Aruba Central
Switch Configuration

a Hewlett Packard
Enterprise company

User Guide

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contents

Contacting Support

Table 1: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

This chapter provides an overview of the supported Aruba switches and describes the procedures for provisioning, configuring, monitoring, and troubleshooting switches from the Central UI.

Aruba Switches

The Aruba Switches enable secure, role-based network access for wired users and devices, independent of their location or application.

The switch operates as a wired access point when deployed with an Aruba Mobility Controller. As a wired access point, users and their devices are authenticated and assigned a unique role by the Mobility Controller. These roles are applied irrespective of whether the user is a Wi-Fi client, or is connected to a port on the Switch. The use of switch allows an enterprise workforce to have consistent and secure access to network resources based on the type of users, client devices, and connection method used.

Supported Switch Platforms

Central supports the following Aruba Switch platforms:

Table 2: *Supported Aruba Switches*

Switch Platform	Supported Software Versions on Central
Aruba 2930M Switch Series	WC.16.04.0004 or later
Aruba 2920 Switch Series	WB.16.02.0012 or later
Aruba 2930F Switch Series	WC.16.02.0012 or later
Aruba 3810 Switch Series	KB 16.03.0003 or later
Aruba 5400R Switch Series	KB.16.04.0008 or later
Aruba 2530 Switch Series	YA/YB 16.04.0008 or later
Aruba 2540 Switch Series	YC.16.02.0012 or later

Legacy Aruba Switch Platforms

Central also supports the following legacy Switch models:

- S1500-12P

- S1500-24P
- S2500-24P
- S3500-24T

Central supports the following ArubaOS software versions on the legacy Switch platforms:

- 7.3.2.6
- 7.4.0.3
- 7.4.0.4

Adding Switches to Central

Central supports zero touch provisioning of the devices. It automatically retrieves the devices associated to a customer account. To synchronize the devices from the inventory, click **Sync Now**. If the retrieval of devices is not complete or successful due to process errors, you can manually add the devices.

To manually add a device, complete the following steps:

1. Click **Global Settings** on the left pane.
2. Click **Devices & Subscriptions**. The **Device Provisioning** page is displayed.
3. Click **Add Devices**. The **Manually Add Devices** window opens.
4. Select one of the following device addition options:

Table 3: *Adding Devices*

Device Addition Option	Description
Aruba Activate Credentials	To retrieve all devices associated to an Activate user account: 1. Select **Aruba Activate Credentials** from the **Add devices using** drop-down list. 2. Enter the username and password of the Activate user account. 3. Click **Next**. The Activate account details and the total number of devices associated with this account are displayed. 4. To add all devices, click **Add <Number> Devices** button. The devices associated with the Activate account are retrieved and added to the list of devices displayed on the **Device Management** page. **NOTE:** You can use this option only once. After the devices are added, Central does not allow you to modify or re-import the devices using your Aruba Activate credentials. If you account is already mapped to an Aruba Activate account, contact Aruba support team.
Bulk addition of devices based on cloud activation key	To retrieve multiple devices from a single purchase order by providing the cloud activation key: 1. Note the Cloud Activation Key and MAC address of the device. To obtain these details: ■ For the Aruba switches, to view the MAC address and the serial number, run the **sh system | in Base** and **sh system | in Serial** commands at the CLI. ■ For legacy Switches, execute the **show inventory | include HW** and **show version** commands on the switch CLI. The activation key is enabled only if the switch has access to the Internet. 2. Select **Cloud Activation Key** from the **Add devices using** drop-down list. 3. Enter the **MAC address** and **Cloud Activation Key** of the device. 4. Click **Next**. 5. To continue adding devices, click **Add <x> Devices**. 6. To restart the device addition procedure, click **Start Again**.
Adding up to 32 devices	To manually add devices by using the serial number and MAC address of the device: 1. Select **Device List (Up to 32 Devices)** from the **Add device using** drop-down list. 2. Enter the MAC address and serial number of the device. 3. Click **Next**. The list of available devices is displayed. 4. Click **Add <x> Devices**.

The provisioning of the legacy Aruba switch fails when the provisioning process is interrupted during the initial booting and if the switch has a static IP address with no DNS server configured.

During Zero Touch Provisioning, the Aruba Switches can join Central only if they are running the factory default configuration, and have a valid IP address and DNS settings from a DHCP server.

