aruba
a Hewlett Packard Enterprise company

AP Discovery Logic and AP Deployment

10:00 GMT | 11:00 CET | 14:00 GST
FEB 27th, 2018

Presenter: Jovin Rosario

jovin.vincent@hpe.com

AIRHEADS COMMUNITY

Agenda

- Introduction
- AP Deployment Policy
- Discovery Logic Workflow
- Troubleshooting

INTRODUCTION

aruba
a Hewlett Packard
Enterprise company

Introduction

- In the earlier versions of ArubaOS, APs are predefined as either controller-based Campus APs or controller-less Instant APs.
- Each Campus AP is shipped with the ArubaOS manufacturing image and must connect to a controller in order to receive configurations.
- Campus APs can only run the ArubaOS image and cannot be converted into Instant APs.
- Each Instant AP is shipped with the Instant manufacturing image and must join an Instant AP cluster in order to receive configurations from a virtual controller.

Introduction

- Instant APs run the Instant image and can also be converted into Campus APs.
- Starting from ArubaOS 8.2.0.0, selected AP Models can run in both controller-based mode and controller-less mode.
- Based on the selected mode, the AP runs a different image:
- Controller-based APs run an ArubaOS image.
- Controller-less APs run an Instant image.

Introduction

- The following APs support both controller-based mode and controller-less mode:
- **AP-203H**
- **AP-203R and AP-203RP**
- **AP-303H**
- **AP-365 and AP-367 accesspoints**

Introduction

- Each AP is shipped with a manufacturing image based on the Instant image.
- When the AP is booted up with the manufacturing image, it enters the managed device and Instant discovery process to determine if it will be upgraded to the controller-based mode (ArubaOS image) or controller-less mode (Instant image).
- After the managed device, Instant virtual controller, or Activate/AirWave/Central is discovered, the AP image is upgraded accordingly.

Introduction

- By default, controller discovery has a higher priority than Instant discovery.
- APs can discover the IP address of a managed device through one of the following methods.
- **Static controller discovery**
- **ADP**
- **DHCPserver**
- **DNSserver**

Preference Role

Users can predefine the AP mode by configuring the preference role. APs with the default preference role follow the standard discovery logic by attempting controller discovery before initiating Instant discovery.

APs with the controller-less preference role bypass controller discovery and immediately initiate Instant discovery.

In the WebUI :

To set the AP preference role to controller-less in the WebUI:

1. Navigate to Maintenance > Access Point > Convert to Instant Mode in the WebUI.
2. Select the AP on which you want to set the preference role to controller-less.
3. Click Convert to Instant Mode.

Preference Role

In the CLI

To set the AP preference role to controller-less in the CLI, execute the following commands:

(host) [mynode] #ap redeploy controller-less

all

ap-group

ap-name

ip-addr

ip6-addr

AP DEPLOYMENT POLICY

aruba
a Hewlett Packard
Enterprise company

AP Deployment Policy

- Starting from ArubaOS 8.2.0.0, users can predefine the AP deployment mode using the AP deployment policy.
- The AP deployment policy redirects the specified APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.
- The AP deployment policy can be configured on:
- APs in the specified IP address ranges—Policy is applied to the APs in the specified IPv4 or IPv6 address range.
- You can define up to 128 IPv4 and IPv6 address ranges for the AP deployment policy
- APs in the default AP group—Policy is applied to the APs in the default AP group.

AP Deployment Policy

APs whose MAC address are included in the blacklist table—Policy is applied to the APs whose MAC addresses are included in the UAP blacklist table when the blacklist policy is enabled on the AP deploy profile.

You must enable the AP deploy profile to enforce the policies configured in the profile.

When the policy is enforced, the managed device automatically identifies the targeted AP, rejects the AP termination, and redirects the AP to upgrade to controller-less mode.

