# TABLE OF CONTENTS

1. OVERVIEW .......................................................................................................................... 3
   1.1 Executive Overview........................................................................................................... 3
   1.2 OS Version....................................................................................................................... 3

2. AOS 8.X INTRODUCTION................................................................................................. 4
   Understanding 8.x Hierarchy.................................................................................................. 5
   Commands to understand 8.x Hierarchy................................................................................. 8
   How to navigate between MM and MD .................................................................................. 12
   Commands to capture system/device info............................................................................ 13
   2.1 Clustering ...................................................................................................................... 15

3. PROCESSES .................................................................................................................... 18
   3.1 Data collection for TAC ................................................................................................. 19
   3.2 Authentication related issues ....................................................................................... 20
   3.3 Client Connectivity issues ............................................................................................. 21
   3.4 AP failing to come up on WLC ....................................................................................... 24
   3.5 AP Crash/reboot issues ................................................................................................. 26
   3.6 High CPU/Memory Utilization on the Controller ........................................................... 26
   High CPU Utilization on the controller ................................................................................. 26
   High Memory Utilization on the Controller ......................................................................... 27
   3.7 Mobility Master crash issues ....................................................................................... 28
   3.8 Controller Crash issues ............................................................................................... 29
   3.9 Controller – MM Related Issues .................................................................................... 30
   3.10 Packet Capture on Aruba Controller ............................................................................. 30
   3.12 Hardware Related Issues .............................................................................................. 32
   3.13 AirWave (AMP) Related Issues .................................................................................. 33

4. SOME USEFUL COMMANDS ....................................................................................... 34
   4.1 Global user table on MM............................................................................................... 34
   4.2 AP related commands ................................................................................................. 35
1. OVERVIEW

1.1 Executive Overview

The purpose of this document is to provide the steps and commands to assist troubleshooting common issues and logs to collect before contacting TAC.

1.2 OS Version

The guide is for Aruba 8.x Architecture. The commands are tested against ArubaOS version 8.5.0.3 release.
2. AOS 8.X INTRODUCTION

ArubaOS 8 delivers unified wired and wireless access, seamless roaming, enterprise grade security and an always-on network with the required performance, user experience and reliability to support high density environments.

The Mobility Master is a new component of the Aruba architecture that enables customers to take advantage of advanced features that require central coordination and for networks to scale due to increased demand for mobile and IoT devices. It also replaces the prior functions of the master controller and can be either deployed as a VM or an x86 hardware appliance. The Mobility Master provides automatic RF optimization and enables hitless failover in an unlikely event of a controller outage. Aruba’s current customers with Mobility Controllers can upgrade from ArubaOS version 6 to version 8 and immediately benefit from some of the new features and capabilities.

8.X Architecture

Aruba OS 8.X Architecture

- Mobility Master is the centralized point, from where you setup the entire configuration for both the Mobility Master itself and all managed controllers.
- Mobility Master consolidates all-master, single master-multiple local, and multiple master-local deployments into a single deployment model.
- Common configurations (default config) across devices are extracted to a shared template, which merges with device-specific configurations to generate the configuration for an individual device.
- Traffic from APs and clients will be handled by Managed Nodes (Managed Devices /Mobility Controllers).
  Mobility Controllers can be MM managed, standalone.
  Managed Devices are MCs managed by Mobility Master.
Comparison of Master Controller and Mobility Master.

<table>
<thead>
<tr>
<th>Master Controller (6.x)</th>
<th>Mobility Master (8.x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A physical appliance</td>
<td>Physical and virtual appliance (VM)</td>
</tr>
<tr>
<td>APs can be terminated</td>
<td>APs can not be terminated</td>
</tr>
<tr>
<td>Can push only partial config to the local Controller</td>
<td>Can push full config to local (MC/MD)</td>
</tr>
<tr>
<td>Configuration Validation is not done</td>
<td>Configuration validation is done before pushing to nodes</td>
</tr>
</tbody>
</table>

Understanding 8.x Hierarchy

Understanding hierarchy in the 8.x architecture is very important to configure and troubleshoot. The following diagram gives a brief of the 8.x configuration hierarchy.

ACRONYMS USED:

- MM - Mobility Master
- MC - Mobility Controller (can be MM managed, standalone, etc.)
- MD - Managed Device (an MC managed by MM)

ABOUT CONFIGURATION HIERARCHY

- A configuration (config) node is a hierarchical level on the MM at which you would apply a certain configuration.
- Two pre-defined config nodes exist - /mm and /md. These nodes cannot be deleted.
- All configuration related to the MM goes under /mm or /mm/mynode.
- Configuration common to both primary and standby MMs goes under /mm.
- Configuration specific to the MM device goes under /mm/mynode.
- You can create multiple config nodes under /md where each config node may have different configuration from other nodes under /md.
- Config nodes under /md can be further classified into group nodes and device nodes.

