Large Scale Aruba Branch Wireless Networks

Author: Manjula Hiripitiya

Contents

1 Introduction

A few decades ago, network access was mainly provided to the users via wired UTP connection and wireless connectivity was just starting to establish as an alternative connectivity method with much lower network speeds. Wireless technologies have evolved rapidly since and is able to provide speeds comparable with a wired connection. Wireless Access is predominantly the end user connectivity method used in homes, small to medium businesses, large corporate and government sectors now.

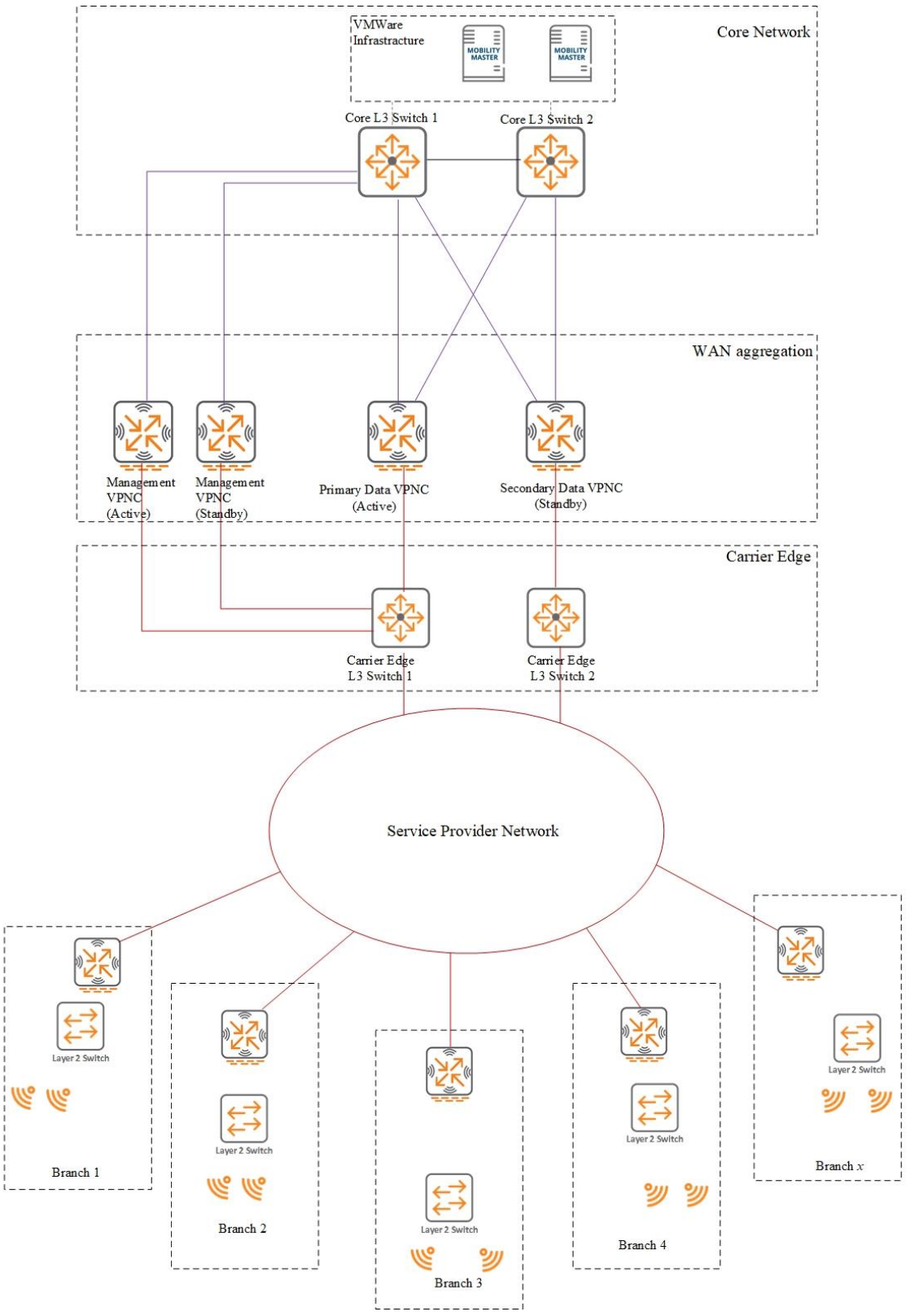
Aruba networks wireless controllers can be utilized to build large scale wireless branch networks and provide wireless access to hundreds of branch sites without having to deploy branch gateway devices separately. Aruba WLCs will function as the Branch WAN Gateway device as well as the wireless controller for the branch site.

1.1 Solution Components

Wireless solution comprises of the following components

- Two Aruba Mobility Masters
- Two Aruba Mobility Controllers acting as Data VPNCs
- Two Aruba Mobility Controllers acting as Management VPNCs
- Any number of Mobility Controllers acting as wireless controllers and the wan gateway device for the branch sites.

1.2 Topology Diagram.



1.3 Solution Features & Benefits.

Aruba Wireless Branch networks provides following benefits.

- Aruba WLC itself functions as the WAN gateway for the branch site, no additional WAN gateway router is required, no additional hardware costs, annual support costs or licensing costs.
- Mobility Masters function as the central point of control, configuration management and monitoring and Licensing.
- Provide redundancy and failover of aggregation devices (Data VPNCs can be deployed two separate data centres providing redundancy)
- Provide redundancy for management access (two management VPNCs can be deployed in a single data centre providing redundancy for management traffic from the Mobility Master to the branch controllers)
- Encryption of traffic from the Branch WLC to the VPNCs (WAN Service provider can't inspect your organizations traffic)
- Branch wireless Controller directly connects to the PoE switch that provide power to the branch access points. WLC can also provide connectivity to the users connecting to the branch switch via UTP.
- Hierarchical configuration structure provide easy deployment of new branch sites since most configurations can be inherited from a higher level of the mobility master configuration hierarchy.
- QoS cab be applied for the wireless traffic as well as WAN traffic.
- Granular Access control can be applied to individual or groups of wireless users.

1.4 Hardware and Software

Solution can be implemented and has been tested on using the following Aruba Wireless Controller hardware and software.

Hostname	Devices	Role	Software Version
MM1 & MM2	Aruba MM-VA-5K Mobility Master Virtual Appliance	Virtual Mobility Masters	8.6.0.6 or 8.6.0.17
data-vpnc-1 & data-vpnc-2	Aruba7220 controller	Data VPNCs	8.6.0.6 or 8.6.0.17
mgmt-vpnc-1 & mgmt-vpnc-2	Aruba 7210 controller	Standby Data VPNCs	8.6.0.6 or 8.6.0.17
Branch*x*-gw-wlc	Aruba 7030 controller	Branch WLC and WAN Gateway	8.6.0.6 or 8.6.0.17

The solution had been tested using the following network hardware, but they can be replaced by compatible equipment from any other network device manufacturer.

Hostname	Devices	Role	Software Version
Core1 & Core 2	Cisco Nexus 7K	Core switch	--

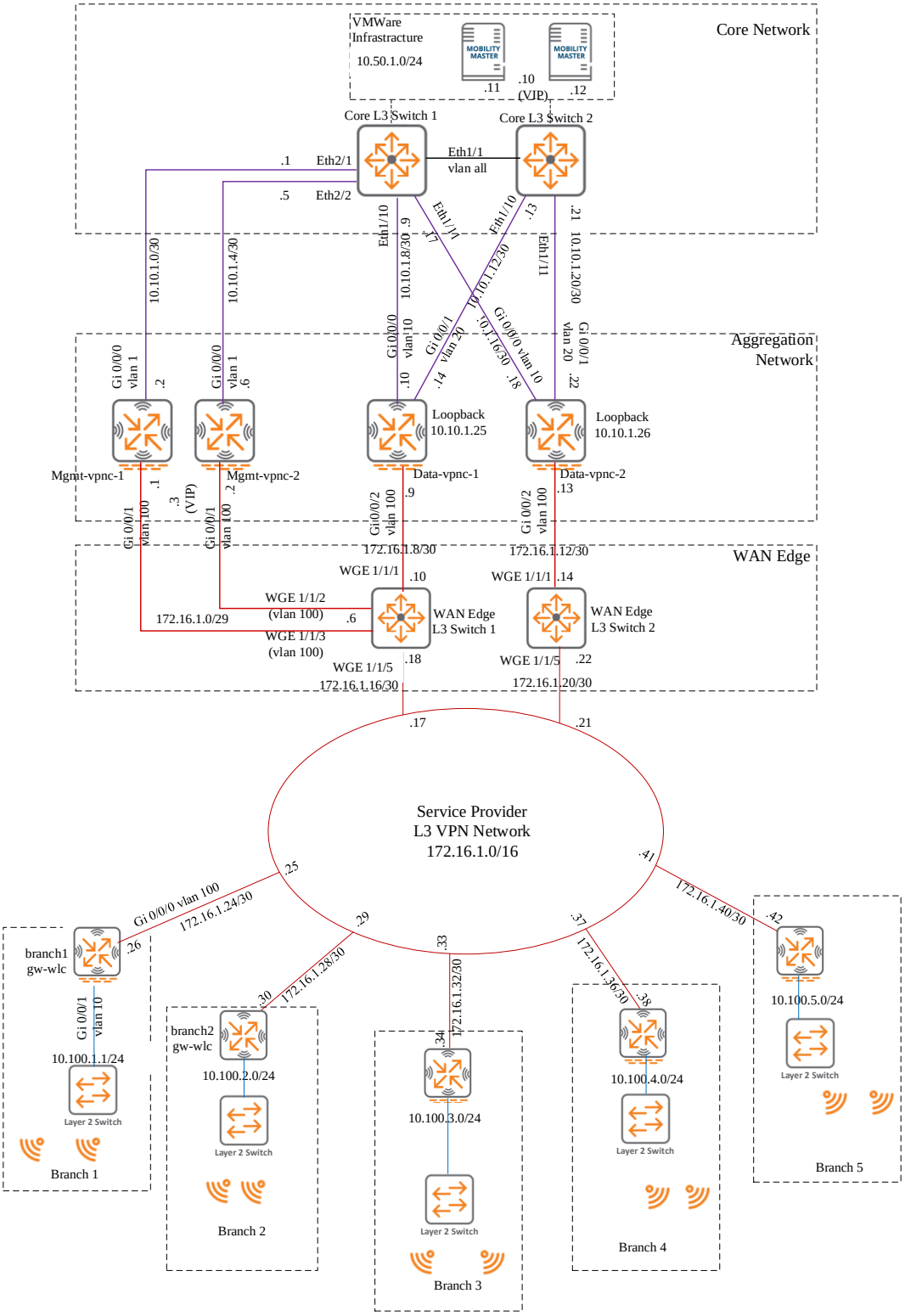
Hostname	Devices	Role	Software Version
WAN-Edge switch 1 & WAN-Edge switch 2	HPE 5945	WAN edge L3 switch	--

