# ArubaOS 6.1.3

ARUBA networks

Release Notes

## Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

## Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

## Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

# Contents

# Chapter 1

# Release Overview

ArubaOS 6.1.3 is a software maintenance release that introduces fixes to many previously outstanding issues. For details on all of the features described in the following sections, see the *ArubaOS 6.1 User Guide*, *ArubaOS 6.1 CLI Reference Guide*, and *ArubaOS 6.1 MIB Reference Guide*.

NOTE

See the "Upgrade Procedures" on page 49 for instructions on how to upgrade your controller to this release.

CAUTION

Authentication module restarts when ESI  parser is configured.
**Workaround:**
Remove all ESI parser related configurations, before controller is upgraded to 6.1.3.0.

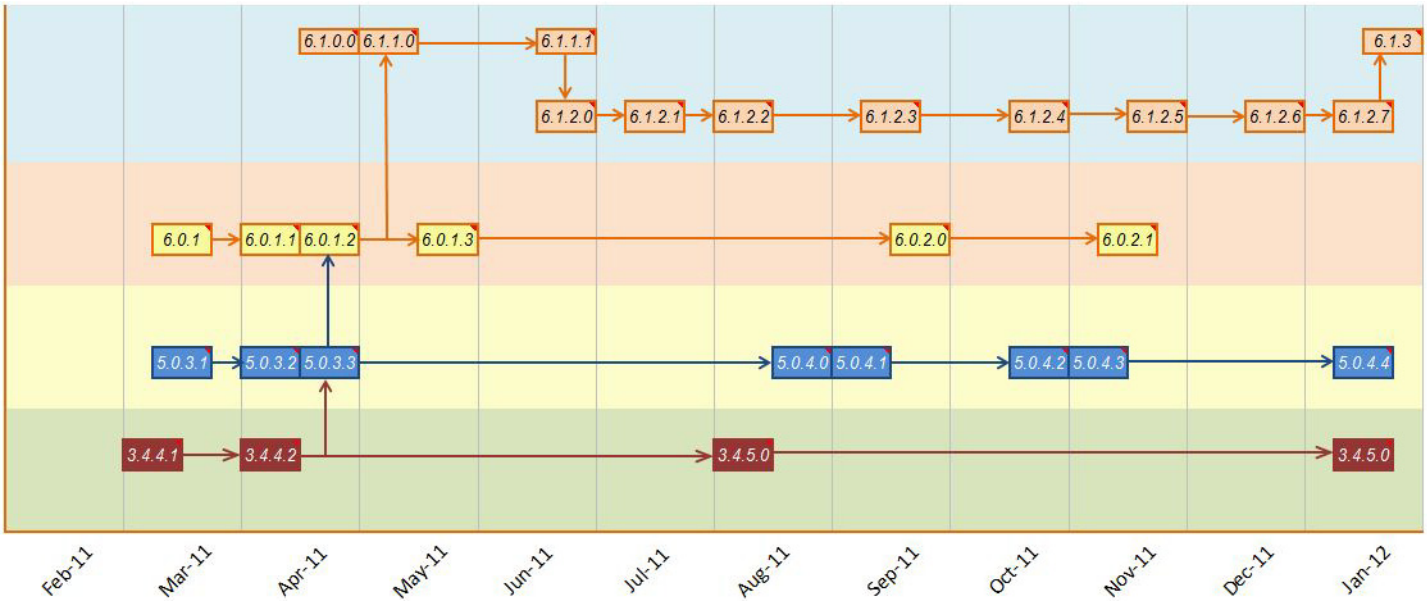
## Release Note Overview

- Chapter 2, "Features" on page 11 provides information on features added in previous releases of ArubaOS 6.1.x.
- Chapter 3, "Fixed Issues" on page 21 describes the issues that have been fixed in this release.
- Chapter 4, "Known Issues and Limitations" on page 31 provides descriptions and workarounds for outstanding issues in ArubaOS 6.0.
- Chapter 5, "Upgrade Procedures" on page 49 cover the procedures for upgrading your controller from any release of ArubaOS to ArubaOS 6.0.

## Release Mapping

The following illustration shows which patches and maintenance releases are included in their entirety in ArubaOS 6.1.3.

**Figure 1** *ArubaOS Releases and Code Stream Integration*




## Supported Browsers

Beginning with ArubaOS 6.0, the following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 8.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Mozilla Firefox 3.x on Windows XP, Windows Vista, Windows 7, and MacOS
- Apple Safari 5.x on MacOS

# Contacting Support

**Table 1** *Web Sites and Emails*

| Web Site | |
|---|---|
| • Main Site | http://www.arubanetworks.com |
| • Support Site | https://support.arubanetworks.com |
| • Software Licensing Site | https://licensing.arubanetworks.com/login.php |
| • Wireless Security Incident Response Team (WSIRT) | http://www.arubanetworks.com/support/wsirt.php |
| **Support Emails** | |
| Americas and APAC | support@arubanetworks.com |
| EMEA | emea_support@arubanetworks.com |
| WSIRT Email<br>Please email details of any security problem found in an Aruba product. | wsirt@arubanetworks.com |

**Table 2** *Contact Phone Numbers*

| Telephone Numbers | |
|---|---|
| • Aruba Corporate | +1 (408) 227-4500 |
| • FAX | +1 (408) 227-4550 |
| **Support** | |
| United States | 800-WI-FI-LAN (800-943-4526) |
| Universal Free Phone Service Number (UIFN): Australia, Canada, China, France, Germany, Hong Kong, Ireland, Israel, Japan, Korea, Singapore, South Africa, Taiwan, and the UK | +800-4WIFI-LAN (+800-49434-526) |
| All other countries | +1 (408) 754-1200 |

# Chapter 2

# Features

This chapter provides a brief summary of the features added in ArubaOS 6.1.3.

## AP-93H

ArubaOS 6.1.3 adds support for the AP-93H wireless access point. The Aruba AP-93H wireless access point provides the same performance as the AP-90 series. However, AP-93H is equipped with additional Ethernet ports and is designed to be mounted on an electrical gang box.

## AP-104

ArubaOS 6.1.3 adds support for the AP-104 wireless access point. The Aruba AP-104 wireless access point provides the same functionality as the AP-105 but is equipped with connectors for external antennas.

## IPv6 Router Advertisements

This release of ArubaOS enables the controllers to send router advertisements (RA) in an IPv6 network. When a host connects to an IPv6 network, it configures itself with a link local address. The link local address allows the host to communicate between the nodes attached to the same link.

The IPv6 stateless autoconfiguration mechanism allows the host to generate its own addresses using a combination of locally available information and information advertised by the routers. The host sends a router solicitation multicast request for its configuration parameters in the IPv6 network. The source address of the Router Solicitation request can be an IP address assigned to the sending interface, or an unspecified address if no address is assigned to the sending interface.

The routers in the network respond with periodic unsolicited RA packets. The RA contains the network part of the Layer 3 IPv6 address (IPv6 Prefix). The host uses the IPv6 prefix provided by the RA; generates the universally unique host part of the address (interface identifier), and combines the two to derive the complete address. To establish continuous connectivity to the default router, the host starts the neighbor reachability state machine for the router.

NOTE

ArubaOS uses Radvd, an open source Linux IPv6 Router Advertisement daemon maintained by Litech Systems Design.

You can perform the following tasks on the controller to enable, configure, and view the IPv6 RA status on a VLAN interface:

- Configure IPv6 RA on a VLAN
- Configure Optional Parameters for RA
  - Configure neighbor discovery reachable time
  - Configure neighbor discovery retransmit time
  - Configure RA DNS
  - Configure RA hop-limit
  - Configure RA interval

- Configure RA lifetime
- Configure RA managed configuration flag
- Configure RA MTU
- Configure RA other configuration flag
- Configure RA Preference
- Configure RA prefix
- View IPv6 RA Status

NOTE

You must enable the global IPv6 option on the controller before configuring IPv6 RA on a VLAN.

## Configuring IPv6 RA on a VLAN

You must configure the IPv6 RA functionality on a VLAN for it to send solicited/unsolicited router advertisements on the IPv6 network. You must do the following configurations for IPv6 RA to work on a VLAN:

- Configure IPv6 global unicast address
- Enable IPv6 RA
- Configure IPv6 RA prefix

NOTE

- The advertised IPv6 prefix length must be 64 bits for the stateless address autoconfiguration to work properly.
- You can configure up to three IPv6 prefixes per VLAN interface.
- Each IPv6 prefix must have an on-link interface address configured on the VLAN.

You can use the WebUI or CLI to configure IPv6 RA on a VLAN.

### Using WebUI

1. Navigate to the **Configuration > Network > IP** page and select the **IP Interfaces** tab.
2. Edit a VLAN # and select **IP version** as *IPv6*.
3. To configure an IPv6 global unicast address, follow the steps below:
   a. Under **Details**, enter the IPv6 address and the prefix-length in the **IP Address/Prefix-length** field.
   b. (Optional) Select the **EUI64 Format** check box, if applicable.
   c. Click **Add** to add the address to the global address list.
4. To enable IPv6 RA on a VLAN, select the **Enable Router Advertisements (RA)** check box under **Neighbour Discovery**.
5. To configure IPv6 RA prefix for a VLAN, follow the steps below:
   a. Under **Neighbour Discovery**, enter an IPv6 prefix in the **IPv6 RA Prefix** field.
   b. Click **Add** to configure an IPv6 prefix for the VLAN.

   You can add up to three IPv6 prefixes per VLAN interface.
6. Click **Apply** to apply the configurations.

### Using CLI

Execute the following commands to configure router advertisements on a VLAN:

```
(host) (config) #interface vlan <vlanid>
(host) (config-subif)#ipv6 address <prefix>/<prefix-length>
```

```
(host) (config-subif)#ipv6 nd ra enable
(host) (config-subif)#ipv6 nd ra prefix X:X:X:X::X/64
```

## Configuring Optional Parameters for RA

In addition to enabling the RA functionality, you can configure the following IPv6 neighbor discovery and RA options on a VLAN:

- Neighbor discovery reachable time: The time, in milliseconds, that a node assumes a neighbor is reachable after receiving a reachability confirmation.
- Neighbor discovery retransmit time: The time, in milliseconds, between retransmitted Neighbor Solicitation messages.
- RA DNS: The IPv6 recursive DNS Server for the VLAN.

NOTE

- On Linux systems, the clients must run the open rdnssd daemon to support the DNS server option.
- Windows 7 does not support DNS server option.

- RA hop-limit: The IPv6 RA hop-limit value. It is the default value to be placed in the Hop Count field of the IP header for outgoing (unicast) IP packets.
- RA interval: The maximum and minimum time interval between sending unsolicited multicast router advertisements from the interface, in seconds.
- RA lifetime: The lifetime associated with the default router in seconds. A value of 0 indicates that the router is not a default router and will not appear on the default router list. The router lifetime applies only to the router's usefulness as a default router; it does not apply to information contained in other message fields or options.
- RA managed configuration flag (Enable DHCP for address): A flag that indicates that the hosts can use the DHCP server for address autoconfiguration besides using RAs.
- RA maximum transmission unit (MTU): The maximum transmission unit that all the nodes on a link use.
- RA other configuration flag (Enable DHCP for other information): A flag that indicates that the hosts can use the administered (stateful) protocol for autoconfiguration of other (non-address) information.
- RA preference: The preference associated with the default router.

You can use the WebUI or CLI to configure these options.

NOTE

It is always recommended to retain the default value of the RA interval to achieve better performance.

CAUTION

If you enable RAs on more than 100 VLAN interfaces, some of the interfaces may not send out the RAs at regular intervals.

### Using the WebUI

1. Navigate to the **Configuration>Network>IP** page.
2. Select the **IP Interfaces** tab.
3. Edit the VLAN on which you want to configure the neighbor discovery or RA options.
4. Select **IP Version** as *IPv6*.
5. Under **Neighbour Discovery**, configure the following neighbor discovery and RA options for the VLAN based on your requirements.

a. Enter a value in the **Reachable Time** field. The allowed range is 0 - 3,600,000 msec. The default value is 0.

b. Enter a value in the **Retransmit Time** field. TThe allowed range is 0 - 3,600,000 msec.he default value is 0.

c. Enter a DNS server name in the **IPv6 Recursive DNS Server** field.

d. Enter a hop-limit value in the **RA hop-limit** field. The allowed range is 1 to 255. The default value is 64.

e. Enter the maximum interval value in the **RA Interval(sec)** field. Allowed range is 4 to1800 seconds. Default value is 600 seconds.

f. Enter a value in the **RA Minimum Interval(sec)** field. Allowed range is 3 to 0.75 times the maximum RA interval value in seconds. The default minimum value is 0.33 times the maximum RA interval value

g. .Enter a value in the **RA Lifetime** field. A value of 0 indicates that the router is not a default router. Apart from a zero value, the allowed range for the lifetime value is RA interval time to 9000 seconds. The default and minimum value is 3 times the RA interval time.

h. Select the **DHCP for address** check box to enable the hosts to use the DHCP server for address autoconfiguration apart from any addresses auto-configured using RA.

i. Enter a value in the **RA MTU Option** option. The allowed range is 1280 to maximum MTU allowed for the link.

j. Select the **DHCP for Other Address** check box to enable the hosts to use the DHCP server for autoconfiguration of other (non-address) information.

k. Select the router preference as **High**, **Medium**, or **Low**.