Group nodes:
- Any user-defined config node under /md can be called a group node.
- For example, both /md/Aruba_Sunnyvale and /md/Aruba_Sunnyvale/Building_1344 are group nodes.
- A config node inherits configuration from all the higher nodes in the hierarchy.
- You can always override configuration received from higher level config nodes. Configuration defined on the lower level config nodes will always take precedence over that defined on the higher level config nodes.
Device nodes:

- MDs can be parked at any configuration node (/md and below). The resulting config node is called a device node.
- MDs are typically parked under the lowest group node in the configuration hierarchy.
Commands to understand 8.x Hierarchy

show switches debug

(host) [mynode] #show switches debug

<table>
<thead>
<tr>
<th>Name</th>
<th>Nodepath</th>
<th>Type</th>
<th>Model</th>
<th>Version</th>
<th>Status</th>
<th>Uptime</th>
<th>CrashInfo</th>
<th>Config Sync</th>
<th>Sync State</th>
</tr>
</thead>
<tbody>
<tr>
<td>mynode</td>
<td>/mynode</td>
<td>Master</td>
<td>ArubaAK-38</td>
<td>8.2.0.0</td>
<td>Up</td>
<td>3d 22h</td>
<td>42s</td>
<td>no</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>VNIC_MyNode_MyNode</td>
<td>MD</td>
<td>ArubaAK-38</td>
<td>8.2.0.0</td>
<td>Up</td>
<td>3d 22h</td>
<td>42s</td>
<td>no</td>
<td>0</td>
</tr>
</tbody>
</table>

The command when executed on the MM(Active), shows all the standby MM and MDs associated to it across different hierarchy/Groups. The command is useful to check the uptime, mac address, IP address, Group, uptime of the different MDs. This is also a good place to check for any crash info on any of the MDs.

show configuration node-hierarchy

(host) [mynode] #show configuration node-hierarchy

The command is only supported on MM. The commands gives a brief of the different groups configured and MDs associated to the group. Please note the type which tells if it is system created (System), or manually configured (Group) or if it’s a device (Device).
show configuration effective

This command shows the effective configuration of devices connected to the node. Use the above command if you're on the MM and you want to see the config that would be pushed to an MD.
In AOS 8, a device node (controller) can get its configuration inherited from different levels of the node hierarchy. The configuration inherited from all different nodes of the node hierarchy comprises the running configuration or the effective configuration of the device.

A device may have multiple higher level nodes. The running configuration may not show from which node a specific configuration got inherited.

Use “Show config effective detail <Node_path>” command to check which configurations are inherited from various nodes.
crypto-local pki PublicCert master-ssh-pub-cert master-ssh-pub-cert
ip access-list eth validuserethacl
    permit any

asa tacacs-accounting

netservice svc-smb-udp udp 445
netservice vnc tcp 5900 5906
netservice svc-noe udp 32512 ALG noe
netservice svc-cfgm-tcp tcp 6211
netservice svc-netbios-nsn tcp 139
netservice svc-syslog udp 514
netservice svc-citrix tcp 2598
netservice svc-igp-tcp tcp 651
netservice svc-v6-icmp 58
netservice svc-12cp udp 1701
netservice svc-http-proxy tcp 3128
netservice svc-papi udp 8211
netservice svc-kerberos udp 88
netservice svc-smb-tcp tcp 445
netservice svc-vmware-rdp tcp 3389
netservice svc-v6-dhcp udp 546 547
netservice svc-sscpcp tcp 2000 ALG sccp
netservice svc-smtp tcp 25
netservice svc-pptp tcp 1723
netservice svc-ips-udp udp 631
netservice svc-web tcp list 80,443
netservice svc-netbios-ns udp 137
netservice svc-ike udp 500
netservice svc-facetime-tcp tcp 5223 ALG facetime
netservice svc-noe-oxo udp 5000 ALG noe
netservice svc-sip-udp udp 5060 ALG sip
netservice svc-microsoft-ds tcp 445
netservice svc-bootp udp 67 68
netservice svc-msrpc-tcp tcp 135 139
netservice svc-ssh tcp 22
netservice svc-dhcp udp 67 68
netservice svc-vdep udp 8200
Show running-config

```
(HTS-MM-VIRTUAL-01) [#yxn] # show running-config
Building Configuration...
version 8.5
service scp
hostname "HTS-MM-VIRTUAL-01"
clock timezone Asia/Kolkata +05 30
location "Building1 floor1"
controller config 100
user-local Mki PublicSert master-ssh-pub-cert master-ssh-pub-cert
ip NSP pool dynamic- cronat 0,0,0,0 0,0,0,0
ip access-list eth validusereth acl
   permit any
   ip access-list geolocation global-geolocation-acl
   netservice svc-smnp-trap udp 192
   netservice svc-netbios-dsrv udp 138
   netservice svc-pcpp-2-top tcp 172
   netservice svc-facetime tcp tcp 5223 alg facetime
   netservice svc-https tcp 443
   netservice svc-dhcp udp 67 68 alg dhcp
   netservice svc-tftp udp 69 alg tftp
   netservice svc-ica tcp 1494
   netservice svc-ips tkp 1723
   netservice svc-tpk tcp 1723
   netservice svc-telnet tcp 23
   netservice svc-tcp tcp 2000 alg tcp
   netservice svc-mortimer udp 8200
   netservice svc-tps tcp 69 alg tftp
   netservice svc-sip tcp 5060 alg sip
   netservice svc-l2tp tcp 515
   netservice svc-web tcp 80 443
   netservice svc-kerberos udp 88
   netservice svc-netbios-ssn tcp 139
   netservice svc-pcpp-udp udp 50002
   netservice svc-pcpp tcp 110
   netservice svc-pcpp-top tcp 50002
   netservice svc-http-proxy tcp 8080
   netservice svc-udp udp 8200
   netservice svc-rtp tcp 8211
   netservice svc-noe udp 35212 alg noe
   netservice svc-dns udp 53 alg dns
   netservice svc-rtp tcp 554 alg rtp
   More: (q) quit (u) pageup (?) search (n) repeat [l]
```