If the switches ship with a version lower than the minimum supported firmware version, a factory reset may be required, so that the switch can initiate a connection to Central. For information, on the minimum firmware versions supported on the switches, see Aruba Switches.

Assigning Groups

After the switches are added in Central, you can assign the switches to groups. Central does not support configuring switches such as Aruba 5400R Switch Series and switch stacks through the UI. These devices can only be configured using templates. Therefore, these devices are assigned to the template groups by default.

Configuring Devices in Template Groups

Central allows you to configure devices using configuration templates or through the **Configuration** menu under **Network Management**. However, the Aruba 5400R Switch Series and switch stacks can be configured only by using the configuration templates.

You can set a group as a template group, so that a common configuration is applied for all devices in the group. For devices mapped to a template group, you can create a template with a standard set of CLI scripts, configuration commands, and variables. If a group is set as a template group, the configuration wizards for the devices in that group are disabled.

Creating a Template Group

To create a template group, complete the following steps:

1. Click the icon next to **All Groups** on the left pane.
2. Click **(+)** to create a new group. The **Create New Group** pane appears.
3. To use this group as a template group, select the **Set this group as a template group** check box.
4. Click **Save**.

Creating a Template

To create a template for the devices in a template group, complete the following steps:

1. Under the Network Management app, click **Configuration** > **Templates**. The **Templates** page opens.
2. Click **+** to add a new template.
3. Add the template name.
4. Select the device. You can create configuration templates for Instant APs and Switches.
5. To create a template, complete the following steps:
   a. Set the model and firmware version parameters to **ALL**.
   b. Add the CLI script content. Note the following points for adding contents to the template:
   - Ensure that the command text indentation matches the indentation in the running configuration.
   - The commands in the template are case-sensitive. The following example illustrates the case discrepancies that the users must avoid in templates and variable definitions.

```
trunk E1-E4 trk1 trunk
interface Trk1
  dhcp-snooping trust
  exit

trunk E1-E4 trk1 trunk
switch-interconnect trk1

trunk E5-E6 trk2 trunk
vlan 5
  name "VLAN5"
  untagged Trk2
  tagged Trk1
  isolate-list Trk1
  ip igmp forcedfastleave Trk1
  ip igmp blocked Trk1
  ip igmp forward Trk1
```

```
  forbid Trk1

loop-protect Trk2

trunk E1-E4 trk1 trunk
trunk E4-E5 trk2 trunk
spanning-tree Trk1 priority 4
spanning-tree Trk2 admin-edge-port

trunk A2-A4 trk1 trunk
igmp fastlearn Trk1

trunk E4-E5 trk2 trunk
ip source-binding 2 4.5.6.7 b05ada-96a4a0 Trk2

[no] ip source-binding trap OutOfResources

snmp-server mib hpSwitchAuthMIB ..

snmp-server mib hpicfMACsec unsecured-access ..

[no] lldp config <P-PORT-LIST> dot1TlvEnable ..

[no] lldp config <P-PORT-LIST> medTlvEnable ..

no lldp config <P-PORT-LIST> medPortLocation..

[no] lldp config <P-PORT-LIST> dot3TlvEnable ..

[no] lldp config <P-PORT-LIST> basicTlvEnable ..

[no] lldp config <P-PORT-LIST> ipAddrEnable <lldp-ip>

trunk-load-balance L4-based
trunk-load-balance L3-based
```

6. If Aruba Switch is selected as the device, perform one of the following tasks:
   - To create a single template for all Switch platforms and firmware versions, select **ALL**.
   - To create a template for a specific model and firmware version, select the Switch model and the firmware version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
7. If you are creating a template for Aruba Switches, ensure that the template contains the following mandatory information:
   - Header that includes a few lines of the **show running-config** command output.
   - Module information

   The following example shows the mandatory lines required in the template:

```
; J9727A Configuration Editor; Created on release #WB.16.03.0000x
; Ver #0e:73.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:2f
module 1 type j9727a
include-credentials
```

8. Click **OK**.

The variables configured for the Instant AP devices functioning as the VCs are replaced with the values configured at the template level.

For Instant APs, the template allows only one **per-ap settings** block and must have the **per-ap-settings %_sys_lan_**

mac% variable. The **per-ap-settings** block uses the variables for the individual APs. The general VC configuration uses variables for master AP to generate the final configuration from the provided template. Hence, Aruba recommends that you upload all variables for all devices in a cluster and change values as required for individual AP variables.