6. Click **Apply** to apply the configurations.

### Using the CLI

Execute the following CLI commands to configure the neighbor discovery and RA options for a VLAN interface:

To configure neighbor discovery reachable time:

```
(host) (config) #interface vlan <vlan-id>
(host) (config-subif)#ipv6 nd reachable-time <value>
```

To configure neighbor discovery retransmit time:

```
(host) (config-subif)#ipv6 nd retransmit-time <value>
```

To configure IPv6 recursive DNS server:

```
(host) (config-subif)#ipv6 nd ra dns X:X:X:X::X
```

To configure RA hop-limit:

```
(host) (config-subif)#ipv6 nd ra hop-limit <value>
```

To configure RA interval:

```
(host) (config-subif)#ipv6 nd ra interval <value> <min-value>
```

To configure RA lifetime:

```
(host) (config-subif)#ipv6 nd ra life-time <value>
```

To enable hosts to use DHCP server for stateful address autoconfiguration:

```
(host) (config-subif)#ipv6 nd ra managed-config-flag
```

To configure maximum transmission unit for RA:

```
(host) (config-subif)#ipv6 nd ra mtu <value>
```

To enable hosts to use DHCP server for other non-address stateful autoconfiguration:

```
(host) (config-subif)#ipv6 nd ra other-config-flag
```

To specify a router preference:

```
(host) (config-subif)#ipv6 nd ra preference [High | Low | Medium]
```

### Viewing IPv6 RA Status

You can execute the following command to view the IPv6 RA status on the VLAN interfaces:

```
(host) #show ipv6 ra status
IPv6 RA Status
--------------
VlanId  State    Prefix(es)
------  -----    ----------
1       enabled  2001:abcd:1234:dead::/64
220     enabled  2200:eab:feed:12::/64
230     enabled  2300:eab:feed::/64
7       enabled  2001:470:faca:2::/64
                 2001:470:faca:3::/64
                 2001:470:faca:4::/64
```

## RADIUS Accounting for Split-Tunnel Remote AP Clients

Remote APs in split-tunnel mode now support RADIUS accounting. If you enable RADIUS accounting in a split-tunnel Remote AP's AAA profile, the controller sends a RADIUS accounting start record to the RADIUS server when a user associates with the remote AP, and sends a stop record when the user logs out or is deleted from the user database. If interim accounting is enabled, the controller sends updates at regular intervals. Each interim record includes cumulative user statistics, including received bytes and packets counters.

Use the following procedures to configure RADIUS accounting for a split-tunnel Remote AP.

### Using the WebUI

1. Navigate to the **Security > Authentication > AAA Profiles** page.
2. Select the split-tunnel AP's AAA profile to display the list of authentication and accounting profiles associated with that AAA profile.
3. Select the **Radius Accounting Server Group** profile associated with the AAA profile.
4. Click the **RADIUS Accounting Server Group** drop-down list and select a RADIUS server group.
5. (Optional) To also enable RADIUS Interim Accounting, select the AAA profile from the profile list, then click the **RADIUS Interim Accounting** checkbox. This option is disabled by default, allowing the controller to send only *start* and *stop* messages RADIUS accounting server.
6. Click Apply to save your settings.

### Using the CLI

```
aaa profile <profile>
   radius-accounting <group>
   radius-interim-accounting
```

## Support for Heartbeats in L2 GRE Tunnels

The controller can determine the status of a GRE tunnel by sending periodic keepalive frames on the tunnel. If you enable tunnel keepalives, the tunnel is considered to be "down" if there is repeated failure of the

keepalives. In this release of ArubaOS, controllers can send keepalive packets to other controllers over an L2 GRE tunnel. Previous releases allowed keepalive packets to be sent only on L3 GRE tunnels. All configuration commands related to the keepalive feature remain the same.

## Increased AP Support for Spectrum Analysis

Starting with ArubaOS 6.1.3, radios on AP-104 and AP-93H devices can be configured as spectrum monitors, and AP-105 radios can be configured as either a spectrum monitor or a **hybrid AP**.

An AP radio in hybrid AP mode will continue to serve clients as an access point while it analyzes spectrum analysis data for the channel the radio uses to serve clients. By default, a hybrid AP only monitors the channel specified in its 802.11a or 802.11g radio profile for spectrum interference. If you want to change the channel monitored by a hybrid AP, you must edit the channel setting in those profiles.

If a radio is configured as a hybrid AP and that AP is enabled with mode-aware ARM, the hybrid AP can change to an Air Monitor (or AM) if too many APs are detected in the area. If the ARM feature changes a hybrid AP to an Air Monitor, that AM will not provide spectrum data after the mode change. The AM will unsubscribe from any connected spectrum analysis client, send a log message warning about the change. If mode-aware ARM changes the AM back to an AP, you must manually subscribe the hybrid AP back to the spectrum analysis client.

The table below lists the AP models that support the spectrum analysis feature. Note that only radios on the AP-105 and AP-130 Series can be configured as hybrid APs.

**Table 1** *Device Support for Spectrum Analysis*

| Device | Configurable as a Spectrum Monitor? | Configurable as a Hybrid AP? |
|---|---|---|
| AP-104 | Yes | No |
| AP-105 | Yes | Yes |
| AP-92 | Yes | No |
| AP-93 | Yes | No |
| AP-93H | Yes | No |
| AP-120 Series | Yes | No |
| AP-130 Series | Yes | Yes |
| AP-175 | Yes | No |

## Even VLAN Pool Assignments

This feature allows for even distribution of VLAN pool assignments. Even VLAN Pool assignment maintains a dynamic latest usage level of the each VLAN ID in the pool. Therefore, as users age out, the number of available addresses increases. This leads to a more even distribution of addresses.

NOTE

Even VLAN Pool Assignment is not allowed for VLAN pools configured directly under a virtual-ap. It should only be used under named VLANs.

NOTE

L2 Mobility is not compatible with the existing implementation of Even VLAN pool assignment.

The following CLI command allows you to set the VLAN assignment. The `hash` value is set by default and is used for all VLAN unless configured as `even`.

```
(config) #vlan-name <vlan-name> pool assignment {even | hash}
```

You can view the current VLAN assignment configuration by executing the `show vlan mapping` command.

## Support for Desktop Virtualization Protocols

This release of ArubaOS supports desktop virtualization protocols by providing preconfigured ACLs for the Citrix ICA protocol. You can apply these ACLs to the user-role when using the Virtual Desktop Infrastructure (VDI) clients. This ensures that any enterprise application that uses the VDI client performs optimally with appropriate QoS.

## Support for SCCP v17

This release of ArubaOS provides support for the SCCP (Skinny Call Control Protocol) versions 17 or later.

## Support for Verizon LTE UML290 4G USB Modem

This release of ArubaOS provides support for 4G networks by allowing you to provision Verizon 4G LTE UML290 modems on the RAP. You can also provision the RAP to support both 4G and 3G USB modems. This enables the RAP to choose the available network in an area automatically. 4G takes precedence over 3G when the RAP tries to auto-select the network. You can also configure the RAP to work exclusively on a 3G or 4G network. It is recommended that you provision the USB modems for the RAP based on your network requirements.

### Points to Remember

- The RAP does not support dynamic plug-and-play for the 4G modems. So, you must provision a RAP with the 4G USB parameters on the controller manually based on its type and family(4G-WiMAX/4G-LTE).
- When a RAP connects to a 4G network, it will be displayed as Remote AP (R) and Cellular (C) on the controller.
- For 3G/4G network switch support, it is recommended to use the UML290 modem with the firmware version L0290VWB522F.242 or later. Using a lower version of the firmware auto-selects the network mode based on the network availability. Whereas, the latest version allows the RAP to lock the modem in a particular network mode (say, 3G only).

NOTE

The 4G-WiMAX family of modems do not support the 3G-4G network switch-over functionality.

### Provisioning RAP for USB Modems

To enable 3G/4G network support, you must provision the RAP with the USB parameters on the controller. You can use the WebUI or CLI to provision the USB parameters.

### Using WebUI

1. Navigate to **Configuration>Wireless>AP Installation** page.
2. Select the **Provisioning** tab.
3. Select an AP and click **Provision**.
4. Under **USB Settings**, select the **USB Parameters** check box.
5. To enable 4G network support, select a driver option in the **4G Device Type** drop-down menu based on your device type:
   - beceem-wimax
   - ether-lte
   - pantech-lte

   To enable 4G-exclusive network support, select a driver option in the **4G Device Type** drop-down menu and select *none* in the **Device Type** drop-down menu.
6. To enable 3G network support, select a driver option from the **Device Type** drop-down menu:
   - acm
   - airprime
   - hso
   - option
   - pantech-3g
   - sierra-evdo
   - sierra-gsm

   To enable 3G-exclusive network support, select a driver option in the **Device Type** drop-down menu and select *none* in the **4G Device Type** drop-down menu.

NOTE

To enable 3G/4G network switch support, select a driver option in both **Device Type** and **4G Device Type** drop-down menus.

7. Click **Apply and Reboot** to reboot the RAP with the new configuration.

### Using CLI

To enable 4G-exclusive network support on the RAP, execute the following commands:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #4g-usb-type <USB modem type>
(host) (Provisioning profile "<profile-name>") #usb-type none
```

To enable 3G-exclusive network support on the RAP, execute the following commands:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #usb-type <USB modem type>
(host) (Provisioning profile "<profile-name>") #4g-usb-type none
```

To enable 3G/4G network switch support, execute the following commands:

```
(host) (config) #ap provisioning-profile <profile-name>
(host) (Provisioning profile "<profile-name>") #4g-usb-type <USB modem type>
(host) (Provisioning profile "<profile-name>") #usb-type <USB modem type>
```

To view the USB modem details on the RAP, execute the following command

```
(host) #show ap debug usb ap-name <ap-name>
```

The following is a sample output that shows the USB information provisioned on the RAP:

```
USB Information
---------------
Parameter                    Value
---------                    -----
Manufacturer                  Pantech,
Product                       PANTECH
Serial Number
Driver                        ptuml_cdc_ether
Vendor ID                     106c
Product ID                    3718
USB Modem State               Active
USB Uplink RSSI(in dBm)       -73
Supported Network Services    CDMA GSM LTE
Firmware Version              L0290VWB522F.242
ESN Number                    990000472325325
Current Network Service       4G-LTE
```

## 802.1x Supplicant Support on an AP

This release of ArubaOS provides 802.1x supplicant support on the Access Point (AP). The AP can be used as a 802.1x supplicant where access to the wired Ethernet network is restricted to those devices that can authenticate using 802.1x.You can provision an AP to act as an 802.1x supplicant and authenticate to the infrastructure using the PEAP protocol.

NOTE

Both Campus APs (CAPs) and Remote APs (RAPs) can be provisioned to use 802.1x authentication.

### Prerequisites

- An AP has to be configured with the credentials for 802.1x authentication. These credentials are stored securely in the AP flash.
- The AP must complete the 802.1x authentication before it sends or receives IP traffic such as DHCP.

NOTE

If the AP cannot complete 802.1x authentication (explicit failure or reply timeout) within 1 minute, the AP will proceed to initiate the IP traffic and attempt to contact the controller. The infrastructure can be configured to allow this. If the AP contacts the controller it will be marked as unprovisioned so that the administrator can take corrective action.

### Provisioning an AP as a 802.1x Supplicant

This section describes how an AP can be provisioned as a 802.1x supplicant using CLI or the WebUI.

#### In the WebUI

To provision an AP as a 802.1x supplicant using the WebUI, follow these steps:

1. Navigate to the **Configuration** > **Wireless** > **AP Installation** > **Provisioning** window. The list of discovered APs are displayed on this page.
2. Select the AP you want to provision.
3. Click **Provision**. The provisioning window opens.
4. Select the **802.1x Parameters using PEAP** checkbox and enter the following credentials:
   a. User Name: Enter the user name of the AP in the **User Name** field.
   b. Password: Enter the password of the AP in the **Password** field.
5. Enter the password again in the **Confirm Password** field and reconfirm it.

6. Click **Apply and Reboot** (at the bottom of the page).

### In the CLI

To provision an AP as a 802.1x supplicant using the CLI, enter the following commands in the config mode:

```
(host) (config)# provision-ap
(host) (AP provisioning) # apdot1x-username <username>
(host) (AP provisioning) # apdot1x-passwd <password>
(host) (AP provisioning) # reprovision ap-name <apname>
```

To view the 802.1x authentication details on the controller:

```
(host) # show ap active
Active AP Table
---------------
Name       Group  IP Address   11g Clients  11g Ch/EIRP/MaxEIRP  11a Clients  11a Ch/
EIRP/MaxEIRP  AP Type  Flags  Uptime  Outer IP
----       -----  ----------   -----------  -------------------  -----------  ---------
----------  -------  -----  ------  --------
AP1X      default   10.3.15.107  0           AP:HT:1/15/21.5      0           AP:HT:44/
15/21       125      1E2    5m:48s  N/A

Flags: a = Reduce ARP packets in the air;  A = Enet1 in active/standby mode;
       B = Battery Boost On; C = Cellular; D = Disconn. Extra Calls On;
       d = Drop Mcast/Bcast On; E = Wired AP enabled; K = 802.11K Enabled;
       L = Client Balancing Enabled; M = Mesh; N = 802.11b protection disabled;
       P = PPPOE; R = Remote AP; X = Maintenance Mode;
       1 = 802.1x authenticated AP; 2 = Using IKE version 2;
```

## VIA Mobile

ArubaOS 6.1.3 introduces support for the VIA Mobile client application on the iOS platform. The application can be downloaded from the Apple App Store at http://www.apple.com/mac/app-store, and provides the following features:

- Automatic configuration updates without user intervention
- FIPS-compliant cryptographic security algorithms
- VPN session continuity allows a client to maintain a user session even when that client moves from one network to another or temporarily loses the Wi-Fi connection.

NOTE

This application is compatible with controllers running ArubaOS 5.x and higher with PEF-VPN licenses. Note that advanced features such as IKEv2 and MOBIKE require ArubaOS 6.1.3 and higher.

# Fixed Issues

The following issues have been fixed in this release of ArubaOS.