This command displays the current MM’s/MC’s configuration, including all the pending changes that are yet to be saved.

**How to navigate between MM and MD**

As discussed earlier, the MM is a single point of configuration. The administrator can navigate to different Groups and MDs from the MM itself. Following are few useful commands.

- **pwd**: The command when executed tells what location are you in the configuration hierarchy.
- **cd <node-path>**: The command is used to navigate between different locations in the configuration hierarchy.
- **mdconnect**: The command is used to login to the MD. This requires that you are already into the configuration hierarchy for the MD.
• **logon <MD-IP>**: The command is used to login to the MD via the IP address of the MD.

**Commands to capture system/device info**

**show version**

```
# show version
Aruba Operating System Software.
ArubaOS Image: ArubaOS-VA, Version 8.5.0.3
(c) Copyright 2019 Hewlett Packard Enterprise Development LP.
Compiled on 2019-10-01 at 00155127 UTC (Build 72499) by pbuild
B105 Version: Phoenix Technologies LTD, 6.00
Matrix 12/11/2018
Switch uptime is 10 days 10 minutes 33 seconds
Boot Cause: Power Cycle (Exception=64150)
Supervisor Card
Processor(s):
  Total CPUs: 6, Sockets: 1, Cores Per CPU: 6
  Socket 0: ND EPIC 7551 32-Core Processor
  711M bytes of memory
  4096M bytes of Supervisor Card system flash.
```

The command can be executed on the MM/MD and is useful to check the software version of the device, uptime of the device, the last reboot reason for the device and memory size.

**show inventory**

```
# show inventory
Supervisor Card 210:
  Serial #: 0L005325 (Date:01/09/19)
  CPU Card Serial#:
  210214H (Date:01/09/19)
  Interface Card Serial#:
  210029004 (Date:01/09/19)
  Interface Card Assembly#:
  21X008858
  Interface Card Revision:
  (Rev:04.0)
  SC Model#:
  Aruba7200XM
  MAC Addr:
  08:16:10:11:01:05 to 08:16:10:11:01:07
  CPLD Version:
  (Rev: 3.6)
  Power Supply 0
  Present: No
  Present: Yes
  LVOK: Yes
  Fan OK: Yes
  Aruba Model No: 2S10037
  Serial No:
  Q2814929088
  MFG Date: 12/15/18
```

The command can be executed on the MM/MD and is useful to check the hardware details of the device, including serial number, power supply status, fan status etc.
show switchinfo

```
[MM-VM-VIRTUAL-01] [mynode] $ show switchinfo

Hostname is MM-VM-VIRTUAL-01
Location not configured
System Time Thu Mar 5 17:52:20 IST 2020
Aruba Operating System Software.
ArubaOS (MODEL: ArubaOS-10.X), Version 8.5.0.3
Website: https://www.arubanetworks.com
Copyright 2019 Hewlett Packard Enterprise Development LP.
Compiled on 2019-10-01 at 08:59:27 UTC (Build 72498) by pbuild
BIOS Version: Phoenix Technologies LTD. 6.00
Build: 12/12/2010
Switch uptime is 10 days 10 minutes 48 seconds
Reboot Cause: Power Cycle (Intentcause: 86c50)
Supervisor Card
Processor(s):
Total CPU(s): 1, Sockets: 1, Cores Per CPU: 6
Socket 01 and HYPER 7951 3T-Core Processor
77136 bytes of memory
828M bytes of Supervisor Card system flash.
Config ID: 96
Boot Partition: PARTITION 0

system administratively down line protocol is down
Hardware is Ethernet, address is 00:0C:29:0E:1E:5A
VLAN is up (line protocol is up)
Hardware is Ethernet, Interface address is 00:0C:29:0E:1E:46 (via 00:0C:29:0E:1E:47)
Description: 802.1Q VLAN
IPV6 Router Advertisements are disabled
Routing Interface is enable. Broadcasting mode is enable
Directed broadcast is disabled, BDMC Optimisation disabled ProxyARP disabled Suppress ARP enable
Load distribution 002, loopback not set
MTU 1500 bytes
Last clearing of "show interface" counters 10 day 0 hr 18 min 48 sec
link status last changed 10 day 0 hr 18 min 48 sec
Proxy ARP is disabled for the Interface

switchport master
masterip 10.37.84.40
Configuration unchanged since last save
No AP crash information available.
No controller crash information available.
Reboot Cause Power Cycle (Intentcause: 86c50)
```