If any device in the cluster has any missing variables, the configuration push to those AP devices in the cluster fails. The audit trail for such instances shows the missing variables.

Editing a Template

To edit or delete a template, select the template row and click the edit or delete icon, respectively.

Sample Template

The following example shows the typical contents allowed in a template file for Instant APs:

```
organization %org%
virtual-controller-ip 1.1.1.1
syslog-level debug
syslog-level warn ap-debug
per-ap-settings %_sys_lan_mac%
hostname %hostname%
zonename %zonename%

wlan ssid-profile %ssid_name%
%if disable_ssid=true%
disable-ssid
%endif%
%if ssid_security=wpa2%
opmode wpa2-aes
%else%
opmode opensystem
%endif%

%if condition1=true%
routing-profile 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile 10.60.0.0 255.255.255.0 10.60.0.255
%endif%
%endif%
```

Managing Variable Files

The variable files consist of a set of configuration values defined for devices in the network.

For Instant APs, you can configure a variable file with a set of values defined for a specific AP device that functions as the VC in the network. When the variable file is uploaded, the configuration values are applied on the Instant AP devices in the cluster.

The following conditions apply to the variable files:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, %if var=100% is supported and %if 100=var% is not supported.
- The < or <= or > or >= operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as %if dpi_value > 2.8%, it is converted as %if dpi_value > 2 for comparison.
- The variable names should not include white space, and the **&** and **%** special characters. The variable names must match regular expression [a-zA-Z0-9_]. If the variables values with **%** are defined, ensure that the variable is surrounded by space. For example, *wlan ssid-profile %ssid_name%*.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended template and variable name is *wlan ssid-profile "emp ssid*", the template must be defined template as "*wlan ssid-profile %ssid_name%*" and variable as *"ssid_name": "\"emp ssid\""*.

Uploading Variable Files

To upload a variable file, complete the following steps:

1. Click **Download Sample Variables File**. Save the JSON file with the sample variables.
2. Edit the variable file to customize the definitions.
3. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
4. Click **Network Management** > **Configuration** > **Variables**. The **Variables** page opens.
5. Click **Upload Variables File** and select the variable file to upload.
6. Click **Open**. The content of the variable file is displayed in the **Variables** table.
7. To search for a variable, specify a search term and click the Search icon.

Downloading Variable Files

To download the variable file applied for the devices, click the download icon in the **Variables** table.

Sample Variable File

The following example shows the typical contents of a variable file for Instant APs:

```
{
"CK0036968": {
"_sys_serial": "CK0036968",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:7a",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_1"
},
"CJ0219729": {
"_sys_serial": "CJ0219729",
"ssid": "s1",
```

```
"_sys_lan_mac": "ac:a3:1e:cb:04:92",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_2"
},
"CK0112486": {
"_sys_serial": "CK0112486",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c8:29:76",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_3"
},
"CT0779001": {
"_sys_serial": "CT0779001",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c5:c6:b0",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_4"
},
"CM0640401": {
"_sys_serial": "CM0640401",
"ssid": "s1",
"_sys_lan_mac": "84:d4:7e:c4:8f:2c",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_6"
},
"CK0037015": {
"_sys_serial": "CK0037015",
"ssid": "s1",
"_sys_lan_mac": "ac:a3:1e:c5:db:d8",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_7"
},
```

```
"CK0324517": {
"_sys_serial": "CK0324517",
"ssid": "s1",
"_sys_lan_mac": "f0:5c:19:c0:71:24",
"vc_name": "test_config_CK0036968",
"org": "Uber_org_test",
"vc_dns_ip":"22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_8"
}
}
```


Check the audit trail (**All Groups** > **Maintenance** > **Audit Trail**) to troubleshoot issues pertaining to template-based configuration.

Configuring Switches in UI Groups

This section describes the configuration procedures for the switches in the UI groups:

- Configuring Switch Parameters on page 14
- Configuring Ports on page 15
- Configuring Access Policies on page 17
- Configuring VLANs on page 16
- Configuring DHCP Pools on page 18
- Applying Configuration Changes through CLI Snippets on page 19
- Configuring System Parameters for a Switch on page 19

Configuring Switch Parameters

You can export configurations from an existing Switch to a new Switch within the same group. In this case, the new configuration of the Switch overwrites the existing configuration (including the device override).

You can configure parameters of a Switch through the UI. By default, these parameters have the values configured using the Switch.