## Access Point

**Table 1** *Access Point Fixed Issues*

| Bug ID | Description |
|---|---|
| 59484 | Nothing is written into the HAL registers (disable or enable interrupts) if reset/chan change is in progress. |
| 44112 | This release has resolved an issue that caused RAP-2WG APs to perform unwanted reboots has been fixed. |
| 52450 | APs no longer ignore association requests if all the APs associated to a local controller rebootstrap at the same time. |
| 61340<br>61342 | Improvements to the **pppd** service and timer checks prevents Remote APs from performing unwanted reboots. |
| 61720 | The default regulatory domain profile for the country code JP3 contains all valid channels for that regulatory domain. |
| 62267 | Heartbeats from an AP-125 correctly appear in the output of the **show ap debug system-status** command. |
| 59027 | The Bridge user-entry now correctly ages out, if the user has roamed to another RAP on a different management VLAN. |
| 52892 | AP-68P no longer drops frames greater than 1468 bytes for a bridged VAP with a VLAN. |
| 53835 | AP-124abg and AP-125abg now accept FCC DFS channels. |
| 55939 | A Regulatory domain for AP-124 and AP-125 in Croatia had been approved but was not enabled in AOS. The Croatia country code was enabled in the controller and the AP's regulatory domain was integrated in AOS. |
| 57249 | Client can associate as 40Mhz capable with ZA regulatory domain. Before the fix, with ZA regulatory domain client could associate only as 20Mhz capable. |
| 58380 | AP-125 no longer crashes after repeated VAP enable or disable attempts. |
| 58534 | AP-125 no longer crashes after upgrading to new build. |
| 58261 | AP-105 crash with araw call trace `tlb_do_page_faults` no longer occurs. |
| 57578 | AP kernel panic messages no longer occur. |
| 51460 | AP-125 no longer crashes due to a kernel page fault at the virtual address. |
| 54256,<br>54609,<br>57659 | An AP crash due to a kernal page fault caused by a stack corruption has been fixed. |

**Table 1** *Access Point Fixed Issues*

| Bug ID | Description |
|---|---|
| 53897, 52825, 55118, 53365, 59274, 61930 | An AP-125 crash caused by a node leak has been fixed. |
| 59367, 59371 | An unwanted AP reboot caused by a kernel panic at ath_process_uapsd_trigger message no longer occurs. |
| 59643 | An unwanted AP reboot caused by a kernel panic at bogus non HT station count 0 - ieee80211_node_leave no longer occurs. |
| 56707 | The show AP database command no longer displays the Local controllers down on the Master, when all the APs on the Local controllers are up. |
| 53438 | AP-61 no longer incorrectly reboots with "Kernel Panic Error." |
| 57802 | The ESI-installed blacklist entries are no longer unexpectedly installed as "Permanent" instead of being governed by the Virtual AP's "Blacklist Timeout". |
| 59239 | Better mechansims to debug low free memory on APs are now available. |
| 59706, 61804 | An unwanted AP reboot caused by a kernel panic at aruba_deferred_set_channel message no longer occurs. |

## ARM

**Table 2** *ARM Fixed Issues*

| Bug ID | Description |
|---|---|
| 53389, 61564 | The packet capture no longer triggers an ARM channel change with reason "INV". |

## Captive Portal

**Table 3** *Captive Portal Fixed Issues*

| Bug ID | Description |
|---|---|
| 56272 | Incorrectly encoded redirect URLs from a captive network no longer cause a problem. |
| 45571, 58833 | Captive portal is now working on the local controllers when the guest VLAN has “ip nat inside” enabled. |
| 58729 | The command `ipv6 cp-redirect-address disable` now works correctly. |

## Configuration

**Table 4** *Configuration Fixed Issues*

| Bug ID | Description |
|---|---|
| 48961 | When the port status is changed to "down," the speed/duplex configuration is no longer incorrectly removed. |
| 52248 | The manual blacklist command now accepts the MAC address without a colon. |
| 48836, 51456 | The `backup flash` command no longer falsely displays an error on legacy platforms. |
| 51159 | M3 no longer sticks in bootloop due to configuration corruption. |

## Dot 1X

**Table 5** *Dot 1X Fixed Issues*

| Bug ID | Description |
|---|---|
| 43431, 50855 | Client blacklisting now works correctly when `max-authentication-failures` is set to 2 or a larger value. |

## Dynamic Authorization

**Table 6** *Dynamic Authorization Fixed Issues*

| Bug ID | Description |
|---|---|
| 48793 | The disconnect ACK now uses the correct source IP address and Amigopod does not drop it. |

## ESI

**Table 7** *ESI Fixed Issues*

| Bug ID | Description |
|---|---|
| 57802 | The ESI-installed blacklist entries are no longer unexpectedly installed as "Permanent" instead of being governed by the Virtual AP's "Blacklist Timeout". |
| 53189 | Improvements to the syslog process allow you to change user roles through the Extended Services Interface (ESI). |

## Hardware Management

**Table 8** *Hardware Management Fixed Issues*

| Bug ID | Description |
|---|---|
| 49504 | The `show inventory` command now correctly displays the serial number and other data on M3 slot #1. |
| 49956 | The syslog is now sent out following a fan failure. |

## Interface

**Table 9** *Interface Fixed Issues*

| Bug ID | Description |
|---|---|
| 62298 | On a 3000 Series controller, using SFP-SX transceivers, the link state will indicate going up continuously in the syslog. The actual link state itself does not flap. However due to the link up transitions internally, STP, OSPF, LACP will not converge. If you are not running any ofthese protocols on that port, there should be no effect. |

## IPSec

**Table 10** *IPSec Fixed Issues*

| Bug ID | Description |
|---|---|
| 56371 | A Redundant-Master controller will no longer reboot with “Reboot Cause: Nanny rebooted machine - isakmpd process died." |

## LDAP

**Table 11** *LDAP Fixed Issues*

| Bug ID | Description |
|---|---|
| 53218 | Auth module no longer crashes during an LDAP authentication timeout. |

## Local DB

**Table 12** *Local DB Fixed Issues*

| Bug ID | Description |
|---|---|
| 53391 | The local user DB now adds the Remote IP correctly even when the first octet of the IP address is greater than 127. |

## MAC Based Authentication

**Table 13** *MAC Based Authentication Fixed Issues*

| Bug ID | Description |
|---|---|
| 55202, 55003 | After failing MAC authentication and falling into the Initial-Role of the AAA profile, if the user attempts to reconnect, MAC authentication will correctly happen again. |

## Management

**Table 14** *Fixed Management Issues*

| Bug ID | Description |
|---|---|
| 53984<br>63277<br>53904 | AMs no longer report rogues with SSID 'tarpit' in environments where no wireless neighbors should be seen. No SSID 'tarpit' was configured. And this was reported from multiple devices. |
| 62296, 62297, 62502, 62477, 62468 | An Aruba 651 controller is no longer susceptible to continuous rebooting if its internal AP (radio) is configured in Air Monitor mode (am-mode). |
| 58601 | The controller no longer gets SQL syntax error messages after upgrading. |

## Mesh

**Table 15** *Mesh Fixed Issues*

| Bug ID | Description |
|---|---|
| 55740 | Mesh points no longer crash in node_cleanup() after downgrading the controller. |

## OSPF

**Table 16** *OSPF Fixed Issues*

| Bug ID | Description |
|---|---|
| 56398 | The loopback address can now be advertised through OSPF when the loopback address is in a different subnet than any configured VLANs. |

## Platform/Datapath

**Table 17** *Platform/Datapath Fixed Issues*

| Bug ID | Description |
|---|---|
| 52093 | Issuing the CLI command l**ocal-userdb-guest del username <name>** and **local-user del username <name>** no longer causes a controller to run low on memory and unexpectedly reboot. |
| 52492, 53600, 56561, 54231, 57302, 55620, 61152, 61155, 56928 | An unexpected controller reboot due to a hard watchdog accompanied by “reason for reboot: unknown” has been fixed. Additionally, a change has been made to ArubaOS to prevent the use of “reason for reboot: unknown” for unexpected reboots. Unknown reboots we caused by flash write failures. Now, the flash write is retried by performing an erase followed by another write. |
| 53332 | Improvements to the **Datapath** module prevent the controller from performing unwanted reboots. |
| 60373 | Improvements to SOS crash dump collection allow datapath crashes to recover more quickly. |

**Table 17** *Platform/Datapath Fixed Issues*

| Bug ID | Description |
|---|---|
| 60431, 63006 | Issuing the CLI command show trunk no longer causes the **fpapps** module to stop responding when the controller includes a large number of non-contiguous VLANs. |
| 46116 | The TCP maximum segment size for TKIP tunnels has been reduced to better accommodate the WEPCRC length. |
| 58502 | Packets are now sent from the Trunk port on the controller to a client on the trunk port behind a RAP with a proper VLAN tag. |
| 52845 | Proxy-arp now provides support for split-tunnels. |
| 54191, 55794 | FTP data transfer and reuse of a stray session no longer triggers a race condition and datapath timeout exception. |
| 54943 | Users are now able to get IP address on VMWare Fusion. |
| 52092 | Client with .255 IP address can now ping across L2 GRE. |
| 52732 | M3 datapath no longer crashes. |
| 60670 | The 620 controller no longer reboots due to a datapath exception when connected to a Bell ADSL modem. |
| 59078 | Controller tagged VLAN traffic received through trunk port is no longer sent out the egress port without a PPPoE header. |
| 53821, 54053, 55125, 55130, 55616, 56657, 59457, 62102, 62006, 62206 | The mysql process now begins before any other processes to help prevent an unexpected controller reboot that occured following a number of module crashes. |
| 50914 | The cfgm local is now able to successfully create a socket for connecting to the cfgm master and receive its configuration. |
| 54194, 54238 | Improvements to the PAPI timeout handler prevent memory errors that could trigger unwanted controller reboots. The PAPI timeout handler now validates the buffer before taking any action. |

## PPPoE

**Table 18** *PPPoE Fixed Issues*

| Bug ID | Description |
|---|---|
| 58097 | A local 620 controller connected through a DSL modem using PPPoE is now able to reach the master controller. |

## RADIUS

**Table 19** *RADIUS Fixed Issues*

| Bug ID | Description |
|---|---|
| 53709 | A RADIUS packet no longer limits a client's username to 32 bytes when EAP termination is enabled on the controller. |

## Remote Access Point

**Table 20** *Remote Access Point Fixed Issues*

| Bug ID | Description |
|---|---|
| 59723, 59743 | User traffic will be passed normally if the client connects to a VAP in split-tunnel forwarding mode, the client has a inital user role of **denyall** (any any any deny), even if the wireless adapter on the client is disabled then reenabled. |
| 60167 | If PPPoE remote APs using certficates and IKEv2 have a static inner IP addresses but then later change their outer IP address or port during rebootstrap, the inner IP route is retained when the remote APs establish a new IKE SA to the controller. |
| 61000 | Improvements to the handling of HELLO packets allow remote APs to be able to properly associate to their controller upon upgrading to ArubaOS 6.1.3. |
| 60458 | Remote AP mesh portal and wired bridging are no longer failing. Customer required LAN extension by using enet port of mesh point to locally bridge via Remote Mesh Portal. This bridge failed as the incoming user on the mesh point did not pickup a valid user ACL. All traffic (except ARP) was blocked by the firewall on the Remote Mesh Portal. |
| 53408 | When the VLAN ID is not set in the virtual-ap profile, the VAP survives when connectivity to the controller is lost and the AP is rebooted. |
| 59744 | The RAP-2WG now correctly switches to the second controller IP returned by the DNS server when the first one is not reachable. |
| 44973 | The Group Key is now present on a bridge/split VAP and now correctly matches with the controller auth. |
| 45719 | The RAP now comes up when connected to a DSL modem (Dlink) with a DHCP scope in the range of 192.168.11.x and 192.168.11.1 as its own IP. |
| 47990 | Backup SSID users correctly show up on the L3 user table and do not incorrectly age out. |
| 59036 | Clients can now send  traffic if the controller is not reachable from a RAP, clients are connected to backup/always/persistent bride mode VAP's, and no PEFNG is installed. |

## Role/VLAN Derivation

**Table 21** *Role/VLAN Derivation Fixed Issues*

| Bug ID | Description |
|---|---|
| 55438 | The dhcp-option user derivation rules that involve multiple dhcp-options now work correctly. |

## Security

**Table 22** *Security Fixed Issues*

| Bug ID | Description |
|---|---|
| 57474 | This release includes ability to filter the IPsec mirroring to a single peer with the CLI command **firewall session-mirror-ipsec peer <peer_ip>**. |
| 61551 | Improvements to the **Auth** module prevent the controller from performing unwanted reboots. |
| 52494 | An unexpected controller reboot due by an auth module crash caused by a memory leak has been fixed. |
| 55519 | Auth module now operates correctly on the controller and Authmgr no longer registers 100% busy. |
| 51888 | Successful authentication no longer incorrectly displays the error log. |
| 52592 | The “show global-user-table” command no longer takes 2 minutes to respond in a master/backup scenario. |
| 52181 | Rule can now be removed from an ACL |
| 59661 | An unexpected controller reboot due by an auth module crash caused by a memory leak has been fixed. |
| 58786 | The "authmgr get segfault" message no longer occurs while processing a new user and trying to perform "devid cache lookup mac." |
| 51393 | MIPT phones no longer reboot with “any any udp 68 deny rule” in validuser ACL. |

## SNMP

**Table 23** *SNMP Fixed Issues*

| Bug ID | Description |
|---|---|
| 53988 | L2 roams now generate the `wlsxUserEntryAttributesChanged` message. |

## Station Management

**Table 24** *Station Management Fixed Issues*

| Bug ID | Description |
|---|---|
| 54334 | Upgrading no longer corrupts the wlanAPBssidAPMacAddress OID. |

## TACACS

**Table 25** *TACACS Fixed Issues*

| Bug ID | Description |
|---|---|
| 60667 | Authentication improvements allow TACACS command accounting to function correctly, even in environments with up to 400milliseconds delay between the controller and the TACACS server. |

## Voice Platform

**Table 26** *Voice Platform Fixed Issues*

| Bug ID | Description |
|---|---|
| 58895 | Applying a “noe-acl” no longer causes RTP packets to be dropped for IP Touch 310/610 phones. |
| 57869 | High CPU in STM no longer causes APs to drop from controller due to certain netservice configuration. |

## Voice SCCP

**Table 27** *Voice SCCP Fixed Issues*

| Bug ID | Description |
|---|---|
| 58554 | The CAC call status for an Alcatel OmniTouch 8128 phone properly resets back to zero after session termination. |
| 44110 | Cisco Phones plugged in the wire behind the RAP are no longer unnecessarily re-registering with Call Manager. |

## WebUI-Configuration

**Table 28** *WebUI-Configuration Fixed Issues*

| Bug ID | Description |
|---|---|
| 54467 | When an AP is provisioned with a white space in between the AP name (example: "AP NAME"), the AP provisioning page no longer comes up blank. |
| 55205 | The Netdestination entries can now be deleted. |
| 52453 | WPA-PSK Pre-Shared Keys are now accepted by the controller GUI. |
| 54387 | There is no issue with VLAN pool in the GUI. |
| 54516 | Alcatel-Lucent SR-1-123255069: IE no longer has a Red Cross mark in the Guest Provisioning (Page Design field). |

## WebUI-Monitoring

**Table 29** *WebUI-Monitoring Fixed Issues*

| Bug ID | Description |
|---|---|
| 58485 | WebUI now correctly displays the EVENTS and REPORTS tab. |
| 55949 | WebUI Mesh now correctly shows "Rate RX/TX" in the "Last Update" field. |
| 50500 | Client activity is now displayed properly on WebUI for wired clients on Remote AP. |

## WISPr

**Table 30** *WISPr Fixed Issues*

| Bug ID | Description |
|---|---|
| 60529 | Trying to emulate WISPr client using wget no longer gets wrong redirection if custom SSL cert is used. |

## XML API

**Table 31** *XML API Fixed Issues*

| Bug ID | Description |
|---|---|
| 58882 | A RADIUS accounting start message will not be sent to the RADIUS server if a user is deleted via an XML API **user_delete** command issued from an external XML API server. |
| 49321 | The Radius attributes in "Aruba-Location-Id" are filled correctly when forward mode is split-tunnel. |

# Chapter 4

# Known Issues and Limitations

This chapter describes the known issues and limitations in this version of ArubaOS.

