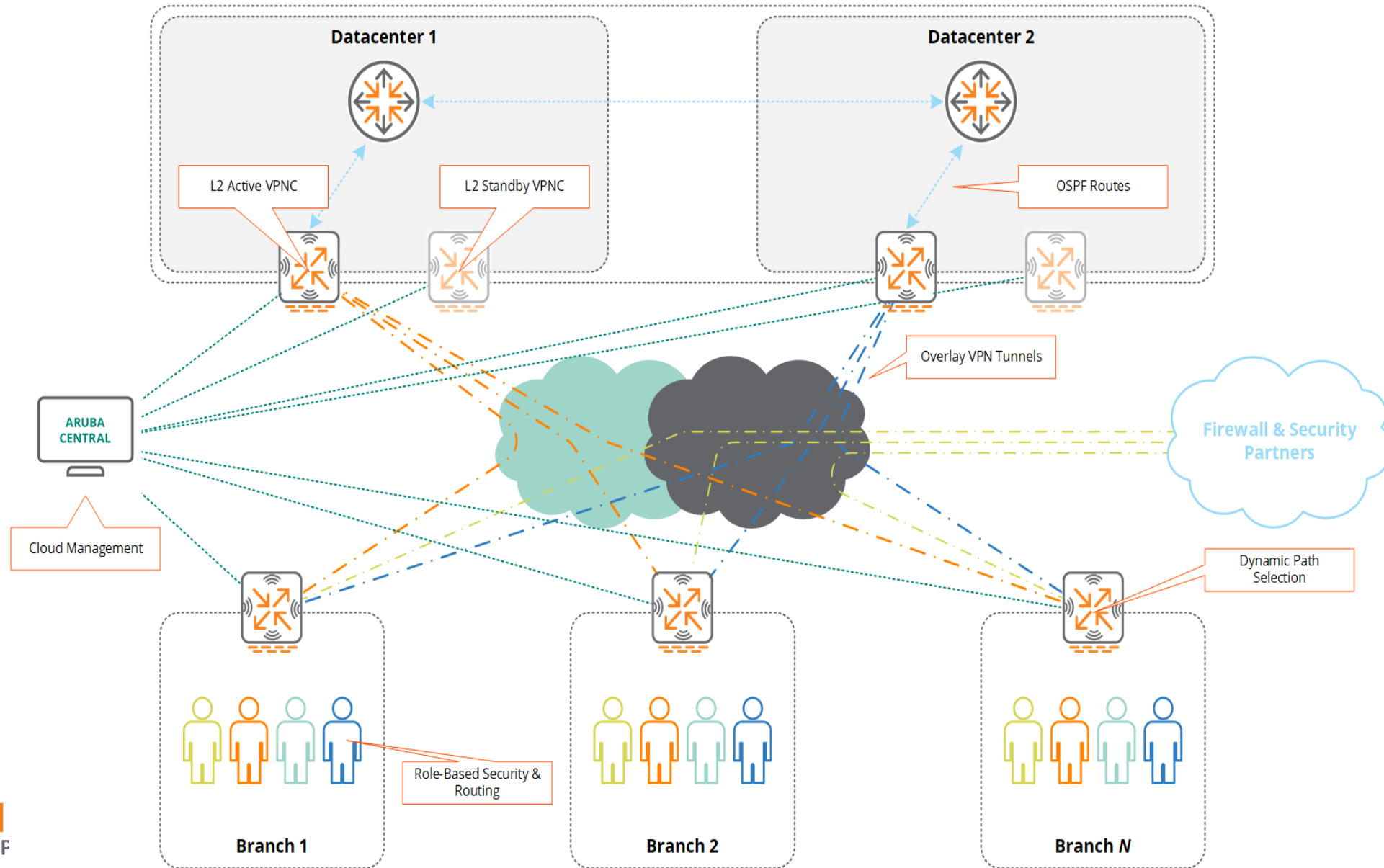
John Schaap
john.schaap@hpe.com

25 October 2018

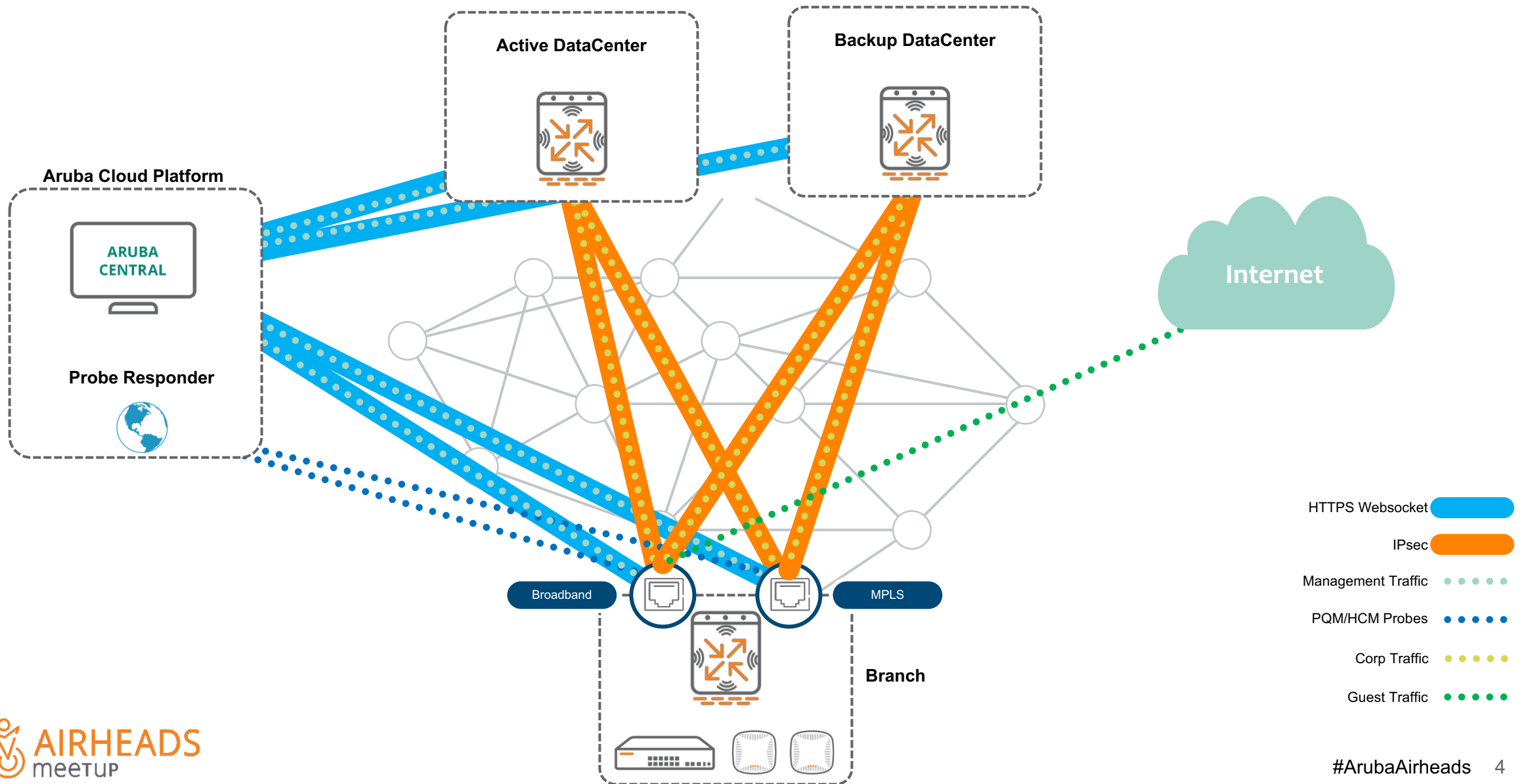
Aruba Distributed Architectures



SD-WAN solution Overview

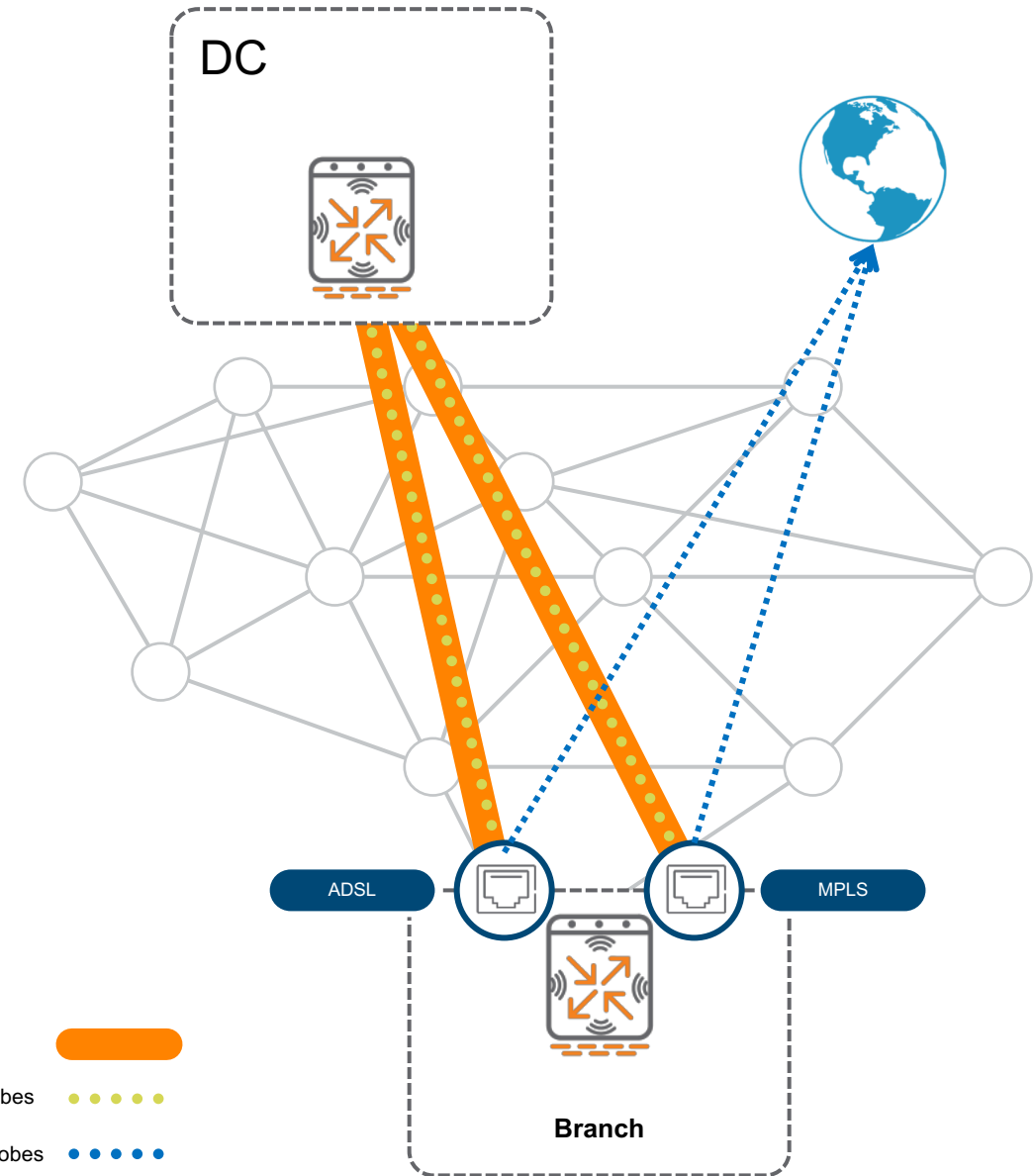


Overview Architecture



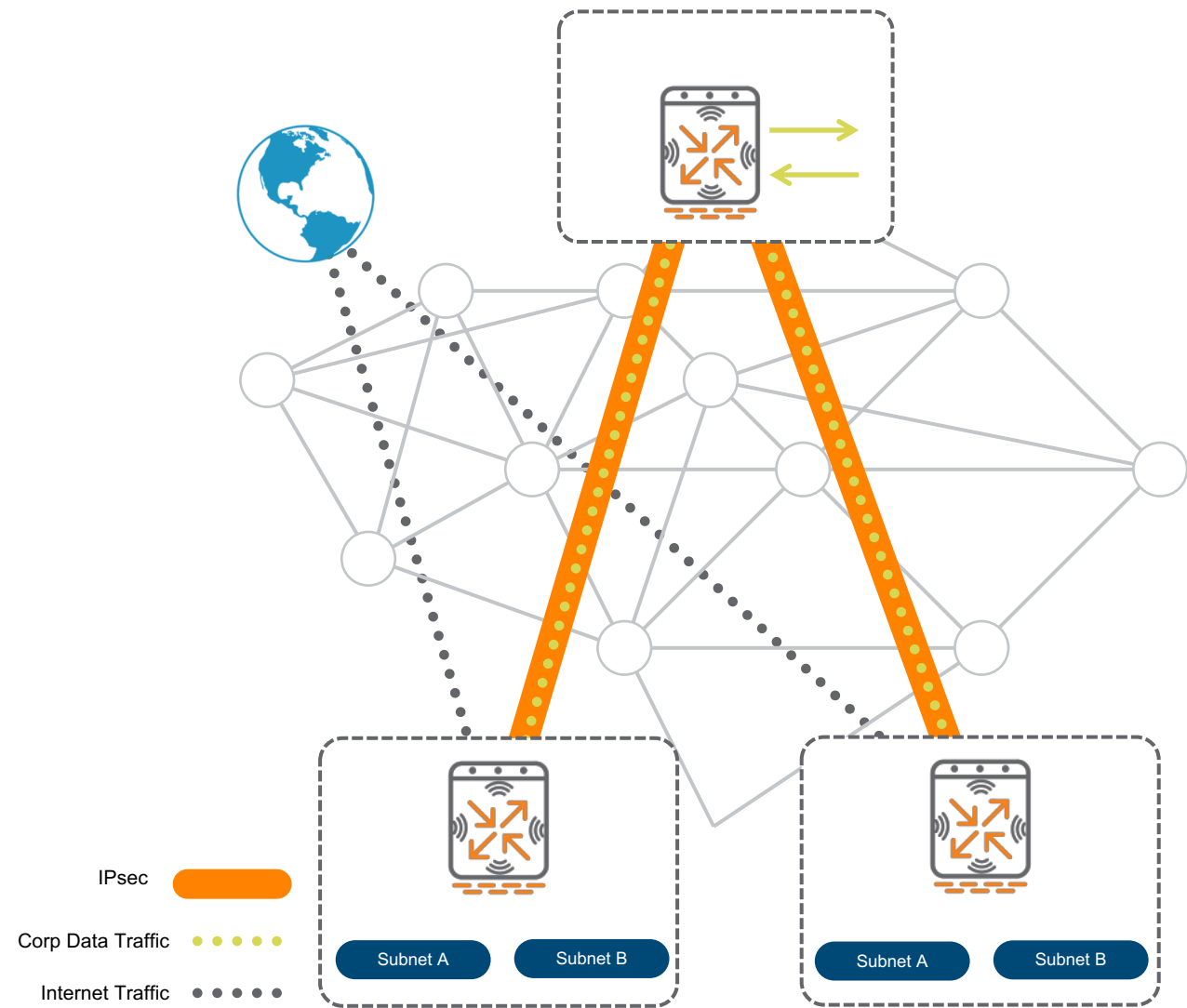
WAN Health Check Monitor

- ICMP Probes measure Internet reachability.
Recommended: **pqm.arubanetworks.com**
- DPD probes monitor tunnel status
- If HCM reports uplink down
 - No src-natted traffic
 - No communication with Aruba Central
- If DPD reports tunnel down
 - Tunnels are torn down