The command can be executed on the MM/MD and this provides useful information like the device role, master ip, mgmt details etc.

show ip interface brief

```
[MM-VM-VIRTUAL-01] [mynode] $ show ip interface brief

Interface IP Address / IP Netmask Admin Protocol VRRP-IP
vlan 84 10.17.84.27 / 255.255.255.0 up up 10.17.84.40
vlan 13 unassigned / unassigned up up
loopback unassigned / unassigned up up
ame unassigned / unassigned down down
```

The command can be executed on the MM/MD and is useful to check the ip address and the L3 interface details on the device.

show port status

```
[MM-VM-VIRTUAL-01] [mynode] $ show port status

Port Status

Slot-Port PortType AdminState OperState Poe Trusted SpanningTree PortMode Speed Duplex PortError
----------- ---------- ---------- -------- -------- ---------- ---------- --------- ------- ------------
0/0/0 GE      Enabled Up        N/A Yes       Disabled Access 10 Gbps Full -
0/0/1 GE      Disabled Down     N/A Yes       Disabled Access Auto Auto -
```

This command can be executed on the MM/MD and is useful to check the status of the physical ports on the individual device.
Show controller-ip

```
(HTS-MM-VIRTUAL-01) [mynode] #show controller-ip
Switch IP Address: 10.17.84.27
Switch IP is configured to be Vlan Interface: 84
Switch IPv6 address is not configured.
(HTS-MM-VIRTUAL-01) [mynode] #
```

The command can be executed on the MM/MD and is useful to check the controller-ip configured. The controller-ip is used for the control plane functions.

2.1 Clustering

The Aruba 8.x Architecture brings in the clustering feature which provides resiliency and load sharing features. A cluster is a combination of multiple managed devices working together to provide:

- **Seamless Campus Roaming:** Clients stay anchored to a single MC when roaming across controllers.
- **Stateful Client Failover:** User traffic uninterrupted upon cluster member failure.
- **AP and Client Load Balancing:** APs and Users automatically load balanced across cluster members.
- **Live Upgrade:** Live in service Upgrade of Cluster Nodes and APs.

**Cluster Roles**

Two Managed Devices (MD) Roles:

- AP Anchor Controller (AAC)
- User Anchor Controller (UAC)

**Redundancy**

- Standby AAC (S-AAC)
- Standby UAC (S-UAC).

**AP Anchor Controller (AAC):** AP sets up Active Tunnels with its Local clients.

**Standby AAC (S-AAC):** S-AAC is dynamically assigned from other cluster members. AP sets up Standby Tunnels with S-AAC.
AAC Failover:

1. AAC fails and Failure detected by S-AAC.
2. S-AAC instructs AP to fail over and AP tears its Active tunnel with failed AAC.
3. Standby tunnel with S-AAC becomes Active.
4. New S-AAC is assigned by Cluster Leader.
Before we jump into User Anchor Controller (UAC), let’s see how a user remains anchored to a single controller (UAC).

1. User is mapped to its UAC via a hashing algorithm at AP level.
2. Hashing → Index to Mapping Table.
3. Same Mapping is pushed to all APs by Cluster Leader.
4. Cluster Leader selects Standby UAC (S-UAC) on per User basis.

5. AP creates dynamic tunnel to client UAC.
6. When client roams, old AP tears down dynamic tunnel.
7. User traffic is always tunneled to its UAC.
UAC and SUAC on Mobility Master Dashboard.

Below commands from MM show how to find the UAC of a user.

show aaa cluster essid <essid value> users

Example: show aaa cluster essid TEST users

Active Users for ESSID : TEST

<table>
<thead>
<tr>
<th>BUCKET</th>
<th>MAC</th>
<th>IP</th>
<th>ActiveUAC</th>
<th>StandbyUAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>178</td>
<td>5a:10:5e:5a:21:c9</td>
<td>10.0.0.9</td>
<td>10.1.2.36</td>
<td>10.1.2.3</td>
</tr>
</tbody>
</table>

→ we can also find this using this shortcut

cluster-debug calc-sta-uac <station-MAC address> <Essid name>

Example: cluster-debug calc-sta-uac 5a:10:5e:5a:21:c9 TEST

STA Index:178
STA A-UAC:10.1.2.36
STA S-UAC:10.1.2.35

3. PROCESSES

TAC supports the customer network, administrators to troubleshoot/fix issues in the network, however it reduces the time to isolate and fix the issue if network administrator can share the following information while opening the TAC cases.