## Maximum DHCP Lease Per Platform

**Table 1** *Maximum DHCP Lease Per Platform*

| Platform | Description |
|---|---|
| M3 | 512 |
| 3200 | 512 |
| 3400 | 512 |
| 3600 | 512 |
| 600 Series | 512 |

## Access Point

**Table 2** *Access Point Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 60537 | The AP is in the D (dirty) state for a long time before recovering. The output of `show ap details advanced` shows that the controller is attempting to send logging config messages to the AP, but they are not acknowledged.<br>**Workaround:**<br>None. |
| 61526 | The AP is rebootstrapping with multiple simultaneous VoIP calls running and WMM disabled. When WMM is disabled and simultaneous VoIP calls are made among six Cisco phones in tunnel mode, the APs rebootstrap within a few minutes. Numerous messages on the AP console state `XQ MAX DEPTH!!!` just before the AP rebootstraps.<br>**Workaround:**<br>The Cisco phone supports WMM, so always enable WMM in the SSID profile. |
| 61938 | AP-105s do not accept DHCPOFFER from a router. After an auth crash and an fpapps/datapath crash, the APs did not attempt to contact the backup-lms. Eventually, after a 2160 DHCPDISCOVER (360 x 6), the AP rebooted and cleared the condition.<br>**Workaround:**<br>None. |
| 55186 | The AP-105 and AP-90 series access points do not work properly on 2.4 GHz when located close to a cellular DAS antenna.<br>**Workaround:**<br>Move the cellular DAS antenna away from the AP. |

**Table 2** *Access Point Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 57624 | AP-105s might not come up when connected to a Cisco PoE switch (WS-C6509-E:WS-X6148A-GE-45AF). The APs are not powering up despite the maximum amount of power being allocated to the port the AP is connected to. The following error messages were returned when a `shutdown` or `no shutdown` was executed on the port the AP was connected to:<br>`%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on GigabitEthernet9/48 (not half duplex), with SEP001BD5E87C32 Port 1 (half duplex).`<br>`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`<br>`%C6K_POWER-SP-1-PD_HW_FAULTY: The device connected to port 3/2 has a hardware problem. Power is turned off on the port.`<br>**Workaround:**<br>None. |
| 56883 | An issue has been identified where a client's signal-to-noise ratio (SNR) becomes 0 after completing a roam. Additionally, it can take anywhere from 10 seconds to 1 min for the clients SNR to return to a non-zero value.<br>**Workaround:**<br>None. |
| 56678 | In Advanced Monitoring, the client goodput value might display half of the expected value. The cause for this is currently unknown.<br>**Workaround:**<br>None. |

## ARM

**Table 3** *ARM Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62878 | If band steering is enabled, errors in the voice-aware band steering feature can cause active 802.11a/g capable voice clients to be disassociated from an AP if those clients roam to a new 802.11g radio.<br>**Workaround:**<br>None. |
| 56760 | Per-SSID bandwidth contracts do not work well with de-tunnel mode with UDP traffic. For example:<br>• the actual bandwidth allocation is around 25% off compared to the configured bandwidth allocation. With tunnel mode, the error rate is only 5-10%.<br>• the maximum UDP throughput for a single client is only 155 Mbps, which is about 30Mbps off when compared to 183 Mbps in tunnel mode.<br>**Workaround:**<br>None. |

## Captive Portal

**Table 4** *Captive Portal Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 63253 | Wired IPv6 users from untrusted port channels do not get captive portal.<br>**Workaround:**<br>None. |

## DHCP

**Table 5** *DHCP Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 55010 | Wired clients connect to and receive an IP address from a different VLAN after the controller is rebooted instead of connecting to the VLAN they were connected to prior to the reboot.<br>**Workaround:**<br>The client must renew its IP address using the `ipconfig release` and `ipconfig renew` commands. |

## Dot 1x

**Table 6** *Dot 1x Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 58530 | The key exchange is stuck due to MC ignoring Key4 response from client. |
| 56236<br>55579 | A replay counter mismatch is seen during a 4 way handshake in wpa2-aes mode.<br><br>The client does not connect to the AP. After the 4-way handshake, the client tries to get the IP address but fails. Then the client ends the deauth packet to the AP. The Error log displays `WPA2 Key message 4 from Station did not match the replay counter`.<br><br>The client successfully connects with the same mixed mode configuration with wp-psk-tkip security.<br><br>The same message is displayed, which is also seen with standalone security wpa2-psk-aes only, but the device connects successfully.<br><br>**Workaround:**<br>This is a client-specific issue and happens because of slower responding clients. You could change the timeout on the controller. |
| 62437 | The aaa state for the user (AP) is not cleared after performing AP-Dot1x authentication. The IP address from the VLAN gets stuck with the MAC address of the AP, even though the AP has moved to a different VLAN. The aaa state for the IP address does not get cleared.<br>**Workaround:**<br>None. |

## ESI

**Table 7** *ESI Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 63601/ 58098 | Authentication module restarts when ESI parser is configured.<br>**Workaround:**<br>Remove all ESI parser related configurations, before controller is upgraded to 6.1.3.0. |

## IPSec

**Table 8** *IPSec Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 56606 | The following show commands return the `% Invalid input detected at '^' marker` error message instead of returning any information in the Tech Support logs.<br>`show crypto l2tp`<br>`show crypto-local pki trustpoint`<br>`show poe`<br>`show mux config`<br>`show mux state`<br>`show voice prioritization`<br>**Workaround:**<br>None. |

## IPv6

**Table 9** *IPv6 Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 63124 | An IPv6 network carrying IPv4 DNS “A” queries does not work correctly and clients are unable to browse public networks.<br>**Workaround:**<br>None. |
| 57059 | When the maximum IPv6 addresses are configured on a controller, basic routing fails. This issue only occurs in IPv6.<br>**Workaround:**<br>Configure only the required number of IPv6 addresses. |
| 55786 | IPv6 ping fails to the controller on 600 Series controllers with `broadcast-filter all` enabled on User-vlan.<br>**Workaround:**<br>Disable `broadcast-filter all`. |
| 57067 | IPv6 APs are not coming up on a controller that is connected to an untrusted port. The IPv6 APs go into the ap-role. However, since the ap-role does not have any IPv6 ACLs, the APs are not coming up on the controller.<br>**Workaround:**<br>Add IPv6 ACLs to the ap-role. |

**Table 9** *IPv6 Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 57124 | Neighbor Discovery does not work with `bcmc-optimization` enabled. Enabling `bcmc-optimization` could cause ping to the controller interface to fail from the users, which internally would affect WebUI access and other IPv6 features.<br>**Workaround:**<br>Disable `bcmc-optimization` from the VLAN interface. |
| 57239 | Datapath Utilization might spike with multiple IPv6 user traffic coming from Android devices.<br>**Workaround:**<br>Reload the controller. |
| 50648 | Any IPv6 sessions greater than 420k might experience packet loss and the allocation failure counter under `show datapath session ipv6 counters` will increase.<br>**Workaround:**<br>None. |

## Licensing

**Table 10** *Licensing Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 55839 | When the `Available Campus APs` shows 0, no new APs are able to come up unless some used licenses become free.<br>**Workaround:**<br>None. |

## L2TP

**Table 11** *L2TP Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62174 | An exhausted RAP L2TP pool can cause RAPs to go down. The controller gradually adds more RAPs up to a peak of 256 APs.<br>**Workaround:**<br>None. |

## MAC Based Authentication

**Table 12** *MAC Based Authentication Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 56130 | User is falling into logon role instead of mac-auth role. This occurs when roaming between wireless and wired user.<br>**Workaround:**<br>None. |

## Management

**Table 13** *Management Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 63134 | The webserver cannot revert to factory cert when the custom cert expires and is deleted.<br>**Workaround:**<br>None. |
| 63008<br>63011 | In some cases, when an in-use CA certificate is allowed to expire, then deleted and replaced with a new one, clients may not be able to authenticate. Additionally, the reference counter for the replaced certificate shows zero (0) when there is a dot1x profile referencing the certificate.<br>**Workaround:**<br>Execute the `write mem` CLI command to complete the process. |

## Mesh

**Table 14** *Mesh Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 56642 | In some cases, an AP-135 configured as a mesh point fails to upgrade in the mesh link to an AP-125 mesh portal using HT and `mesh-ht-ssid-profile`. This issue only occurs in mixed-AP deployments.<br>**Workaround:**<br>If the supported-MCS is configured to 0-15, the issue is solved. |

## OCSP/CRL

**Table 15** *OCSP/CRL Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 55419 | The certmgr module becomes busy when a large number of OCSP requests hit the certmgr when OCSP server is not reachable. This issue will appear whenever there is misconfiguration or outage between the controller and the OCSP responder.<br>**Workaround:**<br>None. |

## OSPF

**Table 16** *OSPF Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62839 | The OSPF process may fail to respond if the controller has OSPF enabled, OSPF neighborship established and the DHCP IP Helper Addresses configured on the same VLAN as OSPF.<br>**Workaround:**<br>None. |
| 54117 | 16-character OSPF authentication keys are truncated to 15 characters in the output of the `show ip ospf interface` command.<br>**Workaround:**<br>Use a 15-character (or less) authentication password. |

**Table 16** *OSPF Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 56326 | In some cases, your controller might unexpectedly reboot due to an OSPF module crash.<br>**Workaround:**<br>None. |

## Platform/Datapath

**Table 17** *Platform/Datapath Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 63602 | The dot1x AP cannot be brought up when the AP system profile **`native-vlan-id`** is configured. |
| 53804 | The Fpcli crashed on M3 while continuously trying to execute two `show ap debug` commands.<br>**Workaround:**<br>None. |
| 61667 | The firewall `broadcast-filter arp` command causes the local controller to use the incorrect route-cache entry.<br>**Workaround:**<br>Disable the broadcast-filter firewall knob. |
| 61908 | The `write mem` failed due to busy CFGM module.<br>**Workaround:**<br>None. |
| 62493 | Running `bcmc-optimization` with rap wifi and wired-ports in tunnel mode breaks connectivity<br>**Workaround:**<br>None. |
| 62526 | The CFGM crashes on the controller.<br>**Workaround:**<br>None. |
| 63393 | A datapath crash can occur during a race window (5 millisecond ) when the controller detects more than 4 IPv6 addresses per user.<br>**Workaround:**<br>None. |
| 63279 | Station entries are not cleaned up after a user disconnected from the AP.<br>**Workaround:**<br>None. |
| 63164 | The mobile IP module might crash when there are several hundred mobile clients in addition to another 1000+ users and all are L2 roaming.<br>**Workaround:**<br>None. |
| 63163 | Mobility enabled datapath bridge entrries are getting deleted for untrusted users. Mobility is deleting and adding the datapath bridge entry for the clients even when there is active traffic going on. It happens only when Mobility is turned on.<br>**Workaround:**<br>None. |

**Table 17** *Platform/Datapath Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 62838 | If an AP comes up on an untrusted port where the first port rule is `allowall` , that AP's sessions may be denied.<br>**Workaround:**<br>None. |
| 61493 | The local controllers reboot with `datapath timeout`. This might be caused by setting `mgmt-server type amp primary-server`.<br>**Workaround:**<br>None |
| 61517 | The datapath module might crash on the controller.<br>**Workaround:**<br>Reboot the controller. |
| 62238 | Unknown unicast flood is being sent to all tunnels. In a network where the user VLANs extend from the controller to an uplink Cisco switch, there are certain applications that try to reach the users connected behind a RAP. The Cisco environment has the Arp Ageout and the Cam table ageout set to 4 hours. This causes any traffic sent to the controller for any user who has aged out to get flooded to all users in that VLAN.<br>**Workaround:**<br>None. |
| 57378 | If the WMS process on the master controller is too busy, you cannot run commands like: `write memory` and `show running-config` as it throws the error message: `WMS process busy please try later`.<br>**Workaround:**<br>None. |
| 62445 | Nanny rebooted machine - fpapps process died.<br>**Workaround:**<br>None. |
| 62527 | WebUI phonehome crash.<br>**Workaround:**<br>None. |
| 62551 | The kernel module crashed on the standby controller while running ArubaOS 6.1.2.5. The Reboot Cause shows `User pushed reset` when we are not able to write the cause of the reboot. The cause could be software watchdogs, SOS crashes, bus/cache errors, and busy CPUs.<br>**Workaround:**<br>None. |
| 62552 | The kernel module crashed on the Master while running ArubaOS 6.1.2.5.<br>**Workaround:**<br>None. |
| 61272, 60744, 60992 | When upgrading a local or master controller to ArubaOS 6.1.2.6, when any APs failover to a LMS backup controller that has already been upgraded, that backup controller no longer crashes.<br>**Workaround:**<br>None. |
| 57344, 57864 | In some cases, the crypto engine may become stalled on a controller causing it to lose connection to its master controller and preventing all 802.1x clients from connecting to the network. Additionally, the number of IPSec and AESCCM encryption failures continues to go up and the controller cannot send a single IPSec or AES packet.<br>**Workaround:**<br>None. |