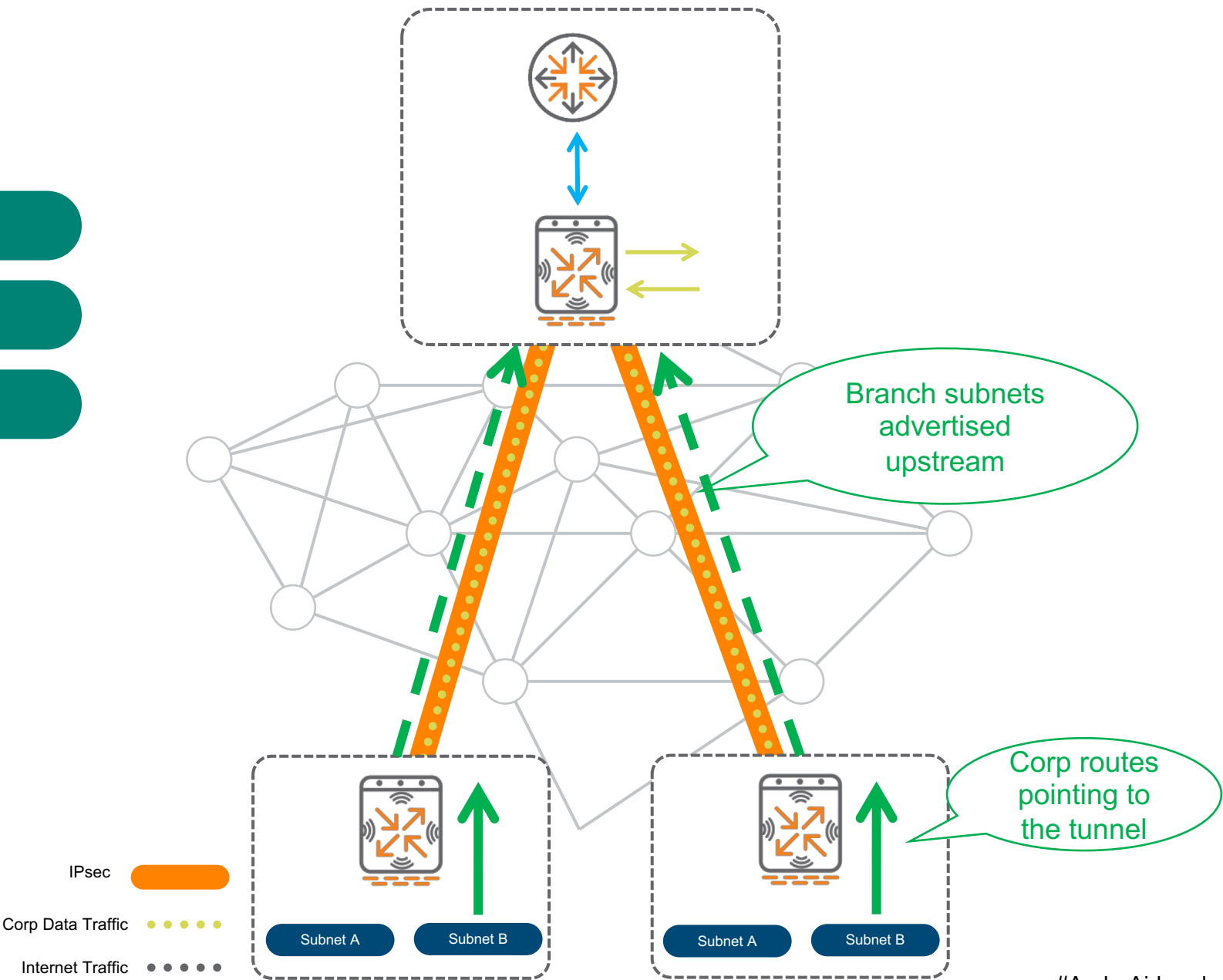
Step 1: Build a secure overlay

Automatic tunnel establishment



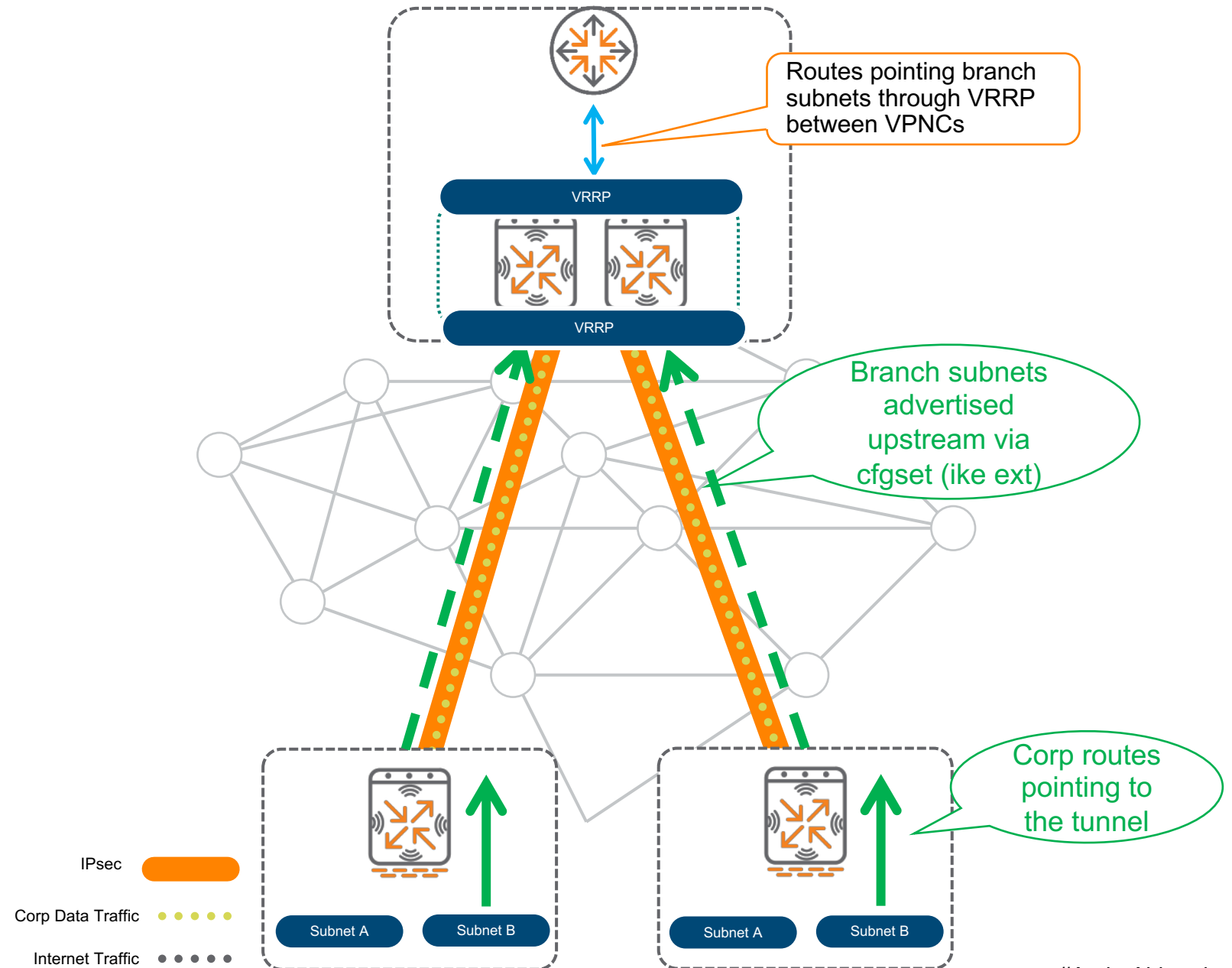
Auto Hub & Spoke

- 1 Bring UP tunnels
- 2 Advertise branch subnets
- 3 Add routes to tunnels



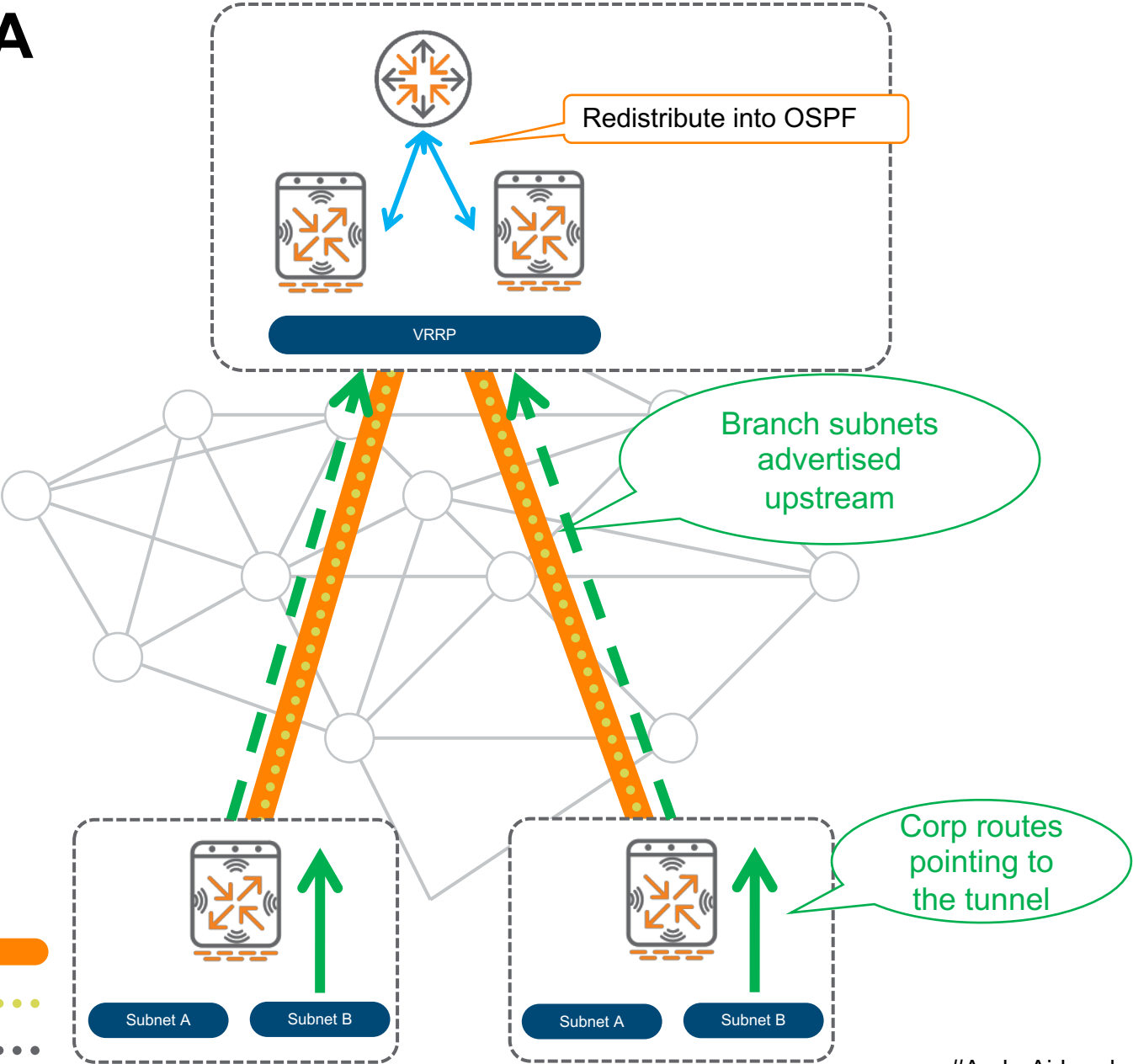
Single DC L2 HA

Using static routes

