ArubaOS 8: Campus Design and Deployment Best Practices

Amish Shah - Sr. Product Manager
Agenda

• VRD architecture
• Hierarchy
• Zero Touch Provisioning
• Unified AP
• AP Provisioning
• Campus Deployments with Cluster
• Branch with VPNC
• Guest with MultiZone
• Dynamic Segmentation
• Client Troubleshooting
Aruba Enterprise WLAN Network Architecture
Access Points and Controllers
Campus AP Platform Portfolio

340 Series (AP-34x)
802.11ac 4x4:4SS, MU-MIMO, VHT160
1x 2.5GE + 1x 1GE, USB, BLE, dual 5GHz, 802.3at POE
11ac W2 Flagship

310 Series (AP/IAP-31x)
802.11ac 4x4:4SS*, MU-MIMO, VHT160
1x GE, USB, BLE, 802.3af POE
Baseline 4x4 11ac W2 platform

300 Series (AP/IAP-30x)
802.11ac 3x3:3SS*, MU-MIMO
1x GE, USB, BLE, 802.3af POE
Entry-level 3x3 11ac W2 platform

303 Series (AP-303/303P)
Dual radio, 802.11ac 2x2:2SS, MU-MIMO
1xGE, BLE, 802.3af/at/bt POE, PSE*
Low-cost 2x2 11ac W2 platform

AP 555
802.11ax 8x8:8SS / 4x4:4SS (Tri-Radio mode)
2x 5GE, USB, BLE / 15.4, 37RU, VHT160
11ax Flagship, 802.3bt POE

530 Series (AP-53x)
802.11ax 4x4:4SS / 4x4:4SS
2x 5GE, USB, BLE / 15.4, 37RU, VHT160
11ax High-end, 802.3bt POE

510 Series (AP-51x)
802.11ax 4x4:4SS / 2x2:2SS
1x 2.5GE + 1x 1GE, USB, BLE / 15.4, 16RU, VHT160
11ax Baseline / mid-range, 802.3at POE

802.11ac Wave 2
802.11ax Wave 1

@ArubaAPAC | #ATM19APAC
AP Modes

Controller-managed AP

Remote AP

Controller-less AP (Instant AP)
Flexible architecture supports both a centralized as well as a distributed (Instant) deployment mode

Remote APs, VIA Mobile/Laptop Client
- Small, temporary & home office Wi-Fi

Distributed, controllerless WLAN with Aruba Instant
- Simplified branch deployment with clusters

Controller-based WLAN with ArubaOS
- Centralized encryption with advanced services at scale

SAME AP HARDWARE, SAME ENTERPRISE-GRADE PERFORMANCE & FEATURES
Mobility Master

• Next Generation of Master Controller
  • Centralized Management and Visibility

• Deployment Flexibility
  • Virtual Mobility Master
  • Mobility Master Hardware Appliance

• Highly Scalable
  • 10k Devices
  • 100k Clients

• Centralized Licensing
Hierarchy Based Configuration
New Hierarchical Config Model in Mobility Master

- Mobility Master
  - MM2
  - MM1
- Managed Network (6)
  - Aruba-Sunnyvale (6)
    - Building-1322 (2)
      - VMC-1322-1
      - VMC-1322-2
    - Building-1341 (2)
      - VMC-1341-1
      - VMC-1341-2
    - Building-1344 (2)
      - VMC-1344-1
      - VMC-1344-2
- Aruba Sunnyvale
  - Building 1322
    - VMC-1322-1
    - VMC-1322-2
  - Building 1341
    - VMC-1341-1
    - VMC-1341-2
  - Building 1344
    - VMC-1344-1
    - VMC-1344-2
Hierarchical Configuration
Inheritance/ Override

```
aaa authentication-server radius "aruba-west"
  host "1.1.1.1"
  key ddf573d07a415e3a0b4ed2a1
!
aaa server-group "aruba-employee"
  auth-server aruba-west position 1
!
aaa profile "aruba-employee"
  authentication-dot1x "aruba-employee"
    dot1x-default-role "logon"
    dot1x-server-group "aruba-employee"
  !
wlan ssid-profile "aruba-employee"
  essid "aruba-employee"
  opmode wpa2-aes
!
wlan virtual-ap "aruba-employee"
  aaa-profile "aruba-employee"
  vlan 1
  ssid-profile "aruba-employee"
!
ap-group "default"
  virtual-ap "aruba-employee"
!
```