**Table 17** *Platform/Datapath Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 54635 | High datapath utilization is observed when Apple iDevices negotiate BA with AMSDU traffic.<br>**Workaround:**<br>Starting in ArubaOS 6.1.2.4, you can prevent iDevices from sending AMSDU using the `no ba-amsdu-enable` option in the `wlan ht-ssid-profile` command. This prevents iDevices from setting up BA with AMSDU and reverting to MPDU-Agg. |
| 57450 | Port Channel (LACP) with PVST+ disabled might result in packet loss between controllers.<br>**Workaround:**<br>Disable Port Channel or enable PVST+. |
| 54869 | In some cases, the kernel module restart might lead to an unexpected controller reboot. Additionally, the reason for reboot was incorrectly reported as `Reboot Cause: User reboot.`<br>**Workaround:**<br>None. |
| 58487 | In some cases, with CPSEC enabled, APs might take a long time (more than 30 minutes) to come up. This is due to CPSEC SA setup timing out because the AP is not receiving the fourth IKE packet from the controller.<br>**Workaround:**<br>None. |
| 59190 | In some cases, a bwm-contract applied to initial role may cause a 50% degradation on captive portal performance. In this scenario, a bwm-contract is applied downstream on the initial role and both sides on captive-portal final role. However, it is observed that the direction the bwm is applied does not matter.<br>**Workaround:**<br>None. |
| 59334 | In some cases, the kernel module might restart due to a control processor kernel panic. This may lead to an unexpected controller reboot.<br>**Workaround:**<br>None. |
| 55948 | The error message `Unable to open system file /dev/max6657 in check_max6657, hwMon.c:2123` can randomly appear in the errorlog of the controller. The message appears when the temperature sensor in the controller is not responding.<br>**Workaround:**<br>Rebooting the controller can resolve the issue. |
| 55998 | When copying a software image from one partition to another on the same controller, the ancillary image is not copied along with the core image. This will cause ArubaOS to report that ancillary verification has failed.<br>**Workaround:**<br>Copy the image file to each partition from an external source. |
| 54854, 54851, 54856, 54852 | In some cases, the nanny module might restart due to a low memory state. This may lead to an unexpected controller reboot.<br>**Workaround:**<br>None. |

**Table 17** *Platform/Datapath Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 55222 | During an upgrade, 3200 and 600 Series controllers may receive the incorrect ancillary.tar files. This issue can occur in the following scenario:<br>1. Run 6.1.2.2 from partition 0.<br>2. Copy 6.1.2.2 to partition 1.<br>3. Copy 3.4.3.3 to partition 1.<br>4. Downgrade to 3.4.3.3.<br>5. Copy 6.1.2.2 to partition 1.<br>6. Upgrade to 6.1.2.2.<br>**Workaround:**<br>Performing an additional upgrade to 6.1.2.2 resolves this issue. |
| 54156, 55217 | ArubaOS does not support APs connected to Tunneled Node ports.<br>**Workaround:**<br>None. |

## Port Channel

**Table 18** *Port Channel Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62936 | If the native VLAN of a trunk LACP port channel is set as untrusted, LACP member ports may stop responding upon upgrading the controller to ArubaOS 6.1.3 or later.<br>**Workaround:**<br>None. |

## PPTP

**Table 19** *PPTP Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 55177 | MacBook clients running Mac OS 10.6.7 connected to a controller configured as a PPTP server are disconnected if idle for 10 minutes. This does not affect Windows clients.<br>**Workaround:**<br>None. |

## RADIUS

**Table 20** *Radius Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62337 | The Ap-Group and AP-Location-Id in the RADIUS request remains empty when the user is wired.<br>**Workaround:**<br>None. |
| 62902 | The `Radius Accounting stats` and `Acct-Session-id` data shown in the output of the `aaa state user <username>` command may not be correct if this command is issued for users in tunnel forwarding mode.<br>**Workaround:**<br>None. |

**Table 20** *Radius Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 57005 | A controller might report incorrect values in the Radius Accounting Stop packet for Acct-Input-Octets/Acct-Output-Octets attribute.<br>**Workaround:**<br>None. |

## Remote Access Point

**Table 21** *Remote Access Point Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 61936 | CPSEC CAP should not use random IKE source port.<br>**Workaround:**<br>None. |
| 59019 | The RAP dynamically changes the source port while setting up IPSec, and creates the issue of the intermediate firewall dropping packets.<br>**Workaround:**<br>None. |
| 62556 | The RAP is not falling to TFTP, if FTP is denied or has failed. If the FTP ACL is missing in AP role, either due to a upgrade issue or due to a configuration error, the AP does not fail back to TFTP and reboots.<br>**Workaround:**<br>The workaround is to add the `svc-ftp` rule under ap-role. |
| 63123 | The bond0 interface on an AP-124 configured as a Remote AP may become unresponsive if tunnel-mode Virtual APs are removed from the Remote AP and persistant and standard bridge-mode Virtual APs are added to the Remote AP.<br>**Workaround:**<br>None. |
| 63073 | If you configure a user role on a bridge-mode virtual AP with an access control list that contains more ACE entries than are supported by the AP, then try to save this setting, the AP will not be able to save the ACL to its flash memory. However, if you modify the ACL to use a supported number of ACE entries, the AP will not be able to save this setting to its flash memory until after the AP has rebooted.<br>**Workaround:**<br>Reboot the AP before trying to save the modified user role. |
| 62823 | The controller will not display output for the `show user location <ap name>` command if the Remote AP has a space in the RAP name, unless the RAP name is contained within quotation marks.<br>**Workaround:**<br>Put the Remote AP name in quotation marks when issuing this command. For example, `show user location "branch rap"`. |
| 51546 | 3G to wired failover might cause interruptions in packet flow and leaves the USB-connected 3G modem in a hung state.<br>**Workaround:**<br>None. |

**Table 21** *Remote Access Point Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 59433 | When wireless clients in a split-tunnel role roam from one RAP to another RAP, TCP based sessions fail. The TCP connection continues for a few seconds after the roam is complete but, shortly after, the file transfer stops.<br>**Workaround:**<br>None. |
| 56841, 53410 | In cases when large ACLs are pushed to RAPs/APs deployed in a network with a large amount of loss, it is possible for AP to get stuck in ACL configuration state. The controller attempts to send the large ACL to AP and AP fails to acknowledge this as it never receives all the fragments. This process continues and the AP never receives any more ACLs from the controller once it gets into this state.<br>**Workaround:**<br>This issue can be prevented by creating ACLs that are as small as possible. |
| 57196 | The following commands cannot be executed on a controller where a RAP is terminating behind a RAP. Note that this issue appears only when the RAP's uplink is an EVDO/3G modem.<br>`show ap monitor ap-list  ap-name <ap-name>`<br>`show ap debug system-status ap-name <ap-name>`<br>`show ap debug radio-stats ap-name <ap-name> radio 0 advanced`<br>`show ap debug radio-stats ap-name <ap-name> radio 1 advanced`<br>**Workaround:**<br>None. |
| 56875 | A RAP cannot roll back from a secondary cellular connection to the primary Ethernet when validuser ACL does not permit svc-natt.<br>**Workaround:**<br>Modify the validuser ACL by adding the following:<br>`any host <public IP of controller> svc-natt permit`<br>Also, in cases where a RAP is deployed in an MPLS network and the master is configured as FQDN, make sure to add the following to the validuser ACL:<br>`any host <MPLS IP of controller> svc-natt permit` |
| 53755 | It may take longer for a RAP to dial a 4G call when the 4G signal strength is lower than -70 dBm.<br>**Workaround:**<br>None. |
| 55088, 52199 | IP addresses for bridge and split-tunnel mode wireless clients do not appear in the ID page of the WebUI.<br>**Workaround:**<br>None. |
| 53946, 35982 | RAP 4G diagnostics features such as ping, nslookup, and routetrace do not display properly on the LD page.<br>**Workaround:**<br>None. |

## Role and VLAN Derivation

**Table 22** *Role and VLAN Derivation Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 51691, 56746 | DHCP Fingerprinting & Captive Portal cannot be used together.<br>**Workaround:**<br>None. |

**Table 22** *Role and VLAN Derivation Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 52733 | MDAC is being used to identify smartphones by DHCP fingerprint. While matching fingerprints, the client (smartphone) will be put into another user role (e.g device-role). Device-role binds a VLAN rather than default VLAN of VAP. However `show user-table verbose` displays the wrong VLAN.<br>**Workaround:**<br>None. |
| 54037 | In some cases, the maximum number of supported stations (8k entries) is being reached on the controller because idle user entries are not being released. Once the controller reaches this stage, some of the new user entries are placed in VLAN1.<br>**Workaround:**<br>None. |
| 55867 | Clients doing Machine-auth will fall into the default VLAN if an external server is used for VLAN derivation.<br>**Workaround:**<br>None. |

## Security

**Table 23** *Security Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 63287 | The Auth module crashes on the local controller.<br>**Workaround:**<br>Disable the broadcast-filter firewall knob. |
| 62097<br>63014 | The timer handle is not invalidated after a timeout.<br>**Workaround:**<br>Move the cellular DAS antenna away from the AP. |
| 62437 | The AAA state for the an AP does not get cleared after the AP completes 802.1x authentication. The IP address from the AP's first assigned VLAN stays associated to the AP's MAC address, even after the AP moves to a different VLAN.<br>**Workaround:**<br>Manually change the AAA state of the AP and reboot the controller. |
| 55913 | When `aaa user delete all` is issued to kick out all the users, sometimes one user is created in the user-table with a logon role instead of the assigned role (authenticated). In addition, two users are connected to an open SSID in de-tunnel mode and no traffic is sent at that moment.<br>**Workaround:**<br>None. |
| 60976 | Crash occured due to auth.<br>"Any update on this bug? Please provide an update as customer is looking for an update."<br>**Workaround:**<br>None. |

**Table 23** *Security Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 61687 | The old user entry in the user table is not removed even after the client is disassociated to a different network. When a new user connects to the SSID, it is getting the IP addrress as the old user entry in the user table, which was there for couple of days. Because of the old entry, the new client is unable to pass any traffic that also gets the same IP<br>**Workaround:**<br>"This issue seems the same as the description in Bug 61423. Let's collect more information for this investigation. (Liang-Chih Yuan) |
| 61690 | In an ACL with the following lines:<br>`ip access-list session good`<br>`any any any  deny blacklist log`<br>The ACL has the enabled the blacklist option and the valid client is falling on the MAC auth default role. The non-valid client is falling on the Deny all, but the non-valid clients are not getting blacklisted.<br>**Workaround:**<br>None. |
| 61964 | The controller is not able to fetch the ACL details if there are many ACE entries. When an ACL with 480 ACE entries is configured, the `show acl ace-table acl` command is not able to display ACE Entries and throws the error message `Module Authentication is busy`.<br>**Workaround:**<br>The workaround is to have 200 ACE entries or less. |
| 62099 | 100 user entries were stuck in the user-table for more than 2 days. This issue was seen when a combination of dot1x, VPN, and captive portal users (2000 total users) were added to the controller.<br>**Workaround:**<br>Use the `aaa user delete all` command to delete the user entries from the user-table. |
| 62253 | The controller misses sending user account interim updates to the RADIUS server if it has many users.<br>**Workaround:**<br>None. |
| 62613 | Clients could not connect to an 802.1x SSID. The issue was first seen on ArubaOS 6.1.2.5.<br>**Workaround:**<br>The `logging level debug security` command greatly increases the load on the AUTHMGR process, especially when there are a lot of authentication activities. This command is only intended for temporary debugging scenarios. It is a known limitation that at that logging level, AUTHMGR process will slow down and will not be able to keep up with authentication requests as well as in less intense logging levels. The recommendation is to not turn on debug level for logging in production networks during normal hours. |
| 47868 | The name option under the netdestination6 alias option is not available.<br>**Workaround:**<br>Provide the host/network IP address instead of a name. |
| 50396 | `Deny-inter-user-bridging` does not block the IPv6 traffic between the untrusted clients on the same VLAN.<br>**Workaround:**<br>None. |
| 59925, 61118 | The command `show user` incorrectly displays wired users coming from a port channel or GRE tunnel as wireless users.<br>**Workaround:**<br>None. |

**Table 23** *Security Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 60152 | Very intermittently, wireless clients fail to complete 802.1x authentication after association and they become stuck at eap-term-start and show failure in auth-tracebuff. This occurs when termination is enabled on the controller.<br>**Workaround:**<br>None. |
| 63008, 63011 | In some cases, when an in-use CA certificate is allowed to expire, then deleted and replaced with a new one, clients may not be able to authenticate. Additionally, the reference counter for the replaced certificate shows zero (0) when there is a dot1x profile referencing the certificate.<br>**Workaround:**<br>Use the `write mem` command to complete the process. |
| 55629 | RAPs are not able to associate with dot1x clients if the username entry in the local DB has more than 31 characters.<br>**Workaround:**<br>Change the username to have 31 characters or less. |
| 56932 | You cannot add a single netdestination for all multicast addresses using 240.0.0.0 as the netmask. 240.0.0.0 will be read as an invalid input. For example:<br>`(config-test) #network 224.0.0.0 240.0.0.0`<br>`^`<br>`% Invalid input detected at '^' marker.`<br>**Workaround:**<br>None. |
| 54413, 55132 | The following error messages appear in the syslog while SNMP is trying to obtain that user's user entry:<br>`snmp_handle_new_user_request:550: Failed to get SOS user entry for SNMP.`<br>**Workaround:**<br>None. |
| 56588 | Per-vlan aaa profiles do not work if a station-table entry exists with the same MAC address as a client but with different aaa profile assigned when the client's traffic first hit the controller's untrusted port.<br>**Workaround:**<br>None. |
| 54224 | With tunnel mode WPA2 SSIDs and CPSec enabled on those SSIDs, after times of very low traffic, the controller blocks users from associating. Additionally, WPA2 key exchange failures are seen in the syslog.<br>**Workaround:**<br>Rebooting the controller solves the issue temporarily, disabling CPSec solves it permanently. |
| 53957, 54024, 54787, 57113, 57110 | When attempting to connect via captive portal, if the auth module and datapath are out of sync, users receive the `Web Authentication disabled. Please contact the administrator for assistance` warning message.<br>**Workaround:**<br>You must delete the aaa users in question from the user-table and have them reconnect. |
| 55898 | The command `show user` does not display the correct information for captive portal users when those users are connected through an L3 gateway.<br>**Workaround:**<br>None. |