1.5 Interface / IP address Allocation

Hostname	Interface Name (Speed)	VLAN	IP address/Mask	Description
MM1	Gi 0/0/0	50	10.50.1.11	MM Uplink to VM virtual switch
MM2	Gi 0/0/0	50	10.50.1.12	MM Uplink to VM virtual switch
mgmt-vpnc-1	Gi 0/0/0 (1G)	1	10.10.1.2/30	Link to Core-1
mgmt-vpnc-1	Gi 0/0/1 (1G)	100	172.16.1.1/29	Link to WAN-Edge-Switch-1
mgmt-vpnc-2	Gi 0/0/0 (1G)	1	10.10.1.6/30	Link to Core-1
mgmt-vpnc-2	Gi 0/0/1 (1G)	100	172.16.1.2/29	Link to WAN-Edge-Switch-1
data-vpnc-1	Gi 0/0/0 (10G)	10	10.10.1.10/30	Link to Core-1
data-vpnc-1	Gi 0/0/1 (10G)	20	10.10.1.14/30	Link to Core-2
data-vpnc-1	Gi 0/0/2 (10G)	100	172.16.1.9/30	Link to WAN-Edge-Switch-1
data-vpnc-2	Gi 0/0/0 (10G)	10	10.10.1.18/30	Link to Core-1
data-vpnc-2	Gi 0/0/1 (10G)	20	10.10.1.22/30	Link to Core-2
data-vpnc-2	Gi 0/0/2 (10G)	100	172.16.1.13/30	Link to WAN-Edge-Switch-2
Core-1	Eth2/1 (1G)	Routed	10.10.1.1/30	Link to mgmt-vpnc-1
Core-1	Eth2/2 (1G)	Routed	10.10.1.5/30	Link to mgmt-vpnc-2
Core-1	Eth1/10 (10G)	Routed	10.10.1.9/30	Link to data-vpnc-1
Core-1	Eth1/11 (10G)	Routed	10.10.1.17/30	Link to data-vpnc-2
Core-1	Eth1/1 (10G)	All vlans	N/A	Link to Core-2
Core-2	Eth1/10 (10G)	Routed	10.10.1.13/30	Link to data-vpnc-1
Core-2	Eth1/11 (10G)	Routed	10.10.1.21/30	Link to data-vpnc-2
Core-2	Eth1/1 (10G)	All vlans	N/A	Link to Core-2
WAN-Edge-1	WGE 0/0/1 (10G)	Routed	172.16.1.10/30	Link to Data-vpnc-1
WAN-Edge-1	WGE 0/0/2 (1G)	100	172.16.1.6/29	Link to mgmt-vpnc-1
WAN-Edge-1	WGE 0/0/3 (1G)	100		Link to mgmt-vpnc-2
WAN-Edge-1	WGE 0/0/5 (10G)	Routed	172.16.1.18/30	Uplink to WAN Service Provider
WAN-Edge-2	WGE 0/0/1 (10G)	Routed	172.16.1.14/30	Link to Data-vpnc-2

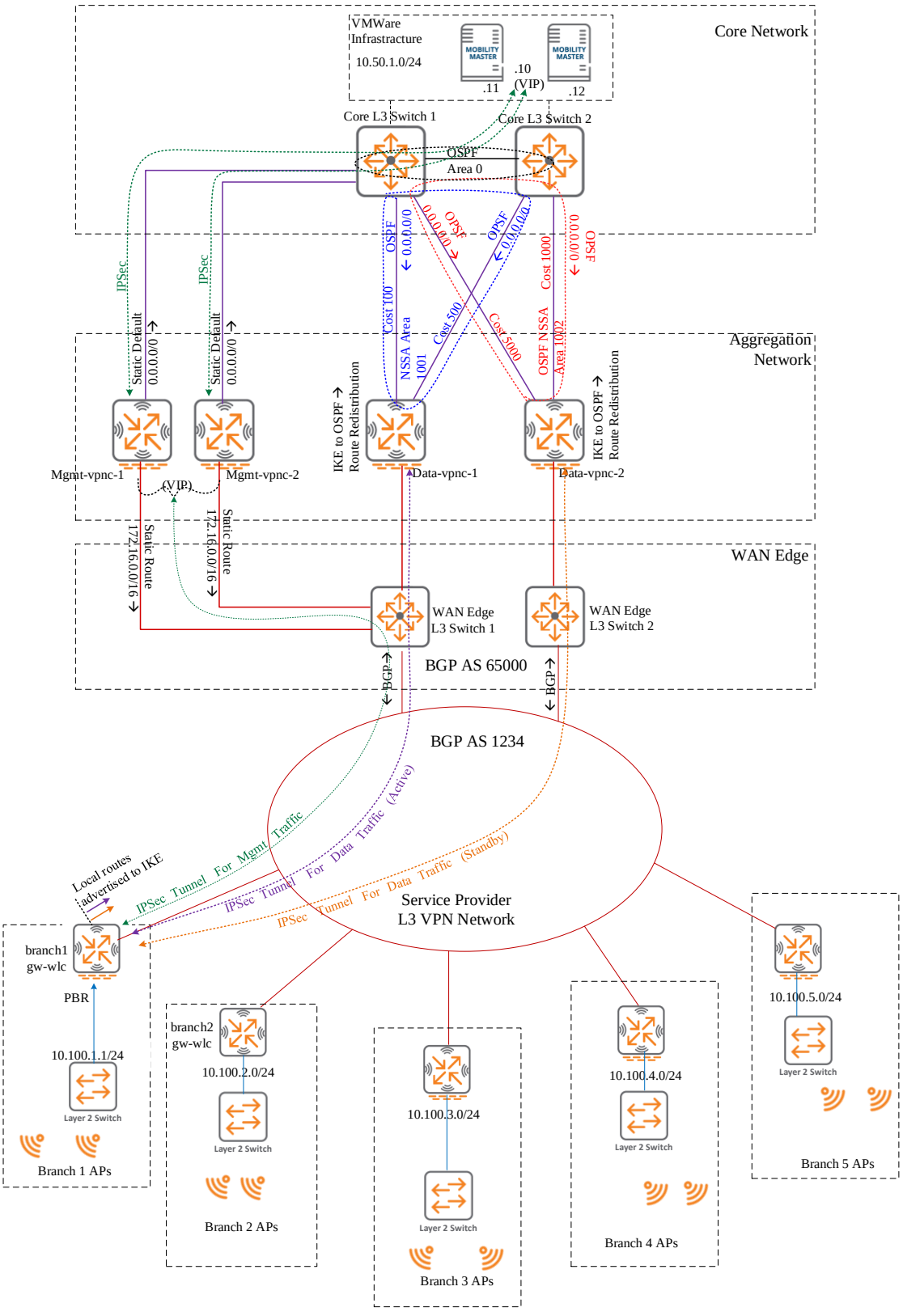
Hostname	Interface Name (Speed)	VLAN	IP address/Mask	Description
WAN-Edge-2	WGE 0/0/5 (10G)	Routed	172.16.1.22/30	Uplink to WAN Service Provider
Branch1-gw-wlc	Gi 0/0/0 (1G)	100	172.16.1.26/30	Uplink to WAN Service Provider
Branch1-gw-wlc	Gi 0/0/1 (1G)	10	10.100.1.1/24	Link to Branch LAN L2 Switch
Branch2-gw-wlc	Gi 0/0/0 (1G)	100	172.16.1.30/30	Uplink to WAN Service Provider
Branch2-gw-wlc	Gi 0/0/1 (1G)	10	10.100.2.1/24	Link to Branch LAN L2 Switch
Branch3-gw-wlc	Gi 0/0/0 (1G)	100	172.16.1.34/30	Uplink to WAN Service Provider
Branch3-gw-wlc	Gi 0/0/1 (1G)	10	10.100.3.1/24	Link to Branch LAN L2 Switch
Branch4-gw-wlc	Gi 0/0/0 (1G)	100	172.16.1.38/30	Uplink to WAN Service Provider
Branch4-gw-wlc	Gi 0/0/1 (1G)	10	10.100.4.1/24	Link to Branch LAN L2 Switch
Branch5-gw-wlc	Gi 0/0/0 (1G)	100	172.16.1.42/30	Uplink to WAN Service Provider
Branch5-gw-wlc	Gi 0/0/1 (1G)	10	10.100.5.1/24	Link to Branch LAN L2 Switch

1.6 Topology Diagram with IP/Interface Information



Head office (DC) of the Company has two 10 Gbps WAN uplinks to terminating on two separate WAN-Edge switches for redundancy. Each data-vpnc is connected to the core switches and wan-edge switches using a 10G uplinks they participate in forwarding user's traffic from branches. The mgmt-vpncs are connected using 1G uplinks because they are only used for communications between the mobility master and branch-gw-wlcs and do not forward user's traffic.