Override Radius IP

VMC-1322-1 MC Config
Hierarchical Configuration
Inheritance/Override

```bash
aaa authentication-server radius
"aruba-west"
  host "2.2.2.2"
  key ddf573d07a415e3a0b4ed2a1
!
aaa server-group "aruba-employee"
  auth-server aruba-west position 1
!
aaa profile "aruba-employee"
  authentication-dot1x "aruba-employee"
    dot1x-default-role "authenticated"
    dot1x-server-group "aruba-employee"
  !
wlan ssid-profile "aruba-employee"
  essid "aruba-employee"
  opmode wpa2-aes
!
wlan virtual-ap "aruba-employee"
  aaa-profile "aruba-employee"
  vlan 1
  ssid-profile "aruba-employee"
  !
ap-group "default"
  virtual-ap "aruba-employee"
!
```
Hierarchical Configuration
Inheritance/Override

AAA Authentication Server
radius "aruba-west"
    host "2.2.2.2"
    key ddf573d07a415e3a0b4ed2a1

AAA Server Group "aruba-employee"
    auth-server aruba-west position 1

AAA Profile "aruba-employee"
    authentication-dot1x "aruba-employee"
        dot1x-default-role "authenticated"
        dot1x-server-group "aruba-employee"

WLAN SSID Profile "aruba-employee"
    essid "aruba-employee"
    opmode wpa2-aes

WLAN Virtual AP "aruba-employee"
    aaa-profile "aruba-employee"
    vlan 199
    ssid-profile "aruba-employee"

AP Group "default"
    virtual-ap "aruba-employee"
New Hierarchical Config Model in Mobility Master

- Managed Network
  - Building 1322
    - VMC-1322-1
    - VMC-1322-2
  - Building 1341
    - VMC-1341-1
    - VMC-1341-2
  - Building 1344
    - VMC-1344-1
    - VMC-1344-2

Global WLAN, Roles and Firewall Policies
VLAN ID, VLAN interface, Site-specific WLANs
Hostnames, IP addresses, Cluster memberships

More Generic
More specific

How does a Controller find Mobility Master?

1. Automatic Provisioning via Aruba Activate
   - MD → MM Provisioning Rules

2. DHCP Option 43 (New in AOS 8.4)
   - Using Global or Per Scope Options

   - Full-Setup using CLI or Web-UI for each Mobility Controller (one at a time)
Zero Touch Provisioning

- Mobility Controller
- DHCP/DNS
- Activate
- Mobility Master

DHCP/DNS

HTTPS

MM information (certificate, IP, node path, VPNC details)

HTTPS

Configure MM for activate & DNS

Register certificate

Whitelist download

Configure provisioning rules, folder & controller role

IPSec tunnel UDP port 4500
Redundancy with Clustering
Benefits of Clustering

1. Seamless Campus Roaming
   Clients stay anchored to a single MC when roaming across controllers

2. Stateful Client Failover
   User traffic uninterrupted upon cluster member failure

3. AP and Client Load Balancing
   Users and APs automatically load balanced across cluster members

4. Live Upgrade
   Live rolling upgrade of cluster members and APs
Cluster Capacity Planning
https://ase.arubanetworks.com/solutions/id/197

Cluster AP Sizing Calculator for AOS 8 Provides AP sizing recommendations when deploying a cluster of mobility controllers running AOS 8

How many controllers do I need in cluster?

- # of controllers in cluster depends on #of AP you plan to deploy on that cluster
- Example:
  - If you have 3*7240 controller, you can deploy up to 3072 AP with full redundancy
What happens if entire cluster goes down?

LMS / Bkup-LMS to provide Redundancy w/ Preemption between 2 Clusters
AP Provisioning
How does AP discover Mobility Controller

• Static Assignment (rare)
  • Controller IP address is provisioned and saved in AP Flash

• Dynamic Assignment
  • DHCP request (Option 43)
  • AP multicasts Aruba Discovery Protocol (ADP) packets to group 239.0.82.11
  • AP broadcasts ADP packets to L2/L3 recipients
  • AP sends DNS query
    • Who is “aruba-master.domain.com”
    • “domain.com” supplied by DHCP
    • “DNS server” supplied by DHCP
How does AP Join a Cluster?