It helps a great deal if the issue could be described effectively. The problem description should contain a concise statement of the symptoms like

- What does not work?
- Where does it not work?
- When does it not work?
- How does it not work?
Isolate the symptoms.

- When was the symptom first reported?
- What environment components changed?
- How often do the symptoms occur?
- Are symptoms reproducible?
- What is the impact of the issue?

Please share the network details to the TAC. If possible, share the network topology diagram.

3.1 Data collection for TAC

Capture the logs and tar log tech support and share it to the TAC engineer.

CLI Command:

tar logs tech-support

copy flash: logs.tar scp:<scp server IP address> <username> <file name>

(tftp, ftp are also possible).

This command is available on both MM and MD. On running the “tar log tech-support” command, the device will generate “logs.tar” file in the flash which needs to be exported from the flash of the device.

From Web UI:

1) Log on to the Web UI of the controller(s).

2) Navigation: Select MM >> click Diagnostics >> click Technical support >> click Copy Logs >> click Download logs button >> "Include technical support information" should be checked>> click Apply button.
3) Save this log to your system.

4) Upload the file to the support site.

Collect the following log output during the problem (if Syslog server output can’t be collected).

- show log errorlog all
- show log network all | include '<wireless device's mac address>'
- show log security all | include '<wireless device's mac address>'
- show log system all
- show log user-debug all | include '<wireless device's mac address>'
- show log user all | include '<wireless device's mac address>'
- show log wireless all.

3.2 Authentication related issues

Authentication related issues are one of the most common issues. The network administrator can capture the following information before opening a TAC case to better isolate the issue.

- Validate time setting on client, Aruba Controller and Authentication Server.
- Check for the logs/event logs on the Authentication Server.
- Validate if the issue is specific to a client or to all clients?
- For Windows, if possible, capture the Microsoft tracing “netsh ras set tracing * enable” to debug on the client side. (To make Point-to-Point Protocol (PPP) tracing available, type “netsh ras set tracing ppp enable” and then press ENTER).
Capture the "show auth-tracebuf" command on the Aruba device.

Link for Reference:

“show auth-tracebuf” needs to be collected from the respective controller.

3.3 Client Connectivity issues

Client connectivity is one of the other most common issues seen and there could be multiple reasons for the cause; like RF, Client Driver issues, Client Certificate issues etc. Troubleshooting client connectivity issues could be difficult and please check the following from the user when a client reports an issue.

- Wifi or Wired user
- User is getting disconnected from Wifi (no wifi connected signal)
- Users stay associated but unable to pass traffic.
- Frequent disconnection (Wifi or user traffic).
- Unable to authenticate /Associate to the AP.
- Unable to get IP address.
- Performance issues (low speed, packet loss etc.)
- Disconnect while roaming between access points.
- Single user or multiple user complaints.

We need to identify the type of users

- Smartphones (iPhone, IPAD, Android phones)
- Windows OS or Mac laptops
- Other Application devices
- OS/NIC card model and WLAN driver version

If the user is unable to see the SSID, check if

- this is the only SSID which doesn’t show up?
- the user can see other SSIDs?
- the problem is seen at a single location? If yes, get more details (like channel, power, location) from working and non-working APs.

If the user complains about weak signal, check if

- the problem is with a single SSID or with multiple SSIDs.
- the problem is seen at a single location or at multiple locations.
- the RF settings are as per recommendations.
- the problem is with any specific band (2.4GHz, 5GHz).
- the problem is with specific type of clients.

Also, check the strength of the association (SNR). You can obtain the SNR using "show ap association client-mac <mac>" on MC.
For user-debugging:

User debugging has to be done at the group level on the MM.

logging user-debug <aa:bb:cc:dd:ee:ff> level debugging – can be used at a Group level specifying the mac address of the user.

• If possible, take the Over The Air (OTA) captures and the Datapath captures at the time of the issue. OTA captures are mostly applicable to RF related issues.

Links for Reference

For OTA: https://docs.microsoft.com/en-us/windows/client-management/troubleshoot-tcpip-netmon

For Datapath Capture: https://www.youtube.com/watch?v=dIyl2EGXHVQ

3.4 AP failing to come up on WLC

Many times network administrators come across issues with APs failing to come up on controller”. Please check for the following for such issues.

• Check if AP is getting power (AC/PoE) ?
• Validate if AP has got a valid IP address and gateway?
• Validate how the Controller discovery is happening? Static, DHCP, DNS?
• Validate if the AP is able to learn/discover the controller IP?
• Validate if there is IP reachability between the AP/AP subnet and the Controller?
• If there is any firewall between AP and Controller, validate there are no drops.
• If it’s a new AP validate if the AP is supported model on Controller. Validate the software compatibility between the AP and controller software version.
• Check if the AP is seen in the AP database table.
show ap database

Please take a note of the Flags as the AP could be in the database table but not in the “show ap active” table due to other reasons.