If the switch inherits the group configuration, the configuration parameters are already defined. However, if required, you can edit these parameters.

To view the configuration parameters for the Switch, complete the following steps:

1. Click **Configuration**.
   - To configure a legacy Aruba Switch, click **Switch-MAS**.
   - To configure other Aruba Switches, click **Switch-Aruba**.
2. Click **Switches**. The Switches page displays information described in the following table.

Table 4: *Switches Pane*

Name	Description
MAC Address	MAC address of the Switch
Hostname	Name of the host.
IP Assignment	Method of IP assignment as Static or DHCP.
IP Address	IP address for static IP assignment.
Netmask	Netmask for static IP assignment.
Default Gateway	Default gateway for static IP assignment.

3. To view the details of the switch, click the MAC address of the switch.
4. To edit the switch configuration parameters, click the edit icon.

Configuring Ports

To view the port details of a switch, complete the following steps:

1. Click **Configuration**.
   - To configure a legacy Aruba switch , click **Switch-MAS**.
   - To configure other Aruba switches, click **Switch-Aruba**.
2. Click **Ports**. The **Ports** page displays the list of ports configured on the switch.

For the legacy switches, the **Ports** page displays the following information:

Table 5: *Contents of the Ports Page for Legacy Switches*

Name	Description
Port Number	Indicates the number assigned to the switch port.
Admin Status	Indicates the operational status of the port.
Port Mode	Indicates the mode of operation. The port can be configured to function in Trunk or Access mode.
VLAN	Shows the VLAN to which the port is assigned. Based on the port mode, you can assign different types of VLAN. ■ For **Access** mode, an **Access VLAN** can be specified. ■ For **Trunk** mode, the **Native VLAN** and **Allowed VLAN** can be configured.
Power over Ethernet	Displays the enabled or disabled status of Power over Ethernet (PoE).

Name	Description
Auto Negotiation	Indicates the status of the Auto Negotiation. ■ If auto negotiation is enabled, the Speed and Duplex fields are automatically set to **Auto**. ■ If auto negotiation is disabled, the speed can be set to 10 Mbps, 100 Mbps, or 1 Gbps and the duplex mode can be set to half or full.
Speed/Duplex	Displays the speed and duplex configuration settings for the client traffic.
Trusted	Indicates if the port is trusted.

For the other Aruba switches, the **Ports** page displays the following information:

Table 6: *Contents of the Ports Page for Other Aruba Switches*

Name	Description
Port Number	Indicates the number assigned to the switch port.
Admin Status	Indicates the operational status of the port.
Power over Ethernet	Displays the enabled or disabled status of Power over Ethernet (PoE).
Access Policy (In)	Allows you to apply an existing access policy for the inbound traffic on the port.
Access Policy (Out)	Allows you to apply an existing access policy for the outbound traffic on the port.

3. To edit port details, click **Edit** and configure the port parameters.
4. Click **Save**.

Configuring VLANs

The Aruba switches support the following types of VLANs:

- Port-based VLANs — In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- Tag-based VLANs — In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.

The Aruba legacy switches such as the Mobility Access Switch also support the following types of VLANs.

- Voice VLANs — You can use voice VLANs to separate voice traffic from data traffic when the voice and data traffic are carried over the same Ethernet link.
- MAC-based VLANs — In the case of untrusted interfaces, you can associate a client to a VLAN based on the source MAC of the packet. Based on the MAC, you can assign a role to the user after authentication.

Adding VLAN Details

By default, all the ports in the Switches are assigned to VLAN 1. However, if the ports are assigned to different

VLANs, the VLANs page displays these details.

To add a VLAN, complete the following steps:

1. Click **Configuration**.
   - To configure a legacy Aruba switch , click **Switch-MAS**.
   - To configure other Aruba switches, click **Switch-Aruba**.
2. Click **VLANs**. The **VLANs** page is displayed.
3. Click + add a VLAN and configure the following parameters:
   - **ID**—The VLAN ID.
   - **Description**—A short description for VLAN.
   - **IP Address**—IP address of the VLAN interface.
   - **Netmask**—Netmask of the IP address of the VLAN interface.
   - **DHCP**— Slider for enabling DHCP pool associated with the VLAN.
   - **Access Policy (In)**—Access policy assignment to VLAN for the inbound traffic (vlan-in). The VLAN-IN rule is applied for the bridged and routed inbound packets on a VLAN.
   - **VLAN Port Mode**—Port mode to apply on the VLAN. To apply a port, complete the following steps:
     a. Select the port number.
     b. Select any of the following port modes:
     - **Tagged Ports**—Tagged ports if any. A tagged port will normally carry traffic for multiple VLANs from the switch to other network devices such as an upstream router or an edge switch.
     - **Untagged Ports**—Untagged ports if any. In case of untagged ports, the Ethernet frames are not VLAN tagged.

     c. Click **Apply**.
4. Click **OK**.