In the CLI

To enable the AP deploy profile, execute the following commands:

(host) [mynode] (config) #ap deploy-profile

(host) [mynode] (ap deploy-profile) #enable

AP Deployment Policy

To apply the AP deployment policy to the default AP group, execute the following commands:

(host) [mynode] (config) #ap deploy-profile

(host) [mynode] (ap deploy-profile) #default-ap-group

To apply the AP deployment policy to an IPv4 address range, execute the following commands:

(host) [mynode] (config) #ap deploy-profile

(host) [mynode] (ap deploy-profile) #ip-range

AP Deployment Policy

To apply the AP deployment policy to an IPv6 address range, execute the following commands:
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #ipv6-range

To include AP MAC address to the UAP blacklist table, execute the following command:

(host) [mynode] (config) #uap-blacklist add mac-address *description*

AP Deployment Policy

To apply the AP deployment policy to the blacklisted APs, execute the following commands:

(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #blacklist

To remove the IP address range or default AP group from the profile, execute the following command:

(host) [mynode] (config) #no ap deploy-profile

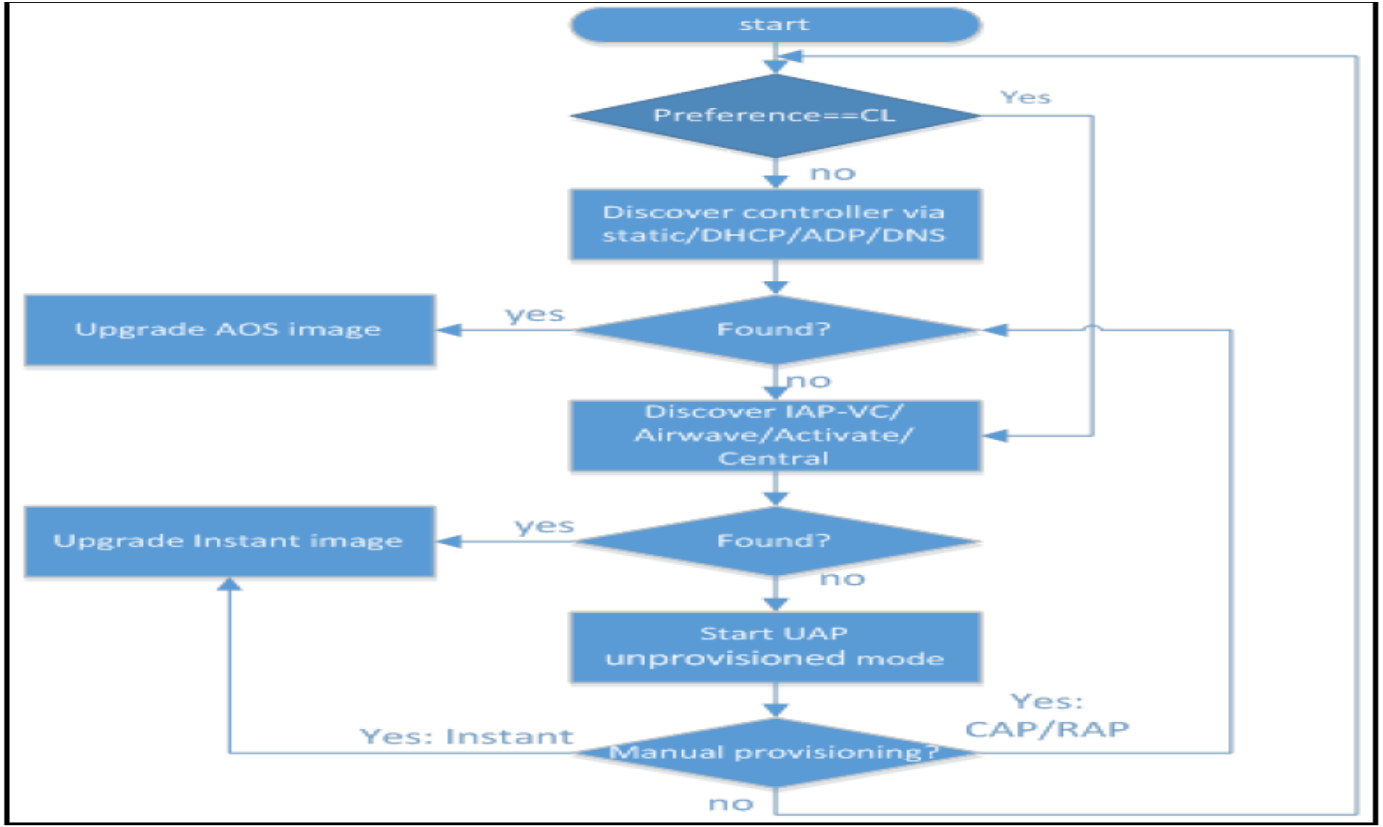
To view the complete list of IP address ranges to which the AP deployment policy is applied, execute the following command:

(host) [mynode] #show ap deploy-profile

DISCOVERY LOGIC WORKFLOW

aruba
a Hewlett Packard
Enterprise company

The following steps describe the AP discovery logic:



AP Discovery Logic

1. The AP boots up with the manufacturing image in unprovisioned mode.

2. The AP enters the controller discovery process using static/DHCP/ADP/DNS based controller discovery. If the preference role is set to controller-less, the AP bypasses controller discovery and immediately enters Instant discovery (Skip to Step 3).

- If a managed device is discovered, the AP receives the managed device's IP address or domain assignment.
- The AP connects to the managed device and downloads the ArubaOS image. After the image is downloaded, the AP reboots.
- The configuration synchronizes, and the AP runs in controller based mode.
- If a managed device is discovered, but the AP deployment policy is applied to this AP, the AP connects to the managed device and downloads the ArubaOS image.
- The managed device rejects the AP termination and redirects the AP to the Instant discovery process.
- If the AP cannot locate any managed device (for example, if the managed device is powered off or becomes unreachable), it enters Instant discovery

AP Discovery Logic

3.The AP enters the Instant discovery process to locate an Instant virtual controller, Activate, AirWave, or Central.

If a virtual controller is discovered, the AP joins the existing Instant AP cluster and downloads the Instant image from the cluster. After the image is downloaded, the AP reboots. The configuration synchronizes, and the AP runs in controller-less mode.

If the AP cannot locate a virtual controller in an existing Instant AP cluster, the AP attempts to locate Activate, AirWave, or Central to upgrade the image and form a new Instant AP cluster.

AP Discovery Logic

APs running the manufacturing image cannot form an Instant AP cluster.

APs that connect to Activate are automatically upgraded from the manufacturing image to the latest Instant or ArubaOS image.

If the AP locates Activate, it receives pre-configured provisioning rules to connect to AirWave, or Central or convert into a Campus AP or Remote AP.

All firmware must be uploaded to AirWave before the AP connects and downloads the Instant image.

If the AP locates AirWave, it can be upgraded to the Instant image. If an enforced image upgrade rule is configured in AirWave, the AP is upgraded to the Instant image configured for the enforced upgrade rule. If no enforced upgrade rule is configured, the AP is upgraded to the latest Instant image in AirWave.

After the AP is upgraded, it reboots in controller-less mode and forms a new Instant AP cluster.

The AP converts into the master, and other un-deployed APs can join the cluster to upgrade to the Instant image.

AP Discovery Logic

If the AP locates Central, it can be upgraded to the Instant image through the **Maintenance > Firmware** page in the Central WebUI.

Central synchronizes with Aruba Activate to retrieve the latest Instant image.

After the AP is upgraded, it reboots in controller-less mode and forms a new InstantAP cluster.

The AP converts into the master, and other un-deployed APs can join the cluster to upgrade to the Instant image.

If the AP cannot locate Activate, AirWave, or Central, it continues to run in unprovisioned mode until the image is upgraded. If the AP is not upgraded to the ArubaOS or Instant image, it enters a 15 minute reboot period.

If there is no keyboard input or WebUI session (manual upgrade) within the 15 minutes, the AP reboots.

Manual Upgrade: To manually convert an AP to an Instant AP in the WebUI:

1. Login to your virtual controller.

2. Connect to the following provisioning SSID broadcasted by the unprovisioned AP: SetMeUp-xx:xx:xx

3. Open a web browser. You will automatically be redirected to a special provisioning page in the WebUI to convert the AP.