1. MM does not terminate AP's
2. AP communicates with Cluster VIP
3. AP is assigned AAC and S-AAC
How does AP Join a Cluster?

1. MM does not terminate AP’s
2. AP communicates with Cluster VIP
3. AP is assigned AAC and S-AAC
4. AP creates active and standby tunnels with AAC and S-AAC respectively
Campus Deployment Topologies
Large Campus Deployment

MM-East Campus

Virtual Appliance

AIRWAVE NETWORK MANAGEMENT

CLEARPASS ACCESS MANAGEMENT

Building 1 Building 2 Building 3

MM-West Campus

Virtual Appliance

AIRWAVE NETWORK MANAGEMENT

CLEARPASS ACCESS MANAGEMENT

Building 4 Building 5 Building 6

8.x

@ArubaAPAC | #ATM19APAC
Global Enterprise Deployment

8.x US Data Center

US-MM

Virtual Appliance

AIRWAVE NETWORK MANAGEMENT

CLEARPASS ACCESS MANAGEMENT

New York

San Jose

8.x EMEA Data Center

EMEA-MM

Virtual Appliance

AIRWAVE NETWORK MANAGEMENT

CLEARPASS ACCESS MANAGEMENT

London

Paris

8.x APJ Data Center

APJ-MM

Virtual Appliance

AIRWAVE NETWORK MANAGEMENT

CLEARPASS ACCESS MANAGEMENT

Beijing

Bangalore

@ArubaAPAC | #ATM19APAC
Campus with Distributed Branches

1. Deploy a Mobility Master
2. Convert Master and Standby Master to VPNC
3. Optional - Terminate MC’s on VPNC
4. Branch Redundancy available with Clustering
MultiZone
MultiZone Use Case: Guest Access

Primary Zone

- Mobility Master/Standby
- Virtual Appliance
- 3-node Cluster

DMZ Zone

- Standalone Active
- Standalone Stdby

Data Tunnel

Primary Tunnel

Secure SSID

Guest SSID
Multizone Deployments
Redundancy in the Data Zone

A Cluster (requires DZ Mobility Master)

Data Zone 1

A pair of standalone MCs w/vrrp

Data Zone 2

Virtual Appliance

Mobility Master/Standby

AIRWAVE NETWORK MANAGEMENT

CLEARPASS ACCESS MANAGEMENT

MC

MC

MC

MC

MC

MC

MC

MC

VRRP

Standalone MC

Standalone MC

Note: HA and Multizone are mutually exclusive!
Anchor Controller for Guest Data

- 6.x
- Master/Master-Standy
- Guest Local
- Employee
- Guest Red VLAN 7
- Local
- DMZ
- GRE Tunnel
- DHCP Request
- DHCP Response
- ICMP Request
- ICMP Response
- GRE Data Tunnel
- Red VLAN 7
- DHCP/DNS
RF Optimization with AirMatch
AirMatch for RF Optimization

- Centralized RF optimization service, models the network as a whole
- Based on AP neighbor path-loss metrics
- Channel bandwidth aware
- Prior 24 hours RF info used for calculation
- Does not impact ClientMatch, AP Scanning behavior or Air Monitor mode
AirMatch Dashboard on AirWave 8.2.6 (ATM 18 Event Network)
AirMatch Reactive Solution

High Noise Events

- AP changes channel using ARM interference index
- Noise threshold configurable in ARM profile
- AP moves back after 30 mins
- If noise again detected, AP moves to new channel and stays there for 12 hrs

Radar Events

- AP immediately vacates the channel
- AP moves back after the radar event timer has expired
- Two consecutive Radar events blacklists the channel
Troubleshooting Tips
Troubleshooting
Effective configuration - combined (inherited+committed) config applied

# show configuration effective detail

(Acme-MM1) [mynode] # cd MC7030-1
(Acme-MM1) [20:4c:03:06:d3:30] #show configuration effective detail

masterip 10.70.148.40 ipsec ***** interface vlan 149
crypto-local pki PublicCert master-ssh-pub-cert master-ssh-pub-cert
crypto-local pki ServerCert acme-mc acme-mc.pfx
ip access-list eth validuserethacl
    permit any

controller-ip vlan 149
controller-ipv6 vlan 149 address 2001::1

vlan 148

vlan 149

vlan 153

vlan-name mgmt-vlan
vlan-name user-vlan
vlan mgmt-vlan 148
vlan user-vlan 153
Troubleshooting