Editing the VLAN Details

To edit the VLAN details, select the VLAN row and click the edit icon.

Deleting VLAN Details

To delete the VLAN details, complete the following steps:

1. Ensure that the VLANs are not tagged to any ports.
2. Click the delete icon for the VLAN you want to delete.

VLAN 1 is the primary VLAN and cannot be deleted.

Configuring Access Policies

To restrict certain types of traffic on physical ports of ArubaSwitches, you can configure ACLs from the Central UI.

To create an access policy, complete the following steps:

1. Click **Configuration** > **Switch-Aruba**.
2. Click +. The **New Access Policy** pop-up opens.
3. Enter a name for the policy.
4. To add a rule to the access policy, click + under **Rules**, and configure the following parameters:

a. **Source**—Select a source of the traffic for which you want to an access rule.

b. **Destination**—Select a destination port.

c. **Protocol**—Select the type of network port or protocol.

d. **Action**—Allow or deny access as required.

5. Click **Ok**.

The access policies must be applied to a Switch port and the VLAN assigned to a port. For more information on, access policy assignment to ports and VLANs, see the following topics:

- Configuring Ports on page 15
- Configuring VLANs on page 16

Configuring DHCP Pools

To configure a new DHCP pool on a switch, complete the following steps:

1. To configure a DHCP pool on a Mobility Access Switch, click **Configuration**> **Switch-MAS** > **DHCP Pools**.

   To configure a DHCP pool on other Aruba switches, click **Configuration** > **Switch-Aruba** > **DHCP Pools**. DHCP is supported only on Aruba Switches running the following versions:

   - Aruba 2920 Switch Series—WB.16.02.0012 or later
   - Aruba 2930F Switch Series—WC.16.02.0012 or later
   - Aruba 2540 Switch Series—YC.16.02.0012 or later

   If any of the devices is running a lower version, a warning message is displayed, and the DHCP configuration changes are pushed only to the devices that support the DHCP. If the devices are upgraded to a supported version or moved out of the group, the warning message will not be displayed.

2. To activate the DHCP service, select the **Enable DHCP service** check box. The DHCP service can be enabled only if there is a valid DHCP pool.

3. To edit the DHCP pool details, click the edit icon.

4. To delete a DHCP pool, click the delete icon. When the **Do you want to delete <DHCP Pool Name>?** pop-up window prompts you, click **Yes**.

Adding a New DHCP Pool

1. To add a new DHCP pool, click **New** and configure the following parameters:

- **Name**—Name of the pool.
- **Network**—A valid network IP address to assigned to the DHCP pool.
- **Netmask**—Netmask of the DHCP pool.
- **Lease Time**—The lease time for the DHCP pool in days-hours-minutes format. You can set a maximum value of 365 days 23 hours and 59 minutes in the DD-HH-MM format.
- **Default Router**—IP address of the default router in the subnet. You can add up to 8 IP addresses.
- **DNS Server**—Address of the DNS server. To add multiple DNS servers, click +. You can add up to 8 DNS servers.
- **WINS Server**—Address of the WINS server. The WINS server address is required for legacy Aruba switches only. To add multiple WINS servers, click +.
- **Netbios server**—Address of the Netbios server. The Netbios server address configuration is not required for legacy Aruba switches. To add multiple WINS servers, click +. You can add up to 8 Netbios servers.
- **IP address Range**—IP address range within the network and network mask combination.

- **Exclude Address Range**—IP address range to exclude. This field is available for legacy Aruba Switches such as Mobility Access Switches. To add multiple excluded address range, click +.
- **Option**—The code and type of the DHCP option to configure. A value within the range of 2-254 with type as hexadecimal and ASCII is valid.
- **Value**—The value to assign to the DHCP option. To add multiple values, click +.

2. Click **Add**.

Applying Configuration Changes through CLI Snippets

Central allows you to modify switch configuration through the UI menu options. However, if certain parameters are not available for configuration in the UI, Aruba recommends that you use CLI snippets to push configuration changes to switches. You can apply configuration changes from CLI snippets to an individual switch or for switches provisioned in a UI or template group.