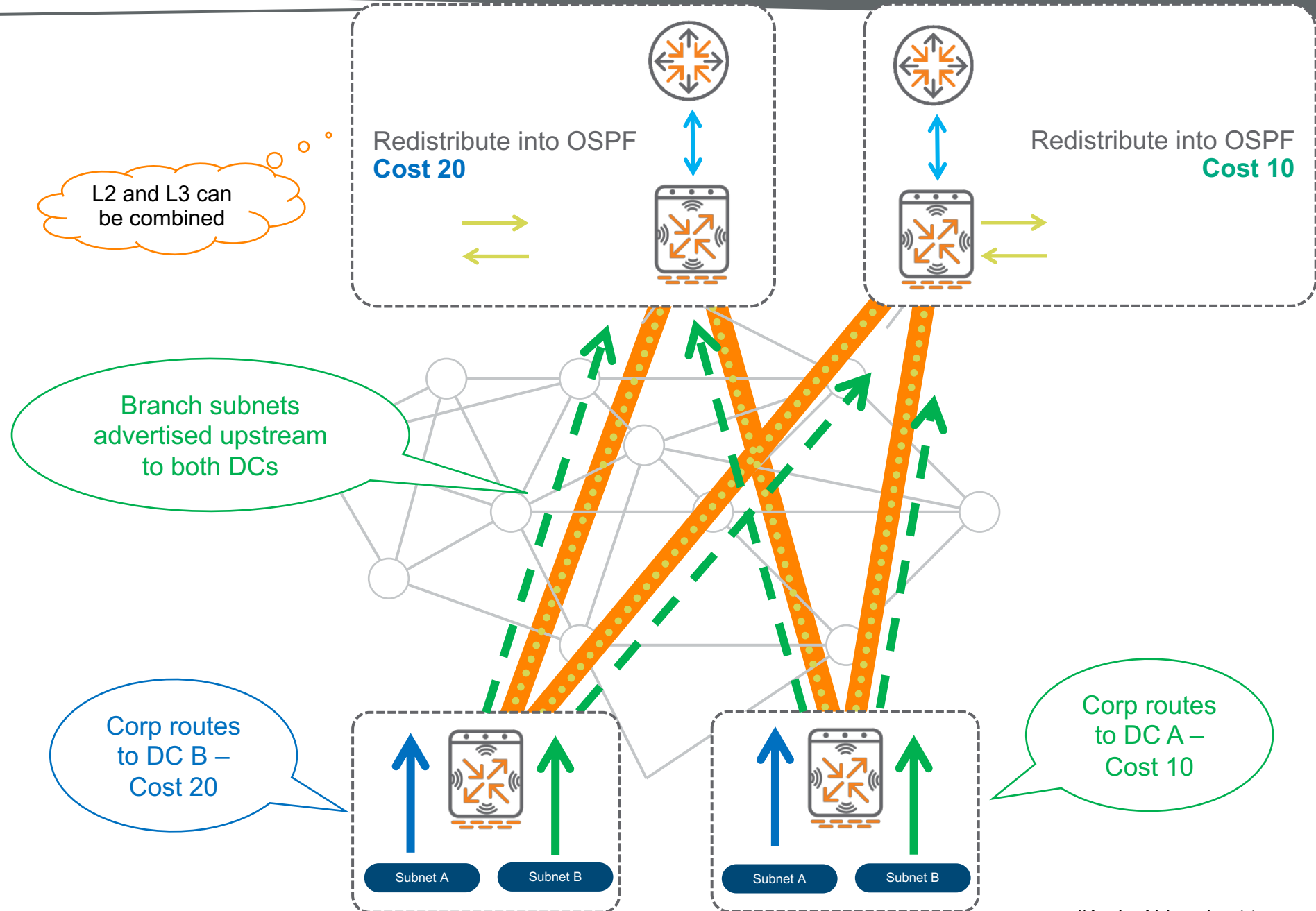


Auto Hub & Spoke – L2 HA

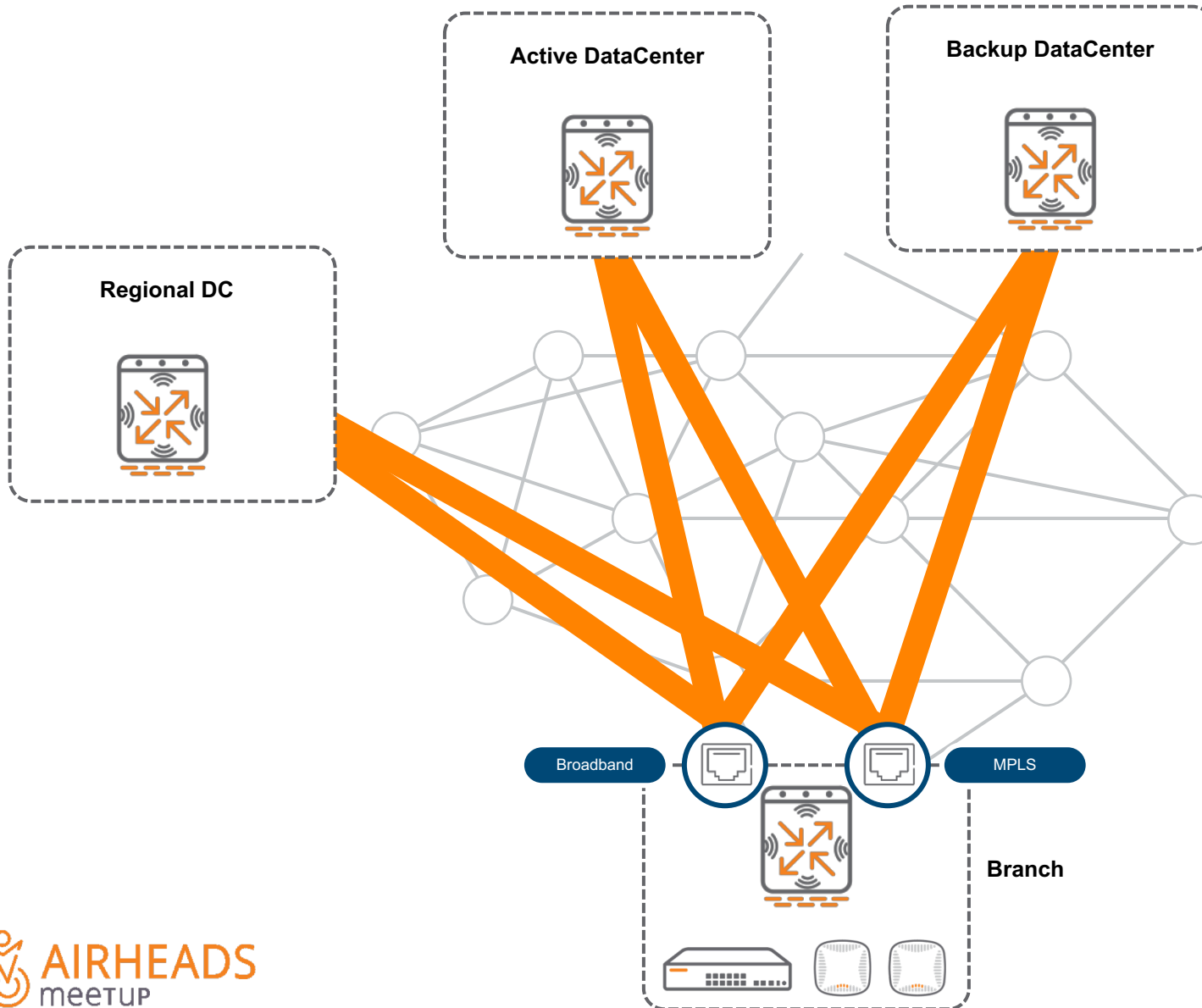
- 1 VRRP between 2 VPNCs
- 2 Track uplink interface/VLAN
- 3 Preempt? – use with caution (and delay)



Multiple hubs



Regional Hubs



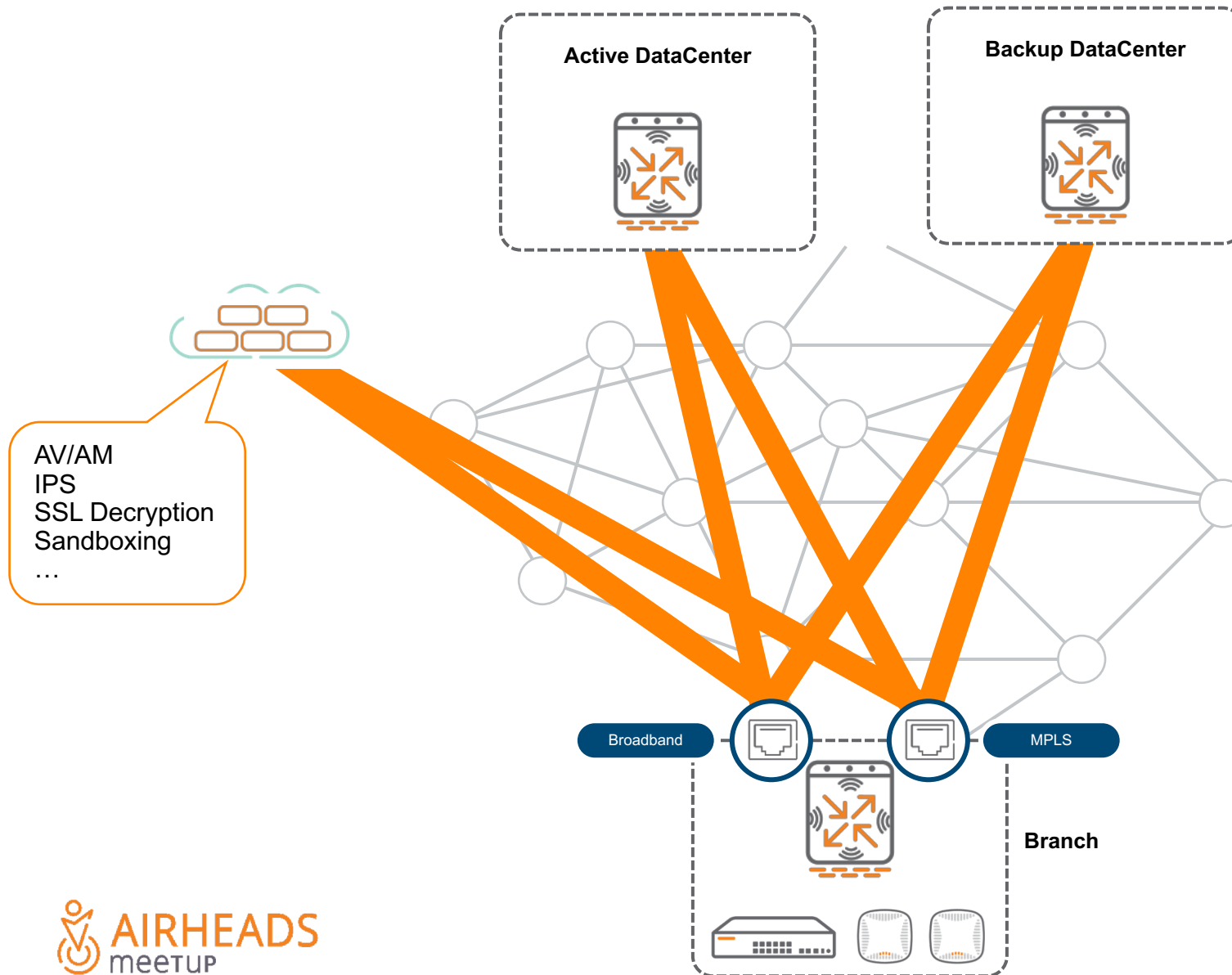
1

More specific route to regional DC