- Check if you have AP license.
- Check for the datapath session table on the controller from the AP IP.
- Check for GRE and PAPI traffic.

For GRE and PAPI Traffic, datapath session table on the controller from the AP IP can be checked this way.

```
show ap database

Flags: F = fast age, S = src NAT, N = dest NAT
D = deny, R = redirect, Y = no syn
H = high prio, P = set prio, T = set ToS
C = client, M = mirror, V = VOIP
Q = Real-Time Quality analysis
U = Upstream Real-Time Quality analysis
I = Deep inspect, U = Locally destined
E = Media Deep Inspect, G = media signal
p = Route Nexthop, h = High Value
A = Application Firewall Inspect
D = Permanent, O = Openflow
L = Log, o = Openflow config revision mismatched
```

```
Datapath Session Table Entries

Flags: F = fast age, S = src NAT, N = dest NAT
D = deny, R = redirect, Y = no syn
H = high prio, P = set prio, T = set ToS
C = client, M = mirror, V = VOIP
Q = Real-Time Quality analysis
U = Upstream Real-Time Quality analysis
I = Deep inspect, U = Locally destined
E = Media Deep Inspect, G = media signal
p = Route Nexthop, h = High Value
A = Application Firewall Inspect
D = Permanent, O = Openflow
L = Log, o = Openflow config revision mismatched

| Source IP or MAC | Destination IP | Protocol | Sport | DPort | Contra | Flags | CPU ID | Prio | ToS | Age |Destina
|------------------|----------------|----------|-------|-------|--------|-------|-------|------|-----|-----|--------
| 10.17.84.16      | 10.17.86.60    |          |       |       |        | 17    | 4500  | 4500 | 0/0 | 0   | 1      | 0/0/0 |
|                  | 10.17.88.60    |          |       |       |        | 17    | 8008  | 8419 | 0/0 | 0   | 0      | tunnel |
| 11.10            | 10.17.84.16    |          |       |       | FYCI   | 47    | 0     | 0    | 0/0 | 0   | 0      | 0/0/0 |
| 583              | 582204         |          |       | 58027084 | FC    | 24    | 10.17.86.60 | 0     | 0    | 0/0 | 0/0/0 |
| 583              | 572580         |          |       | 57180172 | F     | 24    | 10.17.84.16 | 4    | 0    | 0   | 0/0/0 |

PAPI (UDP port 8211); GRE (protocol 47).
```
show datapath session table

The command is useful to capture the communication between the AP and the Controller.

The queried IP here has to be the AP’s IP.

**3.5 AP Crash/reboot issues**

This would cover AP crashes, AP reboots, error messages related to specific AP. Basically for these issues, we need controller logs and AP techsupport file.

For Controller logs, please refer to this link:

AP tech support:
Log the securecrt/putty session and issue the below command:
show ap tech-support ap-name <name of the AP>

**3.6 High CPU/Memory Utilization on the Controller**

**High CPU Utilization on the controller**
As network usage increases with growing users and device population, so do the demands on the controller resources. When the controller’s capacity is exceeded, the CPU utilization spikes up.
Few symptoms of High CPU: Sluggish Web UI, SNMP timeouts, missing data in Airwave graphs.

We need logs.tar when the issue happens.
• Controller tech support log file.  

• When the issue occurs, Please execute below set of show commands at least 5 times with an interval of 5 seconds at each execution

  no paging  
clock cli-timestamp  
show cpuload  
show cpuload current  
show processes sort-by cpu  
show datapath utilization  
show datapath message-queue  
show ap debug counters  
show datapath session  
show log system 20 | include Resource  
show datapath utilization  
show datapath frame all  
show datapath frame  
show datapath frame counters  
show datapath message-queue counters  
show datapath session counters  
show datapath session ipv6 counters  
show datapath session  
show datapath session table  
show datapath session ipv6

NOTE: Above commands in gap of 5 seconds, 10 times.

High Memory Utilization on the Controller

Utilization might be high as a result of some user processes taking up too much memory or a high number of running processes (due to the number of features enabled).

Outputs for below commands would be required.
no paging  
clock cli-timestamp
show memory
show processes sort-by memory
show memory debug
show clock
show memory <process_name>
show storage
show boot

NOTE: Above commands in gap of 5 seconds 10 times

tar crash
tar logs tech-support
tar flash

NOTE: For automated script use below Knowledge Base.

3.7 Mobility Master crash issues

A crash is a situation where the system has detected an unrecoverable error and has restarted itself. The errors that cause crashes are typically detected by processor hardware, which automatically branches to special error handling code.

You can check if the system had a crash from the crash info part of “show switches debug” output. You can see a “yes” if the system had crashed.