**Table 23** *Security Known Issues and Limitations (Continued)*

| Bug ID | Description |
|---|---|
| 56503 | The username shown in the user table is the client's dot1x username instead of the captive portal username when the client disconnects and then reassociates.<br>**Workaround:**<br>None. |
| 56782 | Split-tunnel captive portal does not work in RAP behind RAP configuration. In tunnel mode, a client is able to reach the captive portal logon page and authenticate while, in split-tunnel mode, the client is unable to reach the logon page.<br>**Workaround:**<br>None. |
| 57500 | Custom captive portal login pages do not work when guest logon is enabled. The guest logon field is not displyed on the custom login page. This issue does not occur with the default Aruba login page.<br>**Workaround:**<br>Use the default captive portal page or use user logon. |
| 55375 | In rare cases, RAPs are not able to communicate with the controller. The RAP stays in the down state as seen in AP database on the controller.<br>**Workaround:**<br>Manually reboot the AP. |

## SNMP

**Table 24** *SNMP Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 52186 | The IfHCInOctets and ifHCOutOctets 64 bit counters rolls over at 32-bit boundary on M3 if the packet counters (octets) exceed 32 bits.<br>**Workaround:**<br>None. |

## Station Management

**Table 25** *Station Management Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62365 | The stm module crashes with signatures pointing to `mm_retrieve_stats`.<br>**Workaround:**<br>None. |

## Syslog

**Table 26** *Syslog Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62916 | Access Points may send debug log messages to the Syslog server, even if debug log messages are disabled.<br>**Workaround:**<br>None. |

## Tunneled-Node

**Table 27** *Tunneled-Node Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 61148 | ArubaOS does not allow a tunneled-node client and tunneled-node server to co-exist on the same controller at the same time. The controller must be configured as either a tunneled-node client or a tunneled-node server. By default, the Aruba controller behaves as a tunneled-node server. However, once `tunneled-node-server xxx.xxx.xxx.xxx` is configured on the controller, the controller becomes a tunneled-node client.<br>**Workaround:**<br>To remove the tunneled-node client function, use the command `tunneled-node-server 0.0.0.0` to disable the tunneled-node client on the controller side. |

## Voice

**Table 28** *Voice Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 62413 | The RTP sessions created by VOIP ALGs are deleted if the **`prohibit RST replay`** knob is enabled.<br>**Workaround:**<br>Turn off Prohibit RST replay attack knob in global firewall settings. |
| 56506 | SIP ALG might generate an additional CDR with invalid data when DELTS is received while terminating the call. Additionally, an invalid entry is added to the voice call quality table as well. This is a CLI issue and does not impact functionality.<br>**Workaround:**<br>None. |
| 55058 | Sometimes the CLI output doesn't show the Lync clients getting tagged with the high priority ToS value. This is a CLI display issue and doesn't affect the functionality. It has been seen with Lync clients taking part in conference calls. This issue does not occur with peer-to-peer calls.<br>**Workaround:**<br>None. |

## VRRP

**Table 29** *VRRP Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 55764 | VRRP instances on a standby master controller are not placed in the backup state by default. This may create active instances on standby and the local will try to establish connection with standby master, which will fail.<br>**Workaround:**<br>None. |

## WebUI

**Table 30** *WebUI Known Issues and Limitations*

| Bug ID | Description |
|---|---|
| 55040 | On the WebUI, the U600 modem in the 4G option is missing from the **Wireless > AP Installation > Provisioning Profile** preventing you from creating a provisioning profile for the U600 in 4G.<br>**Workaround:**<br>Either create a provisioning profile with 4G parameters (i.e. usb_type = “beceem-wimax”) from the command line and apply that profile to the ap-group.<br>OR,<br>Choose the correct device type in the USB settings of the AP Installation page through WebUI. |

# Chapter 5

# Upgrade Procedures

This chapter details software and hardware upgrade procedures. Aruba best practices recommend that you schedule a maintenance window when upgrading your controllers.

CAUTION

Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:



NOTE

All versions assume that you have upgraded to the most recent version as posted on the Aruba download site. For instance, 6.0.x assumes you have upgraded to the most recent version of 6.0.

## Important Points to Remember

Upgrading your Aruba infrastructure can be confusing. To optimize your upgrade procedure, take the actions listed below to ensure your upgrade is successful. You should create a permanent list of this information for future use.

- Best practice recommends upgrading during a maintenance window. This will limit the troubleshooting variables.
- Please check the available memory and free disk space requirements prior to upgrading the controller using the WebUI (Install ArubaOS 6.1.3 using the WebUI) or using the CLI (Install ArubaOS 6.1.3 using the CLI).
- Verify your current ArubaOS version (execute the **show version, show image version,** or the **show switches** command).
- Verify which services you are using for each controller (for example, Employee Wireless, Guest Access, Remote AP, Wireless Voice).

- Verify the exact number of access points (APs) you have assigned to each controller.
- List which method each AP uses to discover each controller (DNS, DHCP Option, broadcast), and verify that those methods are operating as expected.
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- List the devices in your infrastructure that are used to provide your wireless users with connectivity (Core switches, radius servers, DHCP servers, firewall, for example).

## Technical Upgrading Best Practices

- Know your topology. The most important path is the connectivity between your APs and their controllers. Connectivity issues will interfere with a successful upgrade. You must have the ability to test and make connectivity changes (routing, switching, DHCP, authentication) to ensure your traffic path is functioning.
- Avoid combining a software upgrade with other upgrades; this will limit your troubleshooting variables.
- Avoid making configuration changes during your upgrade.
- Notify your community, well in advance, of your intention to upgrade.
- Verify that all of your controllers are running the same software version in a master-local relationship. The same software version assures consistent behavior in a multi-controller environment.
- Use FTP to upload software images to the controller. FTP is much faster then TFTP and also offers more resilience over slower links.

NOTE

If you must use TFTP, ensure that your TFTP servers can send more than 30 MB of data.

- Always upgrade the non-boot partition first. If something happens during upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.

## WIP Configuration Changes in Version 6.0

New configuration parameters were added in ArubaOS 6.0. When you upgrade from an ArubaOS version prior to 6.0 to ArubaOS 6.1, new parameters will automatically be added to their respective profiles and given their default value.

If the default value of an existing parameter changed in versions prior to ArubaOS 6.0, profiles using the default value will automatically be changed to use the new default value. If your configuration uses a non-default value prior to upgrade, the value will not be modified during the upgrade process. The following default values were changed:

Detect AP Impersonation—changed from **True** to **False**

Detect Adhoc Network— changed from **True** to **False**

Detect Wireless Bridge—changed from **True** to **False**

Detect 40MHz Intol—changed from **True** to **False**

Detect Active Greenfield mode—changed from **True** to **False**

### WIP Predefined Profiles

Except for predefined profiles IDS Rate Thresholds and IDS Signature, all IDS predefined profiles were deprecated in ArubaOS 6.0. Mapping the deprecated profiles are handled as follows:

- If a predefined profile is referenced by default from another profile, the reference will point to the new default instance of the profile
- If a predefined profile is referenced explicitly (that is, you changed from the default value so that it points to a predefined profile), after the upgrade the reference will point to a profile which is an editable clone of the predefined profile. That profile is named similarly to the predefined profile, except the word "transitional" is inserted after "ids-"

### Wireless Containment Parameter

The wireless-containment parameter in the ids-general-profile went from an enabled/disabled knob to an enumeration (none, deauth-only, tarpit-non-valid-sta, tartip-all-sta).

- If the parameter was set to *enabled* (its default value), the upgrade will render the value as *deauth-only* (the new default value)
- If the parameter was set to *disabled*, the upgrade will render the value as *none*

### Signature Matching profile Default Instance

The default instance of the signature matching profile in ArubaOS contain references to 2 predefined signatures: Deauth-Broadcast and Disassoc-Broadcast (a new signature in 6.0). The default instance of this profile was empty prior to 6.0.

- If the profile was empty, the upgrade will render the profile with both predefined signatures.
- If the profile was not empty, the upgrade will add references to the 2 predefined signatures, if they are not already there.

### WIP Logging Changes

In ArubaOS 6.0, all WIP logs related to intrusion detection and protection are in the 'security' logging category. Previously, most WIP logs were generated under the Wireless Logging category. Many of the logs that were previously generated at the Error level have been moved to the Warning level. In the security logging category, two new subcategories are added:

- The 'ids' subcategory contains 'correlated' WIP logs.
- The 'ids-ap' subcategory contains WIP logs generated by the APs (uncorrelated).

Both of these new WIP logging subcategories: 'ids' and 'ids-ap' are enabled at the Warning level by the upgrade. However, by default, AP logging of WIP events is disabled and correlation of WIP logs is enabled.

## Basic Upgrade Sequence

Testing your clients and ensuring performance and connectivity is probably the most time-consuming part of the upgrade. Best practices recommends that you enlist users in different locations to assist with the validation before you begin the upgrade. The list below is an overview of the upgrade and validation procedures.

NOTE

If you manage your controllers via the AirWave Wireless Management Suite, the AirWave upgrade process automates most of these steps.

1. Upload the same version of the new software image onto all controllers.
2. Reboot all controllers simultaneously.
3. Execute the **ping -t** command to verify all your controllers are up after the reboot.
4. Open a Secure Shell session (SSH) on your Master Controller.
5. Execute the **show ap database** command to determine if your APs are up and ready to accept clients.

6. Execute the **show ap active** to view the up and running APs.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed up and running.

   The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table** *<access point ip address>* command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.

## Managing Flash Memory

All Aruba controllers store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your WLAN network, Aruba recommends the following compact flash memory best practices:

- Do not exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan or VisualRF Plan can consume flash space quickly.

  Warning messages alert you that the file system is running out of space if there is a write attempt to flash and 5 Mbytes or less of space remains.

Other tasks which are sensitive to insufficient flash file system space include:

- DHCP lease and renew information is stored in flash. If the file system is full, DHCP addresses can not be distributed or renewed.
- If a controller encounters a problem and it needs to write a log file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost

CAUTION

In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before rebooting.

## Before you upgrade

You should ensure the following before installing a new image on the controller:

- Make sure you have at least 85 MB of free compact flash space (**show storage** command).
- Run the **tar crash** command to ensure there are no “process died” files clogging up memory and FTP/TFTP the files to another storage device.
- Remove all unnecessary saved files from flash (**delete filename** command).

### Backing up Critical Data

It is important to frequently back up all critical configuration data and files on the compact flash file system to an external server or mass storage facility. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs

- Customer captive portal pages
- Customer x.509 certificates

### Backup and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to back up and restore the entire compact flash file system. The following steps describe how to back up and restore the compact flash file system using the WebUI on the controller:

1. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz.
3. Click **Copy Backup** to copy the file to an external server.

   You can later copy the backup file from the external server to the Compact Flash file system by navigating to the **Maintenance > File > Copy Files** page.
4. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

### Backup and Restore Compact Flash in the CLI

The following steps describe the back up and restore procedure for the entire Compact Flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller. Use the **backup** command to back up the contents of the Compact Flash file system to the file flashbackup.tar.gz:

   ```
   (host) # backup flash
   Please wait while we tar relevant files from flash...
   Please wait while we compress the tar file...
   Checking for free space on flash...
   Copying file to flash...
   File flashbackup.tar.gz created successfully on flash.
   ```
2. Use the **copy** command to transfer the backup flash file to an external server:

   ```
   (host) copy flash: flashbackup.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
   <remote directory>
   ```

   You can later transfer the backup flash file from the external server to the Compact Flash file system with the copy command:

   ```
   (host) # copy tftp: <tftphost> <filename> flash: flashbackup.tar.gz
   ```
3. Use the **restore** command to untar and extract the *flashbackup.tar.gz* file to the Compact Flash file system:

   ```
   (host) # restore flash
   ```

## Licensing Change History and Mapping

License consolidation and even renaming of licenses occur over time. The following changes and/or consolidations were made to the ArubaOS licensing.

### ArubaOS 6.1

- The VIA feature now requires a PEFV license (Policy Enforcement Firewall Virtual Private Network).
- The Walled Garden feature requires the PEFNG or PEFV license.

- Advanced Cryptography License (ACR) is introduced—the ACR license is required for the Suite B Cryptography in IPsec and 802.11 modes. License enforcement behavior controls the total number of concurrent connections (IPsec or 802.11) using Suite B Cryptography.

### ACR Interaction

- On a platform that supports 2048 IPsec tunnels, the maximum number of Suite B IPsec tunnels supported is 2048, even if a larger capacity license is installed.
- An evaluation ACR license is available (EVL-ACR-8192). You can install the ACR evaluation license with a higher capacity than the platform maximum.
- On a platform that supports 2048 IPsec tunnels, with a LIC-ACR-512 installed, only 512 IPsec tunnels can be terminated using Suite B encryption. An additional 1536 IPsec tunnels, using non-Suite B modes (e.g. AES-CBC), can still be supported.
- On a platform with LIC-ACR-512 installed, a mixture of IPsec and 802.11i Suite B connections can be supported. The combined number of these sessions may not exceed 512.
- A single client using both 802.11i Suite B and IPsec Suite B simultaneously will consume two ACR licenses.

## ArubaOS 6.0

- WIP license is changed to RFprotect and includes the WIP and Spectrum Analysis features.

## ArubaOS 5.0

Figure 1 is an up-to-date illustration of the consolidated licenses effective with this release.