1.7 Routing & Traffic Flow Overview



All VPNCs (mgmt & data) has one interface connected to the WAN Service Provider and able to reach the WAN IP address of every branch-gw-wlc via the service provider L3 VPN Network. All links except for the mgmt-vpnc links are point-to-point links and assigned /30 IP subnets. Mgmt-vpnc(s) WAN link require VRRP configuration for redundancy and therefore assigned a /29 subnet.

The WAN-Edge L3 switches are configured to exchange routes with the service provider via BGP. These switches are purely used for configuration flexibility (and future use of other service providers). If you have a single WAN service provider, you can request them to allocate /29 IP subnets for DC uplinks and avoid the using the L3 switches and BGP configuration.

Mgmt-vpncs configured with a static route of 172.16.0.0/16 pointing towards the WAN-Edge switch 1 and default route pointing towards the core-1 switch, mgmt-vpncs do not participate in user data forwarding therefore does not learn dynamic routes (LAN IP subnets of Branch Networks)
Data-vpncs on the other hand, required dynamic routing, they are configured in an OSPF totally-not-so-stubby-area (NSSA) where they learn only the default route from the core switch. Data-vpnc learn the branch route dynamically via IKE extensions when the IPsec communication with branch controller is established. Branch LAN IP routes leant via IKE extensions are marked as type "I" in the routing table of the vpncs. VPNCs redistribute route learnt via IKE to ospf so that the core-1 & 2 learn them dynamically as well. Data-vpncs do not advertise any routes to downstream Branch sites.

Branch-gw-wlcs are configured to advertise its locally connected subnets to the data-vpnc via IKE but rely on Policy Based Routing (PBR) to route traffic to the core network. Branch-gw-wlcs establish two IPSec tunnels to the two Data-vpncs and can be configured to prefer one tunnel over the other for routing. When the primary (lowest cost) IPSec tunnel fails, standby (higher cost) tunnel is used to forward branch user traffic to the core network. Branch routes learn the VRRP IP address of the mobility master via the IPSec tunnel to the active mgmt-vpnc. It is denoted with a route type of "I" in branch-gw-wlcs routing table.

2 Network Infrastructure configurations

Following sections of this document contains the configurations required on the network infrastructure devices to establish the connectivity from branch WLC to the core network.

2.1 WAN-Edge-1 Switch Configuration

WAN-Edge-1 Configuration

```
>
system-view
#
 sysname WAN-Edge-1
#
vlan 100
 name mgmt-vpnc
#
interface Vlan-interface100
 description mgmt-vpnc Vlan
ip address 172.16.1.6 255.255.255.248
#
interface WGE 1/1/1
 port link-mode route
 description "10G link to data-vpnc-1 port Gi 0/0/2"
 duplex full
 speed 10000
ip address 172.16.1.10 255.255.255.252
#
interface WGE 1/1/2
 port link-mode bridge
 description "1G Link to mgmt-vpnc-1 port Gi 0/0/1"
 port access vlan 100
 speed 1000
 duplex full
#
interface WGE 1/1/3
 port link-mode bridge
 description "1G Link to mgmt-vpnc-2 port Gi 0/0/1"
 port access vlan 100
 speed 1000
 duplex full
#

interface WGE 1/1/5
 port link-mode route
 description "WAN Service Provider Uplink-1"
 duplex full
 speed 10000
 ip address 172.16.1.18 255.255.255.252
#
bgp 65000
 graceful-restart
 graceful-restart timer restart 120
 timer keepalive 30 hold 90
 #
  router-id 172.16.1.18
  peer 172.16.1.17 as-number 1234
  peer 172.16.1.17 description "WAN Service Provider"
  peer 172.16.1.17 source-address 172.16.1.18
  #
  address-family ipv4 unicast
   network 172.16.1.0 255.255.255.248
```

WAN-Edge-1 Configuration

```
   network 172.16.1.8 255.255.255.252
   network 172.16.1.16 255.255.255.252
   peer 172.16.1.17 enable
   peer 172.16.1.17 advertise-community
#
```

2.2 WAN-Edge-2 Switch Configuration

WAN-Edge-1 Configuration

```
>
system-view
#
 sysname WAN-Edge-2
#
interface WGE 1/1/1
 port link-mode route
 description "10G link to data-vpnc-2 port Gi 0/0/2"
 duplex full
 speed 10000
ip address 172.16.1.14 255.255.255.252
#
interface WGE 1/1/5
 port link-mode route
 description "WAN Service Provider Uplink-2"
 duplex full
 speed 10000
 ip address 172.16.1.22 255.255.255.252
#
bgp 65000
 graceful-restart
 graceful-restart timer restart 120
 timer keepalive 30 hold 90
 #
  router-id 172.16.1.22
  peer 172.16.1.21 as-number 1234
  peer 172.16.1.21 description "WAN Service Provider"
  peer 172.16.1.21 source-address 172.16.1.22
  #
  address-family ipv4 unicast
   network 172.16.1.12 255.255.255.252
   network 172.16.1.20 255.255.255.252
   peer 172.16.1.21 enable
   peer 172.16.1.21 advertise-community
#
```

2.3 Core-1 Switch Configuration

Core-1 Switch Configuration

```
Core-1>
enable
Core-1#configure terminal

interface Ethernet1/1
  description ** Core-1 to Core-2 Trunk Link **
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  no shutdown
!
interface Ethernet1/10
  description ** 10G Link to Data-vpnc-1 Gi 0/0/0 **
  speed 10000
  duplex full
  ip address 10.10.1.9/30
  ip ospf cost 100
  no ip ospf passive-interface
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.3.233
  no shutdown
!
interface Ethernet1/11
  description ** 10G Link to Data-vpnc-2 Gi 0/0/0 **
  speed 10000
  duplex full
  ip address 10.10.1.17/30
  ip ospf cost 5000
  no ip ospf passive-interface
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.3.234
  no shutdown
!
interface Ethernet2/1
  description ** 1G Link to mgmt-vpnc-1 port Gi0/0/0 **
  speed 10000
  duplex full
  ip address 10.10.1.1/30
  no shutdown
!
interface Ethernet2/2
  description ** 1G Link to mgmt-vpnc-2 port Gi0/0/0 **
  speed 10000
  duplex full
  ip address 10.10.1.5/30
  no shutdown

interface Ethernet1/12
  description ** 10GB Link to VMWare Hosts with Mobility Masters **
  switchport
  switchport mode trunk
  switchport trunk allowed vlan add 50
  no shutdown

interface Vlan50
  ip address 10.50.1.2/24
  ip router ospf 10 area 0.0.0.0
  no ip arp gratuitous hsrp duplicate
  hsrp version 2
  hsrp 50
```

Core-1 Switch Configuration

```
    preempt delay minimum 60
    ip 10.50.1.1
  description ** Mobility Master Vlan **
  no shutdown
!
router ospf 10
   area 0.0.3.233 nssa no-summary no-redistribution
   area 0.0.3.234 nssa no-summary no-redistribution
   redistribute direct
   redistribute static
!
ip route 172.16.1.1/32 10.10.1.2
ip route 172.16.1.2/32 10.10.1.6
!
```

2.4 Core-2 Switch Configuration

Core-2 Switch Configuration

```
Core-2>
enable
Core-2#configure terminal

interface Ethernet1/1
  description ** Core-2 to Core-1 Trunk Link **
  switchport
  switchport mode trunk
  switchport trunk allowed vlan all
  no shutdown
!
interface Ethernet1/10
  description ** 10G Link to Data-vpnc-1 Gi 0/0/1 **
  speed 10000
  duplex full
  ip address 10.10.1.13/30
  ip ospf cost 500
  no ip ospf passive-interface
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.3.233
  no shutdown
!
interface Ethernet1/11
  description ** 10G Link to Data-vpnc-2 Gi 0/0/1 **
  speed 10000
  duplex full
  ip address 10.10.1.21/30
  ip ospf cost 1000
  no ip ospf passive-interface
  ip ospf mtu-ignore
  ip router ospf 10 area 0.0.3.234
  no shutdown
!

interface Ethernet1/12
  description ** 10GB Link to VMWare Hosts with Mobility Masters **
  switchport
```

Core-2 Switch Configuration

```
  switchport mode trunk
  switchport trunk allowed vlan add 50
  no shutdown

interface Vlan50
  ip address 10.50.1.3/24
  ip router ospf 10 area 0.0.0.0
  no ip arp gratuitous hsrp duplicate
  hsrp version 2
  hsrp 50
    preempt delay minimum 60
    priority 90
    ip 10.50.1.1
  description ** Mobility Master Vlan **
  no shutdown
!
router ospf 10
   area 0.0.3.233 nssa no-summary no-redistribution
   area 0.0.3.234 nssa no-summary no-redistribution
   redistribute direct
   redistribute static
```

3 Mobility Masters

Once the network infrastructure devices are configured and connected, Mobility Master Cluster can be deployed to the VMWare hosts, in this reference design Mobility Master VLAN is directly attached to both the core switches with HSRP as the gateway redundancy protocol. It is recommended to have L2 redundant mobility masters when you have layer2 connectivity between the VMWare hosts. (If you can't achieve layer 2 connectivity between VMWare hosts, the Mobility Masters can be deployed in layer 3 redundant configuration). There is plenty of Aruba documentation on Mobility Master Cluster deployment and details are not covered here.

Table below is used to deploy the Mobility master cluster.