Mobility Master crash

- MM CLI prompt shows an asterisk (*) sign constantly.
- (MM) *[mynode] #

Mobility Master tech support log file

How to collect Crash file from MM:

How to collect MM Log with TechSupport file from MM: (applicable for Crash.log)
https://community.arubanetworks.com/t5/Controller-Based-WLANs/How-to-collect-tech-support-logs-from-the-8-x-controller/ta-p/518953
3.8 Controller Crash issues

Check for “show switches debug” output from the controller. Also, run the CLI Command "show switchinfo" to find the cause of the reboot.

```
[SW1-MAN-VIRTUAL-01] (Root) #show switchinfo
Hostname is SW1-MAN-VIRTUAL-01
Location not configured
System Time: Tue Jan 20 10:29:25 IST 2020
Aruba Operating System Software.
ArubaOS (Model: Aruba-MAN), Version 8.5.0.3
Website: http://www.arubanetworks.com
(c) Copyright 2019 Hewlett Packard Enterprise Development LP.
Compiled on 2019-10-01 at 02:59:27 UTC (build 72496) by p4build
BIOS Version: Phoenix Technologies LTD, 6.00
Built: 12/12/2018
Switch uptime is 22 days 3 hours 22 minutes 53 seconds
Reboot Cause: Power Cycle (Intentcauses: 86:59)
Supervisor Card Processor(s):
  Total CPUs: 6, Sockets: 1, Cores Per CPU: 6
  Socket 0: AMD EPYC 7531 2x-Core Processor
  77159 bytes of memory
  4058M bytes of Supervisor Card system flash.
Config ID: 112
Boot Partition: PARTITION 0
agent is administratively down line protocol is down
Hardware is Ethernet, address is 00:0c:29:38:eb:50
LUN 0 is up line protocol is down
Hardware is CPU Interface, Interface address is 00:0c:29:18:eb:67 (bia 00:0c:29:18:eb:67)
Description: BIG-10 VLAN
IPv6 Router Advertisements are disabled
Routing Interface is enabled, Forwarding mode is enabled
Directed broadcast is disabled, BRIC Optimization disabled ProxyARP disabled Suppress ARP enable
Encapsulation 802.1q, loopback not set
MTU 1500 bytes
Last clearing of "show interface" counters 22 day 3 hr 22 min 53 sec
Link status last changed 22 day 3 hr 22 min 53 sec
Proxy Arp is disabled for the Interface
switchrole: master
master/ip10.17.24.40
Configuration Changed since last save
No AP crash information available,
no controller crash information available.
Reboot Cause: Power Cycle (Intentcauses: 86:59)
```

For any controller crash issues, we need

- Controller tech support log file.

**How to collect tech support log file:**

- crash.tar.

**How to collect Crash file from controller:**
https://community.arubanetworks.com/t5/Controller-Based-WLANs/My-controller-just-rebooted-what-should-I-do/ta-p/202893
3.9 Controller – MM Related Issues

Sometimes, the communication between MM and the Managed Device might go down. To troubleshoot further, for any controller and MM communication related issues, we need:

- Controller tech support log file.
- MM Tech support log file (See link under MM Related Issue)

3.10 Packet Capture on Aruba Controller

The Aruba Mobility controller allows you to capture packets for control-path and datapath. For client related troubleshooting in some scenarios it might be required to capture the client packets on the Aruba controller. The following command helps us to capture the client traffic on the Aruba controller. Before initiating the packet capture, identify the Active Anchor controller for the client (Use :cluster-debug calc-sta-uac <station-MAC address> <Essid name> mentioned in 3.2) for which you want to capture the packets.

The command “packet-capture datapath <mac-address> all | decrypted | encrypted” will enable the packet captures.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Capture both decrypted and encrypted packets</td>
</tr>
<tr>
<td>decrypted</td>
<td>Capture decrypted packets only</td>
</tr>
<tr>
<td>encrypted</td>
<td>Capture encrypted packets only</td>
</tr>
</tbody>
</table>

A destination needs to be set for this capture.

(Aruba7240XM_05_95_C0) [mynode] #packet-capture destination

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Send captured packets to an interface</td>
</tr>
<tr>
<td>ip-address</td>
<td>Send captured packets to a remote destination</td>
</tr>
<tr>
<td>local-filesystem</td>
<td>Store captured packets on the controller in pcap files</td>
</tr>
</tbody>
</table>

(Aruba7240XM_05_95_C0) [mynode] #packet-capture destination interface?

<slot/port> Interface in <slot>/<port> format
(Aruba7240XM_05_95_C0) [mynode] #packet-capture destination ip-address ?
<ipaddr> A.B.C.D IP address

(IP address of the host must be able to receive GRE traffic from the controller’s management IP and the host must be running a packet capture software such as Wireshark).