Central does not support CLI snippets for Aruba Mobility Access Switches.

Central supports variable definitions in CLI snippets only for the switches provisioned in a template group. You can also use the CLI snippets to override the variable definitions for each device in a template group.

Adding CLI Snippets for Template Groups

To add a CLI snippet to devices in a template group, complete the following steps:

1. Select the template group from the **Groups** menu.
2. Click **Configuration** > **Advanced Settings**.
3. To apply the configuration changes to a specific Switch model or firmware version, select the desired values for **Model** and **Version**.
4. To apply the configuration changes to all Switches provisioned in the template group, select **All** for **Model** and **Version**.
5. Paste the CLI snippet. The configuration in the CLI snippet is applied to the devices matching the selected criteria. The variables in the CLI snippet are applied for template groups.

Adding CLI Snippets to Switches Provisioned in UI Groups

You can apply a CLI snippet to a switch both at the group and device levels.

To push configuration changes through the CLI snippet, complete the following steps:

1. Select the group from the **Groups** menu.
2. Click **Configuration** > **Switches - Aruba** > **Advanced Settings**.
3. To apply the configuration to all the switches provisioned in the group, select **All** for **Model** and **Version**.
4. To apply the configuration to a specific Switch model and the firmware version, select the desired values for **Model** and **Version**.
5. Paste the CLI snippet. Ensure that the CLI snippet does not include variable definitions. The configuration changes are added to the devices matching the selected criteria.

Configuring System Parameters for a Switch

The **System** menu under **Switch-MAS** and **Switch-Aruba** allows you to configure administrator credentials and enable mode on a switch.

Configuring Administrator Credentials for Mobility Access Switch

To configure administrator credentials for a Mobility Access Switch, complete the following steps:

1. Click the **Configuration**> **Switch-MAS** > **System**. The **System** page opens.
2. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
3. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
4. Click **Save Settings**.

Configuring Administrator and Operator Credentials for Other Aruba Switches

To configure administrator credentials for other Aruba switches, complete the following steps:

1. Click the **Configuration** > **Switch-Aruba** > **System**. The **System** page opens.
2. Enter the username for the administrator user.
3. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
4. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
5. To configure the operator user credentials, complete the following steps:
6. Select the **Set Operator Username** check box.
7. Enter a username and password for the operator user.
8. Confirm the password.
9. Click **Save Settings**.

Configuring a Name Server

To set a static IP switches, you must configure a name server. To configure a name server, complete the following steps:

1. Click **Configuration**.
   - To configure a legacy Aruba switch , click **Switch-MAS**.
   - To configure other Aruba switches, click **Switch-Aruba**.
2. Enter the IP address of the name server obtained from the DNS server in the **Name Server** text box.
3. Click **Save Settings**.

Aruba Switch Stack

The Aruba 2920 Switch Series devices support stacking. A switch stack is a set of switches that are interconnected through stacking ports. In a switch stack, the switches in the same subnet are configured to use a single IP address. The switches in a stack elect a primary member called commander and the remaining switches in the stack function as secondary members. A maximum of four Aruba Switches can be used for forming a switch stack.

For more information on topology and configuration of switch stacks, see *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba 2920 Switch Series.

Provisioning Switch Stacks in Central

Central supports management of Aruba 2920 switch stacks running WB.16.04.0008 or later. The switch elected as the commander establishes a WebSocket connection to Central. The following criteria apply to provisioning and management of switch stacks in Central.

- Switch stacks can be added only to a template group and cannot be moved to a UI group.
- If the standalone switches in a group join to form a switch stack, the switch is moved to the Unprovisioned state.
- If a switch stack is moved from a pre-provisioned group to an existing group in the UI, it will be moved to Unprovisioned state.
- After forming a switch stack, you can remove a member and erase its stacking configuration. However, the member can join Central as a standalone switch only after it is deleted from the switch stack.

Configuring Switch Stacks

The switch stacks are provisioned under template groups in Central. The template groups allow you to configure and modify the settings of a switch stack using configuration templates.

When uploading a configuring template, ensure that the variables are uploaded for all the members of the stack. The template is applied with the variables of the member that is elected as the commander.