Hostname	Interface Name (Speed)	VLAN	IP address/Mask	Description
MM1	Gi 0/0/0	50	10.50.1.11	MM1 Uplink to VM virtual switch
MM2	Gi 0/0/0	50	10.50.1.12	MM2 Uplink to VM virtual switch
MM1 and MM2	Gi 0/0/0	50	10.50.1.10	MM VRRP (Virtual) IP address
-			10.50.1.1	Mobility Master Gateway IP (HSRP IP)

3.1 Mobility Master Configuration Hierarchy

The hierarchical configuration of the mobility master and the configuration inheritance by the devices placed at the lower levels hierarchy makes it easy to deploy branch sites.

The table below shows the placement of Management VPNCs, Data VPNCs and Branch Gateway devices and Groups in the mobility Master configuration Hierarchy.

Configuration Node	Type	Name / Comments
/mm	System	Mobility Master node common to both active and standby mobility Masters
/mm/mynode	System	Configuration settings only applied to the active mobility master device HW MAC Addr of MM1 (00:1a:1e:01:00:01) HW MAC Addr of MM2 (00:1a:1e:01:00:02)
/md	System	Default configuration settings applied to all managed devices, no modifications should happen at this level
/md/Company-XYZ	Group	First group node where custom configuration settings are applied.
/md/Company-XYZ/MGMT-VPNC	Group	Management VPNC group node.
/md/Company-XYZ/mgmt-vpnc/00:1a:1e:00:00:01	Device	Mgmt-vpnc-1 (Configuration settings applied only to the primary Mgmt-vpnc-1) HW MAC Address (/)
/md/Company-XYZ/mgmt-vpnc/00:1a:1e:00:00:02	Device	Mgmt-vpnc-2 (Configuration settings applied only to the primary Mgmt-vpnc-1) HW MAC Address (00:1a:1e:00:00:02)

Configuration Node	Type	Name / Comments
/md/Company-XYZ/data-vpnc	Group	Group node, configuration settings applicable to all data VPNCs are listed here
/md/Company-XYZ/data-vpnc/00:1a:1e:00:01:01	Device	data-vpnc-1 (Configuration settings applied only to the primary Mgmt-vpnc-1) HW MAC Address (00:1a:1e:00:01:01)
/md/Company-XYZ/data-vpnc/00:1a:1e:00:01:02	Device	data-vpnc-2 (Configuration settings applied only to the primary Mgmt-vpnc-1) HW MAC Address (00:1a:1e:00:01:02)
/md/Company-XYZ/branch	Group	Configuration template applied to all Branch Gateway controllers is listed here
/md/Company-XYZ/branch/00:1a:1e:00:03:01	Device	Branch-gw-wlc-1 (branch WAN gateway controller device-1, site specific configurations are applied at this device node level) HW MAC Address of branch-gw-wlc-1(00:1a:1e:00:03:01)
/md/Company-XYZ/branch/00:1a:1e:00:03:02	Device	Branch-gw-wlc-2 (branch WAN gateway controller device-1, site specific configurations are applied at this device node level) HW MAC Address of branch-gw-wlc-2(00:1a:1e:00:03:02)
/md/Company-XYZ/branch/00:1a:1e:00:03:03	Device	Branch-gw-wlc-3 (branch WAN gateway controller device-1, site specific configurations are applied at this device node level) HW MAC Address of branch-gw-wlc-3(00:1a:1e:00:03:03)
/md/Company-XYZ/branch/00:1a:1e:00:03:04	Device	Branch-gw-wlc-4 (branch WAN gateway controller device-1, site specific configurations are applied at this device node level) HW MAC Address of branch-gw-wlc-4(00:1a:1e:00:03:04)
/md/Company-XYZ/branch/00:1a:1e:00:03:05	Device	Branch-gw-wlc-5 (branch WAN gateway controller device-1, site specific configurations are applied at this device node level) HW MAC Address of branch-gw-wlc-5(00:1a:1e:00:03:05)

Table 1 – Mobility Master Configuration Node Hierarchy used to build the Branch Wifi Solution

Note: correct hardware Mac Address of each controller can be found by executing the (show inventory command on each wireless lan controller)

3.2 Mobility Master Configuration

Mobility Master is configured with pre-shared keys in ordered to allow the Management VPNCs and the Data VPNCs to establish IPsec tunnels as shown below.

/mm System Node Configuration
! Data VPNC pre-shared key configuration ! Note that the controller IP address of the VPNC is its WAN side IP address. localip 172.16.1.1 ipsec <ipsec-key> localip 172.16.1.2 ipsec <ipsec-key> ! Management VPNC pre-shared key configuration ! Management VPNCs are configured using their HW Mac Addresses. local-peer-mac 00:1a:1e:00:00:01 ipsec <ipsec-key>

/mm System Node Configuration
local-peer-mac 00:1a:1e:00:00:02 ipsec <ipsec-key>

Note: Branch gateway controllers do not form direct IPsec peering with the mobility master. Therefore IP/mac address information of branch controllers is not configured here.

Any mobility controller that needs to be managed by the mobility master must be placed into the mobility master configuration hierarchy as a device node. This includes any branch site gateway controller device attempting to comminute with the mobility master via the management VPNC as well. Typically, a configuration node for a managed device should be explicitly defined in the mobility master configuration hierarchy. However, due the large number of branch gateways that are deployed, device auto-parking can be enabled. The auto-parking feature allows the mobility master to place managed devices without an explicitly defined configuration node, to be placed under a default group node.

Shown below is the mobility master auto-parking configuration.

/mm/mynode System Node Configuration
(MM1) [mynode] (config) configuration device default-node /md/Company-XYZ/branch

3.3 Automatically generated routes

When a branch sites router boots up and establish the IPSec tunnel with the active management VPNC, the active management VPNC triggers an automatic update in the mobility master. These routes are listed as static routes in the mobility master configuration, and they should not be manually altered by the administrators.

Only a handful of these automatically auto generated static routes are listed as a reference.

/mm/mynode Automatically generated routes
(MM1) [mynode] # ! THESE ROUTES ARE AUTOMATICALLY GENERATED, YOU SHOULD NOT MODIFY THEM. ip route 172.16.1.26 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:01 20 ip route 172.16.1.26 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:02 30 ip route 172.16.1.30 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:01 20 ip route 172.16.1.30 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:02 30 ip route 172.16.1.34 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:01 20 ip route 172.16.1.34 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:02 30 ip route 172.16.1.38 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:01 20 ip route 172.16.1.38 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:02 30 ip route 172.16.1.42 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:01 20 ip route 172.16.1.42 255.255.255.255 ipsec default-local-master-ipsecmap-00:1a:1e:00:00:02 30

As seen above each of the remote site WAN IP address has two static route entries with two different costs, lower cost route always points to the IPsec tunnel to the active management VPNC. These routes are used by the mobility master to establish communications with the branch device via the active management VPNC. Route with cost 30 become active when the ipsec tunnel from the active mobility master to the active mgmt-vpnc has failed.

4 Management VPNC

Branch controllers establish secure communication with the mobility masters via management VPNCs which are deployed at the aggregation layer of the XYZ Company network. The management VPNCs have WAN interface as well as a LAN interface. The branch gateway controller establishes an IPSec tunnel with the active management VPNC and management traffic to and from the mobility master pass through this IPsec tunnel. The management VPNCs are deployed as an active/standby pair. The management VPNC pair require L2 connectivity between the WAN side IP addresses. Each of management VPNCs also establish IPSec tunnels with the active mobility master thus protecting all management communications.

Virtual Router Redundancy Protocol (VRRP) is configured between the two WAN IP addresses of each management VPNC. Whichever controller happens to have the highest VRRP priority, assumes the role of the active management VPNC. Primary VPNC is configured with interface tracking to lower its VRRP priority if its LAN interface goes down and pre-empt its role as the active device again when its LAN interface come back up.

When a branch controller establishes communications with the active management VPNC, active management VPNC advertises a host route to the branch controller for the mobility master IP. This is achieved via ike extensions (this route is visible on the branch gateway device routing table as an ike-overlay route denoted by the letter "I".

The active VPNC also notifies branch "tunnel-up" events to the mobility master, prompting the mobility master to update it's the routing table entry for that branch controller WAN IP address. As mentioned before the active mobility master dynamically adds a static host route entry (cost 20) for the branch controller IP via the IPSec tunnel it has already established with the active management VPNC, when a standby management is also present a second static host route entry will also be added, but with a higher cost (30) via the IPsec tunnel to the standby management VPNC, making it the less preferred path for the mobility master to reach the branch site.

Management VPNC authenticates all the branch sites that attempts to connect to it by validating its factory certificate presented by the branch gateway controller during IPSec tunnel establishment. Branch Gateway controller's factory certificate which is stored in its Trusted Platform Module (TPM) contains its serial number and the mac-address information of the branch controller. Management VPNC is configured with a list of peer mac-address allowed to establish VPN connections to the VPNC. Management VPNC validates the mac-address contained within the factory certificate of the vpn-peer (i.e., Branch Gateway Controller) during the IPsec tunnel establishment. VPNCs are not pre-configured with the IP address information of its potential IPsec VPN peers, it only contains mac-address of the peers allowed to connect to it. Therefore, VPNCs can only act as an IPsec responder for all branch sites. The active management VPNC adds a host route entry to its routing table for each of the branch gateway address and associate the route with the dynamically created "ipsec-map" indicating it should encrypt all IP communications with that branch gateway controller address.

Management VPNC authenticates with the mobility master using pre-shared key just as any other mobility controller directly connecting to the master. During initial configuration of each management VPNC, primary & secondary mobility master mac-addresses are added to the configuration in addition to the Virtual IP address of the mobility master.

Management VPNCs don't participate in forwarding any user traffic, they do not have visibility of branch site LAN/user subnets.