2

Routes only redistributed locally or exported with high cost

Cloud Services integration



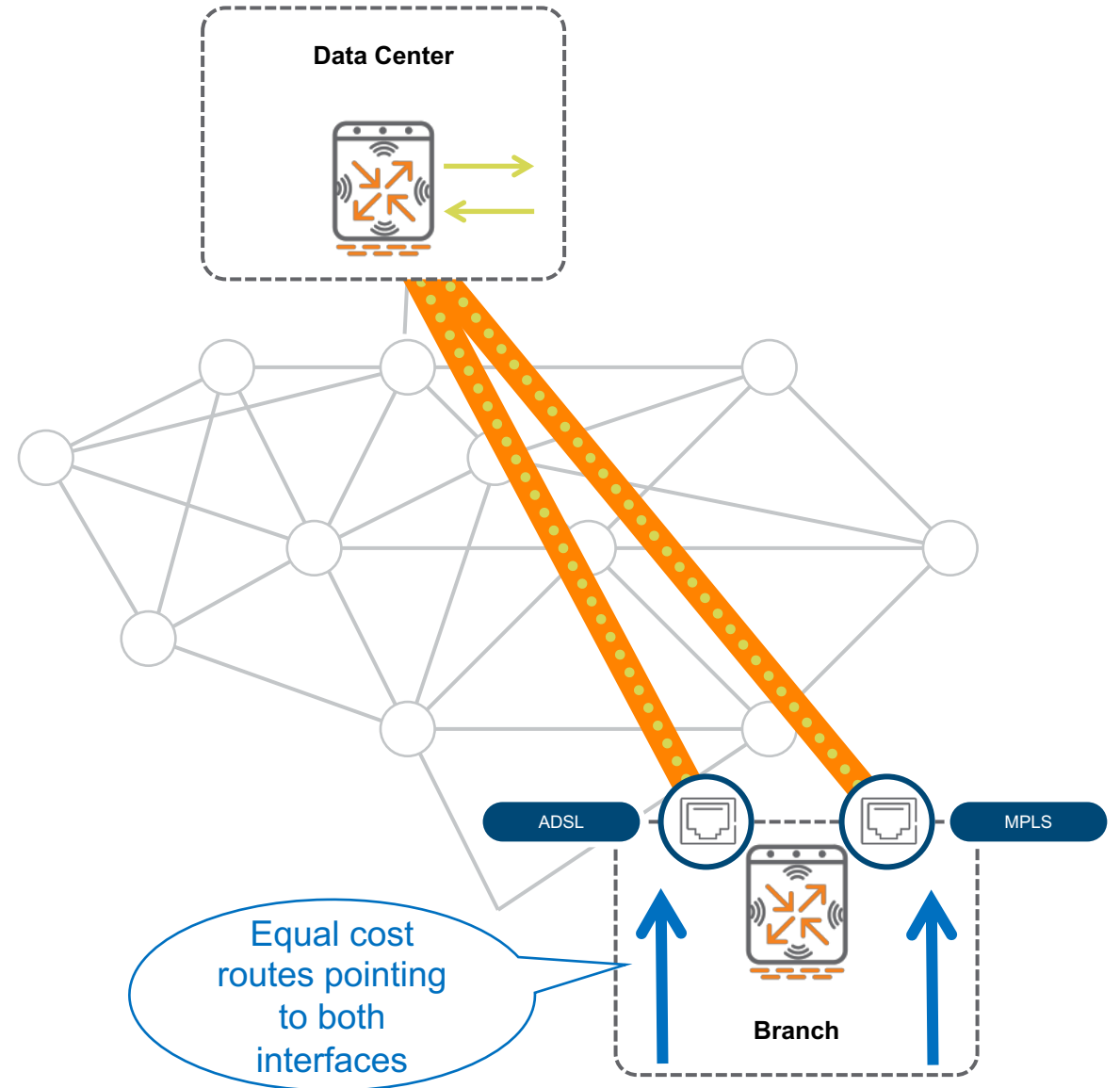
- 1 Set tunnel to Zscaler (site-to-site)
- 2 Create PBR policy to force traffic through ZScaler
- 3 Route advertisement not needed. Zscaler pins the session to the link it came from.