Pending configuration - config that has not been applied yet

# show configuration pending

```
(Acme-MM1)^[Oakmead] (config) #show configuration pending

vlan 148
vlan 153
vlan-name mgmt-vlan
vlan-name user-vlan
vlan mgmt-vlan 148
vlan user-vlan 153
rf dot11a-radio-profile "acme"
!
ap-group "acme"
  dot11a-radio-profile "acme"
  
(Acme-MM1)^[Oakmead] (config) #
```
Troubleshooting
Overrides – View what config parameter has been changed

Value Overridden for Device MC1
This value is set for MC1, overriding these inherited values:
Oak: 10.70.149.10*
* Clicking remove override will restore this value

 表头：WLANs, Radio, Mesh, LMS

- IP address: 10.80.149.10
- Backup IP address: 10.127.33.10
- IPv6 address: 
- Backup IPv6 address: 

- Mobility Master
  - OAK-MM2
  - OAK-MM1
- Managed Network (3)
  - HQ (3)
    - Oak (3)
      - MC1
      - MC2
      - MC3
## Troubleshooting

How to locate a client from the MM?

### 1. By Mac-Address

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>Name</th>
<th>Current switch</th>
<th>Role</th>
<th>Auth</th>
<th>AP name</th>
<th>Roaming</th>
<th>ESSID</th>
<th>Bssid</th>
<th>Phy</th>
<th>Profile</th>
<th>Type</th>
</tr>
</thead>
</table>

### 2. By ESSID

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>Name</th>
<th>Current switch</th>
<th>Role</th>
<th>Auth</th>
<th>AP name</th>
<th>Roaming</th>
<th>ESSID</th>
<th>Bssid</th>
<th>Phy</th>
<th>Profile</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.70.215.235</td>
<td>a0:b8:b4:48:e9:cc</td>
<td>10.70.211.13</td>
<td></td>
<td>authenticated</td>
<td>ap225-1</td>
<td>Wireless</td>
<td>secure-acme</td>
<td>18:64:72:40:bb:12</td>
<td>a-VHT</td>
<td>acme-dotlx-psk</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>10.70.215.253</td>
<td>60:45:bdcf:8c:5a</td>
<td>10.70.211.12</td>
<td></td>
<td>authenticated</td>
<td>ap225-1</td>
<td>Wireless</td>
<td>secure-acme</td>
<td>18:64:72:40:bb:12</td>
<td>a-VHT</td>
<td>acme-dotlx-psk</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting
MDConnect – How to securely login from the MM to any MD

1. Change Directory to the MD by Name

   (Acme-MM1) [mynode] # cd mc7030-1
   (Acme-MM1) [20:4c:03:06:d3:30] #

2. Run the command MDC to securely login to the MD

   (Acme-MM1) [20:4c:03:06:d3:30] # mdc

   Redirecting to Managed Device Shell
   Last login: Thu Mar 22 19:41:27 2018 from 10.70.148.41
   (MC7030-1) [MDC] #
Troubleshooting
MM and MDs Tech Support Logs

1. Tech Support logs at the MM
   
   #tar logs tech-support

2. Tech Support logs at every MD
   
   #tar logs tech-support
Recommended Reading

All the key concepts covered in this session are documented in the ArubaOS 8 Fundamentals Guide in the Reference Architectures section.


http://community.arubanetworks.com/t5/Controller-Based-WLAN/ArubaOS-8-Fundamentals-Guide/ta-p/428914
**Recommended Reading**

Mobile First Campus VRD covering campus deployments with wired and wireless networks
Excellent companion to AOS 8 Fundamentals Guide
Download the Event App
Gain access to the latest event information.

Rate this session
Access this survey via the mobile app and let us know what you think.

Locate this session:
- Agenda
- Select Date
- Find this session
- Click Survey
Join the Airheads Community
Scan the QR code to sign up now!

Ask Aruba
- Session 1: Tuesday, 24 Sep, 2:00pm – 2:45pm
- Session 2: Wednesday, 25 Sep, 1:45pm – 2:30pm
- Location: Town Hall at Tech Playground

Submit your Ask Aruba questions using the mobile app now!

Scan. Play. Win.
Play Now! Switch your thinking, say goodbye to the old ways and get ready for new innovations.

Visit the Tech Playground now!
atmosphere
2019 APAC
amish@hpe.com