4.1 Management VPNC Common Configurations

Branch controller mac addresses that are allowed to connect are common to both the management VPNCs, listed below is a sample of vpn-peer mac configurations

Note: Configuration listed below is inherited by both management VPNCs.

/md/Company-XYZ/mgmt-vpnc Group Node Configuration
! vpn-peer peer-mac 00:1a:1e:00:03:01 cert-auth factory-cert vpn-peer peer-mac 00:1a:1e:00:03:02 cert-auth factory-cert

/md/Company-XYZ/mgmt-vpnc Group Node Configuration

```
vpn-peer peer-mac 00:1a:1e:00:03:03 cert-auth factory-cert
vpn-peer peer-mac 00:1a:1e:00:03:04 cert-auth factory-cert
vpn-peer peer-mac 00:1a:1e:00:03:05 cert-auth factory-cert
!
```

4.2 Primary Management VPNC Configuration

During the initial staging of the mgmt-vpncs, masterip (i.e., MM1 vrrp IP), ipsec-key, DNS, NTP, Timezone and the mac addresses of the MM1 and MM2 is supplied via configuration dialogs, Gi0/0/0 LAN interface is configured as the controller IP address. Then LAN uplink is connected to core switch. Mobility Master should be able to communicate with (ping) the mgmt-vpnc-1 LAN interface IP as well as the WAN interface IP (172.16.1.1). make sure the static route for the WAN IP of the management vpnc exists on the core-1 switch and it is redistributed to ospf.

Once connectivity is verified the mgmt-vpnc-1 controller-ip address is changed to its WAN IP address via MM. mgmt-vpnc-1 will reboot and be rediscovered in MM hierarchy with the new controller IP. Additional configurations can now be pushed to the mgmt-vpnc via mobility master.

Repeat this process for secondary mgmt-vpnc as well.

Shown below is the committed configuration of the primary management vpnc (mgmt-vpnc-1).

/md/Company-XYZ/mgmt-vpnc/00:1a:1e:00:00:01 Device Node Configuration

```
!
masterip 10.50.1.10 ipsec <ipsec-key> peer-mac-1 00:1a:1e:01:00:01 peer-mac-2 00:1a:1e:01:00:02
location "Data Centre/HQ address, Room X, Rack Y, RU xx"
controller-ip vlan 100
vlan 1
!
vlan 100
    description WAN-Uplink
!
interface gigabitethernet 0/0/0
    description " 1G LAN Uplink to Core-1 switch port Eth2/1"
    switchport access vlan 1
    switchport mode access
    trusted
    trusted vlan 1
!
interface gigabitethernet 0/0/1
    description "1G WAN Uplink 1 to WAN-Edge-1 switch port WGE1/1/3"
    switchport access vlan 100
    switchport mode access
    trusted
    trusted vlan 100
!
interface vlan 1
    ip address 10.10.1.2 255.255.255.252
    description LAN
!
interface vlan 100
    ip address 172.16.1.1 255.255.255.248
    description WAN
!
ip route 172.16.0.0 255.255.0.0 172.16.1.6
ip route 10.0.0.0 255.0.0.0 10.10.1.1
ip default-gateway 10.10.1.1
```

/md/Company-XYZ/mgmt-vpnc/00:1a:1e:00:00:01 Device Node Configuration

```
syslocation "Data Centre/HQ address, Room X, Rack Y, RU xx"
mgmt-user admin root <admin-password>
ntp source 1
firewall
    cp-bandwidth-contract trusted-ucast 65535
    cp-bandwidth-contract trusted-mcast 3906
    cp-bandwidth-contract untrusted-ucast 9765
    cp-bandwidth-contract untrusted-mcast 3906
    cp-bandwidth-contract route 976
    cp-bandwidth-contract sessmirr 976
    cp-bandwidth-contract vrrp 512
    cp-bandwidth-contract auth 976
    cp-bandwidth-contract arp-traffic 3906
    cp-bandwidth-contract l2-other 1953
!
ip name-server <DNS-Server-IP>
logging <syslog-Server-IP> type system facility local1 severity informational
hostname mgmt-vpnc-1
clock timezone Australia/Adelaide
geolocation <latitude longitude>
country AU
vrrp 10
    ip address 172.16.1.3
    description "VRRP IP for mgmt-vpnc WAN Links"
    preempt delay 3
    priority 150
    vlan 100
    tracking interface gigabitethernet 0/0/0 sub 60
    no shutdown
!
```

Note: Branch Gateway controllers communicate with the VRRP address of the management VPNCs, therefore only the active management VPNC establish IPSec security associations with branch devices and contain host route entries for the branch site controller-ips. Mgmt-vpnc-1 is VRRP is configured with interface tracking, if its LAN interface become unavailable, mgmt-vpnc-2 will have higher priority and assume active mgmt-vpnc functions.

4.3 Secondary Management VPNC Configuration

Shown below is the committed configuration of the secondary management VPNC (mgmt-vpnc-2).

/md/Company-XYZ/mgmt-vpnc/00:1a:1e:00:00:02 Device Node Configuration

```
masterip 10.50.1.10 ipsec <ipsec-key> peer-mac-1 00:1a:1e:01:00:01 peer-mac-2 00:1a:1e:01:00:02
location "Data Centre/HQ address, Room X, Rack Y, RU zz"
controller-ip vlan 100
vlan 1
!
vlan 100
    description WAN-Uplink
!
interface gigabitethernet 0/0/0
    description " 1G LAN Uplink to Core-1 switch port Eth2/2"
    switchport access vlan 1
    switchport mode access
    trusted
    trusted vlan 1
!
```

/md/Company-XYZ/mgmt-vpnc/00:1a:1e:00:00:02 Device Node Configuration

```
interface gigabitethernet 0/0/1
    description "1G WAN Uplink 1 to WAN-Edge-1 switch port WGE1/1/2"
    switchport access vlan 100
    switchport mode access
    trusted
    trusted vlan 100
!
interface vlan 1
    ip address 10.10.1.2 255.255.255.252
    description LAN
!
interface vlan 100
    ip address 172.16.1.2 255.255.255.248
    description WAN
!
ip route 172.16.0.0 255.255.0.0 172.16.1.6
ip route 10.0.0.0 255.0.0.0 10.10.1.1
ip default-gateway 10.10.1.1
syslocation "Data Centre/HQ address, Room X, Rack Y, RU zz"
mgmt-user admin root <admin-password>
ntp source 1
!
firewall
    cp-bandwidth-contract trusted-ucast 65535
    cp-bandwidth-contract trusted-mcast 3906
    cp-bandwidth-contract untrusted-ucast 9765
    cp-bandwidth-contract untrusted-mcast 3906
    cp-bandwidth-contract route 976
    cp-bandwidth-contract sessmirr 976
    cp-bandwidth-contract vrrp 512
    cp-bandwidth-contract auth 976
    cp-bandwidth-contract arp-traffic 3906
    cp-bandwidth-contract l2-other 1953
!
ip name-server <DNS-Server-IP>
logging <syslog-Server-IP> type system facility local1 severity informational
hostname mgmt-vpnc-1
clock timezone Australia/Adelaide
geolocation <latitude longitude>
country AU
vrrp 10
    ip address 172.16.1.3
    description "VRRP IP for mgmt-vpnc WAN Links"
    preempt delay 3
    priority 100
    vlan 100
    no shutdown
!
```

5 Data VPNC

Data VPNCs participate in forwarding branch user traffic and function as aggregation routers for branch sites. There are two Data VPNC devices deployed for redundancy. It's important to note however, that only one of them can be the active VPNC for all branch sites at a given time the other is on standby.

Since Data VPNCs participate in forwarding traffic for user subnets, Data VPNCs need to "dynamically" learn branch site IP subnets from its branch vpn-peer gateway devices. VPNCs must propagate the leant routing information to its uplink routing peer(s) in the Core Network via a compatible routing protocol (i.e., ospf) for the core network to be able to communicate with the branch site networks.

The communication between a Data VPNC and a branch site router happens via an IPSec tunnel; this, limits choice of routing protocols that can be used between the VPNC and branch-gw-wlc. branch-gw-wlcs are configured to advertise its connected routes to the headend data-vpncs via ike extensions during the IPsec tunnel establishment. Both VPNCs store such routes as ike-overlay routes on their routing table. VPNCs are capable of redistributing ike-overlay routes in to ospf (with the same fixed ospf cost for all branch networks) and advertise to its uplink ospf peer in the Core network as an ospf external type 2 route. It's worth noting however, the VPNCs cannot redistribute routes learnt via ospf into Ike and advertise them to the branch sites, dynamically. In fact, this reference VPNC deployment does not advertise any routes to the branch sites, and branch gateways entirely rely on static routes and policy-based routing for forwarding branch site wireless & wired user traffic.

Each Data VPNC is configured with a unique ospf area (Area 1001 or 1002). The area type is configured as "not-so-stubby-area" (nssa), ospf nssa areas allow the VPNC to advertise routes learnt via other protocols to its uplink Area Border Routers (ABRs) without receiving any inter-area routes from the ABRs. Same ospf area on uplink device (Core switch) is configured as "totally-not-so-stubby-area" which further restricts the route updates and only sends the default route to each data-vpnc.

Note 1: This ospf area configuration was necessary due to the way VPNCs prefer different types of routing protocols. Without nssa areas, ike-overlay routes redistributed by one Data VPNC, propagates via the core network to the other Data VPNC and gets installed in its routing table. Once a branch site route gets installed via ospf in the VPNCs routing table, ospf routes get preferred over same ike-overlay branch route directly learnt via the IPsec tunnel connected to the branch. This can result in unpredictable routing behaviours based on which VPNC's WAN link activates first. The use of nssa areas stops the branch route propagation from one Data VPNC to the other over ospf and provides consistency in routing.