Step 2: Uplink load-balancing

Split-Tunnel – Local peel off

Only for reference – Config is GUI-based

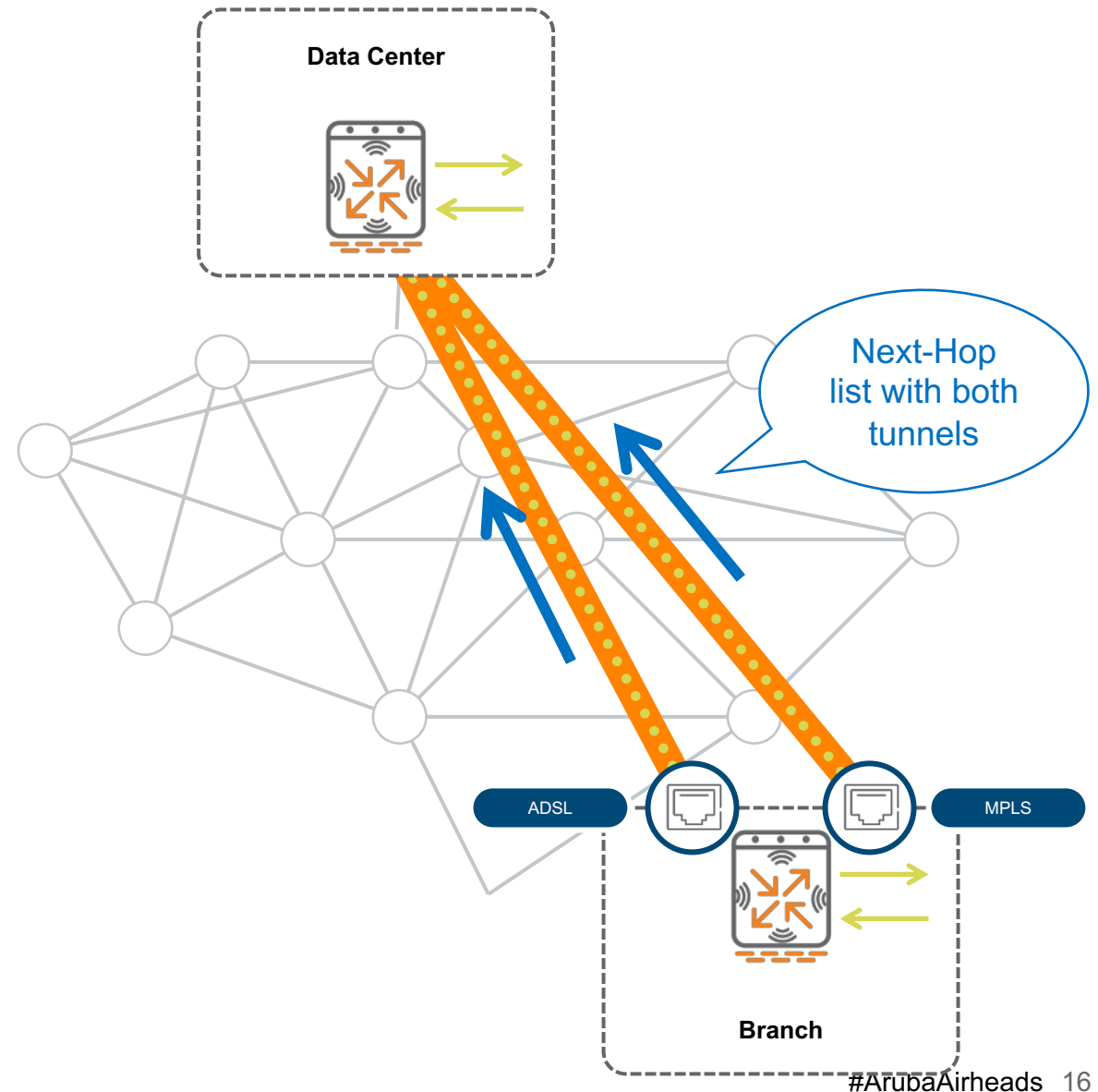
```
!  
ip route 10.0.0.0 255.0.0.0 route tun-vpnc1-mpls 10  
ip route 10.0.0.0 255.0.0.0 route tun-vpnc1-adsl 10  
!  
ip default-gateway mpls-gw  
ip default-gateway adsl-gw  
!
```



Full-Tunnel

Only for reference – Config is GUI-based

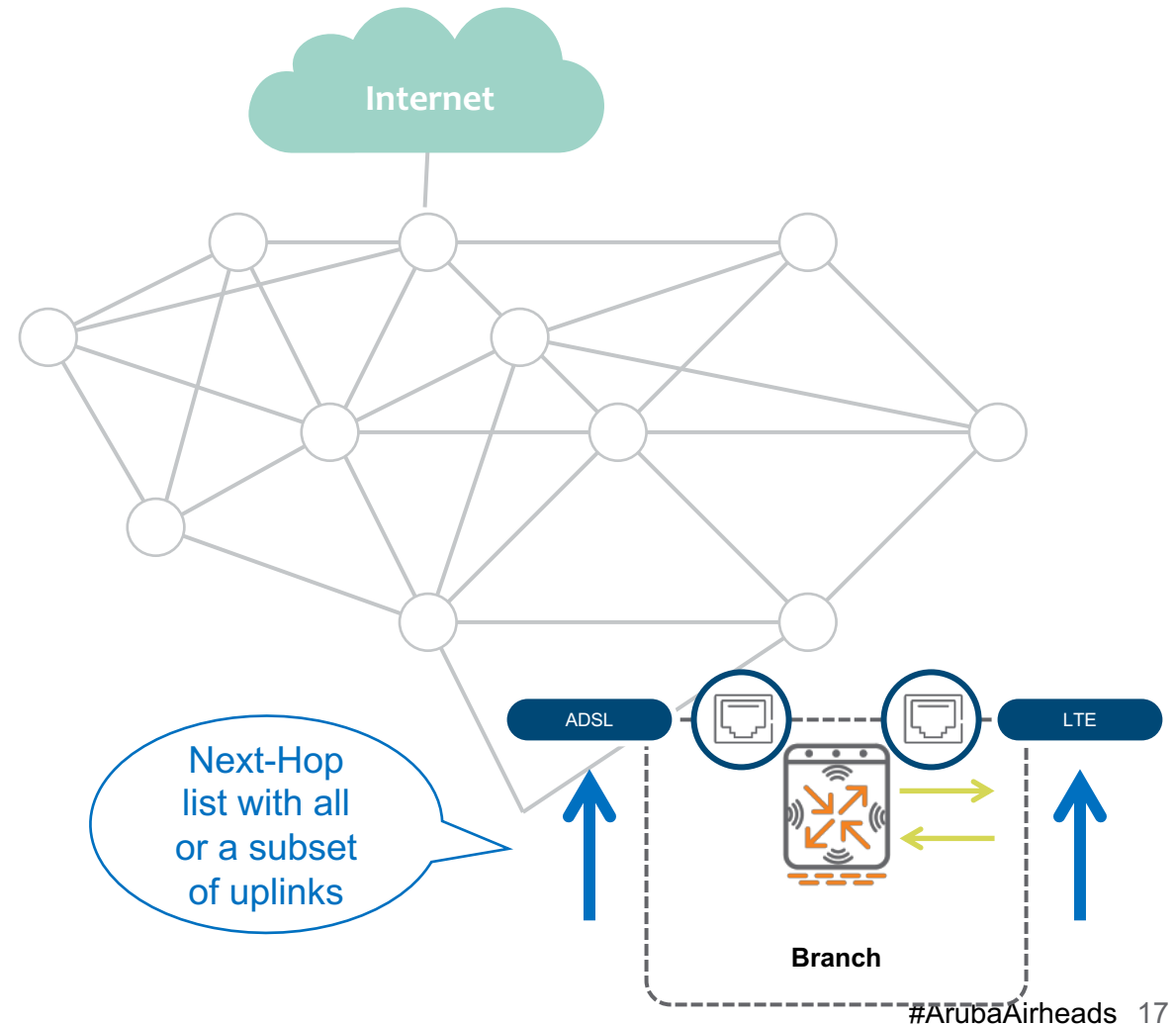
```
ip nexthop-list full-tunnel
 ipsec-map vpnc1-adsl priority 100
 ipsec-map vpnc1-mpls priority 100
 ipsec-map vpnc2-adsl priority 50
 ipsec-map vpnc2-mpls priority 50
!
ip access-list route full-tunnel
 alias local-net alias local-net any forward
 any any any route next-hop-list full-tunnel
!
user-role POS
 access-list session POS
 access-list route full-tunnel
```