- MAP was merged into base ArubaOS
- VPN was merged into base ArubaOS
- RAP was merged into AP license
- PEF (user basis) was converted to PEFNG (AP basis) with ArubaOS 5.0

## ArubaOS 3.4.1

- VOC was merged into PEF. This merge happened with ArubaOS 3.4.1
- IMP was merged into base ArubaOS

## ArubaOS 3.4.0

- ESI was merged into PEF

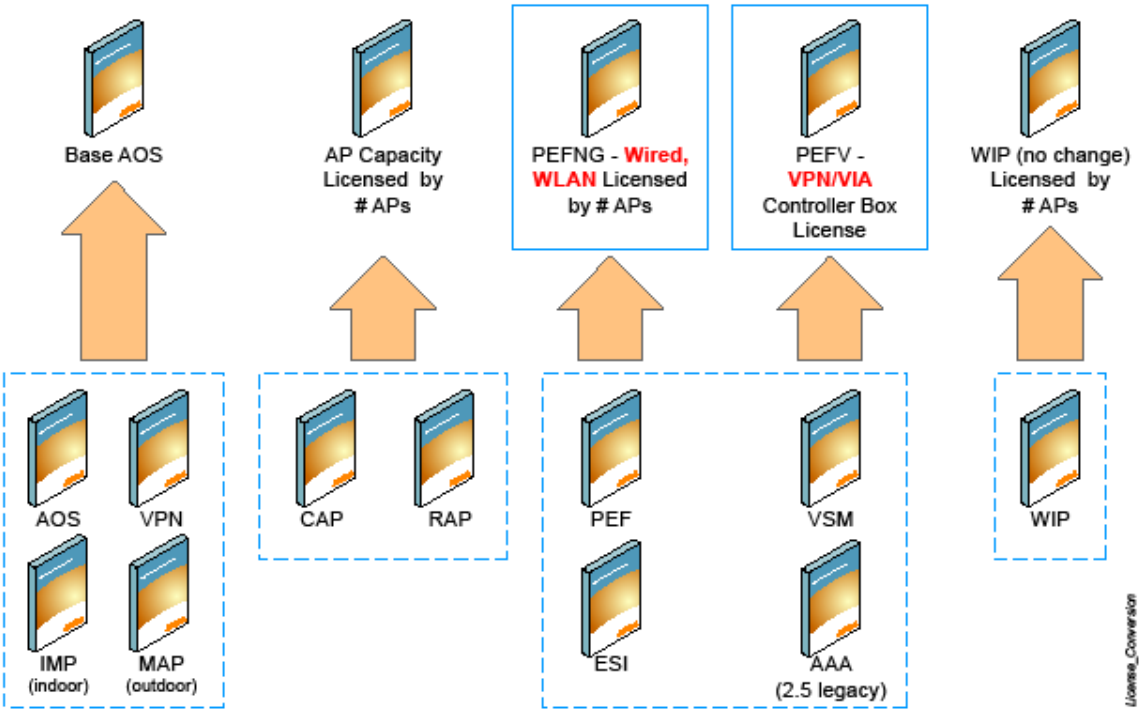
## ArubaOS Legacy and End-of-Life

- AAA was merged into ESI with the release of ArubaOS 2.5.3.
- CIM is End-of-life

NOTE

Releases older than ArubaOS 2.5.4 have been End-of-Lifed.

**Figure 1** *Licensing Consolidation ArubaOS 5.0*




## Upgrading from 5.0.x to 6.1

CAUTION

If you are running ArubaOS 5.0.3.1 (or later) you can directly upgrade to ArubaOS 6.1.3. However, upgrading from an ArubaOS version earlier than 5.0.3.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 5.0.4.x build before upgrading to ArubaOS 6.1.3.

If you are upgrading from 5.0.x to 6.1, your control plane security settings will be retained during the upgrade. If you had enabled the control plane security feature in ArubaOS 5.0, the feature will still be enabled after you upgrade to ArubaOS 6.1. If you to downgrade to ArubaOS 5.0, you will not need to disable control plane security

## Upgrading from 3.x to 6.1

If you are running ArubaOS 3.4.4.1 or a later version in the 3.4.4.x code stream, you can directly upgrade to ArubaOS 6.1.3. However, upgrading from a 3.x ArubaOS version earlier than 3.4.4.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 3.4.4.x build before upgrading to ArubaOS 6.1.3.

NOTE

All versions assume that you have upgraded to the most recent version as posted on the Aruba download site. For instance, 3.3.x assumes you have upgraded to the most recent version of 3.3.x.x.

# Upgrading from RN-3.x.x to 6.1

If you are upgrading from a release older than RN-3.x.x.x release, you must upgrade to the most recent version of ArubaOS 5.0.4.x build that is available on the support site before upgrading to ArubaOS 6.1.3.

NOTE

Once you have completed the upgrade to the latest version of ArubaOS 5.0.4.x, then follow the steps in "Install ArubaOS 6.1.3 using the WebUI" on page 57 to complete your last "upgrade hop".

## Caveat

Should you need to downgrade from ArubaOS 6.1, you can only downgrade to version RN-3.1.4 or higher.

# Upgrading from 6.0.x to 6.1.x

CAUTION

If you are running ArubaOS 6.0.1.0 (or later) you can directly upgrade to ArubaOS 6.1.3. However, upgrading from an ArubaOS version earlier than 6.0.1.0 requires an upgrade hop. You must first upgrade to the latest ArubaOS 6.0.1.x build before upgrading to ArubaOS 6.1.3.Read all the following information before you upgrade to ArubaOS 6.1.3.

Read all the following information before you upgrade to ArubaOS 6.1.3.


- "Caveats" on page 56
- "Load New Licenses" on page 56
- "Save your Configuration" on page 56
- "Install ArubaOS 6.1.3 using the WebUI" on page 57


## Caveats

Before upgrading to ArubaOS 6.1 take note of these known upgrade caveats.

- CPSEC is disabled when you upgrade from 3.4.x to 6.0.1(CPSEC is disabled in 6.0.1) and then to 6.1.
- If you want to downgrade to a prior version, and your current ArubaOS 6.1 configuration has control plane security enabled, disable control plane security before you downgrade.

  For more information on configuring control plane security and auto-certificate provisioning, refer to the *ArubaOS 6.1 User Guide*.

## Load New Licenses

Before you upgrade to ArubaOS 6.1, assess your software license requirements and load any new or expanded licenses you require prior to upgrading to ArubaOS 6.1.

Software licenses in ArubaOS 5.0 were consolidated and in some instances license names and modules were renamed to more accurately represent the modules supported by the licenses (see Figure 1).

For a detailed description of these new license modules, refer to the "Software Licenses" chapter in the user guide.

## Save your Configuration

Before upgrading, save your configuration and back up your controllers data files (see "Managing Flash Memory" on page 52). Saving your configuration saves the **admin** and **enable** passwords in the proper format.

### Saving the Configuration in the WebUI

1. Click on the **Configuration** tab.
2. Click the **Save Configuration** button at the top of the screen.

### Saving the Configuration in the CLI

Enter the following command in enable or config mode:

(host) #write memory

## Install ArubaOS 6.1.3 using the WebUI

CAUTION

ArubaOS 6.x is supported only on the newer MIPS controllers (M3, 3000 and 600 series).
Legacy PPC controllers (200, 800, 2400, SC-I and SC-II) are *not* supported.
DO NOT upgrade to 6.x if your deployments contain a mix of MIPS and PPC controllers in a master-local setup.

CAUTION

When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence.(See "Upgrading in a Multi-Controller Network" on page 63.)

CAUTION

When upgrading the controller, the following is required:
- Using the CLI, confirm (**`show memory`**) that there is at least 75 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
- Confirm (**`show storage`**) that there is at least 75 MB of /flash available.
-If one of the above conditions are not true, you must delete files from the file system before attempting a local file upgrade. Run the dir command to list all files (or use **WebUI > Maintenance > Files**). Delete all unnecessary files including crash files and logs.tar file. To ensure that all temporary (crash) files are removed, perform a tar crash and then remove the crash.tar file from the controller.

CAUTION

You can directly upgrade to ArubaOS 6.1.3 if you are running one of the following 6.0.x releases: [6.0.1.0, 6.0.1.2, 6.0.1.2, 6.0.1.3, or 6.0.1.x]. However, upgrading from a version of ArubaOS 6.0.0.0 or 6.0.0.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 6.0.1.x build before upgrading to ArubaOS 6.1.3. Read all the following information before you upgrade to ArubaOS 6.1.3.

CAUTION

You can directly upgrade to ArubaOS 6.1.3 if you are running one of the following 5.0.x releases: [5.0.3.1, 5.0.3.2, 5.0.3.3, or 5.0.4.x]. However, upgrading from an ArubaOS version earlier than 5.0.3.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 5.0.4.x build before upgrading to ArubaOS 6.1.3. Read all the following information before you upgrade to ArubaOS 6.1.3.

The following steps describe how to install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. If you are running an ArubaOS 3.x.x.x version earlier than ArubaOS 3.4.4.1, you must download the latest version of ArubaOS 3.4.4.x. Then proceed to Step 4.
2. If you are running:
   a. Any ArubaOS RN-3.x.x version, or
   b. ArubaOS 5.0.x.x version earlier than ArubaOS 5.0.3.1, you must download the latest version of ArubaOS 5.0.4.x. Then proceed to Step 4
3. If you are running ArubaOS versions 6.0.0.0 or 6.0.0.1, you must download the latest version of ArubaOS 6.0.1.x.
4. Download ArubaOS 6.1.3 from the customer support site.
5. Upload the new software image(s) to a PC or workstation on your network.
6. Log in to the WebUI from the PC or workstation.
7. Navigate to the **Maintenance>Controller>Image Management** page. Select the **Upload Local File** option, then click **Browse** to navigate to the image file (saved in Step 1 - 4) on your PC or workstation.

   **OPTION 1:** If upgrading from an ArubaOS 3.x.x.x version earlier than 3.4.4.1:

   a. Select the 3.4.4.x image file downloaded in Step 1.
   b. Follow the procedure in Steps 8 - 12.

   **OR**

   **OPTION 2:** If upgrading from any ArubaOS RN-3.x.x version or an ArubaOS 5.0.x.x earlier than 5.0.3.1:

   a. Select the 5.0.4.x image file downloaded in Step 2.
   b. Follow the procedure in Steps 8 - 12.

   **OR**

   **OPTION 3:** If upgrading from ArubaOS versions 6.0.0.0 or 6.0.0.1:

   a. Select the 6.0.1.x image file downloaded in Step 3.
   b. Follow the procedure in Steps 8 - 12.

   **OR**

   **OPTION 4:** If upgrading from any of the following ArubaOS versions:

   - 3.4.4.1 or the latest 3.4.x.x
   - 5.0.3.1 or the latest 5.0.x.x—Review "Upgrading With RAP-5s and RAP-5WNs" on page 59 before proceeding further
   - 6.0.1.0 or the latest 6.0.x.x
   - 6.1.2.0 or the latest 6.1.2.x

   a. Select the ArubaOS 6.1.3 image file downloaded in Step 4.
   a. Follow the procedure in Steps 8 - 12.
8. Make sure you select the non-boot **partition to upgrade**. To see the current boot and non-boot partitions, navigate to the **Maintenance>Controller>Boot Parameters** page.
9. Select **Yes** for **Reboot Controller After Upgrade**.
10. Click **Upgrade**.
11. When the software image is uploaded to the controller, a popup appears. Click **OK** in the popup window. The reboot process starts automatically within a few seconds (unless you cancel it).

12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring>Controller>Controller Summary** page to verify the upgrade, including country code. The **Country** field displays the country code configured on the controller.

> **NOTE**
> If the ArubaOS version on the Controller Summary page shows 6.1.3, the upgrade is completed. Proceed with Step 13 to verify that all the APs are up and active and that clients are able to connect to the APs and can access resources successfully.

13. Execute the **ping -t** command to verify all your controllers are up after the reboot.
14. Open a Secure Shell session (SSH) on your Master Controller.
15. Execute the **show ap database** command to determine if your APs are up and ready to accept clients.
16. Execute the **show ap active** to view the up and running APs.
17. Cycle between step 15 and step 16 until a sufficient amount of APs are confirmed up and running.

    The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table** *<access point ip address>* command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
18. Verify that the number of access points and clients are what you would expected.
19. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.
20. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See "Backing up Critical Data" on page 52 for information on creating a backup.
21. Repeat steps 7 (option 4) through 20 to complete the upgrade to ArubaOS 6.1.3.

## Upgrading With RAP-5s and RAP-5WNs

If you have completed the first upgrade hop to the latest ArubaOS 5.0.4.x version, and your WLAN includes RAP-5/RAP-5WN, do not proceed until completing the following process. Once complete, proceed to step 21 on page 59.

1. Check the provisioning image version on your RAP-5/RAP-5WN Access Points by executing the following command:

   ```
   show ap image version
   ```
2. If the Flash (Provisioning/Backup) Image Version String shows the letters "rn" for example as 3.3.2.11-rn-3.0, note down those AP names and IP addresses.
3. For each of the RAP-5/RAP-5WN noted in the step-ii, upgrade the provisioning image on the backup flash partition by executing the following command:

   ```
   apflash ap-name <Name_of_RAP> backup-partition
   ```

   The RAP-5/RAP-5WN will reboot to complete the provisioning image upgrade.
4. When all the RAP-5/RAP-5WN with a 3.3.2.x-based RN provisioning image have successfully upgraded, verify that the provisioning image by executing the following command:

   ```
   show ap image version
   ```

   The Flash (Provisioning/Backup) Image Version String should now show for example 5.0.3.3 and not contain the letters "rn".
5. If you omit the above process or fail to complete the Flash (Provisioning/Backup) Image upgrade to 5.0.4.x and the RAP-5/RAP-5WN was reset to factory defaults, the RAP will not be able to connect to the controller running 6.1.2.x and upgrade its production software image.