Note 2: Data VPNCs do require redundant uplink ospf peers for full redundancy since the branch-gw-wlcs rely on PBR and static routes, Branch-gw-wlcs are unable to detect a failure happening on the LAN facing interface of the VPNC. Therefore, it's crucial to provide uplink redundancy and provide uplink ospf peer redundancy to each of the Data VPNCs. Each of the Data VPNC has two uplinks to two switches on the core network.

5.1 Data VPNC Common Configurations

Like the management VPNC, a Data VPNC also authenticates the branch controllers that can connect to it using the mac address information contained within branch gateway-wireless controller's factory certificate, during the initial IPsec tunnel establishment.

Listed below are the vpn-peer mac address configurations which are inherited by both the Data VPNCs. It allows a properly configured branch device to establish and IPSec tunnel with the VPNC.

/md/Company-XYZ/data-vpnc Group Node Configuration
vpn-peer peer-mac 00:1a:1e:00:03:01 cert-auth factory-cert vpn-peer peer-mac 00:1a:1e:00:03:02 cert-auth factory-cert vpn-peer peer-mac 00:1a:1e:00:03:03 cert-auth factory-cert vpn-peer peer-mac 00:1a:1e:00:03:04 cert-auth factory-cert vpn-peer peer-mac 00:1a:1e:00:03:05 cert-auth factory-cert

5.2 Primary Data VPNC Configuration

The data vpncs are deployed just like any regular wireless controller directly managed by the mobility master cluster. Branch-gw controllers do NOT establish communications with the mobility master via data vpncs, therefore, during the initial configuration dialogs data vpncs are provisioned as regular wireless lan controllers, the ability to accept ipsec connections from the branch-gw-controllers is later added when the lan interface is connected to the core switches, connectivity to the mobility master is established and "vpn-peer" configurations are inherited from the configuration hierarchy.

When data-vpnc is visible to the mobility master, ospf configuration is added by modifying the configuration device node (individual data-vpnc node) level of the mobility manager configuration hierarchy. Note what the WAN link address of the data-vpnc is redistributed to ospf so the core-network and mobility master can reach (ping) the WAN interface IP address.

Once reachability from the mobility master to the WAN IP address of the data-vpnc is tested then you must change the controller-ip address of the data-vpnc to its WAN link IP address, data-vpnc will reboot and reappear in mobility master configuration hierarchy with the new controller-ip. Repeat this process for the secondary data-vpnc as well.

Shown below is the full configuration applied to the data-vpnc-1.

/md/Company-XYZ/data-vpnc/00:1a:1e:00:01:01 Device Node Configuration

```
masterip 10.50.1.10 ipsec <ipsec-key> interface vlan 100
location "Data Centre/HQ address, Room A, Rack B, RU xx"
controller-ip vlan 100

vlan 10
   description Core-1 switch Uplink
!
vlan 20
   description Core-2 switch Uplink
!
vlan 100
   description WAN-Edge-1 Uplink
!
interface gigabitethernet 0/0/0
   description "10G Uplink to Core-1 port Eth1/10"
   switchport access vlan 10
   switchport mode access
   trusted
   trusted vlan 10
!
interface gigabitethernet 0/0/1
   description "10G Uplink to Core-2 port Eth1/10"
   switchport access vlan 20
   switchport mode access
   trusted
   trusted vlan 20
!
interface gigabitethernet 0/0/2
   description "10G Uplink to WAN-Edge-1 switch port WGE 1/1/1"
   switchport access vlan 100
   switchport mode access
   trusted
   trusted vlan 100
interface vlan 1
   shutdown
!
interface vlan 10
   ip address 10.10.1.10 255.255.255.252
   description Core-1 Uplink
   ip ospf area 0.0.3.233
   ip ospf cost 100
!
```

/md/Company-XYZ/data-vpnc/00:1a:1e:00:01:01 Device Node Configuration

```
interface vlan 20
    ip address 10.10.1.14 255.255.255.252
    description Core-2 Uplink
    ip ospf area 0.0.3.233
    ip ospf cost 500
!
interface vlan 100
    ip address 172.16.1.9 255.255.255.252
    description WAN Uplink
    ip ospf area 0.0.3.233
!
interface loopback
    ip address 172.16.1.25 255.255.255.255
    description Loopback
    ip ospf area 0.0.3.233
ip route 172.16.0.0 255.255.0.0 172.16.1.10
syslocation "Data Centre/HQ address, Room A, Rack B, RU xx"
snmp-server community <snmp-server-community-value>
syscontact "<contact-phone-number>"
snmp-server host <snmp-server-ip> version <version> <community-value> udp-port 162
snmp-server source controller-ip
mgmt-user admin root <admin-password>
ntp server <NTP-Server-IP>
ntp source loopback
firewall
    jumbo mtu 9216
    dpi
    cp-bandwidth-contract trusted-ucast 65535
    cp-bandwidth-contract trusted-mcast 3906
    cp-bandwidth-contract untrusted-ucast 9765
    cp-bandwidth-contract untrusted-mcast 3906
    cp-bandwidth-contract route 976
    cp-bandwidth-contract sessmirr 976
    cp-bandwidth-contract vrrp 512
    cp-bandwidth-contract auth 976
    cp-bandwidth-contract arp-traffic 3906
    cp-bandwidth-contract l2-other 1953
!
ip name-server <DNS-Server-IP>
ip domain-name <DNS-Domain-Name>
ip-flow-export-profile
    enable
    upload-all-interval 1
    collector-ip <NetFlow-collector-IP>
    port <NetFlow-collector-port>
!
router ospf router-id 10.10.1.25
router ospf
router ospf redistribute ike-overlay 500
router ospf redistribute vlan 100
router ospf redistribute loopback
router ospf area 0.0.3.233/
    nssa
!
snmp-server enable trap
snmp-server trap source 10.10.1.25
firewall-visibility
hostname data-vpnc-1
clock timezone Australia/Adelaide
banner motd ^
***** As-per-organization security warning messages*****
^
geolocation <latitude longitude>
country AU
```

5.3 Standby Data VPNC Configuration

Shown below is the committed configuration of the Standby Data VPNC (data-vpnc-2).

/md/Company-XYZ/data-vpnc/00:1a:1e:00:01:02 Device Node Configuration

```
!
masterip 10.50.1.10 ipsec <ipsec-key> interface vlan 100
location "Data Centre/HQ address, Room A, Rack C, RU x"
controller-ip vlan 100

vlan 10
   description Core-1 switch Uplink
!
vlan 20
   description Core-2 switch Uplink
!
vlan 100
   description WAN-Edge-2 Uplink
!
interface gigabitethernet 0/0/0
   description "10G Uplink to Core-1 port Eth1/11"
   switchport access vlan 10
   switchport mode access
   trusted
   trusted vlan 10
!
interface gigabitethernet 0/0/1
   description "10G Uplink to Core-2 port Eth1/11"
   switchport access vlan 20
   switchport mode access
   trusted
   trusted vlan 20
!
interface gigabitethernet 0/0/2
   description "10G Uplink to WAN-Edge-2 switch port WGE 1/1/1"
   switchport access vlan 100
   switchport mode access
   trusted
   trusted vlan 100
!
--interface port-channel 0 – 7 - unused --configs omitted --
!

interface vlan 1
   shutdown
!
interface vlan 10
   ip address 10.10.1.18 255.255.255.252
   description Core-1 Uplink
   ip ospf area 0.0.3.234
   ip ospf cost 5000
!
interface vlan 20
   ip address 10.10.1.22 255.255.255.252
   description Core-2 Uplink
   ip ospf area 0.0.3.234
   ip ospf cost 1000
!
interface vlan 100
   ip address 172.16.1.13 255.255.255.252
   description WAN Uplink
   ip ospf area 0.0.3.234
!
interface loopback
```

/md/Company-XYZ/data-vpnc/00:1a:1e:00:01:02 Device Node Configuration

```
    ip address 172.16.1.26 255.255.255.255
    description Loopback
    ip ospf area 0.0.3.234


ip route 172.16.0.0 255.255.0.0 172.16.1.14
syslocation ""Data Centre/HQ address, Room A, Rack C, RU x"
snmp-server community <snmp-server-community-value>
syscontact "<contact-phone-number>"
snmp-server host <snmp-server-ip> version <version> <community-value> udp-port 162
snmp-server source controller-ip
mgmt-user admin root <admin-password>
ntp server <NTP-Server-IP>
ntp source loopback
firewall
    jumbo mtu 9216
    dpi
    cp-bandwidth-contract trusted-ucast 65535
    cp-bandwidth-contract trusted-mcast 3906
    cp-bandwidth-contract untrusted-ucast 9765
    cp-bandwidth-contract untrusted-mcast 3906
    cp-bandwidth-contract route 976
    cp-bandwidth-contract sessmirr 976
    cp-bandwidth-contract vrrp 512
    cp-bandwidth-contract auth 976
    cp-bandwidth-contract arp-traffic 3906
    cp-bandwidth-contract l2-other 1953
!
ip name-server <DNS-Server-IP>
ip domain-name <DNS-Domain-Name>
ip-flow-export-profile
    enable
    upload-all-interval 1
    collector-ip <NetFlow-collector-IP>
    port <NetFlow-collector-port>
!

router ospf router-id 10.10.1.26
router ospf
router ospf redistribute ike-overlay 20000
router ospf redistribute vlan 100
router ospf redistribute loopback
router ospf area 0.0.3.234
    nssa
!
snmp-server enable trap
snmp-server trap source 10.10.1.26
firewall-visibility
hostname data-vpnc-2
clock timezone Australia/Adelaide
banner motd ^
***** As-per-organization security warning messages*****
^
geolocation <latitude longitude>
country AU
!
```

6 Branch Wireless Controllers

Aruba wireless controllers deployed at the branch site is the final key component of the branch wireless solution. Controllers can be deployed with minimal a configuration at a branch site which allows them to establish communications with the mobility master via the active management VPNC. Large portion of the branch site configurations is then propagated to the site controller automatically. The configuration settings unique to the branch site can then be adjusted by modifying settings under the respective device node of the mobility master configuration hierarchy. As a result, connecting a new branch site and providing wireless (as well as wired) network access can be done in a remarkably short timeframe.