4. Under Access Point Setup, select Image File or Image URL to upload the Instant image.

If you select Image File, click Browse to locate and select an Instant image file from your local file explorer.

If you select Image URL, enter the web address of the Instant image under URL.

5. Click Save.

After the AP is upgraded, it reboots in controller-less mode.

Controller-based AP via Aruba Activate

If the AP cannot locate any managed device during the controller discovery process, the AP enters Instant discovery. During the Instant discovery process, the AP attempts to connect through Activate if it cannot locate an Instant virtual controller.

If Activate is provisioned to convert APs to controller-based Campus APs or Remote APs, any AP that connects to Activate is converted into a Campus AP or Remote AP.

APs are upgraded to the ArubaOS image via Activate through the following steps:

1. The AP boots up with the manufacturing image in unprovisioned mode.

2. The AP enters the controller discovery process using static/DHCP/ADP/DNS based controller discovery.

3. If the AP cannot locate any managed device, it enters the Instant discovery process to locate an Instant virtual controller, Activate, AirWave, or Central.

4. The AP attempts to locate a virtual controller in an existing Instant AP cluster. If the AP cannot locate any virtual controllers, it attempts to connect through Activate.

5. If the AP connects to Activate, it checks for provisioning rules to convert into a Campus AP or Remote AP.

Manually: convert an AP to a Campus AP or Remote AP in the WebUI:

1. On your device, connect to the following provisioning SSID broadcasted by the unprovisioned AP: SetMeUp-xx:xx:xx

2. Open a web browser. You will automatically be redirected to a special provisioning page in the WebUI to convert the AP.

3. Under Convert to, select CAP or RAP.

4. Enter the IP address or host name of the managed device to which the Remote AP or Campus AP will be connected.

5. Click Save.

After the AP is upgraded, it reboots as a Campus AP or Remote AP.

TROUBLESHOOTING THE AP DISCOVERY LOGIC

aruba
a Hewlett Packard Enterprise company

Troubleshooting

The following sections describe troubleshooting scenarios users may encounter in the AP discovery logic.

Identifying the controller discovery method

APs can obtain the IP address of a managed device through one of the following methods:

Static controller discovery

ADP

DHCP server

DNS server

Execute the **show log provision** command on the AP to determine which controller discovery method was used to upgrade the AP to the ArubaOS image.

Troubleshooting

The AP is unable to upgrade to the ArubaOS image

There are several reasons why an AP may not be able to upgrade to the ArubaOS image, even when a managed device is configured.

ADP is disabled

If the ADP is disabled on the managed device, the AP will not be able to locate any managed device on its own. Execute **adp discovery enable** command in the CLI to enable ADP.

The AP preference role is set to controller-less

If the AP preference role is set to controller-less, the AP bypasses controller discovery and immediately initiates Instant discovery.

Use one of the following methods to check if the AP preference role has been set to controller-less: Execute the **apboot> printenv** command on the AP console to view the current environment variable settings. The uap_controller_less field indicates if the preference role is set to controller-less:

uap_controller_less=1: The controller-less preference role is enabled.

uap_controller_less=0: The controller-less preference role is disabled.

Troubleshooting

Check the boot up log from the AP console. If the preference role is set to controller-less, the “ADP is disabled by uap_controller_less” message appears.

Execute the **show log provision** command on the AP console to view the AP provisioning logs. If the preference role is set to controller-less, the “Controller discovery is disabled by ap-env uap_controller_less” message appears.

The AP is not factory default.

If the AP is not set to factory default (manufacturing image in unprovisioned mode), it cannot enter the controller discovery process.

Use one of the following methods to check if the AP is factory default:

Check the boot up log from the AP console. If the AP is not factory default, the “Not factory_default ap. Do not run ADP.” message appears.

Execute the **show log provision** command on the AP. If the AP is not factory default, the “Controller discovery is disabled since UAP is not factory default status” message appears.

Troubleshooting

APs remain in unprovisioned mode after failing both controller and Instant discovery.

If the AP is unable to upgrade to the ArubaOS or Instant image through the controller and Instant discovery process, it can be upgraded manually using the SetMeUp-xx:xx:xx provisioning SSID.