Local-breakout

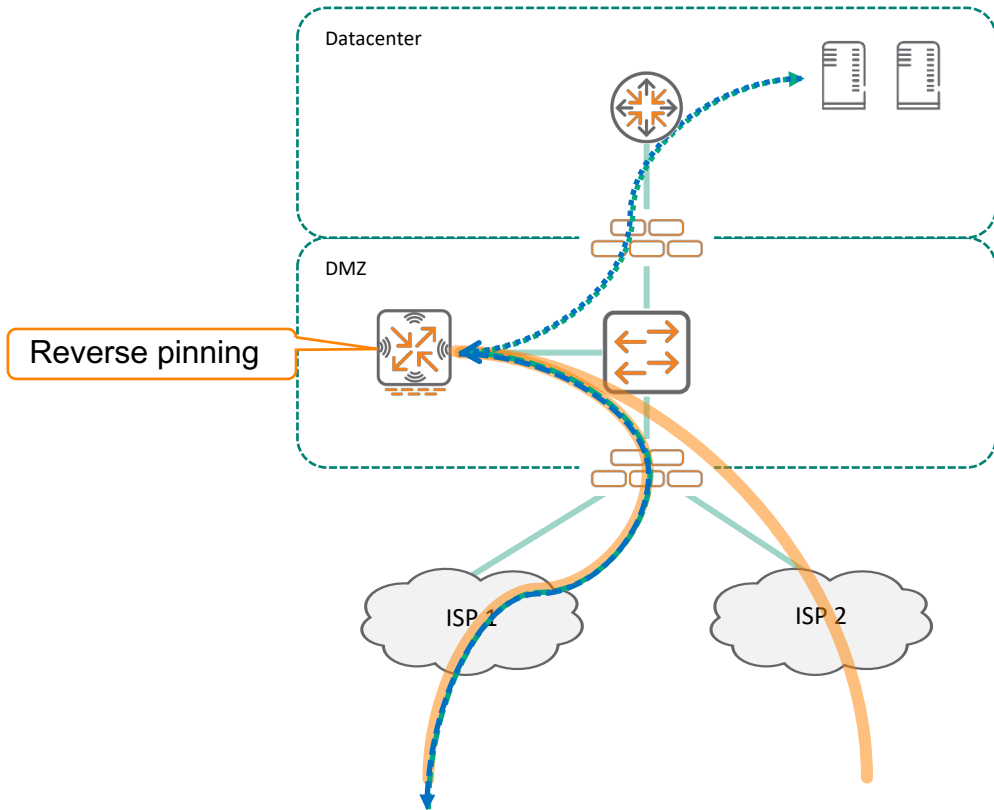
Only for reference – Config is GUI-based

```
ip nexthop-list local-breakout
  ip dhcp vlan 4093 priority 100
  ip dhcp vlan 4094 priority 100
!
!
ip access-list route local-breakout
  alias local-net alias local-net any forward
  any any any route next-hop-list local-breakout
!
user-role guest
  access-list session guest
  access-list route local-breakout
```



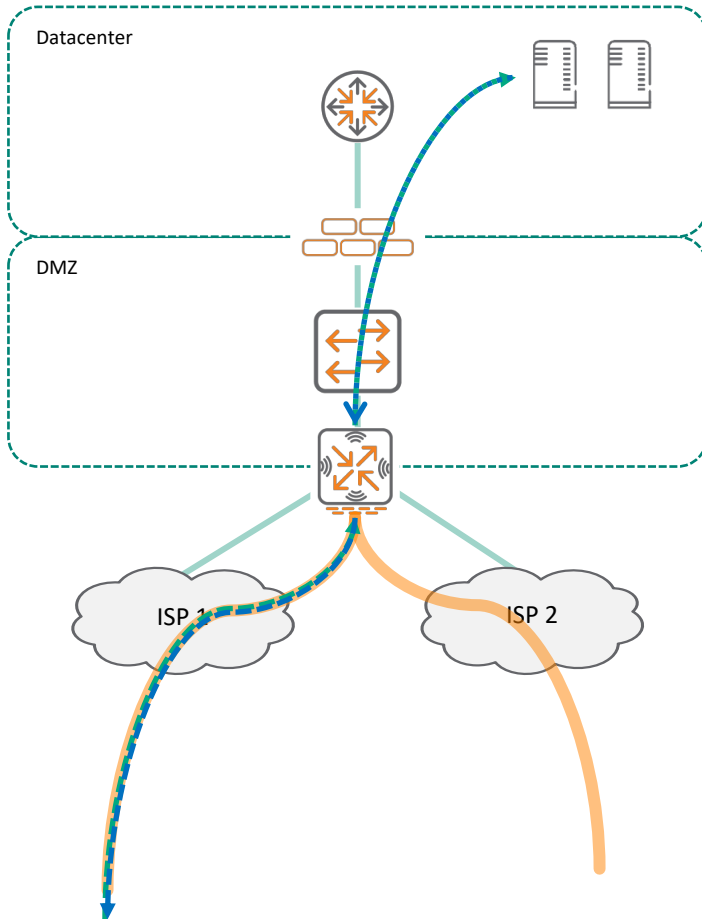
Not so fast: DC Architectures...