Although the Aruba wireless controller deployed at the branch site functions as the gateway router for the site as well, they are vastly different to a traditional WAN router in the way they are configured, managed and forward user traffic. These differences need to be clearly understood by the individuals deploying them to the branch sites and perform ongoing management and monitoring functions.

Rest of this document will focus entirely on branch wireless controller, deployment procedure, WLAN configuration, AP Group configuration, RF configuration settings and LAN traffic forwarding of the branch controller.

6.1 Branch Wireless Controller Deployment

Branch wireless controller deployment can be summarized in 3 steps.

- Prestaging
- Automated configurations
- Applying site specific configuration

6.1.1 Pre-staging a branch wireless controller.

Upon first boot-up, Aruba wireless controller in its factory default setting will request the user to enter basic configuration information for that controller. Depending on the answers user enters during the prompts subsequent questions will differ. During the pre-staging following information need to be entered by the engineer configuring the device.

- System name (aka hostname)
- Switch Role (Mobility Master /Standalone Controller / Managed Device of an MM):
- Master IP address
- If a VPN concentrator is in use
- VPN concentrator IP address
- Authentication Method used by the VPNC
- Mac address of the Primary VPNC
- Mac address of the Redundant VPNC
- If L3 Redundant Mobility Master is present
- Uplink Interface configuration settings (VLAN, dot1.q, IP/Mask)
- Default Gateway Address
- DNS Server IP address
- If IPv6 used
- If a Port-Channel is used

- Country Code
- Timezone / UTC time
- Admin Password

Note: In the tested design, Only the System name, IP link IP address/Mask and the Default Gateway are site specific, other configurations are common to all branch sites.

Table below lists all parameters and values that are entered during the pre-staging of a branch wireless controller; select full-set up during auto-provisioning settings prompt.

Configuration Parameter	Value (/comments)
Enter System name [Aruba7030]:	Device name of the branch site wireless lan controller (e.g., branch1-gw-wlc)
Enter Switch Role (master | standalone | md) [md]:	Press enter to select default option [md]
Enter IP type to terminate IPSec tunnel (ipv4|ipv6) [ipv4]:	Press enter to select default option [ipv4]
Enter Master switch IP address or FQDN:	10.50.1.10
Is this a VPN concentrator for managed device to reach Master switch (yes | no) [no]:	Press enter to select default option [no]
This device connects to Master switch via VPN concentrator (yes | no) [no]:	yes
Enter VPN concentrator IP address or FQDN:	172.16.1.3 (this is the vrrp address of mgmt-vpnc WAN interface)
VPN concentrator Authentication method (FactoryCert | PSKwithMAC) [FactoryCert]:	Press enter to select default option [FactoryCert]
Enter VPN concentrator MAC address:	00:1a:1e:00:00:01 (This is the mgmt-vpnc-1 controller HW mac)
Enter Redundant VPN concentrator MAC address [none]:	00:1a:1e:00:00:02 (This is the mgmt-vpnc-2 controller HW mac)
Do you want to enable L3 Redundancy (yes | no) [no]:	Press enter to select default option [no]
Enter Uplink Vlan ID [1]:	100 (Tested branch site deployment always use vlan 100 as its WAN interface for consistency)
Enter Uplink port [GE 0/0/0]:	Press enter to select default option [GE 0/0/0] (Ge0/0/0 interface is always used to connect to WAN)
Enter Uplink port mode (access | trunk) [access]:	Press enter to select default option [access] (WAN interface always configured as an access port)
Enter Uplink Vlan IP assignment method (dhcp |static | pppoe) [static]:	Press enter to select default option [static] (WAN interface IP address is statically configured)
Enter Uplink Vlan Static IP address [172.16.0.254]:	172.16.1.24 (enter the unique WAN IP address provided by WAN Service Provider for the branch CE device)
Enter Uplink Vlan Static IP netmask [255.255.255.0]:	255.255.255.252(/30 mask is used for WAN Links)

Configuration Parameter	Value (/comments)
Enter IP default gateway [none]:	172.16.1.25 (enter the unique WAN Gateway IP address provided of the WAN Service Provider PE device)
Enter DNS IP address [none]:	10.x.x.x (DNS Server IP address of the ABC Company)
Do you wish to configure IPV6 address on vlan (yes | no) [yes]:	no
Do you want to configure dynamic port-channel (yes | no) [no]:	Press enter to select default option [no] (WAN interface is not configured as a port-channel)
Enter Country code (ISO-3166), <ctrl-I> for supported list:	AU (Make sure your country code is entered correctly, once saved this setting can't be modified without resetting the controller to factory default setting)
You have chosen Country code AU for Australia (yes | no)? :	yes
Enter the controller's IANA Time zone [America/Los_Angeles]:	Australia/Adelaide
Enter Time in UTC [HH:MM:SS]:	HH:MM:SS (Check the UTC time at the time of provisioning, enter the value in the given format)
Enter Date (MM/DD/YYYY) []:	MM/DD/YYYY (Confirm the date at of provisioning, enter the value in the given format)
Do you want to create admin account (yes | no) [yes]:	Press enter to select default option [yes]
Enter Password for admin login (up to 32 chars):	<admin-password> (enter the admin user password)

Confirm and save the pre-stage configuration settings. Branch wireless controller will reboot as a managed device and can only be configured by the mobility master under normal operation.

Note: Disaster recovery mode allows managed devices to be configured in situations when the managed device has lost communication with mobility master.

As part of the pre-staging process Aruba Branch wireless controllers should be upgraded to the standard operating environment (SOE) software version of the ABC Company. Aruba wireless controller software version should be equal to (as a best practice) or lower than the software version of the mobility master that manages it. The tested solution was initially built using software version 8.6.0.6_77124 for all devices and later upgraded to 8.6.0.17_83573.

Caution: Some Aruba software versions have unresolved software bugs that impact traffic between the branch controller and data-vpnc due to IPsec packet fragmentation and impact user applications. It is strongly recommended to test the user applications such as web-browsing and MS-teams calls if you decide to use a different software version for your branch wireless network deployment than versions mentioned here.

Following CLI command can be used to upgrade software version of an Aruba7030 branch controller (usb drive containing the correct software image file should be connected to the controller at the time of executing this command)

Aruba 7030 Controller Software image upgrade via CLI
copy usb: partition 1 ArubaOS_70xx_8.6.0.17_83573 system: partition 0

Note: if you are using different wireless controller model, please download the correct software version for that model from https://asp.arubanetworks.com/downloads website.

6.1.2 Automated Configurations.

When the Pre-staged Aruba controller is connected to the WAN Link at the branch site, Branch controller will establish an IPsec tunnel the active management VPNC. The management VPNC then triggers a route update via IPsec (ike-overlay route) to the branch controller indicating that it can reach the mobility master via the newly formed IPsec tunnel. Management VPNC also triggers route change on Mobility master that it can reach the branch controller WAN IP address via the MM←→mgmt-vpnc ipsec tunnel. When the communication between the mobility master and branch gateway controller is established, all settings applied at higher levels of the device configuration hierarchy propagates automatically to the branch device.

A significant portion of configuration settings common to all branch sites, are stored as a configuration template at the "/md/Company-XYZ/branch" group level of the configuration node hierarchy. Settings include tunnels to data-vpncs, static routes, PBR and all WLAN configuration settings. Modification of the configuration settings at this level should be done with caution.

Shown below is the full configuration template that automatically gets applied to all branch sites.

/md/Company-XYZ/branch Group Node Configuration

```
!
ip radius source-interface vlan 10
ip radius nas-ip nas-vlan 10
ip access-list route tunnel-to-vpncs
    any network 10.0.0.0 255.0.0.0 any forward
    any network 172.16.0.0 255.255.0.0 any forward
    any any any route next-hop-list vpncs
!
vlan 10
!
vlan 100
!
vlan-name LAN
vlan-name WAN
!
vlan WAN 100
!
interface gigabitethernet 0/0/1
    description Branch LAN
    trusted
    lldp transmit
    lldp receive
    trusted vlan 1-4094
!
interface vlan 100
    ip address dhcp-client
!
!  Two static routes to all internal corporate networks point to the IPsec tunnels with two different costs, route with
higher cost only gets activated when the primary IPsec tunnel is down
!
ip route 10.0.0.0 255.0.0.0 ipsec data-vpnc-00:1a:1e:00:01:01 10
ip route 10.0.0.0 255.0.0.0 ipsec data-vpnc-00:1a:1e:00:01:02 20
!
! configure a next-hop list which will be used for Policy Based Routing (PBR)
!
ip nexthop-list vpncs
    ipsec-map data-vpnc-00:1a:1e:00:01:01 priority 200
    ipsec-map data-vpnc-00:1a:1e:00:01:02 priority 100
!
Configure the Data VPNC IPsec Tunnels, this is common to all branch sites
!
vpnip 172.16.1.9 ipsec-factory-cert vpnc-mac-1 00:1a:1e:00:01:01 interface vlan 100
vpnip 172.16.1.13 ipsec-factory-cert vpnc-mac-1 00:1a:1e:00:01:02 interface vlan 100
!
mgmt-user admin root <password>
```