## Install ArubaOS 6.1.3 using the CLI

CAUTION

When upgrading the controller, the following is required:
- Confirm (`show memory`) that there is at least 60 MB of free memory available. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up upgrade immediately.
- Confirm (`show storage`) that there is at least 85 MB of /flash available.
- If one of the above conditions are not true, you must delete files from the file system before attempting a local file upgrade. Run the dir command to list all files (or use WebUI>Maintenance>Files). Delete all unnecessary files including crash files and logs.tar file. To ensure that all temporary (crash) files are removed, perform a tar crash and then remove the crash.tar file from the controller.

CAUTION

You can directly upgrade to ArubaOS 6.1.3 if you are running one of the following 6.0.x releases: [6.0.1.0, 6.0.1.2, 6.0.1.2, 6.0.1.3, or 6.0.1.x]. However, upgrading from a version of ArubaOS 6.0.0.0 or 6.0.0.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 6.0.1.x build before upgrading to ArubaOS 6.1.3. Read all the following information before you upgrade to ArubaOS 6.1.3.

CAUTION

You can directly upgrade to ArubaOS 6.1.3 if you are running one of the following 5.0.x releases: [5.0.3.1, 5.0.3.2, 5.0.3.3, or 5.0.4.x]. However, upgrading from any ArubaOS RN-3.x.x version or ArubaOS 5.0.x.x version earlier than 5.0.3.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 5.0.4.x build before upgrading to ArubaOS 6.1.3. Read all the following information before you upgrade to ArubaOS 6.1.3.

CAUTION

You can directly upgrade to ArubaOS 6.1.3 if you are running one of the following 3.4.4.x releases: [3.4.4.1, 3.4.4.2, 3.4.4.3, or a later 3.4.x.x]. However, upgrading from an ArubaOS 3.x.x.x version earlier than 3.4.4.1 requires an upgrade hop. You must first upgrade to the latest ArubaOS 3.4.x.x build before upgrading to ArubaOS 6.1.3. Read all the following information before you upgrade to ArubaOS 6.1.3.

Follow these steps to upgrade a controller to ArubaOS version 6.1 using the CLI.

1. There are 4 upgrade paths to ArubaOS 6.1.3. Depending on the current ArubaOS version running on the Aruba controller(s), you will have to perform an upgrade hop as explained in options 1 to 4.

**Option 1:** If upgrading from an ArubaOS 3.x.x.x version earlier than 3.4.4.1:

a. Download the latest version of ArubaOS 3.4.4.x

b. Upgrade to ArubaOS 3.4.4.x using the CLI upgrade process in the ArubaOS 3.4.4.x Release Notes

**OR**

**Option 2:** If upgrading from

- Any ArubaOS RN-3.x.x version, or
- ArubaOS 5.0.x.x version earlier than 5.0.3.1,

a. Download the latest version of ArubaOS 5.0.4.x

b. Upgrade to ArubaOS 5.0.4.x using the CLI upgrade process in the ArubaOS 5.0.4.x Release Notes

NOTE

Review "Upgrading With RAP-5s and RAP-5WNs" on page 59 before proceeding to upgrade to ArubaOS 6.1.3

**OR**

**Option 3:** If upgrading from ArubaOS versions 6.0.0.0 or 6.0.0.1:

a. Download the latest ArubaOS 6.0.1.x version

b. Upgrade to ArubaOS 6.0.1.x using the CLI upgrade process in the ArubaOS 6.0.1.x Release Notes

c. Follow the procedure in Steps 8 - 12.

**OR**

**Option 4:** If upgrading from any of the following ArubaOS versions

- 3.4.4.1 or the latest 3.4.x.x
- 5.0.3.1 or the latest 5.0.x.x —Review "Upgrading With RAP-5s and RAP-5WNs" on page 59 before proceeding further
- 6.0.1.0 or the latest 6.0.1.x
- 6.1.2.0 or the latest 6.1.2.1

Proceed with step 2

2. Download ArubaOS 6.1.3 from the customer support site.
3. From a laptop/desktop, execute the **ping -t** command to verify all your controllers are up after the reboot following the first upgrade hop in Step 1.
4. Open a Secure Shell session (SSH) on your Master (and Local) Controller(s).
5. Execute the **show ap database** command to determine the state of all your APs.
6. Execute the **show ap active** command to view the already up and running APs ready to accept clients.
7. Cycle between step 5 and step 6 until a sufficient amount of APs are confirmed to be up and running. The **show ap database** command displays all of the APs, up or down. If some access points are down, execute the **show datapath session table <access point ip address>** command and verify traffic is passing. If not, attempt to ping them. If they still do not respond, execute a **show ap database long** command to view the wired mac address of the AP; locate it in your infrastructure.
8. Verify that the number of access points and clients are what you would expect.
9. Test a different type of client for each access method (802.1x, VPN, Remote AP, Captive Portal, Voice) and in different locations when possible.
10. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See "Backing up Critical Data" on page 52 for information on creating a backup.
11. Use the following command to check the current running ArubaOS version:

```
(hostname)# show version
Aruba Operating System Software.
ArubaOS (MODEL: 3200-US), Version 6.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-03-09 at 09:11:59 PDT 6.1.0.0 (Digitally Signed - Production Build)

ROM: System Bootstrap, Version CPBoot 1.0.0.0 (build 21294)
Built: 2009-05-11 16:02:29
Built by: p4build@re_client_21294

Switch uptime is 46 days 9 hours 57 minutes 10 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLS 204 (revision A1) with 907M bytes of memory.
32K bytes of non-volatile configuration memory.
```

```
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

12. Execute the **ping** command to verify the network connection from the target controller to the FTP/TFTP server:

```
(hostname)# ping <ftphost>
```

or

```
(hostname)# ping <tftphost>
```

13. Make sure you load the new software image onto the non-boot partition. The active boot partition is marked as “Default boot.”
14. Use the following command to check the ArubaOS images loaded on the controller's flash partitions:

```
(hostname) #show image version
----------------------------------
Partition               : 0:0 (/dev/mtdblock9) **Default boot**
Software Version        : ArubaOS 5.0.3.3
Build number            : 28008
Label                   : 28008
Built on                : Thu Apr 21 12:09:15 PDT 2011
----------------------------------
Partition               : 0:1 (/dev/mtdblock10)
Software Version        : ArubaOS 5.0.3.0
Build number            : 26207
Label                   : 26207
Built on                : Tue Nov 30 08:35:45 PST 2010
```

15. Use the **copy** command to load the new image onto the controller:

```
(hostname)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
```

or

```
(hostname)# copy tftp: <tftphost> <image filename> system: partition 1
```

16. Execute the **show image version** command to verify the new image is loaded:

```
(hostname)# show image version
----------------------------------
Partition               : 0:0 (/dev/mtdblock9)
Software Version        : ArubaOS 5.0.3.3
Build number            : 28008
Label                   : 28008
Built on                : Thu Apr 21 12:09:15 PDT 2011
----------------------------------
Partition               : 0:1 (/dev/mtdblock10) **Default boot**
Software Version        : ArubaOS 6.1.3
Build number            : 29381
Label                   : 29381
Built on                : Fri Jul 23 00:03:14 PDT 2011
```

17. Reboot the controller:

```
(hostname)# reload
```

18. Execute the **show version** command to verify the upgrade is complete.

```
(hostname)# show version
Aruba Operating System Software.
ArubaOS (MODEL: 3200-US), Version 6.1.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-03-09 at 09:11:59 PDT 6.1.0.0 (Digitally Signed - Production Build)

ROM: System Bootstrap, Version CPBoot 1.0.0.0 (build 23274)
Built: 2010-01-19 11:11:41
Built by: p4build@re_client_23274

Switch uptime is 4 minutes 24 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLS 204 (revision A1) with 890M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

19. Repeat Steps 5 through 10 to verify the WLAN is up and running.

## Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in "Backing up Critical Data" on page 52.

NOTE

For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to ArubaOS 6.1.3:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and reloaded simultaneously, use the following guidelines:
   a. Remove the link between the master and local mobility controllers.
   b. Upgrade the software image, then reload the master and local controllers one by one.
   c. Verify that the master and all local controllers are upgraded properly.
   d. Connect the link between the master and local controllers.

### Pre-shared Key for Inter-Controller Communication

A pre-shared key (PSK) is used to create IPSec tunnels between a master and backup master controllers and between master and local controllers. These inter-controller IPSec tunnels carry management traffic such as mobility, configuration, and master-local information.

NOTE

An inter-controller IPSec tunnel can be used to route data between networks attached to the controllers. To route traffic, configure a static route on each controller specifying the destination network and the name of the IPSec tunnel.

There is a default PSK to allow inter-controller communications, however, for security you need to configure a a unique PSK for each controller pair. You can use either the WebUI or CLI to configure a 6-64 character PSK on master and local controllers.

CAUTION

Do not use the default global PSK on a master or standalone controller. If you have a multi-controller network then configure the local controllers to match the new IPSec PSK key on the master controller. Leaving the PSK set to the default value exposes the IPSec channel to serious risk, therefore you should always configure a unique PSK for each controller pair.

## Downgrading after an Upgrade

If necessary, you can return to your previous version of ArubaOS.

WARNING

If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. Any new entries that were created in ArubaOS 6.1.3 will be lost after downgrade (this warning does not apply to upgrades from 3.4.x to 6.1),

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Verify that Control Plane Security (CPSec) is disabled.
2. Set the controller to boot with the previously-saved pre-6.1 configuration file.

CAUTION

If you do not use a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from 6.1.3 to 5.0.3.2, due to changes made to WIPS in 6.x, the new predefined IDS profile assigned to an AP group will not be recognized by the older version of ArubaOS. This unrecognized profile will prevent associated APs from coming and display a profile error.

These new IDS profiles begin with ids-transitional while older IDS profiles do not include transitional. If you think you have encountered this, use the `show profile-errors` and `show ap-group commands` to view the IDS profile associated with AP Group.

3. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

NOTE

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file that will be used on the next controller reload. An error message displays if a system boot parameters are set for incompatible image and configuration files.

After downgrading the software on the controller:

- Restore pre-6.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.1.3 flash backup file.
- You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.1.3, the changes will not appear in RF Plan in the downgraded ArubaOS version.
- If you installed any certificates while running ArubaOS 6.1.3, you need to reinstall the certificates in the downgraded ArubaOS version.

The following sections describe how to use the WebUI or CLI to downgrade the software on the controller.

Be sure to back up your controller before reverting the OS.


When reverting the controller software, whenever possible use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

## Downgrading using the WebUI

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
   a. For Source Selection, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
   b. For Destination Selection, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the saved pre-upgrade configuration file from the Configuration File menu.
   b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
   a. Enter the FTP/TFTP server address and image file name.
   b. Select the backup system partition.
   c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
   a. Select the system partition that contains the pre-upgrade image file as the boot partition.
   b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

## Downgrading using the CLI

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
or
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```

2. Set the controller to boot with your pre-upgrade configuration file.

```
# boot config-file <backup configuration filename>
```

3. Execute the **show image version** command to view the partition on which your previous software image is stored.

   In the following example, partition 0, the backup system partition, contains the backup release 5.0.3.3. Partition 1, the default boot partition, contains the ArubaOS 6.1.3 image:

```
#show image version
---------------------------------
Partition                : 0:0 (/dev/hda1)
Software Version         : ArubaOS 5.0.3.3 (Digitally Signed - Production Build)
Build number             : 20219
Built on                 : 2010-12-11 20:51:46 PST
---------------------------------
Partition                : 0:1 (/dev/hda2) **Default boot**
Software Version         : ArubaOS 6.1.2.0 (Digitally Signed - Production Build)
Build number             : 28864
Built on                 : 2011-06-22 2:11:59 PST 2011
```

NOTE

You cannot load a new image into the active system partition (the default boot).

4. Set the backup system partition as the new boot partition:

```
# boot system partition 0
```

5. Reboot the controller:

```
# reload
```

6. When the boot process is complete, verify that the controller is using the correct software:

```
# show image version
```

## Controller Migration

This section outlines the steps involved in migrating from an Aruba PPC controller environment to MIPS controller environment. These steps takes into consideration the common Aruba WLAN controller environment. You must have an operational PPC controller in the environment when migrating to a new controller. The controllers are classified as:

- MIPS Controllers—M3, 3000 Series, 600 Series
- PPC Controllers—200, 800, 2400, 5000 and SC1/SC2

NOTE

Use this procedure to upgrade from one Aruba controller model to another. Take care to ensure that the new controller has equal or greater capacity than the controller you are replacing and verify that your new controller supports the ArubaOS version you are migrating to.

Migration instructions include:


- "Single Controller Environment" on page 66
- "Multiple Master Controller Environment" on page 67
- "Master/Local Controller Environment" on page 67


### Single Controller Environment

A single controller environment is one active controller, or one master controller that may have standby master controller that backs up the master controller.

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

### Multiple Master Controller Environment

An all master environment is considered an extension of the single master controller. You can back up the master controllers with a standby controller. In an all master controller deployment, each master controller is migrated as if it were in a standalone single controller environment.

For every master-standby controller pair

- Replacing the standby controller—Does not require downtime
- Replacing the master controller—Requires downtime

### Master/Local Controller Environment

In a master/local environment, replace the master controller first and then replace the local controllers.

- Replacing the local standbys (when present)
- Replacing local controllers—one controller at a time

### Before You Start

You must have:

- Administrative access to the controller via the network
- Administrative access to the controller via the controller's serial port
- Pre-configured FTP/TFTP server that can be reached from the controller
- Aruba serial cable
- The ArubaOS version (same as the rest of the network)

### Basic Migration Steps

1. Ensure that the ArubaOS version on the newer controllers match the ArubaOS version on the rest of the controllers in your network.
2. Backup the old controller data and move the backup files to a safe place that is easily accessible through FTP/TFTP.
3. Physically swap the hardware (for example, mounting, cabling, power).
4. Initialize the new controller with the correct license.
5. Install the backed up data onto the new controller.
6. Test the new setup.

## Before You Call Technical Support

Before you place a call to Technical Support, please follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. Provide the syslog file of the controller at the time of the problem.

   Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture from the controller.

4. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have:
   - an outage in a network that worked in the past.
   - a network configuration that has never worked.
   - a brand new installation.
5. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration.
6. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless sniffer traces taken during the time of the problem.
10. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
11. Provide the controller site access information, if possible.