(Aruba7240XM_05_95_C0) [mynode] #packet-capture destination local-filesystem ?
<cr>

When we use Local file system, capture will be saved in the logs.tar of the controller.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#packet-capture datapath</td>
<td>Capture all packets.</td>
</tr>
<tr>
<td>ipsec</td>
<td>Capture all packets in ipsec mode.</td>
</tr>
<tr>
<td>mac</td>
<td>Capture packets of user by MAC address.</td>
</tr>
<tr>
<td>&lt;mac-address&gt; mac</td>
<td>MAC address of the user.</td>
</tr>
<tr>
<td>#packet-capture destination</td>
<td>Send captured packets to an interface.</td>
</tr>
<tr>
<td>interface &lt;ip-address&gt;</td>
<td>Send captured packets to a remote destination.</td>
</tr>
<tr>
<td>local-filesystem</td>
<td>Store captured packets on the controller.</td>
</tr>
<tr>
<td>#packet-capture destination</td>
<td>Capture packets to a local filesystem.</td>
</tr>
<tr>
<td>interface &lt;ip-address&gt;</td>
<td>Capture packets to a local filesystem.</td>
</tr>
</tbody>
</table>

Also, “packet-capture copy-to-flash datapath-pcap” can be used to copy the packet capture to the flash.

scp/ftp the file out from the flash.

Here is the example.

→ 10.17.84.17 is the MD I logged into, used the client MAC : 20:4c:03:62:aa:d3 for captures (can get the user list from "show user").
→ Show packet-capture datapath-pcap will give you the captures.

→ These captures can be copied to the flash using “packet-capture copy-to-flash datapath-pcap”. You’ll have a file with “datapath-pcap.tar.gz” in the flash.

Give a destination filename and use SCP to get the complete file.

3.12 Hardware Related Issues
Have the below details before opening up a TAC Case.
Details noticed about hardware and troubleshooting performed:
a. What is the LED status?
b. Does the device boot up?
c. What is the power source?
d. If device boots up, collect the console output.
e. Was the device working or is it a dead on arrival?
f. Was there any power fluctuation in the network?

Also, share below details for processing RMA:

- Shipping Address with Zip code
- Contact Person Name
- Contact Number
- Email Address
- Serial Number

### 3.13 AirWave (AMP) Related Issues

Open a support ticket and provide the following

a. If the NOC team member is opening a case on behalf of another, please provide the original Point of Contact just in case we need further clarification.
b. Detailed problem description.
c. Date and time of the reported issue.
d. Screenshot showing the issue.
e. AMP name and serial number
f. If it’s not a VisualRF issue grab the system diagnostic if possible
g. If it’s VisualRF related issue, grab the VisualRF diagnostic if possible.

Make sure that the NOC team member is able to get on a remote session as soon as possible.
4. SOME USEFUL COMMANDS

4.1 Global user table on MM

On MM, the “show global-user list” command shows the list of clients connected to all the MDs connected.

It’s always good to login to the MDs under the MM and run a “show user-table” command.

From MM, login to individual MDs and run the “show user-table” command.

It could be more efficient to just open 2 SSH sessions (one to each cluster member/tower) based on the topology/design.

On MM, when you enter “show user-table”, you are prompted with “This command is not applicable on master-switch”.

(HTS-MM-VIRTUAL-01) [mynode] #show user-table
This command is not applicable on master switch...

(HTS-MM-VIRTUAL-01) [mynode] #
4.2 AP related commands

**show ap tech-support ap-name <>**

**Usage:** show ap tech-support ap-name <ap-name> [<filename>]

This command is introduced in ArubaOS 8.0.0.0 and displays all information for an AP or save that information to a file on the controller. This information can be used by Aruba technical support to diagnose a problem with an AP.

- `<ap-name>`: Name of the AP for which you want to view tech support data.
- `<filename>`: Save the output of this command to a file on the controller with the specified filename.

**show ap debug system-status**

**Usage:** show ap debug system-status

- `ap-name <ap-name>`
- `bssid <bssid>`
- `ip-addr <ip-addr>`
- `ip6-addr <ip6-addr>`

This command is introduced in ArubaOS 8.0.0.0, shows detailed system status information for an AP.

- `ap-name <ap-name>`: Show system status data for an AP with a specific name.
- `bssid <bssid>`: Show system status data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP’s MAC address.
- `ip-addr <ip-addr>`: Show system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
- `ip6-addr <ip6-addr>`: Show system status data for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

For more information on this command, please refer to

https://www.arubanetworks.com/techdocs/ArubaOS_83_Web_HELP/Content/ArubaFrameStyles/1CommandList/show_ap_debug_system_sta.htm?Highlight=show%20ap%20debug%20system%20status%20ap-name

**show ap cluster-tech-support ap-name <>**

**Usage:** show ap cluster-tech-support {ap-name <ap-name>} [<filename>]

This command is introduced in ArubaOS 8.0.0.0 and shows the cluster information of an AP.
ap-name <ap-name> - Shows cluster information of an AP for specified AP name.

<filename> - Stores output in specified filename.

**Show ap ?**
Generic search to show AP commands available.