/md/Company-XYZ/branch Group Node Configuration

```
ntp server <ntp-server-ip>
!
! Enable Deep packet inspection and web-content classification, by the way, web-cc require a license.
!
firewall
    dpi
    web-cc
!
firewall-visibility
!
ip name-server <dns-server-ip>
ip domain-name <dns.domain.name>
!
!
! WiFi Configurations common to all branch sites below.
!
ip access-list session denyalldefault
    any any any deny
    ipv6 any any any deny
!
user-role XYZ-WiFi
    access-list session allowall
!
user-role DenyAllDefault
    access-list session denyalldefault
!
ip access-list session apprf-xyz-wifi-sacl
!
vlan-name XYZ-WiFi
!
aaa rfc-3576-server "<Primary-Radius-Server-IP>"
    key <key>
!
aaa rfc-3576-server "<Secondary-Radius-Server-IP>"
    key <key>
!
aaa authentication dot1x "XYZ-WiFi"
!
! Define Radius Servers and Server Group
!
aaa authentication-server radius "Primary-Radius-Server-Name"
    host "<Primary-Radius-Server-IP>"
    key <key>
!
aaa authentication-server radius "Secondary-Radius-Server-Name"
    host "<Secondary-Radius-Server-IP>"
    key <key>
!
aaa server-group "XYZ-Radius-Server-Group"
  load-balance
 auth-server <Primary-Radius-Server-Name> position 1
 auth-server <Secondary-Radius-Server-Name> position 2
!
! Define the AAA Profiles for authenticating WiFi clients
!
aaa profile "XYZ-WiFi-AAA"
    initial-role "DenyAllDefault"
    mac-default-role "DenyAllDefault"
    authentication-dot1x "XYZ-WiFi "
    dot1x-default-role "authenticated"
    dot1x-server-group "XYZ-Radius-Server-Group"
    radius-accounting "XYZ-Radius-Server-Group "
    rfc-3576-server "<Primary-Radius-Server-IP>"
    rfc-3576-server "<Secondary-Radius-Server-IP>"
```

Author: Manjula Hiripitiya

/md/Company-XYZ/branch Group Node Configuration

```
!
web-server profile
   web-https-port-443
!
! Allow APs to auto-register with the branch controller, but it is recommended to disable auto provisioning after the
! branch AP deployment is over.
!
control-plane-security
   auto-cert-prov
!
! following intelligent power monitoring commands in the AP system profile are optional
!
ap system-profile "branch-ap-system-default"
   ipm-enable
   ipm-power-reduction-step-prio ipm-step disable_usb priority 1
   ipm-power-reduction-step-prio ipm-step cpu_throttle_75 priority 2
   ipm-power-reduction-step-prio ipm-step radio_2ghz_power_3dB priority 3
   ipm-power-reduction-step-prio ipm-step cpu_throttle_50 priority 4
!
! set max channel-bandwidth on the 5GHz band to 40 MHz and Tx-Power as required
!
rf dot11a-radio-profile "branch-dot11a-radio-default"
   spectrum-monitoring
   max-channel-bandwidth 40MHz
   min-channel-bandwidth 40MHz
   eirp-min 12
   eirp-max 18
!
! set max channel-bandwidth on the 2.4GHz band to 20 MHz and Tx power lower than the 5GHz band so wifi clients
! prefer the stronger signal and connect to 5GHz instead of the 2.4GHz
!
rf dot11g-radio-profile "branch-dot11g-radio-default"
   spectrum-monitoring
   max-channel-bandwidth 20MHz
   eirp-min 1
   eirp-max 6
!
! set the mandatory (basic) data rates to 12 and 24 and higher supported rates, you should use lower basic rates
!  only when you have to support 802.11b only legacy clients. Also enable wireless multimedia support and qbss
! load element on the beacon and probe responses
!
wlan ssid-profile "XYZ-WiFi-SSID"
   essid "XYZ-WiFi"
   opmode wpa2-aes
   a-basic-rates 12 24
   a-tx-rates 12 18 24 36 48 54
   g-basic-rates 12
   g-tx-rates 12 18 24 36 48 54
   wmm
   qbss-load-enable
   advertise-location
   advertise-ap-name
!
! Define the Virtual AP Profile which acts as a container for SSID profile , AAA profile , Specify the default vlan
! (a named-vlan which will be mapped to Branch user vlan of each site at the site controller configuration level)
!
wlan virtual-ap "XYZ-WiFi-VAP"
   aaa-profile "XYZ-WiFi-AAA"
   vlan XYZ-WiFi
   ssid-profile " XYZ-WiFi-SSID"
!
! Specify Airwave Management Server and the information that should be pushed to the Server
!
mgmt-server profile "default-amp"
```

Author: Manjula Hiripitiya

/md/Company-XYZ/branch Group Node Configuration

```
    user-visibility-enable
    uccmonitoring-enable
    airgroupinfo-enable
!
! specify AP group name, here we have used "default" AP groups since APs join the "default" AP groups when the
! first boot up and discover the branch controller, immediately advertise the SSID and start servicing WiFi
! clients at the branch site without having to provision them manually, this was done to reduce effort required to
! deploy APs at the branch sites, but if you require higher security, use custom AP group and manual AP
! provisioning.
!
ap-group "default"
    virtual-ap "XYZ-WiFi-VAP"
    dot11a-radio-profile "branch-dot11a-radio-default"
    dot11g-radio-profile "branch-dot11g-radio-default"
    ap-system-profile "branch-ap-system-default"
!
--Optional-Configs--
!
snmp-server community <snmp-string>
snmp-server host <snmp-server-ip> version 2c <snmp-string> udp-port 162
!
ip-flow-export-profile
    enable
    upload-all-interval 1
    collector-ip <netflow-collector-ip>
    port <netflow-collector-port>
!
logging <syslog-server-ip> source-interface 1000 type system severity notifications
!
banner motd ^
*************************************************************************
*                            Banner if required                         *
*************************************************************************
^
```

Modification of the configuration settings at this level impacts all branch sites.

6.1.3 Applying Branch Site Specific Configurations.

Ones the Branch controller is connected to the Branch WAN link and automatic configuration settings are propagated down to the branch gateway controller; additional site-specific configurations can be applied. This is achieved by modifying settings at the specific branch controller node level of the Mobility Master (MM) configuration hierarchy. Setting include additional User vlans on the site and routes advertised via IPSec and SNMP location settings, DHCP Server/Relay settings etc.

Listed below is the configuration of a sample branch site controller (branch1-gw-wlc)

/md/Company-XYZ/Branch/00:1a:1e:00:03:01 Device Node Configuration

```
!
masterip 10.50.1.10 vpn-ip 172.16.1.3 ipsec-factory-cert vpn-mac-1 00:1a:1e:00:00:01 vpn-mac-2
00:1a:1e:00:00:02 interface vlan 100
location "Branch1, Branch1 Steet Address"
controller-ip vlan 100
!
vlan 10
vlan 100
```

/md/Company-XYZ/Branch/00:1a:1e:00:03:01 Device Node Configuration

```
!
! Map the named VLAN assigned WiFi Clients to the same vlan ID of the Branch wired users VLAN, you can use a
! separate vlan altogether if you wish, remember to advertise that vlan via ike over the IPsec tunnels.
!
vlan XYZ-WiFi 10
!
no spanning-tree
!
! it is recommended to set the speed and duplex of the WAN interface to the values supported by the WAN Service
! Providers Switch/NTU
!
interface gigabitethernet 0/0/0
    speed <xxx>
    duplex full
    description "WAN Link to Service Provider"
    switchport access vlan 100
    trusted
    trusted vlan 100
!
! configure the Controller interface connecting to the Branch LAN as a trunk port, you can add additional VLANs for
! the branch site.
!
interface gigabitethernet 0/0/1
    description "Branch LAN - PoE-Switch UpLink"
    switchport mode trunk
    switchport trunk allowed vlan 10
    trusted
    lldp transmit
    lldp receive
    trusted vlan 1-4094
!
! configure the L3 SVI for the branch LAN, notice the PBR ACL applied for the inbound traffic & Configure DHCP
! relay
!
interface vlan 10
    ip address 10.100.1.1 255.255.255.0
    ip helper-address <dhcp-server-ip>
    description "SVI for Site LAN Interface"
    operstate up
    ip access-group in tunnel-to-vpncs
!
interface vlan 100
    ip address 172.16.1.26 255.255.255.252
!
! default-gateways the Service Provider side IP of the WAN interface, this is only used by the branch-gw-wlc to
! reach the VPNC IP addresses, user traffic is tunnelled via IPsec tunnels to the Data-VPNCs
!
ip default-gateway 172.16.1.25
!
! Advertise the LAN subnet via ike extension to the Upstream Data-VPNCs, add additional vlans present on the
! branch site as a comma separated list.
!
crypto-local isakmp route ipsec data-vpnc-00:1a:1e:00:01:01 vlan 10
crypto-local isakmp route ipsec data-vpnc-00:1a:1e:00:01:02 vlan 10
!
syslocation "Brach1 Site Location, Street Address"
syscontact "Tech Support Contact Phone No:"
mgmt-user admin root <password>
ssh mgmt-auth public-key
!
ip name-server <dns-server-ip>
snmp-server trap source 10.100.1.1
hostname branch1-gw-wlc
country <Country Code>
```

Author: Manjula Hiripitiya

Note: some of the configuration settings listed above are entered during the prestaging process and you are only required to add the rest of the configurations under the branch device level of the mobility master configuration hierarchy.

Connect the LAN interface of the Branch-gw-WLC to the Branch PoE Access switch, APs should boot up, obtain an IP address from the DHCP server, discover the branch controller, join the default ap group and start advertising the XYZ-WiFi SSID and provide Wireless connectivity to the Branch site.

Users and other devices such as printers directly connecting to the branch switch via UTP should also be able to connect obtain an IP address and connect to the XYZ Company corporate network.