Datacenter Topologies – Single Armed VPNC



- 1 Traffic comes into VPNC from tunnel A
- 2 Reverse pinning - Traffic goes back through the original tunnel

Detail about Reverse-pinning (applies to all topologies)



Branch-initiated traffic

- 1 Traffic comes into VPNC from tunnel A
- 2 Reverse pinning - Traffic goes back through the original tunnel

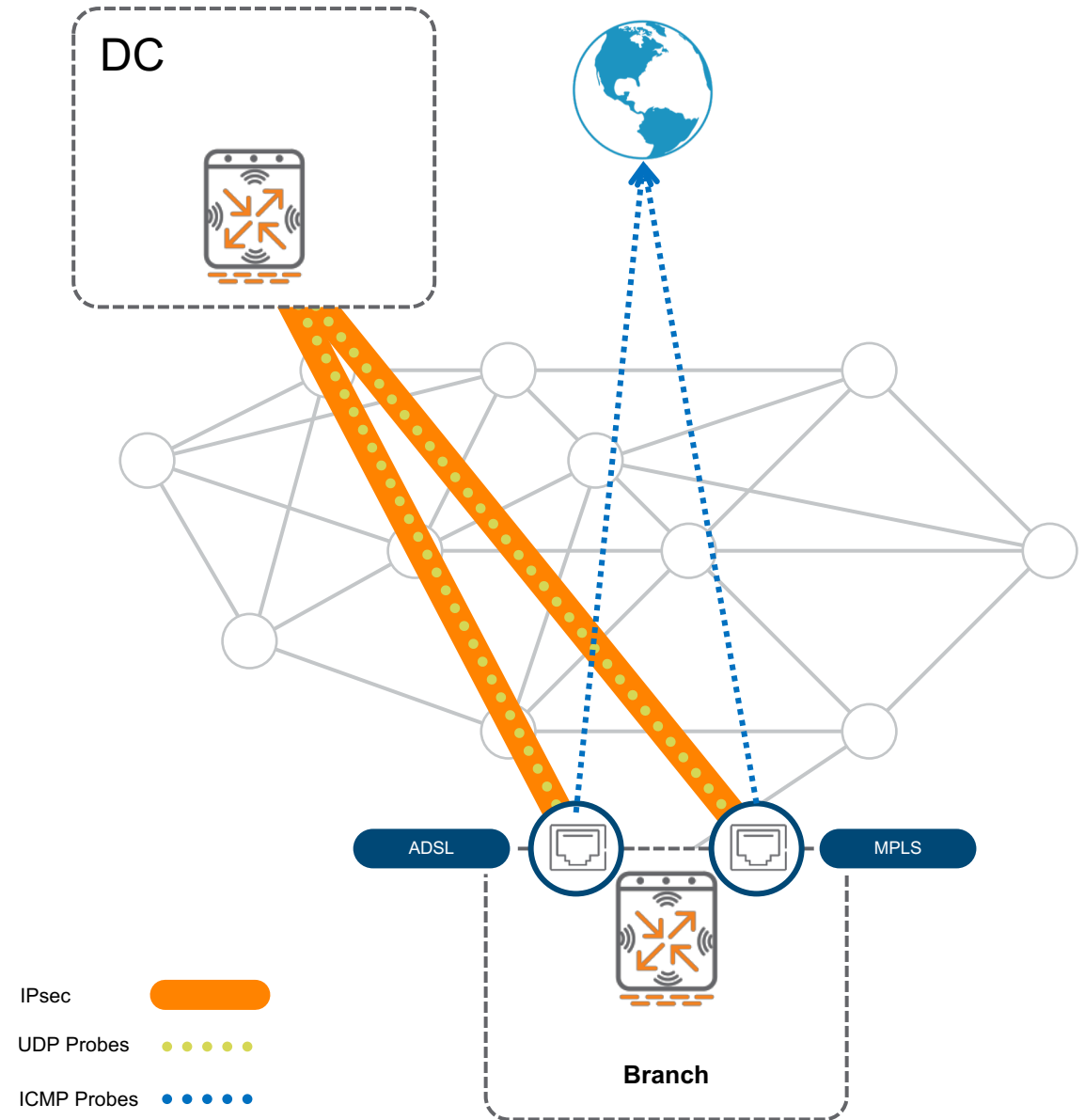
DC-initiated traffic

- 1 Traffic sourced from DC goes to the Branch
- 2 VPNC has equal cost multipath towards the branch
- 3 Branch sends return traffic based on configured policy
- 4 VPNC "pins" the session to the path chosen by the BGW

Step 3: Dynamic Path Selection

Path Quality Monitoring



- ICMP Probes measure latency and packet loss > Global probe responder service: **pqm.arubanetworks.com**
- UDP Probes (UDP 4500) measure latency, packet loss and jitter – MOS is derived from these values
- Probes can be sent through the underlay or through the overlay



WAN Policies

1 Specify 'Interesting' Traffic

Traffic Specification Rules for Employee Mission Critical Policy

SOURCE	DESTINATION	APPLICATION	
Employee	Any	Workday	 
Employee	20.20.20.0/24	Exchange	
Employee	30.30.30.0/24	TCP Port 22	



2 Choose SLA parameters to measure WAN performance

Select SLA for Employee Mission Critical Policy

NAME	LATENCY (MS)	JITTER (MS)	LOSS (%)	UTILIZATION (%)
Highly Available	150	150	1	20
Best for Internet	100	100	5	80
Best for Voice	50	25	5	80



Probe Options for Highly Available SLA

Destination IP:

Protocol: ☒ ICMP ☐ UDP

Probe interval: sec.

Bursts per probe:


3 Configure path preference parameters

WAN Path Selection for Employee Mission Critical Policy

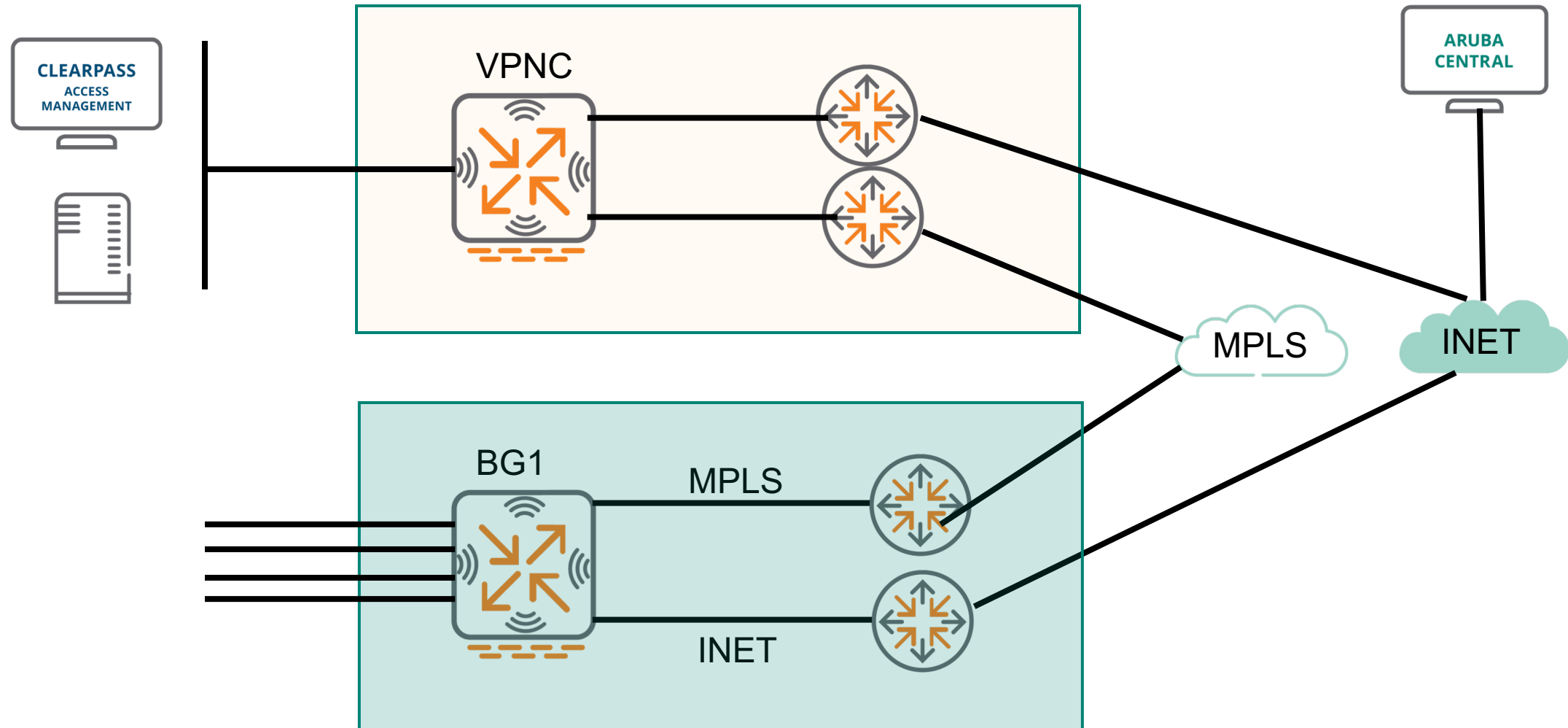
☐ Direct to Internet

Primary path: 

Secondary path: 

Last resort path: 

Demo





AIRHEADS

meetup

Thank You