Execute the **show network** command on the AP to check if the AP is connected to the SetMeUp-xx:xx:xx provisioning SSID.

If the AP is connected to a different SSID, it is not factory default.

Troubleshooting

The managed device is not running the correct image version

An AP can only be converted into a controller-based AP if the managed device to which it connects is running ArubaOS 8.2.0.0. Managed devices that run a different version of ArubaOS do not support the AP discovery logic and cannot convert the AP to controller-based mode.

The AP is attempting to connect to a fake controller.

If the AP fails to convert into a controller-based AP, the managed device to which it attempted to connect may be fake.

Execute the **show log provision** command on the managed device to check if the AP failed to connect after 10 attempts.

FTP or TFTP permission is denied on the managed device

In order to download the ArubaOS image from the managed device, the AP must establish a FTP or TFTP connection to the managed device. If FTP or TFTP permission is denied on the managed device, the connection attempt is dropped, and the AP cannot download the ArubaOS image.

Use one of the following methods to check if FTP or TFTP permission is denied on the managed device:

Execute the **show log upgrade** command on the AP.

If FTP or TFTP permission is denied, the AP fails to connect to the managed device, and the following messages appear in the upgrade log:

Connecting to <Controller Ip address>… failed: Connection time out.

Error: failed to retrieve image

Info: try with tftp to download the image

Troubleshooting

Access controls can be applied to a managed device port to filter traffic between the managed device and the APs.

Traffic must meet all criteria on the ACL in order to reach the managed device or AP.

If it does not meet the criteria, the connection is dropped.

Execute the **show interface fastethernet access-group** command to view the ACLs that have been applied to the port.

Troubleshooting

Execute the **show ip access-list <string>** command on the controller to view the detailed configuration for the ACL that has been applied to the port.

Execute the **interface fastethernet|gigabitethernet} ip access-group {in|out|session {vlan <vlanID>}}** command to apply an ACL to a port.

Execute the **no interface {fastethernet|gigabitethernet} ip access-group {in|out|session {vlan <vlanID>}}** command to remove an ACL from a port.

Troubleshooting

Execute the **ip access-list extended {<number>|<name>} deny <protocol>** command to reject traffic for a specific protocol. If you reject traffic for the UDP, TFTP traffic is dropped.

If you reject traffic for the TCP, FTP traffic is dropped.

Execute the **ip access-list extended {number>|<name>} permit <protocol>** command to allow traffic for a specific protocol. If you allow traffic for the UDP, TFTP traffic can reach the managed device or AP.

If you allow traffic for the TCP, FTP traffic can reach the managed device or AP.

Troubleshooting

The AP is unable to upgrade to the Instant image

If the AP is marked as CAP-only, it cannot be upgraded to the Instant image.

CAP-only APs can only be upgraded to the ArubaOS image.

Execute the **show log provision** command on the AP to check if your AP is CAP-only. If your AP is CAP-only, the CAP-only sku message appears.

Accessing the CLI after an image upgrade

After the AP image is upgraded, users cannot access the CLI for the first 180 seconds of uptime.

The following message appears when a user attempts to login to the CLI during the initial 180 second uptime period:

login as: admin

System uptime is 147 seconds and CLI is not ready yet, please try again later

The AP does not reboot after an upgrade failure

If an AP fails to upgrade to the ArubaOS or Instant image during the controller and Instant discovery process, it enters a 15 minute reboot period.

After the AP is rebooted, it restarts the discovery process. However, there are several conditions that can prevent the AP from completing the reboot.

WebUI session connected to the AP (manual image upgrade).

Pending image upgrade.

Discovery of an AMP server.

Discovery of a Central server.

The AP does not reboot after an upgrade failure

Execute the **show log provision** command on the AP to determine why the AP has not rebooted. The provisioning log displays one of the following messages:

Could not reboot- upgrade is pending

Could not reboot- keyboard input

Could not reboot- airwave is found

Could not reboot- UI session and Could not reboot- central is found

QUESTIONS?

aruba
a Hewlett Packard
Enterprise company

THANK YOU!

aruba
a Hewlett Packard
Enterprise company