To create a configuration template for switch stack, complete the following steps:

1. Click the **Groups** menu to create a group.
2. Select the **Set this device group as Template Group** check box and save the group.
3. Go to **Configuration** > **Templates**.
4. In the **Templates** page, click **+** to create a template for the Aruba switch stack.
5. Specify a name for the template.
6. Select Aruba Switch from the **Device** drop-down list.
7. Select the Aruba Switch model in the **Model** drop-down list.
8. Select the Aruba Switch software version in the **Version** drop-down list.
9. Enter the template text in the **Template** box.
10. Click **Save**.

Central does not support the use of part number (J-number) in place of Switch model number in configuration templates for the Aruba switch stack.

The following pre-defined variables are refreshed and re-imported from a switch stack when a new stack member is added or removed, or when a failover occurs.

- _sys_template_header

- _sys_module_command
- _sys_stack_command
- _sys_oobm_command
- _sys_vlan_1_untag_command
- _sys_vlan_1_tag_command

Monitoring Switch Stacks

Switch Stack

The **Monitoring** > **Switches** page displays the status and usage of all switches and switch stacks provisioned in Central. To view information pertaining to switch stacks, on the **Switches** page, click the **List** tab and select the **Stacks** option.

The following table describes the information displayed on the **Stacks** page:

Table 7: *Stacks Page*

Stacks Pane Content	Description
Name	Displays the name of the switch stack. A green bullet preceding the stack name indicates that it is UP. A red bullet indicates that the stack is DOWN.
Location	Displays the location of the switch stack.
Group	Displays a list of switch stacks sorted based on maximum usage. It also shows the data traffic transmitted (Tx) and received (Rx) from clients.
Clients	Displays the number of clients connected to the switch stack.
IP Address	Displays the IP address of the switch stack.

Stack Details

To view the details of the switch stack, select **Monitoring > Switches > List > Stacks** pane and click the stack for which you want to view the details. The **Stack Details** page opens.

The following table describes the contents of **Stack Details** page:

Table 8: *Stack Details Page*

Data Pane Content	Description
Status	Indicates the operational status of the switch stack.
Uptime	Indicates the time since which the switch stack is operational.
Individual stack members	Indicates the number of switches forming the switch stack (categorized as member, commander, and standby)
Ports	Displays the following details of the switch ports:

Table 8: *Stack Details Page*

Data Pane Content	Description
	Graphs ■ Throughput—Aggregate client data traffic detected on the switch stack ■ Connected Clients—Number of clients connected to the switch stack Table column headers ■ Port#—Port number ■ Oper Stat—Operational status of the switch stack ■ PoE—PoE status of the port ■ Type—Type of switch stack port ■ Mode—Operational mode of the port ■ Tx Usage—Client data transmission details ■ Rx Usage—Data traffic received from the clients connected to the port ■ Trusted—Ports marked as trusted.
Uplink	Displays the Uplink Stats graph. The graph displays the uplink statistics for the inbound and outbound data traffic.
Info	Displays the following details for the switch stack: Stack Details ■ Stack Name—Name of the switch stack ■ Split Policy—Details on how the stack is split ■ Stack Status—Shows if the switch stack is active or not ■ Member Count—Shows number of members on the switch stack ■ Topology—Type of switch stack topology Member Details ■ Member Serial Number—Serial number of member switch. ■ Member ID—Member identification number ■ Member Status—Status of the member ■ Serial Number—Serial number of the switch stack ■ Public IP— The public IP address of the switch stack ■ Management IP— Management IP address of the switch stack ■ MAC address—MAC address of the switch stack ■ Power Consumption— Power drawn from the switch stack in watts (W). ■ CPU (graph)—percentage of CPU utilization with pointer to Green, Amber, or Red portion of the graph. ■ Uplink Ports—Displays the uplink statistics of ports ■ Member Role—Displays member role ■ Switch Model Type—Hardware model of the switch stack ■ Firmware Version—Firmware version of the switch stack ■ Fan Speed—Fan speed of the switch stack. For the other switches, the Fan Speed field shows **Ok** to indicate that the fan speed is fine. ■ Group Name—Name of the group to which switch is assigned ■ Location—Location in which the switch stack is installed ■ Memory (graph)—Percentage of memory utilization with an indicator to Green, Amber, or Red portion of the graph
Alerts and Event logs	Displays the alerts details and event log generated for this switch stack. Alerts table—Shows Date/Time at which alert is generated and the description for the alert Event Log table—Shows Date/Time at which the event occurred and a description of the event
Map	Displays the geographical location of the switch stack.